POL00028135

POST 113/132

CONTENTS

POL00028135

CHAPTER 1. INTRODUCTION

This Statement of Service Requirements (SSR) is supplied to remaining qualifying prospective Service Providers who responded satisfactorily to Notice Reference 94/S 165-58937/EN in the Official Journal of the European Communities published on 30 August 1994 and were shortlisted following the evaluation of their response to a Request for a Statement of Capability. Relevant information has been provided previously in:

- the information pack containing the prospectus "Bringing Technology to Post Offices and Benefit Payments"; and
- the "Request for a Statement of Capability".

Reference may be made to information contained in these earlier documents.

Nothing in this SSR or any of the documents mentioned above, binds the Contracting Authorities to award a contract to any bidder, and nothing in this SSR or any of the documents mentioned above is to be taken as constituting an agreement, offer or representation that a contract will be awarded in accordance with any procedure referred to in the aforementioned documents or at all.

1.1 PURPOSE

1.1.1. The purpose of this document is to specify the requirements of the Contracting Authorities, who are Post Office Counters Ltd (POCL) and the Department of Social Security (DSS). The Benefit Agency (BA) is the project sponsor on behalf of the DSS, DHSS Northern Ireland and other government agencies. The requirements are for the design, development, integration, support, operation and management of computer and related services referred to in this and the documents previously provided. Prospective Service Providers should read this SSR carefully before responding.

1.1.2. The requirements are both diverse and complex. Some relate to the provision of a more efficient solution to problems within the existing businesses of BA and POCL (in particular the payment of benefits at post offices) while others concern the provision of a strategic IT infrastructure to support a programme which will incorporate POCL's anticipated future business requirements.

1.1.3. In this SSR, where the business of BA or DSS is described, it should be assumed, unless otherwise stated, that this extends to cover the requirements of other departments and agencies which will use the Benefits Payment Service (BPS).

POL00028135

1.2 OBJECTIVES

1.2.1. All parties recognise and commit to the programme's overall service objectives which can be expressed as:

- a fraud-free method of paying benefits at post offices that is automated, has lower end-to-end costs than the current paper-based process, with continuously reducing overall administration costs year on year;
- extending automation to POCL's other client transactions, its products and its support processes to improve competitiveness, increase efficiency, and to enable greater commercial opportunities for POCL;
- full and speedy reconciliation of benefits payments, with accounting arrangements consistent with recognised accountancy practices;
- an improved service to the parties' customers.

1.2.2. In addition, there are detailed sets of objectives for BA and for POCL, as follows.

BA Objectives

1.2.3. The automation of the benefits payment service through post offices is seen as a major element in the re-engineering of the overall administrative process and the attainment of the BA Business Vision. All objectives will embrace that Vision and in particular the payment system through post offices will:

(a) provide a method of payment which ensures payment of the right money, to the right person at the right time;

(b) provide a fully secure system that eliminates fraud as far as possible and controls residual liabilities;

(c) provide improved systems to detect and monitor unauthorised activity and supply evidence to support prosecution of illegal action;

(d) provide full accounting and reconciliation facilities;

(e) reduce current administration costs, secure the lowest value for money cost for the provision of the new service and provide for continuous improvement in value for money throughout the period of the contract(s);

(f) provide an efficient customer service which is accepted and understood by them, BA staff and POCL agents and staff;

(g) provide flexibility to cope readily with any future changes affecting benefits or customer base and to adapt to developing needs of customer service, accounting or security;

POL00028135

(h) be consistent with the Government's aim of encouraging the use of automated credit transfer (ACT) on a voluntary basis while continuing to provide the option of payment at a post office for those who prefer it;

(i) enable all of a person's benefit entitlement(s) to be paid in one transaction using a single token or card for the identification of all benefits;

(j) ensure that any token or card identification system can migrate to a multi-purpose smart card;

(k) encourage the use of the National Insurance Number (NINO) as the prime reference number for communications between the BA and its customers, their employers, or other Government Agencies;

(l) use IT systems that are robust, as far as possible already proven, and secure against fraud, unauthorised access and disasters, are capable of development and interface with existing systems.

POCL Objectives

1.2.4. The POCL objectives can be summarised as follows:

(a) to provide continued customer choice of services available at post offices and be acceptable to customers;

(b) to retain and strengthen POCL's clear branding links with its customers;

(c) to maintain POCL's customer base;

(d) to support government policy of a nation-wide network of post offices;

(e) to be capable of introduction in all post offices;

(f) to retain and enhance POCL's commercial and financial integrity;

(g) to improve overall efficiency and cost effectiveness for POCL and its clients;

(h) to support and help agents in the development of their private business;

(i) to be acceptable to staff and agents;

(j) to facilitate automation of other areas of POCL infrastructure, e.g. accounting and distribution, and support wider business information needs;

(k) to retain and gain new business by improving quality of service to all clients;

(l) to provide the flexibility to meet a diverse range of existing and potential client needs and applications;

POL00028135

(m) to provide long term stability for the Post Office network as a retail outlet for benefit payments;

(n) to adopt a flexible and efficient approach to IT systems and adhere to industry standards so as to secure the benefits of developments in IT and retail sectors, thereby achieving value for money and faster delivery of new products and services;

(o) to retain customers' trust in the integrity of POCL and improve the quality of service to customers;

(p) to facilitate the provision of added value services, e.g. card and/or token issue and management, that will enhance POCL's service offering;

(q) to ensure the migration of appropriate automated systems without any reduction in service levels;

(r) to be a key enabler in helping improve POCL's competitiveness, in meeting its business partners' needs, and enhancing future business viability.

1.2.5 These factors should be read in conjunction with the details set out in the prospectus information pack.

POL00028135

1.3 SCOPE

1.3.1. The scope of the procurement is represented by the outer boundary in the figure below. The outer boundary shows the scope of the procurement, and the inner boundary the scope of the POCL strategic infrastructure. The service boundaries of importance to the Contracting Authorities for both the full procurement and internal to the services (e.g. to the POCL infrastructure) are emphasised as bold bars in the diagram. Full details of the component parts of this figure are given in Chapter 4.

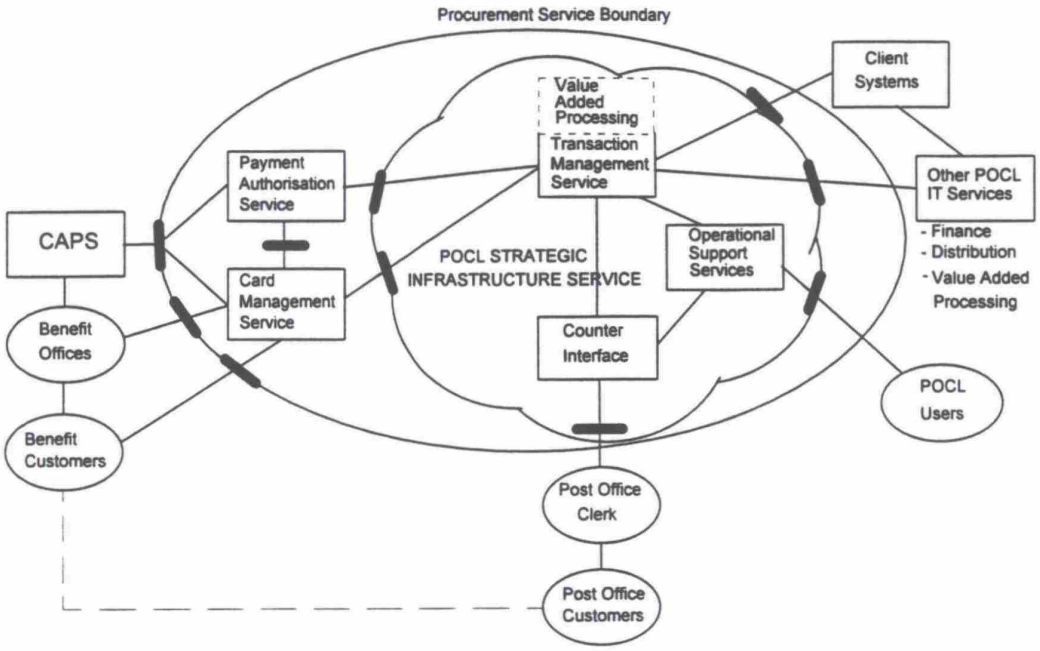


Figure 1-1 Procurement Scope

1.4 REASON FOR PROCUREMENT

1.4.1. Prospective Service Providers have already been given (as part of the information pack) the summaries of two reports jointly prepared by POCL and BA entitled "Order Book Report" and "Girocheque Report". These reports provide information explaining why automation of benefit payments at post offices is necessary.

POL00028135

1.5 MAIN TASKS AND CONSTRAINTS

1.5.1 Tasks

1.5.1.1. The Service Provider's main tasks will comprise:

- the provision, operation, support and management of a strategic IT infrastructure able to support the automation of a wide range of current and new services at post offices, including the automation of benefit payments;
- the automation of the end-to-end benefit payments service;
- any necessary integration with the computer systems of POCL, BA, their authorised agents, or clients;
- migration of existing systems (e.g. ECCO+, ALPS, APT); and
- integration of POCL, BA, and/or third party software applications.

1.5.2 Constraints

1.5.2.1. The detailed design of this service is a matter for the Service Provider but the overall solution proposed must be acceptable to both Contracting Authorities, be economically advantageous to both Contracting Authorities and meet the programme objectives. In particular the Service Provider must have regard to the areas below (which are listed in no significant order and are not exhaustive):

- Legal

  The service must operate within the legislative requirements applying to the Service Provider, POCL, BA, and any authorised agents, customers and clients.

- Security

  The service must operate in accordance with existing security standards adopted by POCL and BA. Any security standards imposed by the Service Provider must be compatible with those of POCL and BA.

- Financing

  It is desirable to procure the services under the Private Finance Initiative of the UK Government.

- Standards and Architecture

  A common set of technical standards and architecture for the boundaries of the services and infrastructure is imperative. The Service Provider's system must be able to exchange information with the computer systems of the Contracting Authorities and their authorised agents and clients.

POL00028135

- Customer Service

  The importance of at least maintaining, if not improving, customer service.

- Emergency Manual Fallback Procedures

  The Service Provider must provide both a manual fallback and a recovery procedure in respect of each element of the service in case of any system failure.

1.6 LOCATIONS AND TIMESCALE

1.6.1. The services provided as a result of this procurement will need to provide:

- the automation and networking of some 19,700 post offices throughout the UK;
- interfaces, including those to support any necessary interrogation of the Service Provider's service and the geographically diverse locations of POCL and BA computer systems, including local benefit offices;
- the necessary interface between the Service Provider's systems and the BA CAPS computer system that will be at a location to be decided;
- installation of the system to new / relocated post offices during and after roll-out;
- an implementation programme to commence in Spring 1996. Further details of the timescale are discussed in chapter 7.

1.7 DOCUMENT STRUCTURE

1.7.1. The SSR comprises the following sections:

1.7.2. **Chapter 1 Introduction** - Introduces the document as a whole. Describes the two contracting authorities and the scope and purpose of each of the following chapters.

1.7.3. **Chapter 2 Background** - Contains the background information about POCL and BA that is not specific to this requirement. Sets the context in terms of size (organisational and financial); and business.

1.7.4. **Chapter 3 Existing Services** - Describes those aspects of the current services that:

(a) will be directly affected/replaced by the procurement;

(b) will be required to interface/exchange data with the new services;

(c) may be added to the infrastructure in the future.

POL00028135

1.7.5. **Chapter 4 Description of Functional Requirements** - Specifies in detail the functional requirements behind the services that are to be provided as a result of this procurement.

1.7.6. **Chapter 5 Steady State Services** - Specifies the service requirements for the "business as normal" state.

1.7.7. **Chapter 6 Pilot Programme** - Specifies the objectives and constraints of the Pilot Programme and makes clear the differing emphasis between the Demonstrator and the Operational Trial.

1.7.8. **Chapter 7 The Roll-out Programme** - Specifies the business objectives, and business imperatives for the roll-out programme.

1.7.9. **Chapter 8 Commercial Requirements** - Sets out the commercial requirements of the procurement.

1.7.10. **Chapter 9 Procurement Requirements** - Specifies the procurement requirements covering timetable, evaluation, delivery of proposals and confidentiality.

1.7.11. **Appendices** Various appendices called up from the main chapters.

POL00028135

CONTENTS

2. BACKGROUND

POL00028135

CHAPTER 2. BACKGROUND

The purpose of this chapter is to provide background information about the Contracting Authorities, non-specific to this requirement, which places them in context in terms of size (both organisational and financial) and business functionality.

2.1 OVERVIEW OF POST OFFICE COUNTERS LTD

2.1.1 Structure and Size

2.1.1.1. POCL is a wholly owned subsidiary of the Post Office. It conducts its business through a national network of some 19,700 offices comprising about 750 directly operated offices (owned and staffed by POCL) and about 18,950 agency offices which are run by individuals or organisations as POCL agents. The turnover for 1993/94 was £1.1 billion, with 28 million customers each week being served by over 65,000 employees, agents and assistants in the UK's largest retail chain.

Staffing

2.1.1.2. POCL has over 14,000 employees and 51,000 agents and assistants. These staff are based in post offices, 7 regional offices, Central Services Group, business centres, and Head Office.

Network of Post Offices

2.1.1.3. POCL's competitive advantage stems from its reach. POCL is an integral part of every community and has more outlets than banks and building societies combined. Since becoming a limited company within the Post Office Group in 1987, POCL can point to a track record of year by year growth in business and achievement of Government profit and efficiency targets. Business volume has grown steadily both in and out of the recession and over the last decade efficiency has improved by 13%.

2.1.1.4. To improve service to customers and reduce costs POCL has been running a programme of converting directly operated offices to agency status and has developed a franchise post office concept which has been very successful. The agents run a variety of private enterprises alongside their post office: typically these are general stores, stationers, or confectioners/tobacconists/newsagents, while some have no private business and only operate a post office counter.

2.1.1.5. POCL is committed to protecting the competitive advantage which comes from its extensive network. This includes the rural network where 'community offices' (offices with restricted opening hours) have been introduced in order to maintain a service to local populations. The network of post offices and its relationship with agents and franchisees will remain under POCL control and is beyond the scope of this procurement.

POL00028135

2.1.2 Main Areas of Business

2.1.2.1. POCL's mission is to be the leading overall provider of benefits distribution, postal services, banking and bill payment facilities. Essentially the organisation is a channel for the movement of cash, information and stock, such as value items and forms, between customers who visit post offices daily and clients, such as BA and Royal Mail, for whom services are provided. Historically, POCL has been restricted in terms of the services it can provide and, as a result, the organisation is largely dependent on a small number of clients. Eight clients generate over 90% of the business carried out in post offices.

2.1.2.2. POCL has had much success recently in expanding its client base - British Gas, National Rivers Authority and the National Lottery are notable examples and it has a growing own label retail segment through a network of almost 200 Post Shops. Bill payment and advance payment schemes have seen an increase in volume linked to the use of an automated payment terminal, described in chapters 3 and 4. With this equipment in place, POCL is aiming to secure a significant share of the utilities prepayment market. POCL has no monopoly: for every service offered, alternative and competitive services are available. Postage stamps can be bought at many other retail outlets, direct debit is an alternative means of paying bills, and ACT is an alternative method of paying benefits.

2.1.2.3. It is the recognition of this competition which drives the business desire to develop an automated solution and improve the way benefits are paid. From an automated platform, POCL can improve the existing services it provides to other clients and exploit new opportunities. POCL sees opportunities in several areas, for example in retail banking by exploiting the opportunities presented by bank branch closures. Broadening the pre-pavment facility is a further opportunity and builds on the strong base already established with the automated payment services.

2.1.3 Commercial Nature of POCL

Finance

2.1.3.1. POCL had an income of £1089m for the year ended 31 March 1994 and made a profit of £12m after taxation.

2.1.3.2. The income arises from POCL's many clients, own label retail products, licences and franchise fee income, as shown in the table below.

Postal Communications (Royal Mail and Parcelforce)	£243M
Licence and Franchisee Fees	£7M
Government Clients	£457M
Retail, Banking and Utilities	£382M
	£1089M

POL00028135

2.1.3.3. POCL prepares and publishes accounts which follow the requirements of the Companies Acts and Stock Exchange Listing rules, and is set targets by the Government. These are:

- Real Unit Costs (RUC)

  This measures the extent to which POCL's costs rise more slowly than prices generally.

- Return On Capital Employed (ROCE)

  This combined profit and asset utilisation target represents the percentage return from the investment in the business.

- External Financing Limit (EFL)

  The Post Office Group is required to generate a cash surplus as a contribution towards the Public Sector Borrowing Requirement. (The target for 1994–95 is £226m.) POCL does not have a specific target for EFL, as it does with RUC and ROCE, but it is required to contribute to the overall Post Office EFL target.

2.1.3.4. The level of profit, income, expenditure, business volume, RUC and ROCE are the six financial key performance indicators utilised to manage POCL business.

Legislative Framework

2.1.3.5. POCL is an ordinary limited company whose shares are wholly owned by the Post Office. However POCL's Memorandum forbids it from doing anything the Post Office is not allowed to do (subject to exceptions sanctioned by the President of the Board of Trade). Further, the Post Office Act 1969 (as amended) requires the Post Office Board to enforce this. Effectively therefore, POCL may only do what the Post Office may do, together with such other things as the President allows. However, the Government's recent green paper has confirmed a proposed enlargement of POCL's commercial freedom.

POL00028135

2.2 OVERVIEW OF DSS AND OTHER RELEVANT AGENCIES

2.2.1 Introduction

2.2.1.1. The DSS is the executive arm of the UK Government responsible for: the development and delivery of the Social Security programme; War Pensions; the National Insurance Fund; and the implementation of the Child Support Act. It comprises a Headquarters which supports ministers in developing and administering policy, six executive agencies performing its business functions and has responsibility for the administration of a number of independent statutory bodies. The management style in the agencies is one of devolved empowerment.

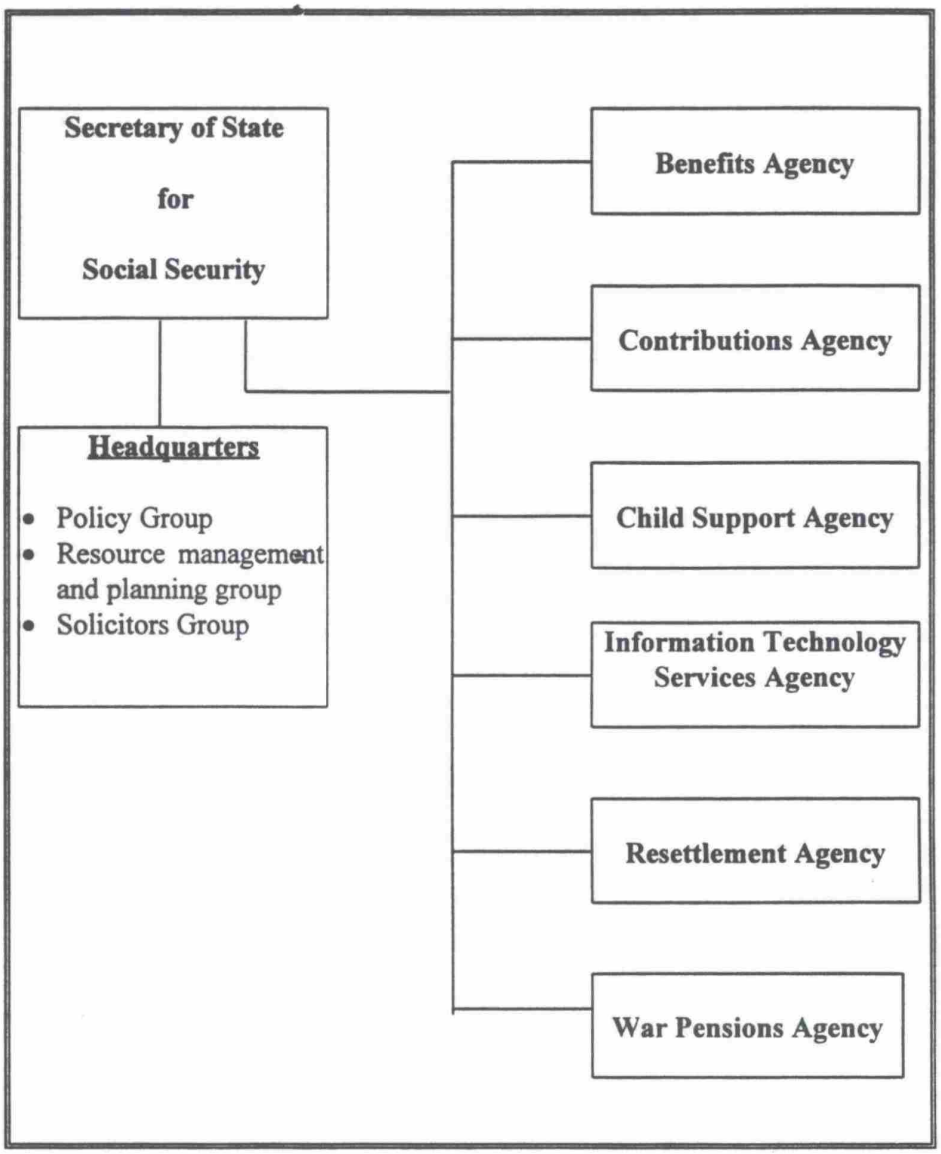


Figure 2-1 The DSS and its Executive Agencies

POL00028135

2.2.2 Relevant Agencies

2.2.2.1. The required service will support some of the business functions of three of the executive agencies within the DSS (BA, Child Support Agency (CSA) and War Pensions Agency (WPA)), the Social Security Agency (SSA) which is an executive agency of the Department of Health and Social Security (Northern Ireland) (DHSS (NI)) and the Employment Service (ES) which is an executive agency of the Department of Employment.

Benefits Agency

2.2.2.2. BA is the largest Government agency. Its primary aim is to help ministers meet social policy goals through the efficient delivery of social security benefits in a manner which meets the customers' needs and achieves best value for money. BA is responsible for administering payments of benefits in three main categories: contributory benefits; income related benefits; and benefits that are dependent on qualifying conditions. Additionally, BA acts as an agent on behalf of the Department of Health for the distribution of milk tokens. In certain circumstances payments of benefit may be made by agents acting on behalf of BA, e.g. ES who make combined payments of Income Support and Unemployment Benefit for those customers with dual qualification, and local authorities who make payment of Housing Benefit in respect of those customers who qualify.

Child Support Agency

2.2.2.3. The primary aims of the CSA are to deliver on behalf of children a fair and effective service for the assessment and payment of maintenance, and to ensure that parents maintain their children whenever they can afford to do so. In some circumstances the CSA make payments to customers by Girocheque.

War Pensions Agency

2.2.2.4. The primary aim of the WPA is to deliver a consistent, efficient and effective service for the assessment and payment of War Pensions and War Widows' Pensions. The WPA administers payments of War Pensions to customers who meet the relevant qualifying conditions.

Social Security Agency (Northern Ireland)

2.2.2.5. The primary objective of the SSA is the payment of benefit to the people of Northern Ireland. The range and rates of benefits payable equate to those on the UK mainland.

The Employment Service

2.2.2.6. The overall aim of the ES is to promote a competitive, efficient and flexible labour market by helping into work unemployed people, especially those who are disadvantaged, and by paying benefits and allowances to those who are entitled to them.

POL00028135

2.2.2.7. One of the ES's areas of responsibility is the delivery of unemployment benefits and training allowances. The ES pays Unemployment Benefit and Income Support on behalf of the DSS, and training allowances on behalf of the Department of Employment (DE), the Scottish Office and the Welsh Office.

2.2.3 Main Areas of Business

2.2.3.1. The main areas of business of the agencies involved in and pertinent to this procurement are broadly similar. They can be divided into services offered to customers and support provided to ministers.

Customer Charters

2.2.3.2. The various agencies operate within the framework of responsibilities documented in their customer charters which detail the service customers have a right to expect from the agency and its staff. The charters set performance targets for the agencies (e.g. BA's administration of claims to benefit).

Assessment of Eligibility and Entitlement

2.2.3.3. Agencies have a responsibility for the assessment of whether a customer, applying for payment of a benefit administered by them, meets the relevant qualification criteria. These differ and are dependent on the type of benefit applied for. Customers provide the appropriate domestic, personal and/or financial information required to officers of the agency. Based on the information provided a decision as to their eligibility to receive the benefit applied for is taken. Dependent on the type of benefit, customers are required to declare any changes in their personal circumstances that may affect their continuing eligibility.

2.2.3.4. Having adjudicated on a customers eligibility to receive benefit, their entitlement is calculated. Once entitlement has been calculated a notification is issued to the customer.

Payment of Benefits

2.2.3.5. The agencies' computer systems, having calculated a customer's entitlement to benefit, transmit payment award details which result in the issue of payments to customers. The rate of payment may not remain constant during the life of a customer's claim.

Advice and guidance

2.2.3.6. As a continuing customer service the agencies provide advice in relation to questions concerning, primarily, entitlement to and payment of benefits. These services generally take the form of telephone advice-lines and may be located on either a national, regional or local basis.

POL00028135

Support of Ministers

2.2.3.7. The DSS assists Government with the administration of existing Government policy, development and implementation of new policies and direct support of ministers in their duties.

2.2.4 Funding

2.2.4.1. The social security programme has two sources of finance. The cost of contributory benefits and their administration is met from the National Insurance Fund. Non-contributory benefits and their administration are financed from money voted by Parliament from general taxation, paid into the Consolidated Fund.

2.2.4.2. Additionally, training payments made by the ES are financed from general taxation via votes held by Department of Employment, Scottish Office and the Welsh Office.

2.2.5 Legislative Framework

2.2.5.1. The DSS and its agencies operate within a legislative framework provided by Acts of Parliament and associated Statutory Instruments. Of particular relevance to this procurement are the Social Security Contributions and Benefits Act 1992, the Claims and Payments regulations, and the Social Security Administration Act 1992.

2.2.5.2. Additionally, training payments made by the ES are covered by the Employment Training Acts of 1973 and 1988.

POL00028135

2.3 KEY FEATURES OF EXISTING POCL BUSINESS

2.3.1 Customers

Service Delivery Performance Targets

2.3.1.1. POCL recognises that the key to sustaining success is through continuous improvement in meeting customer requirements. This means delivering the highest quality service both externally to its customers and clients, and internally to its staff and agents. Its efforts are not going unnoticed.

2.3.1.2. POCL has two stretching performance targets by which it measures its progress to truly satisfying customers' needs. Taking speed of service first, it aims to serve its customers within five minutes and current performance reveals that it is serving more than 97% of customers within that time. POCL's track record on quality of service is shown in Figure 2-2.

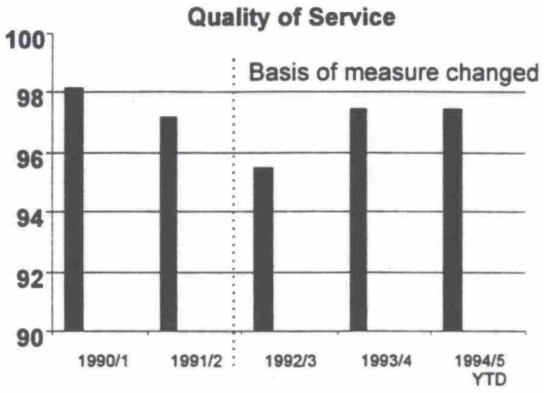


Figure 2-2

2.3.1.3. POCL customers' perception of the overall service provided is also measured and their opinion of other retailers is tracked, benchmarking POCL's performance against high street organisations who score consistently high in terms of customer perception of service. This measure is known within POCL as SMART (Salient Multi Attribute Research Technique). POCL's recent performance is shown in Figure 2-3.

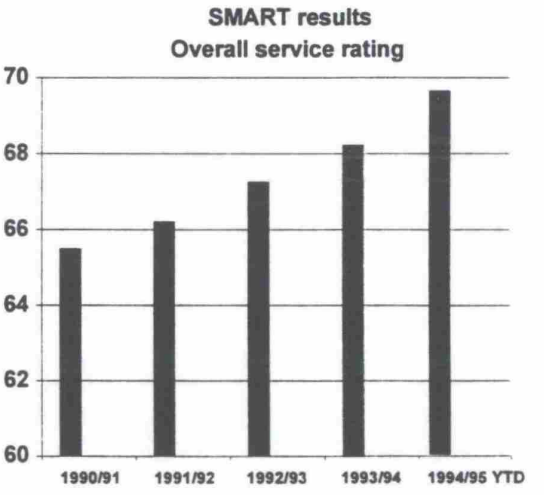


Figure 2-3

Customer Service

2.3.1.4. POCL's Customer Charter is central to improving the opinion that its customers have of post offices. Only by being open with customers will they understand the level of service POCL expects to provide and that they can expect to receive.

2.3.1.5. POCL is making the network more accessible by extending opening hours to reflect the local shopping patterns in local communities and to reflect new business opportunities

POL00028135

(e.g. the National Lottery). POCL is looking more professionally at where post offices are located, how they look, and what type of layout best meets its customers needs. POCL is experimenting with:

- queue hosting, a technique where a member of staff assists customers with forms and queries before reaching the counter;
- dedicated serving positions for high volume or long transactions such as business postings; and
- open plan offices, removing the physical barriers between staff, agents and customers.

2.3.1.6. POCL is committed to its total quality programme which has become firmly embedded in the business. At post offices, this manifests itself as "Putting the Customer First" and forms the basis of local quality improvement projects linked to individual post office customer surveys.

2.3.1.7. During any change therefore (e.g. the introduction of new technology), customer acceptability must be the paramount consideration. POCL must protect its core values of integrity and personal service, and maintain the brand its customers recognise. This means accuracy of transactions, choice and protection of identity.

Customer Profile

2.3.1.8. POCL serves over 28 million customers per week. The table below indicates the profile of customers (in % terms):

Directly Managed Post Offices (750)				Agency Post Offices (19,000)			
Male 50.8		Female 49.2		Male 46.0		Female 54.0	
AB	C1	C2	DE	AB	C1	C2	DE
14.2	26.7	25.9	33.2	13.9	26.6	24.5	35.0

2.3.2 Clients and Services

2.3.2.1. POCL provides services on behalf of a wide range of client organisations and further information on the services is provided in section 3.1.

POL00028135

2.3.2.2. SUMMARY OF SERVICES PROVIDED

Post Office Counters Ltd
Postal Orders, Active Life magazine, stationery, packaging materials, greeting cards and office sundries, Bureau de Change

Royal Mail
Postage Stamp sales
Inland and Overseas Services
Philatelic items

Parcelforce
Postage Stamp sales
Inland and Overseas Services, including Datapost and other guaranteed services

Girobank
Deposits / Withdrawals
Girocheques
Rent Vouchers / Cards
Cash
Cashing Other Banks' Cheques
Transcash Services
International Money Orders

Dept of Social Security
Pensions and Allowances

Camelot
National Lottery

Dept of Health
Issue of E111s
Prescription Charge Refunds
Milk Tokens

Dept of Environment
Game Dealer / Keeper Licences

United Kingdom Passport Agency
British Visitors Passports

BBC
TV Licences
TV Licence Saving Stamps

Driver and Vehicle Licensing Agency
Vehicle Licences
Vehicle Licence Saving Stamps

British Telecom
Telephone Accounts
Telephone Saving Stamps
Phonecards
Payphones
Telemessages
International Telegrams

Transport Schemes
London Regional Transport
Passenger Transport Executive's various travel schemes

Local Authorities
Home Help Stamp schemes
Home Care Stamp schemes

Ministry of Defence
Pensions and Allowances

Royal Mint
Coin sets (selected offices only)

POL00028135

Mercury
Mercurycards
Mercuryphones

Utilities
British Gas Token Schemes
British Gas bill payment
Electricity Token Schemes
Water Company Stamp Schemes

Dept for National Savings
Ordinary and Investment Accounts
Premium and Capital Bonds
Children's Bonus Bonds
Savings Certificates

National Rivers Authority
Rod Licences

POCL also provides clients with an outlet for publicity and leaflets.

2.4 KEY FEATURES OF EXISTING DSS BUSINESS

2.4.1 Introduction

2.4.1.1. This section highlights the high level key features, relevant to benefit payments, of the core business of the DSS, SSA (DHSS NI) and ES which characterise the service provided by the existing agencies and any future Service Providers. The primary function of the agencies is to deliver benefits in accordance with the law and to the satisfaction of ministers and customers. The aim of the agencies is to fulfil this function economically, efficiently and effectively with due regard to the varying needs of their customers.

2.4.2 Performance Targets

2.4.2.1. High level targets, covering a wide range of key issues, are set by the Secretary of State. The chief executives, in consultation with the Department's headquarters additionally set a range of internal targets, relating to matters such as clearance times and accuracy rates for individual benefit types. Performance targets relating to clearance times for processing benefit claim applications appear within the customer charters of the relevant agencies. Customer charters may be purchased from her Majesty's Stationery Office (HMSO).

2.4.3 Customer Issues

2.4.3.1. The DSS pays social security benefits to some 30 million people, who fall within the following broad customer groups (which may be subject to change):

(a) the elderly;

(b) long-term sick and disabled;

(c) short-term sick;

POL00028135

(d) families;

(e) unemployed;

(f) war pensioners;

(g) widows and others.

2.4.3.2. Each agency has a responsibility for the provision of differing services for different customer groups. It is, however, likely that an individual customer will have dealings with more than one agency during their lifetime, and often simultaneously. Generally the output of their contact will be a calculation of entitlement and subsequent award of benefit.

Confidentiality, Integrity and Availability of Information.

2.4.3.3. The DSS must comply with the Data Protection Act 1984 which gives legal rights to individuals about whom information is recorded on computer.

2.4.4 Payment Of Benefit

2.4.4.1. In terms of transactions, at post offices alone (excluding other payment methods such as ACT), BA authorised almost 1000 million individual payments in 1993/94. Full details of volumes can be found in appendix 3-8.

2.4.4.2. There are three broad benefit types administered by the DSS (grouped within which are over 30 individual benefits), each agency being responsible for the administration of a number of the individual benefits which fall within these broad bands. The agencies assess entitlement of customers against the qualifying criteria associated with each benefit type prior to awarding a payment. Each type of benefit is intended to meet different categories of need. The table below (Table 2-5) shows each type, the basis for entitlement and some examples of individual benefits.

Table 2-5 Three Main Benefit Types

Type of Benefit	Basis of Entitlement	Examples
Contributory Benefits	Dependent on customer's National Insurance contribution record.	Retirement Pension Widows' Benefits Incapacity Benefit Unemployment Benefit
Income-Related Benefits	Available to those whose income falls below a certain level, dependent on family circumstances. These benefits take account of capital as well as income	Income Support Housing Benefit Council Tax Benefit Disability Working Allowance Family Credit
Dependent on Qualifying Conditions	Dependent on customer's meeting imposed qualifying conditions	War Pensions Attendance Allowance Disability Living Allowance Child Benefit

POL00028135

New Benefits

2.4.4.3. The current list of individual benefit types is subject to change. Benefits may be introduced, changed or withdrawn according to Acts of Parliament. An example is the recent ministerial announcement concerning the introduction of Job Seekers Allowance in 1996. Take-up of this benefit will lead to the phased withdrawal of Unemployment Benefit.

Rating of Benefits

2.4.4.4. The rate of benefit to which a customer is entitled may change frequently during the life of a claim. There are two main factors which may necessitate the rate of payment changing. These are described in brief below:

(a) Statutory Re-rating

Parliament annually reviews the rate of benefit payments. Decisions are generally announced in November for implementation the following April.

(b) Circumstantial Re-rating

A customer's circumstances may change during the life of their claim to benefit. Dependent on the nature of this change it may lead to a re-assessment of their entitlement to benefit which in turn may require benefit payments to be either increased (up-rated) or decreased (down-rated).

Emergency Procedures

2.4.4.5. The DSS has a statutory obligation to make payments of benefit to those who are entitled and within set performance timescales. DSS, SSA and ES have agreed with POCL, and other agents a set of emergency procedures to ensure the continuing payment of benefit in the event of normal service delivery failure. Existing emergency procedures are detailed in appendix 2-5.

2.4.5 Auditability

2.4.5.1. It is a feature of the existing service that there is a requirement to produce audit trail information in conformance both with the DSS Departmental Security Standards (see appendix 2-3) and the DSS Common Audit Trail Model (see appendix 2-8).

POL00028135

CONTENTS

3. EXISTING SERVICES

POL00028135

CONTENTS

POL00028135

CHAPTER 3. EXISTING SERVICES

This chapter describes the existing service applications administered by the Contracting Authorities, their authorised agents or clients. In the case of POCL, services are provided to a number of diverse customers and clients. In the case of DSS the application detailed describes the end-to-end benefit payment process. In general this chapter describes those aspects of current services that:

(a) will be directly affected or replaced by the service being procured; or

(b) will be required to interface or exchange with the new services; or

(c) may be added to the procured service infrastructure in the future.

3.1 POCL SERVICES

3.1.1 Summary

3.1.1.1. A summary of the wide range of services that POCL offers is given in this section. This section is not intended to represent its clients' requirements for automated products. A summary of the range of services, processing and IT services POCL currently offers and supports is set out below with further details at appendix 3-1. This section is merely intended as background to the products and services and does not represent the specification for automated services.

3.1.1.2. The Service Provider will be expected to work with POCL to develop and engineer both replacement and new products and services, and to consider appropriate product roll-out and implementation plans. The interface with clients, agents and customers will remain under POCL's control. POCL's IS Strategy (see appendix 3-2) defines its approach to automated products and transactions. This section is purely background information to aid understanding of POCL's present product offering.

Benefit Payments

3.1.1.3. Full details of the POCL procedures for benefit payments have been included in section 3.4, and are summarised below.

3.1.1.4. Details of the current order book system for the payment of pensions and allowances are given in section 3.4.7 and this work is carried out on behalf of BA and SSA (NI).

3.1.1.5. Other benefit payments include unemployment benefits and social fund loans which are paid via Girocheques.

3.1.1.6. Pension payments are also made on behalf of the Ministry of Defence via an order book system. Other benefit related products include the issue of milk tokens and prescription refunds on behalf of the Department of Health. Various initiatives have been trialed aimed at reducing fraud including the use of electronic stop notices. Plans are currently underway for the provision during 1995 of an electronic stop notice system at

POL00028135

approximately 1470 post offices in the M25 area using PCs and bar code reading technology (the Automation of London Post Offices project - ALPS). The ALPS project is considered to be completely stand-alone but Service Providers should consider this equipment and functionality as part of their migration proposals. In view of the fact that the ALPS equipment will replace some ECCO+ terminals and automated payment terminals (APT) it is also required to provide additional functionality. More details on ALPS are included in section 3.2.5 and chapter 4.

Postal and Communications

3.1.1.7. Post offices sell a range of stamps, stamp books and related products at all offices for use on inland and international mail. Philatelic products, e.g. first day covers and presentation packs are also available at all directly operated and selected agency offices. Letters, packets and parcels, with payment via stamps or meter impressions, are accepted for both inland and international postings. Priority services such as Recorded, Registered, Guaranteed Delivery, and Datapost are also provided on behalf of both Royal Mail and Parcelforce. There is also an extensive range of support services such as meter resetting.

3.1.1.8. On the communications front, POCL retail BT phonecards and is examining other options for the provision of telephony related products and services.

3.1.1.9. Opportunities in this market range from the use of track and trace technology to improved stock control, management information for retail products and improved product/sales support for staff and agents. There is limited systems support in this area although electronic scales are in use in some offices. The ECCO+ system which is described in chapters 3 and 4 also provides management information via POCL central systems.

Licensing

3.1.1.10. Payment and collection services in the licensing market currently include television licences, motor vehicle licences, fishing and game licences, and the provision of passport services. In addition to the actual purchase there are a range of prepayment options which centre around the purchase and redemption of savings stamps.

3.1.1.11. Some small-scale trials using the automated payment terminal (APT) are underway which involve the provision of savings facilities (for a licence) via a card based system. It is envisaged that full automation would facilitate further development of this along with improved authorisation and processing facilities.

Financial Services

3.1.1.12. POCL is the largest handler of cash in the UK. A range of in-payment and out-payment facilities is operated on behalf of Girobank and the Department for National Savings. Services include business deposits, current and savings accounts, and cash handling facilities, as well as premium bonds and saving certificates.

POL00028135

3.1.1.13. New services in this market include the provision of travel related services such as bureau de change and money transmission, thereby enhancing POCL's existing offering (passports). Plans are also underway to offer a travel insurance facility, and other insurance services are under consideration. POCL also envisages future developments in the cash and savings areas to improve its competitiveness.

3.1.1.14. An automated infrastructure is seen as supporting or complementing the product offering in this area.

Bill Payment

3.1.1.15. A range of bill and prepayment services is offered at post offices for clients such as BT, British Gas and Girobank as well as other major utilities and local authorities.

3.1.1.16. Although some of the products are still manually based, a large percentage of business has now transferred to magnetic stripe or smart card technology, and utilises the automated payment terminal currently being installed in some 5000 offices. Non-automated offices also utilise a POCL document processing facility to process card vouchers and the automated/manual data streams are merged via a central host system. The document processing centre is also used to process cheques and bills. Service Providers will need to consider how data from the document processing centre will be merged with the automated stream to ensure continuity of service.

3.1.1.17. A technical specification for the automated payments terminal is provided at appendix 4-7 together with a specification for the central host system at appendix 4-8.

3.1.1.18. A further phase of development is planned to cater for recharging of British Gas Quantum smart cards and to replace existing client equipment used in a limited number of offices (around 460).

Retail

3.1.1.19. POCL sells personal stationery (including own label) and greeting cards, as well as postal products through some 200 Post Shops (separate retail units within directly operated post offices) and a smaller selected range of products on browser units at approximately 280 post offices. A wholesale offer to agents of POCL's own label product range is being developed and other opportunities e.g. Post Shop franchises, are being tested.

3.1.1.20. Post Shops are equipped with an EPOS terminal, CRISP (Counters Retail Information Systems in PostShops) (see appendix 3-3), which is a stand alone system, but POCL would be interested in integration options.

3.1.1.21. Post Shops are among 4000 outlets which will have on-line Lottery terminals, and a further 6,000 instant games outlets are envisaged. Current plans are for Lottery terminals and communication links to remain separate from other post office systems.

POL00028135

3.1.1.22. Other retail opportunities revolve around developing POCL's consumer offerings in areas such as travel and leisure ticketing, redemptions and membership schemes. Automation would undoubtedly be useful in developing these markets.

3.1.1.23. Interactive media is another business area under consideration which would be assisted by automation.

New Business

3.1.1.24. There will be opportunities in the wider markets enabled by the Government's green paper commitment to greater commercial freedom for POCL. Areas under examination include home shopping ordering, personal applications, family entertainment, cash transfer and insurance products.

POL00028135

3.1.2 Transaction Volumes for POCL Clients

Client / Transaction Type	Number of Transactions (1993/94)
BA pensions and allowances	860M
SSA pensions and allowances	32M
Milk tokens	66M
DSS orders (Giros)	96M
Girobank deposits	112M
Girobank withdrawals	29M
Other Girobank services	21M
Vehicle licences issued	33M
NSB deposits	15M
NSB withdrawals	10M
Other NSB services	1M
Telephone bills paid	39M
Postal Orders (sales and redemptions)	39M
TV licences issued	14M
Retail items	17M
Phonecards	4M
Travel schemes	2M
Automated bill payments	20M
BVPs/BEDs	2M
Letter packets posted	250M
Letter premium services	50M
Ordinary parcels	8.5M
International parcels	1.2M
Datapost	0.5M
Mail order return parcels	35M
Ministry of Defence	1M
Department of Health	
• prescription refunds	0.1M
• E111s	1.7M
Home help savings stamps (not redeemable at post offices)	31M
Other savings stamps (Motor Vehicle Licences, British Telecom, Water, and Northern Ireland Electricity bills redeemable at post offices)	785M

	Value of Sales (Annual)
Postage stamps sold	£1140M

POL00028135

3.2 EXISTING SUPPORT SYSTEMS

3.2.1 Introduction

3.2.1.1. POCL currently operates a range of automated services which need to be taken into consideration by Service Providers. A brief overview of the following services is given in sections 3.2.2 - 3.2.8 below:

- Automated Payments Terminal (APT);
- ECCO+;
- CRISP;
- CAPTURE;
- ALPS/ESNS;
- Host Polling System;
- Document Processing.

3.2.2 Automated Payments Terminal (APT)

3.2.2.1. The APT is a custom-built terminal developed for the bill payment and prepayment markets, based on PC technology. It is housed in a compact counter top unit comprising a full alpha numeric keyboard, a small liquid crystal display, and a tally roll printer. The terminal includes a magnetic card reader, and it can also read and write to smart cards, and recharge smart keys used in utility prepayment meters. The terminals are connected to a phone line, and transaction data is collected daily via a modem by the Host Polling System in Farnborough for consolidation and onward transmission to clients' and central POCL systems. APTs are currently being installed in 5,000 offices throughout the UK, situated according to client needs.

3.2.2.2. Automated payments facilities are also provided on ECCO+ equipment (see section 3.2.3) and will be in ALPS offices (see section 3.2.6). A manual alternative is provided by imprinters in non-automated offices. Imprinters are also provided as a back-up facility in automated offices. Documents from the imprinter transactions are processed at the Document Processing Centre described in section 3.2.8.

3.2.2.3. Appendix 4-7 provides additional details on the APT, its capabilities and constraints, and provides a summary of non-APT local bill payment equipment. Further relevant information can also be found in Appendix 4-8 (Polling and Terminal Control).

3.2.3 ECCO+

3.2.3.1. ECCO+ is an EPOS system based on PC technology at each counter position with a back office processor, designed to capture transaction details, and to facilitate office summarisation and balancing.

POL00028135

3.2.3.2. In addition, a package is available for agency offices wishing to rent ECCO+, and to date some 30 offices have taken up this offer.

3.2.3.3. ECCO+ produces daily and weekly summaries for certain clients, and prepares a weekly cash account which is forwarded to the Client Transaction Processing centres at Chesterfield and Edinburgh. There are currently 671 ECCO+ offices.

3.2.3.4. ECCO+ provides a platform for point of service automation including APTs (utilising the swipe card facility for magnetic stripe card transactions, and also linking the back office processor via a modem to the host polling system). Electronic scales are linked to a number of ECCO+ counter terminals and a purpose built Automated Payments Peripheral Unit (APPU) provides the ability to handle smart card and smart key transactions where required. In a small number of open plan offices De La Rue Teller cash dispensers are used. POCL is investigating the possibility of integrating ECCO+ with the teller cash dispensers.

3.2.3.5. Appendix 4-6 provides details on the ECCO+ system, its capabilities and limitations.

3.2.4 CRISP

3.2.4.1. CRISP (Counters Retail Information System in PostShops) is an EPOS system launched in late 1992 to provide better data capture and transmission from PostShops. There are currently 209 PostShops, a number forecast to rise to 350 by 1999/2000. Data from the CRISP terminals is transferred electronically to a central computer at Chesterfield which processes an average of 150,000 records daily. The system is based on a standard RIVA 6900 EPOS terminal. The software is designed and maintained by RIVA Systems Limited.

3.2.4.2. Appendix 3-3 provides additional details on the CRISP system.

3.2.5 CAPTURE

3.2.5.1. CAPTURE is a PC based cash accounting package, currently sold by POCL to agency offices, that is designed to assist in the accounting and summarisation of transaction data. Approximately 1600 agents have purchased CAPTURE. It is estimated that 2000 offices will be using CAPTURE by March 1996. CAPTURE is available as a package comprising hardware, software, and printer; software plus printer; or software only. CAPTURE is supplied complete with an update and support package. It is a back office, not an EPOS system, and data is not captured in real time. The system produces daily and weekly summaries for certain clients and prepares a printed weekly cash account which is forwarded to the Client Transaction Processing centre at Chesterfield. Other similar systems, developed by third party suppliers are used at a number of offices, but are not supported by POCL.

3.2.5.2. Appendix 3-4 provides additional details on the CAPTURE system.

POL00028135

3.2.6 ALPS

3.2.6.1. ALPS / ESNS is a current development designed to provide the following functionality to post offices within the M25:

- Electronic Stop Notice facility for BA at all offices;
- ECCO+ at larger offices;
- APT where required.

3.2.6.2. ALPS is to be installed in approximately 1470 offices (4200 positions) by August 1995. The system is based on PC technology with a LAN, and incorporates a POCL specific EPOS keyboard. A purpose built APPU provides the ability to handle smart card and smart key transactions. Communications to and from ALPS offices for ESNS and APT functions are facilitated by ISDN links to the Host Polling System in Farnborough.

3.2.6.3. The ESNS system is designed to minimise the risk of fraud in benefits distribution. It does this by the validation of order books at the point of encashment using negative authorisation against an electronic stop notice. The system accesses a national 'stop list' of benefit books to perform a comparison with the bar code record printed on a book that has been presented for encashment. The clerk is given an indication of whether to 'pay', 'pay and impound' , or 'impound only'. The stop lists are updated daily and details of the days transactions are collected and transmitted to BA daily for processing.

3.2.6.4. Technical aspects of the hardware and software are given in appendix 4-5.

3.2.7 Host Polling system

3.2.7.1. The Host Polling System in Farnborough currently performs data polling and distribution services in relation to Automated Payments and ESNS, including the following:

- collection of Automated Payments Transaction data;
- collection of data from the Document Processing centre;
- distribution of new programmes and reference data for automated payment offices;
- separation of transaction data by client;
- format of client files;
- transfer of transaction data to clients during the morning following the data collection;
- transfer of transaction data to finance and administration systems in Chesterfield;
- management control of the terminal population;

POL00028135

- distribution of stop notice data for ESNS;
- collection of BA data from ALPS offices.

3.2.7.2. APT polling (including ECCO+ offices) takes place five nights a week (Monday to Friday). BA transmissions take place additionally on a Saturday.

3.2.7.3. Appendix 4-5 provides additional details the operational requirements of the host polling system and provides further information on equipment and volumes of data.

3.2.8 Document Processing

3.2.8.1. POCL has established a Document Processing centre in central London, which processes BT bills, cheques used in payment at the counter, and imprinter vouchers for automated payments. The centre has recently been registered by the British Standards Institute (BSI) to ISO 9002. The paper documents are read by image scanning equipment. Customer, client and financial details are captured automatically wherever possible.

3.2.8.2. Approximately 100,000,000 cheques and other documents are processed each year.

3.3 OTHER POCL PROCEDURES

3.3.1 Reconciliation and Accounting

3.3.1.1. Post offices currently complete a weekly cash account and there is a wide range of supporting documentation some of which is forwarded with the cash account. The data from the cash accounts is keyed into the system at POCL's financial accounting unit at Chesterfield and forms an integral part of the reconciliation and settlement process.

3.3.1.2. The bulk of the process is manually based and there is a separate feasibility study underway within POCL that is considering the future of transaction information processing. Financial integrity is perceived as one of POCL's key strengths and new systems and interfaces will need to meet appropriate standards in this area.

3.3.2 Distribution

3.3.2.1. POCL's retail network is supported by a network of physical distribution centres. In addition to distributing cash and stock to the outlets and receiving returns, the distribution centres also perform certain transactions on behalf of POCL clients, e.g. accept Girobank business deposits. The transactions are identical to those performed in the outlets, but typically small volume and high value.

3.3.2.2. Information relating to transactions, remittances and returns for each distribution centre is currently recorded on a cash account and supporting documents which are forwarded to the financial accounting unit at Chesterfield where the data is keyed in to the system for reconciliation and accounting purposes.

POL00028135

3.3.2.3. Distribution centres currently operate stand-alone systems to assist in the management of cash and stock distribution. A separate project is investigating the system requirements for distribution.

3.4 BENEFITS PAYMENTS SERVICE

3.4.1 Introduction

3.4.1.1. This section describes the existing computer systems and the end-to-end process and procedures within the benefit payment service that are currently employed by the DSS to ensure that customers receive correct and authorised payments of benefit. The service requirements detailed in this SSR are intended to replace or interface with existing procedures relating to the payment of benefits and their subsequent reconciliation against payment awards. Within the existing process the Instrument of Payment (IOP) represents physical proof of a customer entitlement to receive authorised payments of benefit. Additional authentication (in terms of production of evidence of identity) may be required to support any benefit payment transaction at a post office.

3.4.2 Computer Systems

3.4.2.1. The existing benefit payment process is supported by a number of benefit oriented computer systems. The main systems pertinent to this requirement are:

1.	ISCS	Income Support Computer System — supports payment of Income Support (IS) or combined benefits where IS is a component;
2.	PSCS	Pensions Strategy Computer System — supports payment of a number of benefits, primarily Retirement Pension;
3.	INCAP	Incapacity Benefits computer system — linked to PSCS, supports payment of incapacity benefits;
4.	CHB	Child Benefit computer system — supports payments of Child Benefit;
5.	SFCS	Social Fund Computer System — supports payments of Social Fund;
6.	DLA	Disability Living Allowance computer system — supports payment of Disabled Living Allowance;
7.	NUBS 2	National Unemployment Benefit System — primarily supports the payment of Unemployment Benefit;
8.	DWA	Disabled Working Allowance system — supports the payment of Disabled Working Allowance;
9	FAMC	Family Credit computer system — supports the payment of Family Credit;
10.	WPENS	War Pensions computer system — supports payment to war pensioners.

POL00028135

11	AA65	Attendance Allowance computer system — supports the payment of attendance allowance (only payable to customers over 65 years of age). Comes on-line in April 1995.

3.4.3 Operational Strategy (OPSTRAT)

3.4.3.1. Computer Systems detailed above currently operate within the DSS to capture and maintain the information necessary to enable the payment of benefits. Most of the above systems form the DSS Operational Strategy. They have been designed to a common architectural standard, using where relevant, common processing. The systems run on a mainframe estate located at 4 Area Computer Centres (ACCs) around the UK.

3.4.3.2. Users in approximately 2000 locations (DSS and ES local offices) access OPSTRAT systems from terminals or PCs via the Government Data Network (GDN), an X.25 network utilising low bandwidth (9.6 Kbs) lines.

Common Payments Package (CPP)

3.4.3.3. Each benefits system, with the exception of the Child Benefit system, includes the CPP code used to produce instruments of payment (IOPs). CPP can produce a number of different methods of payment (Order Book, Girocheque, Payable Order and Automated Credit Transfer (ACT)). CPP is also used to produce notifications/letters to be sent to the customer.

3.4.3.4. The output from CPP for the OPSTRAT systems is produced at the ACCs, using impact printers, high speed laser printers and output handling equipment. CPP is tailored to the individual benefits needs of each system.

POL00028135

3.4.4 End-To-End Benefit Payment Process

3.4.4.1. The following page contains a description of the end-to-end benefit payment process at SSADM level 1 (Figure 3-1). The table below explains the acronyms used in this chart:

Key to acronyms used in Figure 3-1

1. ACT	Automated Credit Transfer
2. BACS	Banks Automated Clearing Service
3. BAS	Benefit Apportionment System
4. B2	DSS authorisation to ES, as agent, to make payments of income support to person required to register for work
5. C2	Internal payment instruction authorising payment of Income Support to customers who are sick.
6. D2	Authority to reduce the payments authorised by a B2 or C2 to recover deductions from benefit
7. AAB	DSS Administration and Accounting Branch
8. GIREC	Girocheque Reconciliation System
9. IOP	Instrument of Payment
10. POU	Paid Order Unit (POU) located at Lisahally, Northern Ireland
11. OBS	Other Benefit Systems

POL00028135

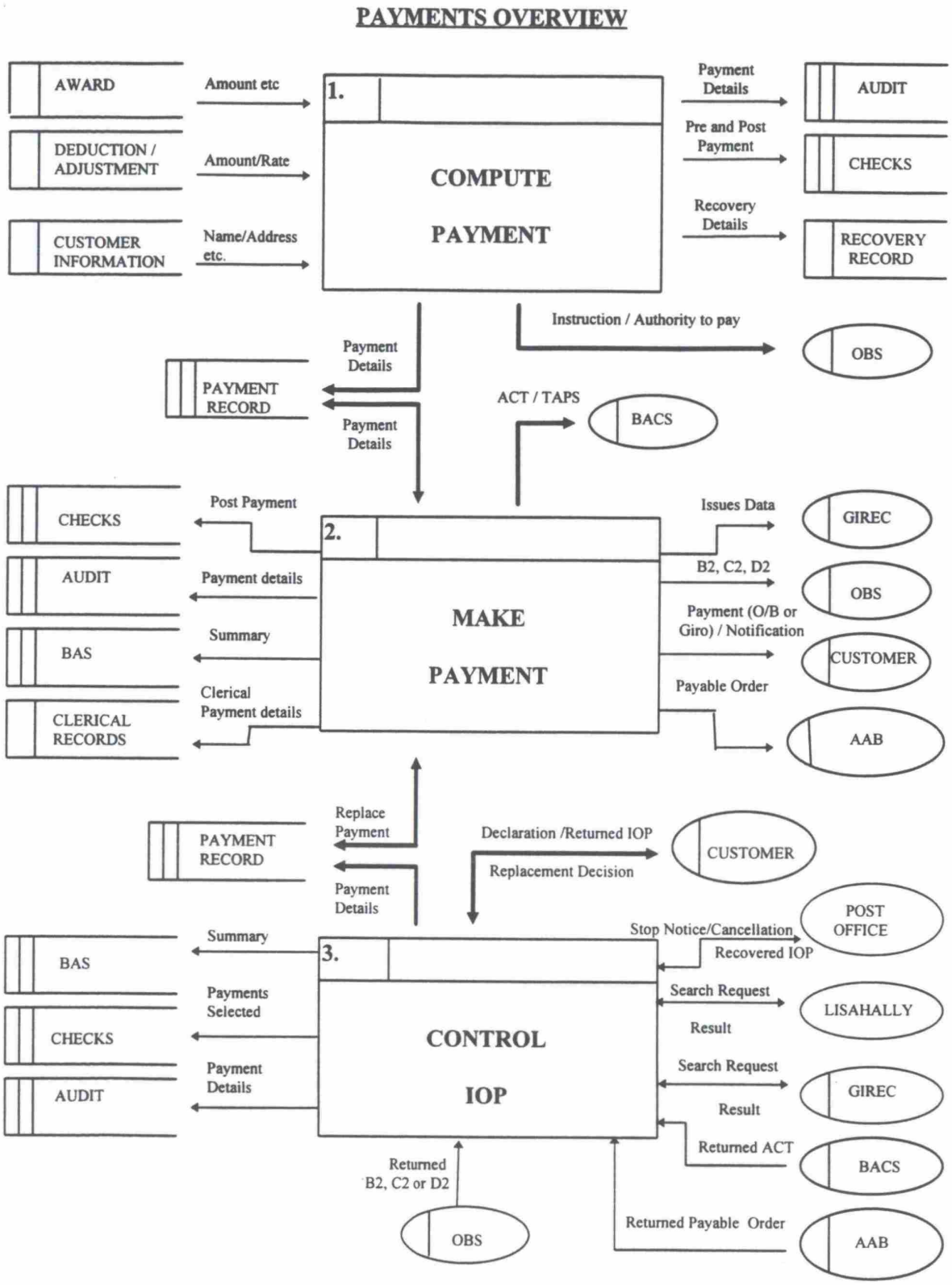


Figure 3-1 End-to-End Benefits Payment Process

POL00028135

3.4.5 Compute Payment

3.4.5.1. This section describes the procedures referred to in Process 1 within Figure 3-1.

3.4.5.2. Prior to the authorisation of an award of benefit payment, a customer's entitlement to receive benefit must be confirmed.

Qualification Criteria

3.4.5.3. Customers wishing to claim benefits administered by the DSS have to satisfy the relevant qualification criteria which relate to their own particular circumstances. These criteria will vary according to the benefit type. Some are dependent on the level of a customer's income (e.g. Income Support), some on their contributions history (e.g. Contributory Retirement Pension) and some on their personal or domestic circumstances (e.g. Child Benefit or War Pensions).

Claims Procedure

3.4.5.4. In order to ascertain whether customers satisfy the above qualification criteria they are required to provide a statement of their personal circumstances. Generally this information is provided on postal application forms which are sent to DSS offices for consideration.

Method of Payment (MOP) and Instrument of Payment (IOP)

3.4.5.5. Having established an entitlement to benefit, a payment is authorised, computed and issued. Except in the case of a small number of low volume benefits, where payment direct to a bank account is not an available option, customers have the choice of payment by ACT or at a post office. The choice is generally made at the time of the initial claim, but the customer may change that option at any time in the life of the claim. If the customer chooses to be paid at a post office, the decision as to whether he is paid by order book or girocheque will usually depend on benefit type but is ultimately at the discretion of the Secretary of State.

3.4.5.6. Should he chose to be paid by ACT, he is required to provide details of the bank account in which he wishes to have payment credited, otherwise he is required to nominate the post office at which he wishes to encash IOPs.

Calculation of Entitlement

3.4.5.7. DSS staff at relevant grades and performing relevant duties are empowered to act as "adjudication officers" and are required to decide on a customer's entitlement to receive benefit. This decision is based on information provided at the time of claim (verification may be required in some circumstances) and the customer's rights under law.

3.4.5.8. OPSTRAT computer systems generate a calculation of entitlement based on input data relating to the customer's personal circumstances.

POL00028135

3.4.5.9. Individual benefit computer systems compute payment awards where relevant taking account of any deductions which may be requested by the customer, an authorised third party (e.g. Local Authorities for payments of Community Charge, or Utilities for payment of outstanding bills), or required by the DSS (e.g. to recover overpayments of benefit or social fund loans made to customers). Payment award data is generated via the CPP.

Multi-Entitlement

3.4.5.10. Customers can have entitlement to receive more than one benefit. In these cases some benefits are combined, two benefit types payable on a single IOP via a single benefit system. Other benefit types do not allow for this, e.g. War Pensions and Child Benefit, in these cases two or more benefits have to be paid via separate benefit systems on separate IOPs.

Generation of Payment

3.4.5.11. Following an authorised award of benefit OPSTRAT systems generate payment files in respect of both paper-based and ACT payments (the latter being routed through BACS). The ACCs administer the payments of all OPSTRAT system generated requests.

3.4.5.12. In the case of a customer choosing payment by the paper-based method, these payment files control the printing of personalised IOPs on stationery (produced to defined security standards) held within the ACC. The personalisation details held on each IOP relate both to the individual customer and the nominated post office. The typical composition of this information is shown below:

	Each customer's personalisation details
1.	Name
2.	Address
3.	National Insurance Number (NINO) or in some instances another form of reference number
4.	IOP serial number
5.	Benefit type payable
6.	Payment award details (amount, period, due date of encashment)

	Each post office's personalisation details
1.	Name
2.	Address
3.	Office identifier (Finance Accounting Division [FAD] Code)

3.4.5.13. Additionally local DSS offices have the capability of issuing payments to those customers in urgent need by the clerical preparation and issue of IOPs.

POL00028135

3.4.6 Make Payment

3.4.6.1. This section describes the procedures referred to in Process 2 within Figure 3-1.

Methods of Payment (MOP)

3.4.6.2. Payments of benefits are currently made by one of the four main methods of payment detailed below. The first two are entirely paper-based, the third (payable orders) is paper-based but makes use of electronic reconciliation, the last is conducted entirely through an electronic medium.

- Order Book

  A book containing up to 52 payment foils, each of which carries personalisation and award details, which are encashable at post offices at a pre-determined frequency. Individual payment foil values are dictated by a series of upper limits which vary according to Order Book and benefit type. The limits currently in operation are:

(i) System-generated books issued in relation to Incapacity Benefit or War Pensions Allowance	From 1 April 1995 upper limit per payment foil = £550
(ii) System-generated books for all other benefit types	Upper limit per payment foil = £350.00
(iii) All non-system Order Books	Upper limit per payment foil = £99.99

  Payments made by this method comprise some 91% of all benefit payments at post offices, by number of transactions, authorised by the DSS and other relevant agencies.

- Girocheque

  A one-time payment voucher carrying personalisation and award details. Values of individual girocheques may fall within two value bandings:

Value :	Redeemable at :
(i) up to £350	Encashable at post offices or through bank or building society accounts;
(ii) between £350 and £5,000	Redeemable only through bank or building society accounts.

POL00028135

- Payable Orders

  This method of payment is generally used to make payments over £5,000 to individuals, utilities, or institutions (where a single payment may cover a number of customers). Payable orders may also be used to administer payments below £5,000, for example when making administrative payments or payment to customers who although resident abroad retain entitlement to benefits paid in the UK.

  All payments made by this method have to be paid through the payee's bank or building society account. Following the presentation of a payable order through a bank account, funds are cleared via the Paymaster system and Banks Automated Clearing System (BACS).

- Automated Credit Transfer (ACT)

  This method utilises the payment of benefits directly to bank or building society accounts nominated by customers. Payments to be made by ACT are written to magnetic tape by the ACCs. Tapes are then sent to BACS for the funds to be credited to the appropriate customer accounts.

Issue System Payments

3.4.6.3. After the IOPs are produced at the ACCs, they are issued to customers. This is achieved in a number of ways dependent on the method of payment:

(a) Order Books:

i. the majority of order books are sent to the customer's nominated post office for collection,

ii. in a small number of instances order books may be issued directly to a customer's home address;

(b) Girocheques:

i. the majority of girocheques are issued directly to the customer's home address,

ii. in a relatively small number of instances (mostly for administrative or security reasons) they may be issued to a DSS or ES office for personal collection,

iii. in a number of post offices in Sunderland a local agreement exists whereby girocheques are issued direct to post offices.

3.4.6.4. ACCs are also responsible for the production of a variety of informative or administrative literature to be issued to customers. Of primary importance to the payment of benefits is the production of payment award notification and Order Book pick up notices. The former advises the customer that an award of payment has been

POL00028135

made and details their entitlement, the latter advises them that an order book has been issued and is ready for collection at their nominated post office. Existing Output Handling Deadlines, with associated service levels for the production and dispatch of IOPs and associated documents, are shown in appendix 3-7.

Issue Clerical or Emergency Payments

3.4.6.5. DSS offices have a facility to issue IOPs without generating a payment award through the benefit systems. In the case of order books this is normally used when, for administrative or security reasons, it is decided to issue a payment locally. In the case of Girocheques it is generally exercised when a customer requires an immediate payment of benefit to satisfy an urgent or emergency need. In the latter case a customer may have no continuing entitlement to payment of benefit. On receipt of an urgent or emergency need payment it may be possible for a customer to nominate the closest post office to the point of issue as the encashment office.

Validity of IOPs

3.4.6.6. IOPs remain valid for encashment for differing periods of time. In the case of order books each payment foil remains valid for three months from its due date of encashment (imprinted on each foil). Girocheques remain valid for one month from the due date of encashment, which is imprinted on the document. Periods of validity are occasionally reviewed by DSS and are subject to change. The DSS is considering whether and when to reduce the validity of the order book foil from 13 weeks to 4 or 5 weeks.

Periodicity of IOPs

3.4.6.7. The frequency with which IOPs may be encashed varies according to both benefit and instrument type. The majority of payment foils are encashable on a weekly basis, however some benefits are payable two or four weekly. Girocheques are intended to act as a one-time payment within one month of the specified due date of encashment. The due date of encashment may allow for entitlement for periods in advance, arrears or a combination dependent on benefit type.

3.4.7 Control IOP

3.4.7.1. This section describes the procedures referred to in Process 3 within Figure 3-1. Payment having been issued to a customer the DSS retains a responsibility for its control, including security, reconciliation and accounting procedures.

Collection of Order Books

3.4.7.2. Generally, Order Books produced by the ACCs and dispatched to post offices are sent through the postal system, with up to three books per envelope. On receipt post office staff remove them from envelopes for sorting and storage prior to handover to customers. At the same time as initial order books are dispatched to post offices customers are issued with a Pick-up Notice (PUN) which informs them of the issue of a

POL00028135

book to their nominated post office for collection. Subsequent order books are collected in exchange for the expired covers of current books following the encashment of the last payment foil.

Stop and Recall Notices

3.4.7.3. Having issued an IOP the DSS may subsequently decide that no payment should be made on it (e.g. in cases of suspected fraud or where the customer has reported its non-receipt, loss or theft) or wish to recall it for re-rating (e.g. due to a reported change in customer circumstances):

- Stop Notices

  In the event of the requirement being to stop a payment, paper stop notices are distributed to the relevant nominated post offices (in the event of widespread fraud a wider circulation is possible). These carry instructions to the counter clerk that, in the event of the identified IOP being presented for payment it should be impounded and no payment made. BA has conducted trials in the London area into the effectiveness of an Electronic Stop Notice System (ESNS) based on machine readable bar-codes imprinted on Order Book covers. Following a successful trial period it is planned to expand this facility to all post offices within the boundary of the M25 motorway (the ALPS project) - see 3.2.6.

- Recall Notices

  In the event of the DSS wishing to recall an order book for re-rating a letter is issued to the customer requesting that they return their book to a local office following encashment on a specified date. The ESNS enables recall notices to be transmitted electronically to post offices within the area covered by the service, allowing clerks to pay a specific date's entitlement, and then subsequently impounding the book for return to DSS local offices.

Encashment at Post Offices

3.4.7.4. Customers present their IOP to post office clerks for payment. The IOP is examined by the clerk who confirms that payment is collectable on that date. In certain circumstances additional supporting identity may be requested of the person presenting the book for encashment. The clerk issues payment (in cash) and authenticates the transaction; in the case of order books by stamping both the payment foil and its associated counterfoil (which remains in the order book) and in the case of girocheques by stamping the IOP and retaining it.

POL00028135

Reconciliation

3.4.7.5. Reconciliation is the process of comparing amounts of benefit issued and paid. The objectives of the reconciliation process are to:

(a) enable full accounting of all transactions;

(b) identify losses to expenditure from fraudulent payment transactions, and:

i. identify customer fraud,

ii. identify counterfeit payments,

iii. identify internal fraud,

iv. identify third party fraud by the general public or others (e.g. employees of Royal Mail);

(c) identify and correct errors;

(d) identify omissions for issue data and/or non-encashments.

Current Procedures

3.4.7.6. The procedures currently used to achieve the above objectives are described below:

(a) Girocheques

The reconciliation of girocheques is contracted to Girobank plc. Information is sent to Girobank from ACCs on computer tape in the case of system generated payments. For clerically issued payments information is recorded manually onto copy sheets and is then transferred onto computer tape and forwarded to Girobank. Additionally all encashed girocheques are also forwarded to Girobank who ensure that for each encashed cheque there exists corresponding issue information, and that discrepancies and omissions are reported. Girobank totals the amounts shown on the issue information for comparison with the claims made by post offices, banks and building societies, and reports discrepancies.

(b) Order Books

There is currently no procedure for the complete reconciliation of order book encashments against issue data. All encashed payment foils are routed from individual post offices to the DSS Paid Order Unit (POU) in Lisahally, Northern Ireland. POU carry out a number of checks to identify incorrect encashments and to detect manipulated or counterfeit foils. Encashed foils are then archived by POU and retained for a period of 12 months for accounting and retrieval purposes.

POL00028135

Security

3.4.7.7. The security aspects may be summarised as follows:

(a) Standards

The DSS benefits payment processes operate within a framework of security and audit standards set by various internal regulatory bodies (see chapter 2 paragraphs 2.4.4, 2.4.5 and 2.4.6).

(b) Investigation

Suspicions or allegations of fraud relating to the IOP system are investigated by specialist teams within the DSS. Large-scale organised criminal attacks (e.g. involving wholesale counterfeiting of IOPs, or burglaries) are investigated by the BA Security Organised Fraud unit, often in conjunction with relevant Police Forces. All investigations and subsequent court proceedings have to be conducted in accordance with the Police and Criminal Evidence Act (PACE) 1984 and other relevant legislation.

(c) Evidential Requirement

In order to support criminal prosecutions relating to attacks on the benefit payment system evidence of fraudulent encashment is required. This evidence is primarily obtained through the following procedures:

i.	Statement of Issue	A statement (accompanied by the relevant PACE certificate) is produced by relevant DSS staff which confirms and details the issue of system produced IOPs. Similar statements may be obtained in relation to clerically produced IOPs;
ii.	Statement of Loss	Statements of Loss are obtained from: individual customers in the event of theft; or relevant DSS officers in the event of burglary;
iii.	Evidence of Encashment	The evidence of a fraudulent or incorrect encashment is currently obtainable by the retrieval of the relevant encashed IOP. In the case of Order Books a search request is issued to the DSS POU who search their archives, retrieve the relevant payment foil and send it to the requesting authority. In the case of Girocheques the encashed cheque is retrieved from Girobank, together with any necessary supporting statements;
iv.	Evidence of Investigation	DSS investigation officers are required to produce supporting evidence and any necessary statements to document the investigation process.

POL00028135

Accounting

3.4.7.8. Departmental Accounting Officers are accountable to Parliament for the use of money voted to departments. The chief executive of each agency acts as the Accounting Officer for their individual budget and portions of relevant votes. The Permanent Secretary of the DSS is the Principal Accounting Officer (PAO) with a responsibility for ensuring the standard of financial management throughout the DSS as a whole. Briefly all Accounting Officers are responsible for:

(a) signing the appropriate (or agency) accounts for the funds for which they are responsible;

(b) the propriety and regularity of expenditure;

(c) prudent and economical administration of funds;

(d) safeguarding public assets;

(e) ensuring that financial considerations are fully taken into account in policy formulation;

(f) appearing as a witness before the Public Accounts Committee (PAC) to answer questions on any areas relating to their duties.

Volumes

3.4.7.9. All volumetric information (e.g. the number of order books issued) can be found in appendix 3-8.

3.4.8 Other Benefit Payment Procedures

Agency/Appointee Procedures

3.4.8.1. Customers, with an authorised entitlement to benefit, may elect to nominate third parties to encash their awarded benefit on their behalf. Further information relating to these procedures is contained within appendix 3-5. This payment to a proxy may take a number of different forms:

(a) Permanent Appointee

A customer, unable to act on their own behalf, may nominate a third party to act as their appointee on a permanent basis. In this instance entitlement is dependent on the customer's circumstances, but payment awards are made to the nominee who encashes them on behalf of the customer.

POL00028135

(b) Temporary Appointee

A facility exists for customers to nominate appointees on a temporary basis, although it is not often exercised by customers.

(c) Permanent Agent

A customer may request a third party to act as their permanent agent. This arrangement must be acceptable to, and authorised by, the DSS. The payment is issued to the customer but the existence and details of any permanent agent are noted on the instrument of payment. Encashments are made by the agent.

(d) Casual Agent

A customer may on an ad hoc basis authorise a third party to collect a payment on their behalf. Each IOP contains a section in which the customer names their chosen agent and authorises them, by signature, to encash the benefit payment.

Alternative Payee Procedures

3.4.8.2. The Secretary of State has the power (always exercised in the case of a married couple) to make arrangements to pay Child Benefit, Family Credit or Disability Working Allowance either to the customer entitled to it, or to the other partner, where the couple live together. In two parent families, where these benefits are paid by order book, the book is issued in the name of the mother with the father's name appearing as alternative payee.

Special Facilities Procedures

3.4.8.3. Special facilities are provided so that customers can encash up to 2 payment foils at post offices other than their nominated one within the lifetime of an order book.

3.4.8.4. There is a facility for advance payment at particular times of the year (e.g. bank holidays) and extra payments (e.g. £10 Christmas bonus).

3.4.8.5. Claimants can change their nominated post office by completing the appropriate form (P80MA).

3.4.8.6. The present system also has a procedure so that claimants unable to read or write can collect their benefit at a post office.

POL00028135

CONTENTS

4. DESCRIPTION OF FUNCTIONAL REQUIREMENTS

POL00028135

CONTENTS

POL00028135

CONTENTS

POL00028135

CONTENTS

POL00028135

CHAPTER 4. DESCRIPTION OF FUNCTIONAL REQUIREMENTS

This chapter details the Contracting Authorities' service and business applications which the Service Provider's service(s) are required to support, and general operational constraints to which they must conform. These are covered as follows:

Section 4.1 overview of required services;

Section 4.2 POCL strategic infrastructure requirements;

Section 4.3 overall benefit payment function;

Section 4.4 exemplar POCL data flows.

Throughout this chapter, to aid Service Provider's understanding of the business requirement, assumptions have been made about the way certain business processes will work. These assumptions reflect current thinking and to an extent current practice, but should not be considered to be definitive. The Service Providers should concentrate on the underlying business requirements, and where considered appropriate propose alternative business processes to exercise innovative thinking, indicating any benefits, costs or risk implications (for example for security or counter service time) of their proposals.

4.1 OVERVIEW OF REQUIRED SERVICES

4.1.1 Introduction

4.1.1.1. The functional requirements of the BA/POCL project are:

- to provide a technology architecture at every post office which will enable POCL in due course to automate all transactions at the counter. The first release will include the Benefits Payment Service (BPS) to be delivered on this platform;
- to support the end-to-end benefit payment needs of BA, of which the POCL automation is one part. The procurement will support other benefit payment requirements in addition to the delivery mechanism which will be installed in post offices.

4.1.1.2. Figure 4-1 below shows the component services (in boxes) within the procurement service boundary (the large oval) that are to be provided by the Service Provider. Outside the procurement service boundary are the services (in boxes) and users (in small ovals) with which and whom the Service Provider will interface. The dotted box around Value Added Processing (VAP) is to indicate that the Transaction Management Service (TMS) is part of VAP. Each of the component services are described under sections 4.2 and 4.3.

POL00028135

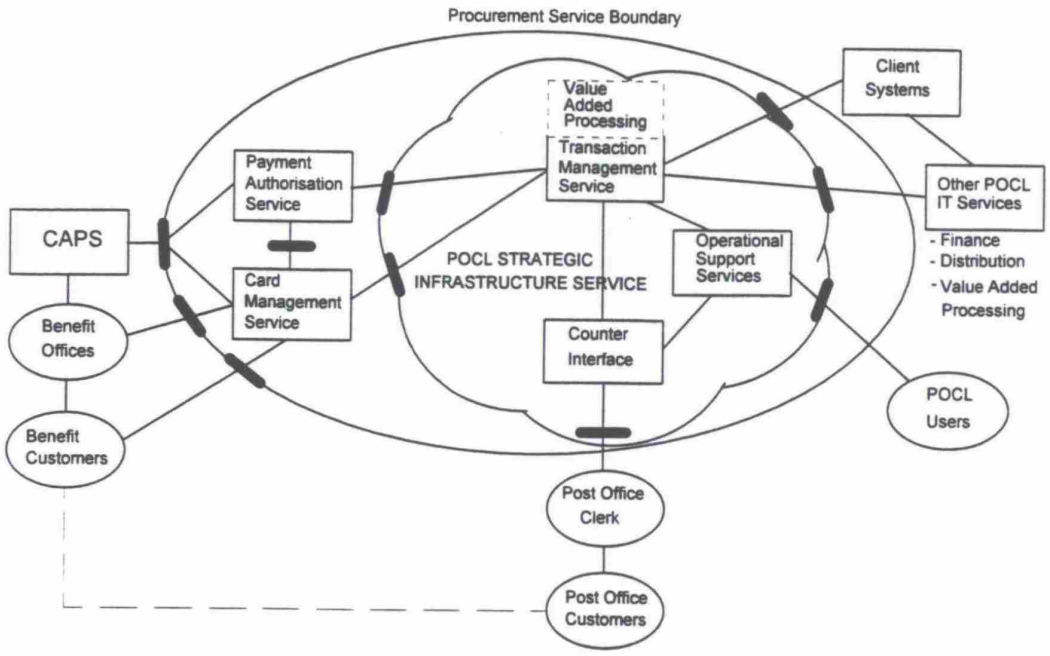


Figure 4-1 The Service Architecture

4.1.1.3. Within this chapter, in order to explain fully the end-to-end business application requirements, assumptions have been made about the split of functionality between the logical components within the procurement service boundary. It is however recognised that there are many options for precisely how such a split can be made. The Service Provider may suggest alternative models if he believes they represent better value for money. However in suggesting alternative models, the Service Provider must keep distinct the service interfaces between the component services and specify how they are defined.

4.1.1.4. In addition, Service Providers are reminded that, whether or not they suggest alternative models, the will be required to bid on the minimum specification which will be given in the contract documents. See OJEC notice (38/94) at paragraph 7.

4.1.2 General Services and Constraints

General

4.1.2.1. Service Providers are required to provide a value for money service which supports the automation of existing and anticipated business requirements of the Contracting Authorities which are specified in this SSR.

4.1.2.2. The prime requirement is for the design, development, integration, support, operation and management of a secure and auditable strategic IT infrastructure which, together with associated service applications, will meet the joint requirements of POCL and BA

POL00028135

specified in this SSR. The Service Provider's proposals must describe how their proposed solutions:

- meet the programme objectives of both the Benefits Agency and POCL set out in chapter 1;
- ensure that all business transactions are conducted in a manner which is acceptable to the Contracting Authorities, their customers, clients and agents;
- are compatible with existing and planned IS/IT security strategies of the Contracting Authorities;
- ensure business transactions are conducted in a manner which is secure, confidential, accountable and auditable;
- provide a foundation for the generation of new business for POCL;
- are in conformity with any legislative requirement imposed on the Contracting Authorities.

Systems Standards

4.1.2.3. The Service Provider must ensure that any services provided by him are able to interface and exchange information with computer systems operated by the Contracting Authorities and their authorised agents or clients and that they conform to the Contracting Authorities relevant data management policies and standards.

4.1.2.4. This chapter and associated appendices sets out an exemplar architecture and standards for the required systems and services. As with business processes, these should not be considered to be definitive. However the Contracting Authorities will be concerned to agree the positioning of the service boundaries and appropriate standards for the associated interfaces. During the contract negotiation phase, Service Providers may wish to discuss the relevance of these, or other, standards. Service Providers should, in response to this SSR, include any reservations they may have about the appropriateness of the standards provided.

Audit

4.1.2.5. Various internal audit services support BA and POCL in monitoring the achievement of business and IS/IT objectives against plans and compliance with financial control and integrity. Service Providers must be able to satisfy the audit requirements and any requirements for external audit, so that they can provide an assurance on the level of adequacy of internal control to the relevant Accounting Officer and/or Finance Director.

POL00028135

Management Information

4.1.2.6. The Contracting Authorities' specific management information requirements will evolve during the course of the procurement. The starting point for this evolution is the set of requirements outlined in the relevant sections of this document (e.g. audit trail data requirement outlined in appendix 2-8). However, the Contracting Authorities should be able to extract any reasonable data relating to the service from the Service Provider's systems to support ad hoc management information needs.

Accounting

4.1.2.7. The services which are outlined in this SSR must contribute towards the generation of separate statements of account for POCL and the DSS agencies involved (and the Service Provider). The requirements outlined in this document will provide the DSS and POCL with accounting information at the individual business transaction level. The Service Provider will be required to ensure that the data passed back to the Contracting Authorities will be accurate, timely and complete.

4.1.2.8. Note that generation of accurate benefit accounts is a major business driver for the DSS and lies behind the creation of the programme of which this procurement forms part.

Security

4.1.2.9. The Service Provider must have, or put in place, a security policy which is compatible with those of the Contracting Authorities.

4.1.2.10. The DSS, in addition to having to comply with requirements imposed by the law, has a well defined security policy which complements that of Her Majesty's Government (HMG).

4.1.2.11. To support the implementation of this security policy, the DSS maintains approximately 1,300 security standards, some of which will be applicable to this service; where a standard is deemed applicable it must be satisfied or alternatively a risk decision can be taken not to implement if this is agreed during contract negotiations.

4.1.2.12. Further detail is given in appendices 2-3 DSS Departmental Security Standards, 4-1 POCL Information Systems Security Policy, 4-2 A Code of Practice for Post Office Systems Security and 4-4 The Post Office (Group) Information Technology Architecture and Policy.

Existing Infrastructure Services

4.1.2.13. The Government and the Post Office both have data and voice networks which Service Providers may wish to consider using on a contractual basis as part of their services. The Post Office also has a number of secure delivery systems which could be used for the supply of cards or other sensitive items. Enquiries about the facilities that might be available in this context should be channelled through the Response Unit (see chapter 9).

POL00028135

4.2 THE POCL STRATEGIC INFRASTRUCTURE

4.2.1 Introduction

4.2.1.1. This section describes the requirements for the POCL strategic infrastructure. This is one of the main elements of the service architecture for this procurement and supports a range of business services at the post office counter.

Outline of the Strategy

4.2.1.2. One of the aims of the BA/POCL project is to provide a technology architecture at every post office, which will enable POCL in due course to automate all transactions at the counter. The first release of this will support, amongst other things, the Benefits Payment Service (BPS).

4.2.1.3. POCL aims to embrace industry standard hardware and software, and packaged rather than bespoke software, where it provides value for money. This new hardware and software is to be known as the automation platform. This architecture must be capable of supporting other POCL and client applications in line with the generic software approach discussed below.

4.2.1.4. POCL recognises two possible approaches for providing software at the counter - the 'Product' approach and the 'Generic' approach. The 'Product' approach broadly means building a separate application for each individual product, and this has been the historical approach to development in the Post Office.

4.2.1.5. The 'Generic' approach means automating common sets of functions which can be put together quickly to service diverse client requirements. This approach has worked well in the POCL automated bill payment area and is the direction in which the retail software industry is moving.

4.2.1.6. POCL has reviewed the high level business and data requirements for current and future counter transactions. This has demonstrated that all types of transaction (including the BA requirement) can be supported at the counter by the 'Generic' approach in 5 generic software modules, which POCL has called Inpay, Outpay, EPOS, Personal Details Capture and Token Management. The following conditions need to be satisfied:

- when the products are engineered into an electronic format, the common business processes required to support them are harmonised (e.g. the look and feel is the same across all types of transaction);
- the software modules are designed to perform standard processes, but on different data sets which are defined by the client transaction (e.g. validation of a credit card should be the same transaction as validation of a benefit card - one transaction gets data automatically from the credit card company, the other from the DSS);

POL00028135

- the shape of the client transactions are defined in rule tables which describe how the 5 generic transaction functions are combined. (e.g. BBC Licence payment would be a 'Generic Personal Details Capture' followed by a 'Generic In-pay', whereas a benefit payment would be a 'Generic Out-pay', both also using the 'Generic EPOS');

- using the rule tables, a data entry screen format can be dynamically selected from a database of screen formats based on the transaction being carried out. (e.g. a fishing licence transaction will call up a fishing licence, whereas a TV licence transaction will call up a different data entry screen format).

4.2.1.7. The 5 generic functions are illustrated more fully later in this chapter and described in appendix 3-2, but in general terms the generic functions are defined by common sets of business functions working upon commonly described data. For example, there should be no material difference in the way a television licence is processed as compared to a vehicle licence, or fishing licence. The business processes and underlying functionality will be common. The detailed data content will obviously vary.

4.2.1.8. POCL seek the Service Provider's confirmation that this concept is feasible, practical, and cost effective: research leads POCL to believe that there are clear benefits to both the Service Provider and BA/POCL in adopting the generic approach. These benefits fall into the following categories:

- **Reduced Cost**: It is hoped that the overall cost of automating products which pass over post office counters will be reduced by using standard code, as compared with writing bespoke application code for each new product. Any increase in short-term costs will need to be weighed against the potential for longer-term savings.

  The cost of adding additional products in the 'Generic' model is small. The cost of adding additional products in the 'Product' model is large - both in terms of application coding and in managing the interfaces needed.

- **Reduced Timescales**: The time to bring a new product to market in the 'Generic' model is low - a small number of days/weeks will be required to develop the data capture screens, test them, and roll out. The time to bring a new product to market under the 'Product' model will be long. Months will be required to develop user requirements, develop code, test, and roll out.

- **Reduced Risk**: In the 'Generic' model, risk is reduced by using established code each time a new product is brought to market. In the 'Product' model there is high development risk each time a new product is required.

- **Reduced Maintenance**: The cost of maintaining the 'Generic' model is relatively low, because there is a small number of well defined interfaces to support. The impact of changes can be easily modelled and tested. The maintenance costs of the 'Product' approach gets higher as more products are added because of the greater complexity of interfaces and monitoring the impact of any changes.

POL00028135

- **Reduced Support:** Authorised end users can update the parameter tables e.g. to introduce new products or price changes, with little or no involvement from IT staff.

4.2.2 Overview of Business Requirements

4.2.2.1. The remaining sections of this chapter set out the generic transaction functions in more detail and explain other key aspects of the Information Systems Strategy, demonstrating how the BA application, as well as other client applications, could be delivered using by this approach.

4.2.2.2. The POCL Information Systems Strategy focuses on the business processes that are required to support the mission and vision of the business. There are five key processing areas which make up the core business of POCL, known as the "Business Value Chain". They are shown in Figure 4-2 below, together with the key data flows that link them together.

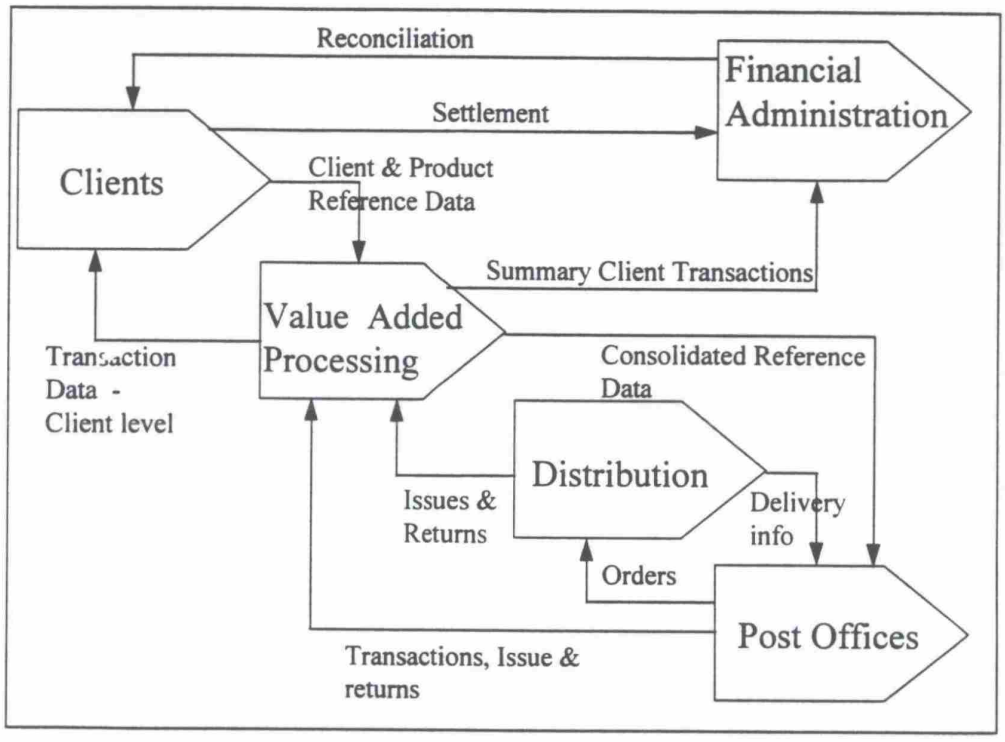


Figure 4-2 The POCL Business Value Chain

4.2.2.3. This procurement is not seeking to procure IT services to support all of these business processes, but only those shown in Figure 4-1 The Service Architecture above. These required services relate to the business processes as shown in Figure 4-3 below.

POL00028135

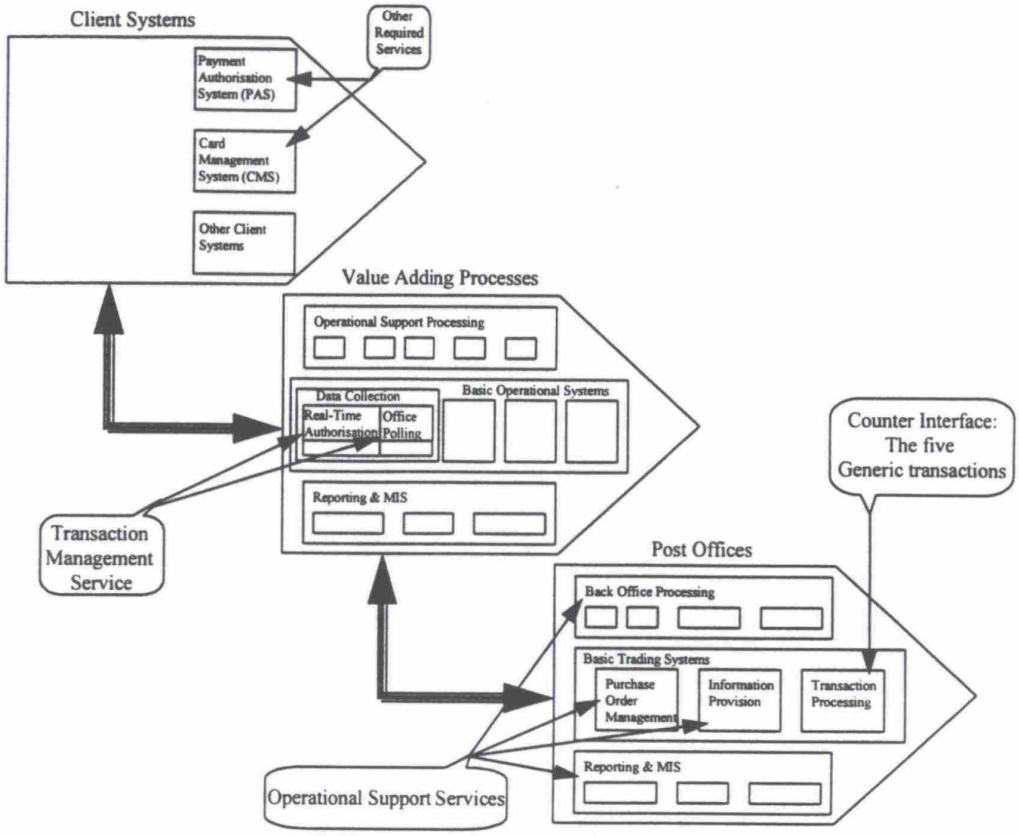


Figure 4-3 Relationship between POCL business value chain and required services

4.2.2.4. Notes:

(a) The POCL IS Strategy is described further in appendix 3-2;

(b) The Financial Administration and Distribution areas as shown in Figure 4-2 The POCL Business Value Chain are outside the scope of this procurement, but are important in terms of their interface with the Transaction Management Service (TMS);

(c) The POCL Strategic Infrastructure needs to be sufficiently flexible to support subsequent applications for POCL, its agents and clients, as well as maintaining or migrating existing functionality.

POL00028135

Overview of Required Services

4.2.2.5. The Service Provider will be required to provide:

(a) the Counter Interface;

(b) the Transaction Management Service (TMS);

(c) the capability to implement specific Operational Support Services as set out under 4.2.5;

(d) interfaces to Client Systems and other POCL services;

(e) ongoing operational management, support, maintenance, and help facilities.

4.2.2.6. In addition to the services detailed here, the Service Provider must ensure an upgrade path to enable post offices to improve and support internal operational effectiveness

4.2.3 The Counter Interface

Counter Functions

4.2.3.1. The "Applications Portfolio for post offices" (see appendix 3-2) identifies five generic functions for the processing of all transactions at the post office counter.

4.2.3.2. POCL's Point of Sale Transactions:

(a) EPOS

To manage all common point of sale transaction activities and complement point of service transactions. Features include: product and price look-up, receipt production, method of payment (EFTPOS etc, plus the Service Provider should be ready to incorporate an 'electronic purse' type method of payment) and authorisation, stock update and token endorsement.

4.2.3.3. POCL's Point of Service Transactions:

(a) Personal Details Capture

To record pertinent / relevant customer details against a counter transaction.

(b) In-Pay

To record the receipt of in payments for deposit to customers' accounts or bill payments.

(c) Out-Pay

To record out payments to customers from their accounts or on behalf of a client.

POL00028135

4.2.3.4. Other transactions:

(a) Token Management

To manage the distribution of client tokens. These are items which are personal to a specific customer, for example order books and mobile telephones.

4.2.3.5. The requirements for the POCL infrastructure services may be satisfied by applying these generic functions to every transaction passing through a POCL outlet. The functions chosen and the order in which they are used will depend on each requirement. A guide to how the functions could be used initially to support the requirement for EPOS, Bill Payment, and Benefits Payments is given in Table 4-1. The list of required transactions is not exhaustive.

Table 4-1 Examples of Transactions vs the Five Generic Functions

	Personal Details Capture	**In-Pay**	**Out-Pay**	**Token Management**	**EPOS**
Benefit Payment			✓		✓
Issue of first card	✓			✓	
Change of address	✓				
Bill Payment		✓			✓
ECCO+ replacement					✓

4.2.3.6. In implementing the above types of transaction, all five of the generic functions will have been covered. The five generic functions should be designed to be sufficiently flexible to permit the implementation of all other post office transactions.

POL00028135

4.2.3.7. Table 4-2 shows examples of a range of post office transactions that could be implemented using this reusable code. Service Providers must realise this list is not exhaustive.

Table 4-2 Further Examples of Transactions vs Functions

	Personal Details Capture	In-Pay	Out-Pay	Token Management	EPOS
Benefit OB Distn				✓	
BT bill payments		✓			
Cash cheque			✓		
COD delivery service	✓				✓
Compensation Fee parcel	✓				✓
Datapost	✓				✓
Deposit		✓			
DVLA V11		✓			
Electricity tokens	✓	✓			✓
Franking machine meters	✓	✓			
Girocheque			✓		
National Savings certificates	✓	✓			✓
New account	✓	✓			✓
Packets / parcels	✓				✓
Postage stamps					✓
Postal Order encashment			✓		
Postal Order sale		✓			✓
Poste Restante				✓	
Premium Bond repayments			✓		
Rail cards	✓				✓
Recorded Delivery	✓				✓
Registered Delivery	✓				✓
Savings bank account	✓	✓			✓
Saving stamps (sales)	✓				✓
Saving stamps (redeem)					✓
Transcash (general)		✓			
TV licence	✓				✓
Undelivered Mail items P739				✓	
Withdrawal			✓		

POL00028135

Constraints Affecting the Counter Interface

Physical Constraints - Environment

4.2.3.8. The counter interface is required for a variety of types of post office, from large multi-position post offices (with, say, 20-30 positions) down to those with only a single position. Also the layout of offices varies, from the traditional counter positions behind glass screens to open plan offices, post offices with Post Shops, 'community' offices in various difficult environments or set up temporarily or seasonally in, say, village halls, mobile post offices (there are four currently) and emergency post offices (currently 17 portacabin units - the equivalent of three standard post offices).

4.2.3.9. The post office counter environment is considered to be more hostile for computer equipment than an office environment. Post offices vary considerably with respect to atmospheric temperature and contamination. The movement of people and paper in particular result in a dusty environment.

Physical Constraints - Equipment

4.2.3.10. The space available on the counter for computer hardware (e.g. screens, keyboard, magnetic swipe reader) is often limited. Hence the equipment will often need to be compact.

4.2.3.11. The choice of screen type (colour or mono), keyboard type and the specifications of the terminal equipment is for the Service Provider to propose and explain. Service Providers should not feel constrained by the technical specifications set out in appendix 4-4 in their proposals for counter equipment.

4.2.3.12. Any equipment proposed must conform to the appropriate health and safety regulations. It must not interfere with the health, comfort or normal pattern of work of staff as a result of emission of acoustic noise, vibrations, heat fumes or other radiation, or as a result of its construction.

Operational Constraints - Staff

4.2.3.13. The counter interface is to be used by counter clerks with a wide range of backgrounds and ages. No assumptions can be made about their previous level of computing experience.

Operational Constraints - User Interface

4.2.3.14. The counter interface needs to provide a consistent interface for handling different types of transactions. This needs to be intuitive for staff to minimise errors and delays. Staff should find the system simple to operate (with minimal training).

4.2.3.15. The interface needs to be adaptable to allow the introduction of new applications and client transactions with the minimum of effort, disruption and re-training.

POL00028135

4.2.3.16. The operation of a transaction must be quick to avoid build-up of queues. At present transactions take from under 5 seconds to several minutes to complete, with a mean of the order of half a minute.

Operational Constraints - Data Capture

4.2.3.17. Given the variety of clients and transaction types, the interface will need to support a variety of card technologies.

Operational Constraints - Printing

4.2.3.18. The equipment at the counter interface will need to produce retail type output, e.g. receipts, printing on cheques and printing on pre-printed forms such as vehicle licences.

Operational Constraints - Migration

4.2.3.19. During roll-out of any new IT services it is important that post offices do not suffer a loss in functionality of their systems. This means migrating from existing systems where they are in operation. Existing systems are described in separate appendices.

4.2.3.20. The minimum application configuration to be available at each post office on the day roll-out reaches it (and therefore to be supported by the infrastructure) is:

- Benefit payments;
- an EPOS application to replace ECCO+ functionality;
- Automated payments migrated from APT (e.g. In-pay);
- Operational Support Services as set out in section 4.2.5;
- Connectivity to the remainder of the POCL business value chain via the TMS element of VAP (indicated in Figure 4-2).

Operational Constraints - Security

4.2.3.21. The counter interface needs to provide security features that work at the level of the individual staff member, e.g. with respect to log-in identification and authorisation to perform functions.

4.2.3.22. Systems need to be trustworthy and, in the event of failure, re-established without loss of integrity. Any disruption to the normal provision of services to customers caused by the failure of computer systems must be minimised. Fall-back and recovery arrangements are needed for continuing to provide post office services when failures occur.

POL00028135

Commercial Constraints - User Interface

4.2.3.23. Where an agent of the post office may in future use the counter infrastructure (e.g. EPOS) for his own business, then it will be necessary to identify the transactions for his business and post office work separately, in particular for financial accounting.

4.2.3.24. The counter interface should be designed so that features can be added or adapted to take advantage of new developments in technology.

4.2.4 Transaction Management Service

4.2.4.1 Overview of the Transaction Management Service

4.2.4.1.1. The TMS is a part of the Value Added Processing business function. This is the business function which allows a small number of clients (currently less than 200) to communicate with a large number of post offices and distribution centres (currently more than 19,000), and in turn allows the post offices and distribution centres to return relevant information to them.

4.2.4.1.2. The purpose of the TMS is to provide the essential data collection and delivery links between post offices, distribution centres, POCL and clients. The TMS will replace the existing host polling centre.

4.2.4.1.3. It is not envisaged that the Service Provider would take on the work currently performed by the client transaction (cash account) processing centres at Chesterfield and Edinburgh or the Document Processing Centre (Data Central) in London. However, the Service Provider may decide that he needs similar facilities to provide contingency, resilience and migration from current paper-based systems.

4.2.4.1.4. The following sub-sections covering TMS discuss:

(a) the interface with POCL's clients;

(b) the interface with Financial Administration;

(c) the interface with Distribution;

(d) the interface with other Value Added Processes; and

(e) audit requirements.

4.2.4.1.5. The interface between the TMS and the Counter Interface service is not discussed as this is entirely within the service boundary.

4.2.4.2 Interface with Other POCL & Client Systems

4.2.4.2.1. The TMS will provide the link between the transactions performed at the Counter Interface and the appropriate POCL systems. In some cases, the Service Provider may

POL00028135

also be required to provide a link to client systems. The Service Provider will also be required to transmit client data to post offices.

4.2.4.2.2. As identified in the prospectus, currently eight clients generate over 90% of the business carried out in post offices. The split, represented by percentage income, is as follows:

- Benefits Agency 32%
- Postal (Royal Mail and Parcelforce) 22%
- Alliance and Leicester / Girobank 20%
- Other Government Departments (Department for National Savings and Driver and Vehicle Licensing Agency) 10%
- Other clients (BT and BBC) 7%

4.2.4.2.3. New business opportunities are also being developed as described in Chapter 3 and the previously received prospectus, including the area of bill payments.

4.2.4.2.4. The nature of the interface with clients and their systems will depend upon the nature of the information that needs to be exchanged to support their transactions. Options include:

(a) on-line authorisation from client systems;

(b) batched authorisations transferred to the TMS for on-line authorisation at the point of sale;

(c) transfer of batched information, with details of each transaction or summaries of transactions;

(d) transfer of client standing data.

4.2.4.2.5. The exact method used for a particular client will be specified on a client by client basis. However it should be possible to change the authorisation approach by changing system parameters.

4.2.4.2.6. In the case of the Benefits Agency, the Benefits Payment Service may use any or all of the above as proposed by the Service Provider and justified on economic, risk and service quality grounds.

POL00028135

4.2.4.3 Interfaces with Financial Administration

4.2.4.3.1. The TMS needs to provide information about counter transactions to the rest of Value Added Processing (VAP) and through VAP to the Financial Administration (FA) business functions. These areas are concerned with the reconciliation of client transactions and the settlement of client monies, as well as statutory accounting and treasury functions.

High Level Functional Objectives

4.2.4.3.2. The high level objective of reconciliation is to substantiate specific accounts in order to demonstrate the completeness and accuracy of the ledgers. This involves specifically reconciling all inter-office remittances and ensuring that errors resulting from cash account processing are investigated and corrected. Our current intention is to retain this function within POCL, but using data supplied by the Service Provider.

4.2.4.3.3. The objectives of settlement are to arrange payments due to clients and to receive payments due from clients in accordance with their contracts. This involves ensuring accurate settlement on the due contracted date and that appropriate funding arrangements are in place so that there is no cash flow disadvantage to POCL. Again, our current intention is to retain this function within POCL, but using data supplied by the Service Provider.

Information Needs

4.2.4.3.4. To achieve these objectives, given the automation of transaction processing at the counter, the following information must be captured:

(a) value of each transaction;

(b) volumes of transactions;

(c) a unique code for each product so that detailed product information can be made available across all clients (e.g. breakdown by denomination of Royal Mail stamps sold);

(d) source (i.e. outlet, clerk and till identification);

(e) client reference and client scheme or product reference for each transaction;

(f) customer identification and details (e.g. for transactions involving cheques, passports, motor tax discs);

(g) method of payment;

(h) date and time of the transaction.

4.2.4.3.5. All the above needs to be captured daily for all transactions and products and made available for the Settlement and Reconciliation.

POL00028135

4.2.4.4 Interface with Distribution

4.2.4.4.1. The TMS also needs to provide information about counter transactions to the Distribution business function and receive information from it. This function plans and controls the physical distribution of cash and stock across the business. The specific requirements for this interface are described in appendix 4-3. In general these cover daily or weekly transfer of details about:

(a) overnight cash holding;

(b) value and transaction stock holding;

(c) remittances and returns.

4.2.4.4.2. The provision of overnight cash holding information will need to be in place from the start of the roll-out of the new service. The other details may not be required by the Distribution systems until later.

4.2.4.4.3. Any services provided by the Service Provider for use in distribution centres must be capable of interfacing with their current stand-alone distribution systems as well as forwarding information on transactions and stock movements via the TMS in the same way as any other outlet. Further discussions with the Service Provider will be necessary in order to determine the precise nature of these interfaces.

4.2.4.5 Interface with other Value Added Processes

4.2.4.5.1. The TMS should have the facility to provide information about relevant counter transactions to other value added processes, as and when systems to support these are put in place. Chapter 3 referred to POCL's Transaction Information Processing project, and it is not currently envisaged that Value Added Processing (VAP) areas other than the TMS will be within this procurement. Service Providers are asked to indicate the feasibility and implications of adding other aspects of VAP to the procurement at a future stage.

4.2.4.6 Audit Requirements in POCL

4.2.4.6.1. The TMS needs to maintain an audit trail of transactions for inspection by POCL's auditors. Arrangements may be made for passing back audit information following closure of reporting period books.

High Level Objective of Internal Control

4.2.4.6.2. The objective of internal control is to ensure that the processing of client transactions is carried out in an orderly and efficient manner, that assets are safeguarded and the completeness and accuracy of records is secured.

POL00028135

Information Needs

4.2.4.6.3. To achieve these objectives, the overall business processes following the automation of transaction processing at the counter are to ensure that the following requirements are met:

(a) POCL and agents' private transactions are separately identifiable;

(b) capture of data at the outlet is complete, accurate and robust e.g. unique reference per transaction;

(c) any transfer of data to/from a central location (repository) is secure, complete, accurate and robust;

(d) whether off or on line the service must be capable of validating transactions by format and value;

(e) in the event of fraud it can be proved that the service was operating without defect;

(f) transaction receipts (identifiable to specific clients) are automatically generated for customers and retained to allow recovery if there is a failure between back up cycles, or to allow problem resolution at post offices;

(g) accountability for cash, stock and any supporting documentation is maintained by each outlet and individual clerk where appropriate;

(h) the method of payment is recorded at the point of sale;

(i) access to the system and to certain functions within the system is restricted and a user log is maintained;

(j) appropriate back ups are taken including a complete record of daily transactions;

(k) it should be possible to require an independent/supervisory check to amend or cancel transactions after a certain level of processing;

(l) both operator and device are uniquely identified within each outlet;

(m) data should undergo a balancing procedure to enable a final review and authorisation;

(n) all transactions are collected using a secure method at the earliest opportunity;

(o) transactions not collected from previous days are clearly identifiable;

(p) all transactions can be reconciled to an appropriate supporting voucher depending on the transaction type. Where necessary these vouchers are to be available for central validation to amounts collected;

POL00028135

(q) the system should maintain an up to date record of cash and stock on hand for audit purposes and be capable of reporting current balances;

(r) all transfers to/from other offices and between staff are clearly identifiable;

(s) all specified summaries are produced automatically when required and all transactions are included since the last summary was completed;

(t) items posted to suspense accounts can be identified for future investigation;

(u) information to show compliance with relevant legislation. e.g. Health and Safety, Data Protection Act, Companies Act;

(v) an outlet must be able to continue operating and to maintain an audit trail in the event of system failure.

4.2.5 Operational Support Services

4.2.5.1 Scope

4.2.5.1.1. It is envisaged that the two parts of the Operational Support Services to be included in the procurement will be Outlet Remuneration & Reconciliation and Reporting & MIS, as outlined below. The former would support Postmaster remuneration, while the latter would allow production of the Cash Account. Both of these are produced by the Capture software and would need to be produced in this solution. The Reporting & MIS function would also allow other financial and management reports (e.g. cash account) to be produced.

4.2.5.1.2. However, as a general rule, the provision of the Operational Support Services within Post Offices will not be part of this procurement. The Service Provider will need to ensure that the capability to add these services is provided.

4.2.5.1.3. During the period of the service contract(s), POCL may request some more, or all, of these services to be implemented, but on a case by case basis, and costed separately.

4.2.5.2 Office Accounting and Cash Account Production

4.2.5.2.1. Together with the facilities offered by the Counter Interface, the purpose of the following is to provide full accounting for individual post offices. These comprise:

(a) Stock Management including cash;

(b) Purchase Order Management;

(c) Financial Accounting;

and are described briefly below.

POL00028135

Stock Management

4.2.5.2.2. To record accurately stock levels (stock keeping) and report re-order requirements (replenishment analysis). The business processes for stock keeping are:

(a) the ability to record the arrival of stock from a stock provider or other post office;

(b) the ability to transfer stock to another post office at the request of that post office;

(c) the ability to record sales of stock. This may be automated with links to the counter interface.

4.2.5.2.3. In addition, replenishment analysis would provide reports at periodic intervals and on request.

Purchase Order Management

4.2.5.2.4. To control the purchase and return of stock from / to stock providers (including other post offices). The business processes cover:

(a) the ability to record details of stock items, including stock provider reference, product code, quantity, price quoted;

(b) the ability to control and monitor orders for stock;

(c) the ability to return stock to the stock providers.

Financial Accounting

4.2.5.2.5. To maintain the financial records of a post office, including features of:

(a) Sales ledger;

(b) Purchase ledger;

(c) General ledger;

(d) Fixed Assets register; and

(e) Outlet Remuneration and Reconciliation.

4.2.5.2.6. The last includes the recording of transactions and the production of reconciliation reports, transaction analysis reports and postmaster remuneration reports.

POL00028135

4.2.5.3 Other Local Support Functions

Staffing

4.2.5.3.1. To record (time and attendance) and manage the availability (scheduling) of staff to ensure standards of service are maintained.

Administration Support

4.2.5.3.2. To provide standard administrative support facilities to POCL management and staff, based on standard PC packaged software.

Reporting and MIS

4.2.5.3.3. To provide reporting facilities to POCL management and staff, covering:

(a) Sales Analysis

To analyse product sales by volume, value and time.

(b) Contribution Analysis

To report on business performance for individual post offices.

(c) Quality of Service

To analyse the transaction time and perform customer counting for individual post offices from transaction details.

4.2.6 Migration of current POCL systems

4.2.6.1 Introduction

4.2.6.1.1. In order to avoid duplicating systems (especially at the counter where space is at a premium), and to ensure that there is a sensible integration of applications, POCL recognises that there will need to be some redevelopment of existing systems and that some will be superseded by the new automated systems. In particular, the following should be noted:

(a) functionality of ECCO+, and APT must be available on the new platform from the outset;

(b) the migration plans for CAPTURE, ALPS and CRISP are yet to be determined;

(c) it is not envisaged that functionality will be provided for National Lottery services which currently use stand-alone systems;

(d) the Service Provider may wish to consider the use of the POCL Document Processing Centre as part of their migration / contingency plans;

POL00028135

(e) the Service Provider will need to consider how to migrate/ integrate services currently provided by the POCL Host Polling centre.

4.2.6.1.2. The functionality and service standards provided by existing systems must be maintained without degradation to POCL, its Clients, Customers, Staff and Agents throughout the development and roll-out of the new automation platform.

4.2.6.1.3. Service Providers are also invited to identify where there is scope for improving upon the current levels of service and functionality.

4.2.6.1.4. Service Providers are asked in particular to reflect the following sections.

4.2.6.2 Specifications of Existing Systems

4.2.6.2.1. These are set out in appendices 3-3, 3-4, 4-5, 4-6 and 4-7; and Service Providers are asked to consider all relevant information e.g. fallback/contingency; customer access (magnetic stripe, smartcards); data transfer requirements and communications.

4.2.6.2.2. Details of current volumes, and future where known, have been included although these are a reflection of the existing systems coverage. Service Providers are asked to indicate any volume constraints given their national roll-out assumptions.

4.2.6.3 Client Specification

4.2.6.3.1. The provision of the APT and ALPS service standards are underpinned by contractual commitments with a range of clients. It is not envisaged that any change to the actual equipment will have contractual implications but it is essential that service provision as per current levels is maintained as an absolute minimum.

4.2.6.3.2. Service Providers are asked to specify the way in which their proposals for integration can be achieved whilst avoiding any disruption to existing system standards and functionality.

4.2.6.3.3. It is emphasised that any contact with clients or agents in respect of these services or this procurement must be channelled via POCL using the procurement contact given in chapter 9.

4.2.6.4 POCL Specification/Interfaces

4.2.6.4.1. Existing systems have a variety of interfaces with POCL's accounting, reconciliation and settlement systems and these are set out at a high level in appendices 4-8.

4.2.6.4.2. It is envisaged that all counter transaction data passing through the counter interface will be passed on to the TMS to enable error checks and reconciliation with financial accounts. Separate POCL projects are addressing the areas of transaction information processing, distribution systems, and the interface with financial administration. Service Providers should ensure that the "data stream interfaces" can, as a minimum, deliver systems which will meet existing specifications.

POL00028135

4.2.6.4.3. Service Providers are asked to highlight any additional benefits e.g. speed/frequency of data provision, over and above the existing specifications.

4.2.6.5 POCL Support Services

4.2.6.5.1. POCL currently operate a range of support services, e.g. help desks, for which high level details are included chapter 5. Service Providers are asked to set out their proposals for integrating these support facilities with any of their own services both during roll-out and in a steady state environment.

4.2.6.6 Intellectual Property Rights/Asset Transition

4.2.6.6.1. Service Providers are requested to set out any proposals for taking over existing equipment/assets whilst noting that the commercial and operational arrangements would need to be discussed and agreed with POCL, and via POCL with appropriate third parties e.g. agents (Capture).

4.2.6.6.2. Service Providers will need to consider with POCL the transfer of Intellectual Property Rights (IPR) arrangements for any new systems and applications in line with the guidance set out in chapter 8.

4.2.6.7 Technical Design/Ergonomic Considerations

4.2.6.7.1. The services to be provided both within post offices and in the TMS must reflect the constraints of the operating environment (section 4.2.3) and POCL technical and commercial considerations.

4.2.6.7.2. The proposals for the TMS should take account of POCL's view that two logical systems for polling individual sets of equipment within post offices are considered undesirable. Alternative physical locations may however be appropriate to facilitate migration or for contingency purposes and Service Providers are asked to specify the reasoning behind their service architecture.

POL00028135

4.2.7 Appendices

4.2.7.1. All future systems work in post offices should take into account:

- the principles outlined in the IS Strategy, and Security Policies and Codes of practice;
- the migration of functionality currently found in the ECCO terminals, the APT terminals, and the Alps project.

4.2.7.2. Details of these can be found in the references noted below.

Reference	Contents
Appendix 3-2	POCL Information Systems Strategy
Appendix 3-3	CRISP technical description
Appendix 3-4	Capture technical description
Appendix 4-1	POCL Information Systems Security Policy
Appendix 4-2	A Code of Practice for Post Office Systems Security
Appendix 4-3	The Distribution interface
Appendix 4-4	The Post Office (Group) Information Technology Architecture and Policy.
Appendix 4-5	The ALPS Project
Appendix 4-6	ECCO+ technical description
Appendix 4-7	APT technical description
Appendix 4-8	Polling and Terminal Control service

POL00028135

4.3 BENEFIT PAYMENT SERVICE

4.3.1 Introduction

4.3.1.1. This section describes the primary business service which will become the mechanism by which Social Security benefit recipients receive their payments in post offices.

4.3.1.2. Today, these customers receive Social Security benefits in the post office (both cash and milk tokens) using an order book of payment foils, or a Girocheque.

4.3.1.3. Under the required service, of which this procurement forms a large part, the encashment of benefit payments will be conducted at post offices by use of a token (hereinafter referred to as a *card*) which, once authenticated, unlocks payment details held in the PAS. To this extent the *value* is held in the system not in the card.

4.3.1.4. The Service Provider's service will receive authorised payments from the CAPS and ensure their availability via the service infrastructure at post offices. This data will comprise benefit payment details, across all benefit types, and customer personal details. The exact nature of the latter are a matter for the judgement of the Service Provider, subject to confirmation of acceptability by the Contracting Authorities. A more detailed description of this service application follows.

4.3.1.5. Payments by card will be utilised for benefit collection at post offices replacing, over time, payments currently made by order book and Girocheque. The Government are committed to offering benefit customers a choice of payment method and will continue to encourage the use of ACT as an alternative to payment in the post office. The new method of payment (MOP) will also be used by the DHSS (Northern Ireland) Social Security Agency (SSA) and the War Pensions Agency (WPA). Further applications may be found for the process in the future such as payments from the Child Support Agency (CSA). In this SSR, where the business of the BA or DSS is described, it should be assumed, unless otherwise stated, that this extends to cover the requirements of other departments and agencies which will use the BPS.

4.3.1.6. Unemployment benefit is currently administered by Employment Services (ES) on behalf of the DSS and this benefit is paid predominantly by Girocheque. However, Unemployment Benefit will be phased out from April 1996 and replaced by Job Seekers Allowance (JSA) which will be administered by BA staff mostly from ES offices. The current planning assumption is that JSA will be paid initially by Girocheque or ACT but will be migrated, with all other BA administered benefits, to the new card method of payment.

4.3.1.7. The benefits which may be covered by the BPS currently include:

- Attendance Allowance;
- Child Benefit;
- Child Special Allowance;

POL00028135

- Christmas Bonus;
- Cold Weather Payments;
- Disability Living Allowance;
- Disability Working Allowance;
- Family Credit;
- Guardians Allowance;
- Invalidity Benefit (to be replaced by Incapacity Benefit from 1/4/95);
- Income Support;
- Industrial Death Benefit;
- Industrial Injuries Disablement Benefit;
- Invalid Care Allowance;
- Maternity Allowance;
- One Parent Benefit;
- Pneumoconiosis, Byssinosis and Miscellaneous Diseases Scheme;
- Reduced Earnings Allowance;
- Retirement Allowance;
- Retirement Pension - Non Contributory;
- Retirement Pension - Contributory;
- Severe Disablement Allowance;
- Sickness Benefit (to be replaced by Incapacity Benefit from 1/4/95);
- Social Fund Grant or Loan;
- Training Allowance;
- Unemployment Benefit (to be replaced by Job Seekers Allowance from 1/4/96);
- War Pensions (this is the generic name for a number of different benefits);
- Widows Pension;
- Widowed Mothers Allowance;

POL00028135

- Widows Payment;
- Workmen's Compensation Scheme.

4.3.1.8. The range of benefits covered by this service will change over time. The service should cater for the payment of: all existing benefits, changes to existing benefits and the introduction of new benefits.

4.3.1.9. Housing Benefit and Council Tax Benefit, paid by Local Authorities on behalf of the DSS, are excluded from this programme.

4.3.2 Functional Summary

4.3.2.1. Figure 4-4 extends the Service Architecture diagram (figure 4-1) which shows the context of the procurement, to show the required and existing DSS systems which are relevant to the programme, of which this procurement is part, and which are described in summary in this section.

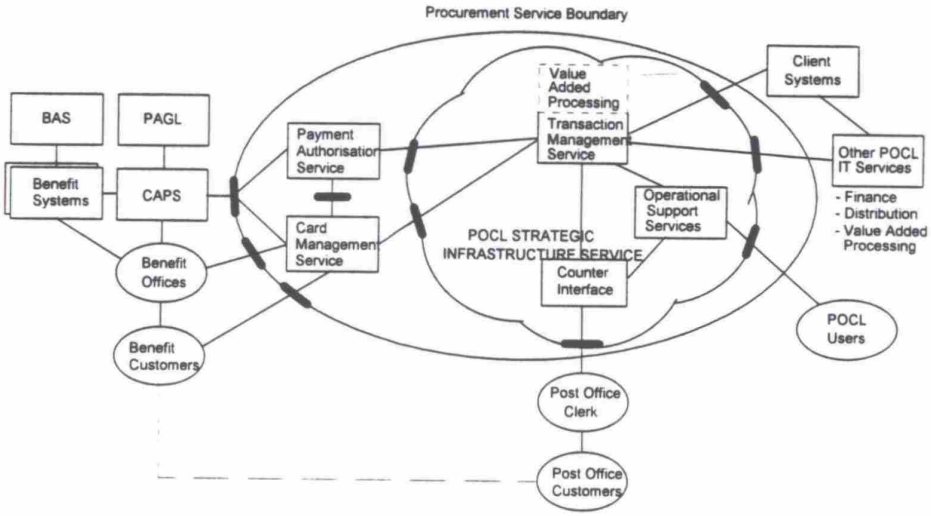


Figure 4-4 The Card Payment Context Diagram

- Benefit Systems — all the existing and future benefit systems (both computerised and clerical). It also includes systems currently accessed by Employment Service Agency to administer Unemployment Benefit (to be replaced by Job Seekers Allowance);
- BAS (Benefit Apportionment System) — an existing system to account for benefit expenditure on a cash basis by apportioning disbursements according to analysis of payments issued;

POL00028135

- Benefit Offices — About 2,000 locations from which benefits are administered. Currently this includes all BA, WPA, ES and SSA locations. However, the Service Provider should note that future changes in benefit administration, along with other uses of the services, will result in changes (potentially significant) to this estate over time;

- CAPS (Customer Accounting and Payment System) — a new system which creates a customer account for each benefit customer and, for card payments, releases authorised payments into PAS;

- PAGL (Programme Accounting General Ledger) — a new system to generate and maintain full benefit accounts, eventually on an accruals basis;

- Payment Authorisation Service (PAS) — a new service which authorises, via the POCL Strategic Infrastructure, benefit payments for collection in post offices;

- Card Management Service (CMS) — a new service which manages the production, distribution and monitoring of benefit payment cards to benefit customers.

Benefit Systems

4.3.2.3. BA will, by the time the first card payments are issued, administer in excess of 30 benefits from approximately 2,000 locations (including ES locations from which Job Seekers Allowance will be administered) including central benefit processing sites, the largest of which are at Blackpool and Newcastle. The administration of all but a few benefits (in all, less than 500,000 recipients) is supported by existing computer systems which are located in four Area Computer Centres at Swindon, Washington, Livingston and Norcross (Fylde). As used in this document 'benefit system' refers to both the computerised and the clerical systems.

4.3.2.4. Under current arrangements, the majority of benefits are paid by order book. Alternative methods of payment for most benefits are Girocheque, ACT or payable order (in certain emergency circumstances, benefits can also be paid directly in cash). The problems with the current methods of payment at post offices and the solution to those problems — which has led to the creation of this programme — are explored fully in "Strategy for Benefit Payment at Post Office Counters", *BA/POCL*, February 1994, an abridged version of which has been sent to all bidding Service Providers.

4.3.2.5. Currently, benefit systems either print the physical instruments of payment (IOP) directly (a limited number are produced manually) or, in the case of ACT, feed directly into BACS. Today there is no one system which records all the payments that may have been made to an individual. Most of the benefit systems are designed to calculate future payments (up to a maximum of 52 weeks in advance) within various constraints (for example where the nature of the benefit rules limit the length of each award or where there is an impending benefit rate change). CAPS, to be built as part of this programme, will accept this *string* of future benefit payments. CAPS is to be developed as a component of the programme of which this procurement forms part.

POL00028135

4.3.2.6. It is important to note that the award of benefit has to be adjudicated (legally authorised) and that these adjudications can only take place within the benefit systems under the control of authorised officials. The services which are being procured as part of this programme are concerned purely (in relation to the BPS) with paying benefits and not awarding benefits; this is an important separation.

CAPS — Customer Accounting and Payments System

4.3.2.8. CAPS will evolve to be the primary 'Benefit Customer Account' for all benefit payments, debts and recoveries, including payments currently made by non-computerised benefit systems.

4.3.2.9. It is assumed that CAPS will eventually hold, by customer, details of all benefit payment transactions — both future (as they are calculated by benefit systems) and previous (for up to two years) — irrespective of the method by which the payment is made. The question of whether CAPS holds details of order book and Girocheque payments for accounting and customer account enquiry purposes in the interim (before the roll-out of cards is complete) is still under consideration.

4.3.2.10. Although CAPS holds strings of future payments, where calculated by the benefits systems, the assumption in the SSR is that CAPS only releases an individual authorised payment into PAS just prior (making allowance for transmission and processing delay) to the due date for encashment in the post office. The CAPS design will also cater for the early release of authorised payments into PAS to allow for public holidays.

4.3.2.11. In addition to authorised payments, CAPS also receives from the benefit systems notifications of debt decisions (e.g. the recognition within the benefit systems that an overpayment has occurred). Although these debt decisions are needed to create complete customer and benefit accounts they have no impact on the BPS. However, benefit systems can make provision to recover these debts through future benefit payments — such reduced payments will be notified to PAS by CAPS in the normal way.

4.3.2.12. Where debts are recovered from the customer directly (rather than from benefit) these repayments are recorded on CAPS. This, again, does not impact the BPS.

4.3.2.13. The vast majority of customer enquiries handled in benefit offices are about payments. Therefore an important benefit of CAPS to the BA (in conjunction with other components of the BPS) is its ability to provide benefit staff with a single, complete information source for a customer's payments.

4.3.2.14. To support card payment and accounting functions, CAPS must source personal details for three categories of individual:

- all current BA, SSA and WPA customers (i.e. currently or recently in receipt of benefit);
- all ex-customers of BA, SSA or WPA that have an outstanding debt;

POL00028135

- all individuals who act as an appointee, permanent agent or are an alternative payee for a BA, SSA, WPA customer and are paid those benefits using the *card* MOP and are not also in either category above (termed proxies).

4.3.2.15. CAPS needs personal details for a number of purposes, either for its own use or to pass to client services such as CMS and PAS:

- to verify that changes to personal details are, in fact, reported by the correct individual;
- for use on enquiry screens and reports to confirm that the correct individual is being dealt with;
- to contact individuals (e.g. to send them card pick-up notices via CMS or to send them customer account statements);
- to send to CMS where some personal details are used on the card;
- to send to PAS to control payments (e.g. notification of appointee);
- to set up a CAPS account (even where the account holder is not paid any benefit by card);
- to send to PAS for authentication at the post office.

4.3.2.16. The sourcing of personal details for CAPS, which has a wider dimension than for other DSS systems, is still under discussion in the Department.

CMS — Card Management Service

4.3.2.18. CMS (described in more detail in 4.3.7) is responsible for arranging the supply, personalisation and distribution of the card and monitoring its status throughout its life.

4.3.2.19. CMS receives an initial instruction from CAPS when an individual needs to be supplied with a card for the first time. It is assumed that cards will be refreshed, as decided by the Service Provider and agreed with the DSS, automatically by CMS and not under the control of CAPS.

4.3.2.20. CAPS could make available to CMS certain personal details which may be needed to manage the card process (although this does not preclude data being gathered via another route).

4.3.2.21. It is possible that the physical components of the CMS could be used to provide other card service offerings; including cards to be used for non-benefit payment purposes elsewhere in POCL's domain.

POL00028135

PAS — Payment Authorisation Service

4.3.2.23. PAS (described in more detail in 4.3.6) is closely coupled to (but separate from) CMS and receives authorised payments from CAPS. When the customer arrives at a post office counter, PAS authorises any payments via the POCL Strategic Infrastructure.

4.3.2.24. PAS, via POCL Strategic Infrastructure, records the encashment and passes back a confirmation of the encashment to CAPS.

4.3.2.25. Individual authorised payments can be stopped in PAS (upon receipt of a stop instruction from CAPS) if they have not been encashed.

4.3.2.26. Authorised payments in PAS can only be cashed in a post office between their due date and their expiry date. Subject to CAPS control, early encashment may be available due to public holidays. If an authorised payment expires in PAS it is made void and a confirmation passed back to CAPS.

PAGL — Programme Accounting General Ledger

4.3.2.28. The PAGL will hold, in summarised form, all the transactions that flow through CAPS to create a set of accounts for benefit expenditure. Where authorised payments combine more than one benefit component the accounting analysis will be done at the individual component level.

4.3.2.29. It is assumed that PAGL will be able to create accounts on both a cash basis and eventually on an accruals basis in order to feed into Resource Accounts for the Department.

4.3.2.30. The ability of the new BPS described in this SSR, along with CAPS and PAGL, to generate accurate benefit accounts is a major driver in the DSS behind the creation of the programme of which this procurement forms part.

BAS — Benefit Apportionment System

4.3.2.32. The BAS is currently used to apportion expenditure to create benefit accounts from an analysis of the issued payments. It is probable that BAS will continue in operation while order books are still in use and for an extended period until PAGL is fully operational and working smoothly. PAGL will eventually supersede BAS.

4.3.3 Key Business Events

4.3.3.1. To provide a context for the components described above, this section shows how they could be combined to support some of the key business events supported by the BPS. It should be emphasised that these examples:

- are purely illustrative and do not intend to restrict Service Provider proposals;
- do not represent all the business events that must be supported by the BPS.

POL00028135

4.3.3.2. Supply a customer with their first card:

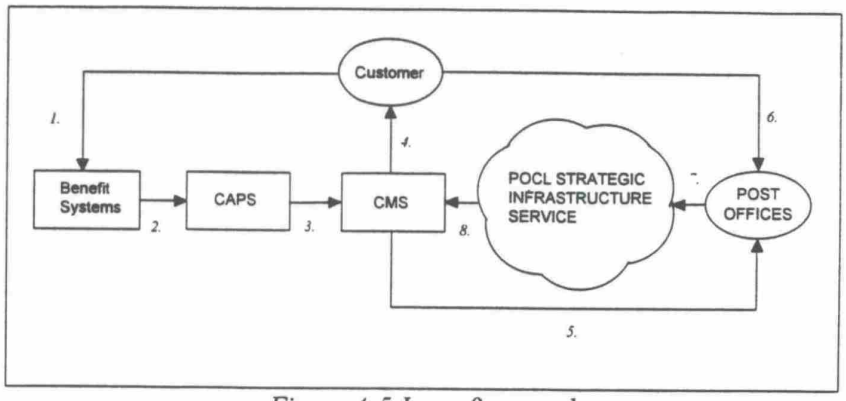


Figure 4-5 Issue first card

- illustrated in Figure 4-5, the customer selects (or is switched to) the card method of payment) which is notified to the benefit system (step 1) (which will automatically update CAPS). Alternatively the necessary details to switch the customer to card MOP are already held in which case the benefit system directly notifies CAPS (step 2);
- CAPS sends an instruction to CMS notifying the customer's need for a card (step 3) along with relevant personal details;
- CMS sends the card to the post office (step 5) which confirms its arrival (step 7/8) via the POCL Infrastructure. CMS then issues a pick up notice to the customer (step 4);
- the customer collects the card at the post office (step 6) and the post office informs CMS of the collection (step 7/8).

4.3.3.3. Make a benefit payment to a 'card' customer:

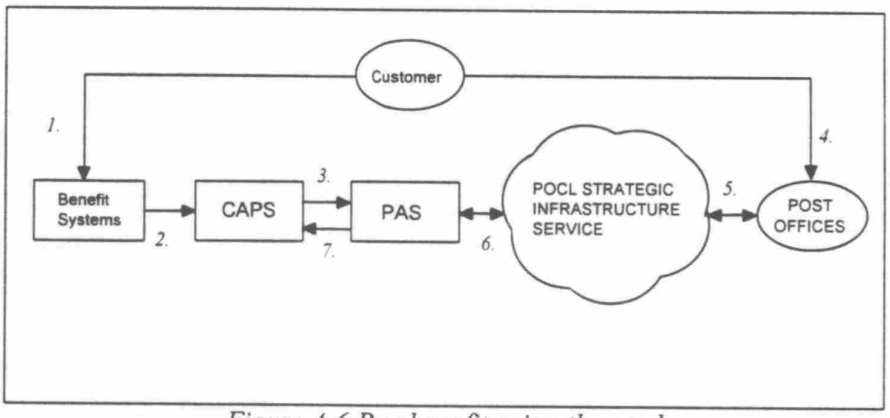


Figure 4-6 Pay benefit using the card

POL00028135

- illustrated in Figure 4-6, the customer sends in a claim form or notifies a change of circumstance (step 1); the benefit systems record the evidence and make an award;
- the benefit systems pass authorised payments to CAPS (step 2) which, at some time before they are due, passes them to PAS (step 3);
- the customer comes into the post office to collect the payment (step 4) and presents a card which is used to authenticate the individual in PAS via the POCL Infrastructure (step 5/6);
- the customer encashes the required payments and a confirmation is sent back to PAS via the POCL Infrastructure (step 5/6); PAS then sends a confirmation back to CAPS (step 7).

4.3.3.4. Card reported stolen:

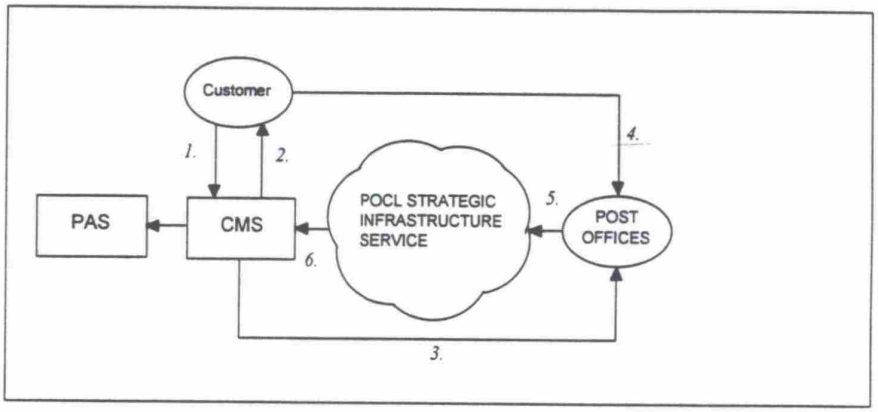


Figure 4-7 Card reported stolen

- illustrated in Figure 4-7 the customer reports that his card has been stolen (step 1) to CMS help desk (the customer can also report the theft of the card via the benefit office, but the preferred route will be direct to the CMS help desk). CMS help desk confirms with the customer (either at the time of contact or by a pick up notice) the post office from which he should collect the replacement card (step 2);
- CMS invalidates the old card (informing PAS to prevent further encashments);
- CMS sends the replacement card to the post office (step 3) which confirms its arrival via the POCL Infrastructure (step 5/6) to CMS;
- the customer collects the replacement card at the post office (step 4) and the post office informs CMS of the collection via the POCL Infrastructure (step 5/6).

POL00028135

4.3.3.5. Change of Customer's Name:

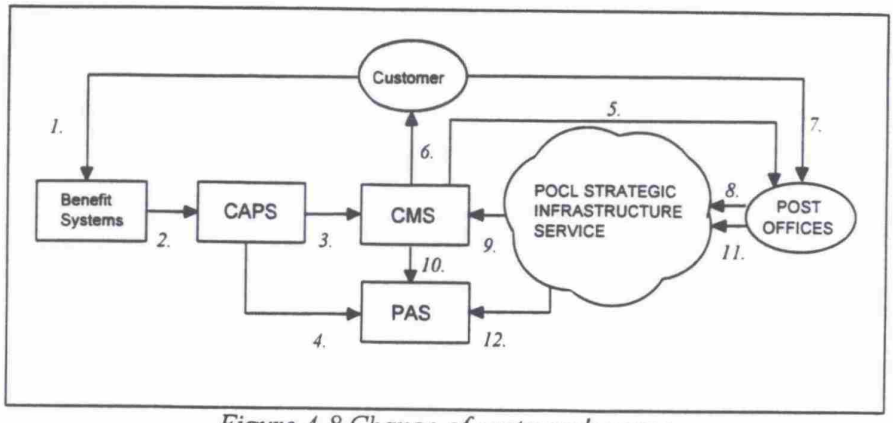


Figure 4-8 Change of customer's name

- illustrated in Figure 4-8 the customer notifies their change of name to the benefit system (step 1) which then informs CAPS (step 2);
- CAPS sends notifications to CMS and PAS notifying the customer's new name (steps 3/4);
- CMS sends a new card to the post office (step 5) which confirms its arrival (step 8/9). CMS then issues a pick up notice to the customer (step 6);
- the customer collects the new card at the post office (step 7) in exchange for her/his old card (and pick up notice) and the post office informs CMS, via the POCL Strategic Infrastructure, of the collection (step 8/9). CMS invalidates the old card at this point;
- CMS then informs PAS that the old card has been invalidated and the new one is now active (step 10). PAS now accepts, via the POCL Infrastructure, the new card in future authentication attempts (steps 11/12).

4.3.4 Scope for the Service Provider

Services <u>Included</u> within the Scope of this Procurement

<u>End-to-End Design of the Benefit Payment Service</u>

4.3.4.2. The Service Provider is required to design a total service that extends from the information links with the CAPS system to the appropriate BA customer encashing a payment at the post office. Where the Service Provider develops and operates components of this end-to-end service, they will be required to accept responsibility for those components in terms of service quality, service levels and risk.

4.3.4.3. In addition to this end-to-end design the Service Provider should show how their proposed technical components within that design — PAS, CMS and the POCL

POL00028135

Strategic Infrastructure — interact with their proposed non-technical, service related components.

4.3.4.4. The Contracting Authorities will need to be satisfied that the proposed services can contribute to the overall acceptability of the business service, and that the characteristics of the service (e.g. the authentication process) are acceptable both legally and socially. During the contract negotiation phase of the procurement such acceptability will be confirmed, and the effect of any restrictions discussed.

Payment Authorisation Service (PAS)

4.3.4.5. The Service Provider will provide the service which allows, and reports on, the encashment of specific payments by specific customers. The payment details will be provided by CAPS, and the system will provide the service through the interface to the POCL Strategic Infrastructure to enable the counter clerk to make a valid payment to a customer. The risk of authorising the encashment will be the Service Provider's. Full details of PAS are provided in 4.3.6.

Card Management Service (CMS)

4.3.4.6. The Service Provider will be responsible for the service of producing, issuing, replacing and renewing the card which will be the primary means of identifying customers of the end-to-end benefit payment system. The CAPS system will provide business led prompts for changing the state of a card (e.g. new customer, deceased customer), and there will be a series of other events the service must react to (e.g. reported loss, reported damage, card life expiry). Full details of CMS are provided in 4.3.7.

Services Excluded from the Scope of this Procurement

Benefit Systems

4.3.4.8. The Service Provider will not be required to adopt or replace the systems which already exist to adjudicate on and calculate the payment of benefits. These systems will provide payment and personal details to CAPS which will, in turn, pass the relevant information to the Service Provider's PAS and CMS.

Benefit Apportionment System (BAS), Programme Accounting General Ledger (PAGL)

4.3.4.9. The existing and proposed BAS and PAGL systems will not form part of the services falling under this procurement. The services will have no direct interfaces with PAS or CMS. All such interfacing will be handled by the CAPS service.

Customer Accounting and Payment System (CAPS)

4.3.4.10. The initial version of CAPS is currently being designed by the DSS and will be developed by the DSS Information Technology Services Agency (ITSA). Its operational capability will be provided for the Department by a third party Service Provider through ITSA's 'Focus 95' service delivery outsourcing programme.

POL00028135

Services which, <u>at the Option of the Service Provider</u>, may be Included within the Scope of this Procurement

4.3.4.12. The Service Provider is free to propose an extension of the scope of the services defined in this requirement, other than into the areas specifically excluded above. In this case the Service Provider must fully justify the benefit to the Contracting Authorities of the extension in terms of value for money and service quality, and must accept the right of the authorities to decline such extensions at their sole discretion.

4.3.5 Benefit Payment Service Features

4.3.5.1 Card

4.3.5.1.1. The card is a token with no intrinsic value, the purpose of which is to identify the holder. Further information (to be agreed with the Service Provider) will be used to verify that the person holding the card is the one identified by it (authentication) for the purpose of paying DSS benefits and other DSS purposes. If successfully authenticated, the person will then be able to collect the payments they have been authorised to receive. All payment items must be collected and taken in full.

4.3.5.1.2. When fully rolled out, cards (plus any alternative temporary token, see 4.3.7.1) will support the only Method of Payment available in post offices, with the exception of ACT payments made into National Savings or Girobank accounts - these can also be withdrawn at post offices.

4.3.5.1.3. It is currently assumed that customers will hold only one valid card at any point in time, even if the customer is acting as appointee or agent for another customer. However, the assumption may not hold and the Service Provider must provide the flexibility to allow customers to have more than one active card. Any valid card must allow the individual to collect all benefits to which they are entitled.

4.3.5.1.4. It should be noted that cards may have more than one livery (even within a single agency's customer base); for example SSA and WPA cards may be different from BA cards. It should be possible to replace or renew a card with one of a different livery. Any card held by a customer must give access to all payments due, even across agencies.

4.3.5.1.5. The Service Provider must consider the requirement to print any collateral material, which supports card issue and processing, in multiple languages including non-European languages. In particular, the Service Provider should note that it is Governmental policy to use the Welsh language where applicable — the Service Provider should note that this requirement extends across the entire BPS (and indeed all other services at post offices). Any constraints of the Service Provider's service in these areas must be identified.

4.3.5.1.6. The DSS will, in consultation with POCL, agree the design of the card with the Service Provider and any such design will ultimately require the approval of the Secretary of State for Social Security. The DSS may require, over time, design changes to the card which the Service Provider would need to support.

POL00028135

4.3.5.1.7. The details that are visible on the card can be proposed by the Service Provider but should include:

- National Insurance Number (NINO) to facilitate client identification by the DSS and to encourage wider recognition of NINO amongst DSS customers for use in their contacts with the Department;
- customer's requested name to allow differentiation of cards within the household;
- card number to support keyed entry (if the card cannot be machine read);
- expiry date.

4.3.5.1.8. Every card number should be unique. Service Providers should conform to card industry numbering standards and may use a numeric version of the customer's NINO within the card number scheme if they wish.

4.3.5.1.9. Although no constraints are placed on the technology used for the card (for example, magnetic stripes are not mandated), Service Provider's card proposals should, where possible, conform to the relevant financial industry standards. Indeed, it is thought that to maximise customer acceptance of the card it is desirable to assume the characteristics of payment methods with which the public may already be familiar.

4.3.5.1.10. Any use of the card for a purpose other than the card MOP at post offices, would require the approval of the Secretary of State for Social Security. Such approval is unlikely to be given except for:

- DSS purposes other than the payment of benefit;
- other applications at the post office counter (which of course would also need POCL approval).

4.3.5.1.11. The Service Provider should note that proposals for such additional uses are not sought as part of this procurement.

4.3.5.1.12. The Service Provider should note that the Home Secretary has announced plans to evaluate the potential uses of a UK Government smart card and that such a card could be used to collect Social Security benefits in addition to other uses. The Service Provider is required to:

- provide a defined migration path to smart card technology;
- indicate how their services could be adapted to utilise, for the purpose of benefit encashment at post offices, such a card issued by a third party.

4.3.5.2 Authentication

4.3.5.2.1. To ensure that benefit payments are encashed by the right person (and hence ensure the valueless nature of the card), it is expected that some form of authentication will be

POL00028135

required. The purpose of authentication is to ensure that the customer is who he (and the card) says he is.

4.3.5.2.2. It is for the Service Provider to propose the preferred means of authenticating card holders (including the initial and repeated collection, or "registration", of such data). To facilitate this the DSS can make available to PAS (via CAPS) the following data items from the current systems:

	Composite List Personal Details Available via CAPS:
1.	National Insurance Number of Customer
2.	National Insurance Numbers of all individuals that can act as a proxy for this customer (appointees, alternative payees, permanent agents)
3.	Address (including No Fixed Abode — NFA — and Dead Letter Office — DLO — indicators)
4.	Surname, forenames and title
5.	Requested title (full style of a customer's address where this is not catered for by the surname, forename and title fields e.g. 'The Warden of St. Annes')
6.	Date of Birth
7.	Customer Sex
8.	Date of death
9.	Nominated post office (if appropriate)

4.3.5.2.3. Beyond this list of data items, the Service Provider is at liberty to collect, via their own arrangements, additional personal data for authentication purposes. However, such additional data collection is subject to the following constraints:

- additional data items are the property of the Secretary of State for Social Security;
- Secretary of State for Social Security approval is needed for the collection of each such additional item;
- for additional items of data that are mandatory for making benefit payments by card, that the necessary powers to collect such information are conferred by the Social Security Administration Act and that such powers may not be directly transferable to the Service Provider.

4.3.5.2.4. In designing their authentication proposals, the Service Provider should consider the following:

- there is a very broad range of people that must be able to use this method of payment effectively;

POL00028135

- for the most disadvantaged, it is quite likely that this is the only method of payment open to them;
- for these groups careful consideration should be given to the appropriateness and effectiveness of Personal Identification Numbers (PINs);
- it is unlikely that certain biometrics, such as finger prints or palm geometry, which might be considered intrusive, would be acceptable forms of authentication (although photographs and behavioural biometrics such as dynamic and static signature recognition may be acceptable);
- authentication procedures (and possibly cards) that differ across client groups (e.g. pensioners / working age) may be proposed. However, such proposals must not be discriminatory on any other basis and would be subject to approval by the Secretary of State for Social Security;
- authentication procedures must not impair customer service levels; in particular it is expected that there will not be any increase in counter service time. The time taken will be an important evaluation criterion;
- it should be possible to invalidate cards and record and retain other proofs of identity or cards used in attempted fraudulent transactions without breaching confidentiality, and to retain necessary evidence.

4.3.5.2.5. Any primary or secondary research available to the Service Provider in support of their proposed forms of authentication would be of interest to the Contracting Authorities.

4.3.5.2.6. The Service Provider should be able to demonstrate that a series of successively more secure anti-fraud measures can be deployed using the proposed underlying architecture, infrastructure and interfaces without the need for significant re-engineering. Such measures could be kept in reserve and deployed as needed.

4.3.5.3 Proxy Arrangements under Cards

4.3.5.3.1. The end-to-end benefit payments system must support payments to persons other than the beneficiary in all of the following cases:

- the beneficiary has an appointee;
- the beneficiary has nominated a permanent agent;
- the beneficiary has nominated an alternative payee (for those benefits where this facility is currently or in future is made available);
- the customer has authorised a casual agent to collect payments due.

4.3.5.3.2. All proxy arrangements, except casual agents, must be approved by the DSS. The Service Provider will then be informed of such arrangements (and hence of the potential need for cards) on either a customer basis or individual payment basis.

POL00028135

4.3.5.3.3. The Service Provider should propose mechanisms that will support a *fraud-resistant* casual agent encashment facility.

Appointees

4.3.5.3.4. Where an individual is appointed to collect benefit on the customer's behalf the customer will not be able to collect the payment in their own right. This will be reflected in the authorised payment passed from CAPS to PAS (the customer's National Insurance Number will not be included in the 'allowed payee' list, see 4.3.6.2). Note that institutional appointees are usually paid via ACT.

4.3.5.3.5. Appointees act for the customer in collecting all designated benefits that the customer is entitled to. This includes any previously issued payments that have not yet been collected, as well as all future payments. The customer, for whom the appointee acts, should also be able to collect any previously issued (but uncollected) payments, although, in practice, this is unlikely to happen. The customer should not be able to collect future payments.

4.3.5.3.6. The nominated appointee will have a separate card (unless the appointee opts to have the payments made by an alternative MOP). If the nominated appointee is in receipt of benefit in their own right, or acts as agent or appointee for other customers, then the same card will be used by the appointee to encash all the payments they are authorised for (except where such payments are not issued via the card MOP). See also section 4.3.5.1. (cards).

4.3.5.3.7. It should be noted that, in addition to appointees, War Pensions have the ability to pay pension to other persons where the Secretary of State representative decides it is appropriate.

Permanent Agents

4.3.5.3.8. The customer, can under certain circumstances, nominate a permanent agent who may collect nominated benefits (not necessarily all) on their behalf. The customer can also collect these payments. Some benefits may not allow permanent agent encashment – such situations will be notified to PAS by CAPS on a payment basis.

4.3.5.3.9. The nominated permanent agent will have a separate card to the customer. If the permanent agent is in receipt of benefit in their own right, or acts as agent or appointee for other customers, then the agent's card will be used by the agent to encash all the payments they are authorised for (except where such payments are not issued via the card MOP). See also section 4.3.5.1.

Casual Agents

4.3.5.3.10. At any time and for any reason, a customer may wish to nominate any other individual to act as a casual agent for the collection of any payments that the customer is entitled to. Such a casual agent may or may not be known to the DSS, the Service Provider or the post office.

POL00028135

4.3.5.3.11. At present, for order books, the customer currently signs the front of each foil to be encashed (in the normal place) and hands over the whole book to the casual agent. As well as confirming entitlement of the customer to the benefit, the signature informs the post office that the payment may be collected by the agent, whose name is written in the appropriate place on the back of the foil.

4.3.5.3.12. The agent takes the book to the post office and collects the money. The only requirement is that the agent signs the back of each foil. He may also be asked to provide some form of identity (such as a driving licence). New procedures are being introduced for some benefits that will require casual agents to bring evidence of identity of the customer too. Apart from the name and the signature, no other information is recorded about the casual agent.

4.3.5.3.13. The process is similar for a Girocheque unless it is crossed, in which case it can only be paid into a bank account.

4.3.5.3.14. Any post office restriction that applies to the customer will also apply to the casual agent when cashing the customer's benefit payments.

4.3.5.3.15. Whilst providing a high level of customer service, this arrangement represents a significant risk to payment security and is currently a potential source of fraud. Some possible scenarios are as follows:

- the order book / Girocheque may be stolen, in which case the criminal can sign the foils and complete the casual agent details for himself. The post office does not verify the customer signature against any independent source;
- customers may give up or sell their order book / Girocheque;
- customers can be forced to confer casual agent status under duress.

4.3.5.3.16. Such problems occur because there is currently no method of confirming that the casual agent has been appointed in good faith and no independent mechanism for verifying the arrangement.

4.3.5.3.17. However, it is a requirement that customers that are unable to come to their post office should still be able to receive their benefit. It is also desirable that at least some of the wider customer service flexibility implied in the current arrangements should be available in the new service, albeit with different procedures. The Service Provider must propose how a casual agent facility would be provided and describe the balance struck between customer service and security: the Service Provider might consider that where a casual agent is able to present their own benefit payment card, which can be authenticated in the normal way, as a form of identity then the need for additional checks may be reduced.

POL00028135

Alternative Payees

4.3.5.3.18. Under certain circumstances — generally dictated by specific benefit rules — an alternative payee can be nominated for the benefit (currently for Family Credit, Disability Working Allowance and Child Benefit).

4.3.5.3.19. The purpose of the alternative payee arrangement is to continue to allow the primary customer to have the control over whether they or the alternative payee collect each payment (primarily in order to allow a mother to gain primary access to the benefit).

4.3.5.3.20. In circumstances where an alternative payee is a beneficiary in their own right and has a separate card, payments made to the primary customer should not automatically be available to be encashed by the alternative payee without prior authorisation by the primary customer.

4.3.5.3.21. The Service Provider is encouraged to propose mechanisms which achieve the same policy goal in a cost effective manner (it should be noted that the majority of alternative payees do not receive another benefit in their own right and therefore may not necessarily have a card for any other purpose).

General

4.3.5.3.22. Where a customer receives his or her benefit using the card MOP, alternative payees and permanent agents must also use the card MOP for those payments. An appointee can choose to switch to ACT.

4.3.5.3.23. The security constraints governing the issue and use of cards for appointees, permanent agents and alternative payees will be at least as stringent as those governing the use of cards by the primary customer.

4.3.5.3.24. It is assumed that if a customer has an appointee they cannot also nominate an agent (casual or permanent), or have an alternate payee.

4.3.5.3.25. It is assumed that a customer can nominate a permanent agent in addition to having an alternate payee.

4.3.5.3.26. Under any of the proxy arrangements discussed above, authentication is at least as stringent as that required for beneficiaries and is as already described. Authentication provides to the Service Provider a greater level of confidence that the person requesting encashment is who the card (or temporary token) says he is. Entitlement of that person to payments (his own and others) is indicated by the payment data and not the card.

4.3.5.4 POCL Counter Service

Introduction

4.3.5.4.1. This section describes the specific counter transactions that will be required at the post office to support the BPS. These relate to the collection of new cards and the encashment of card benefit payments. Different arrangements will need to be proposed

POL00028135

by the Service Provider for situations when a post office is unable to use PAS (for whatever reason).

4.3.5.4.2. The Service Provider should balance very carefully the need to deploy counter measures against fraud with the need to maintain high levels of customer service and safety, whilst designing to minimise total service transaction times (these times will be taken into account during evaluation).

4.3.5.4.3. The Service Provider should ensure that the Benefit Payment Service is available to all customers or potential customers, including the elderly, those with disabilities and those of no fixed abode. It should also be provided in all post offices. There should be no service differentiation between different customers or post offices.

Collection of New Card

4.3.5.4.4. Although the description below presumes that the new card will be sent to post offices, the supplied service should not preclude them being sent directly to the customer or distributed by some other channel which the Service Provider might recommend. The Service Provider will be responsible for getting the card to the customer.

4.3.5.4.5. New cards may be sent to the post office as they are issued. If so, they must be handed over to the customer upon presentation of appropriate identification (for example a card pick up notice, PUN, that has been issued by CMS). Some form of authentication may also be required as proposed by the Service Provider and agreed with the Contracting Authorities.

4.3.5.4.6. It should be noted that the Service Provider's proposed card distribution procedures should allow for the circumstance where the customer, say through illness or severe disability, is unable to visit a post office, DSS office or other office in person. If the Service Provider's proposals allow for agent collection of cards then the following might be considered:

- where an agent is able to present their own benefit payment card, which can be authenticated on-line in the normal way, as a form of identity then the need for additional checks may be reduced;

- although the card may have been collected by an agent it may be appropriate to require some special procedure when the card is used for the first time.

4.3.5.4.7. The Service Provider will need to cater for the situation where the customer arrives at the post office (assuming distribution of cards via post offices) with a valid PUN and for some reason the card is not available for collection (e.g. the card could not be read when it first arrived at the post office).

Payment Encashment

4.3.5.4.8. Customers will attend the post office to collect card payments as they do now for order book and Girocheque payments. The service should ensure that payments can only be encashed by a person who has been authorised by the DSS, their authorised agents or an

POL00028135

authorised customer. The service should also support payment to authorised customers who are unable to attend the post office.

4.3.5.4.9. Upon presentation of the card at the counter a number of stages will be required, as described below.

Customer Identification

4.3.5.4.10. To identify the customer, the reference identifier for the card will be entered onto PAS via the POCL Strategic Infrastructure (e.g. by swiping the card or by keying the card number), which will check that the card is valid (using positive validation) and indicate the recorded card holder.

Authentication

4.3.5.4.11. Having confirmed the validity of the card, an authentication stage will be required to ensure that the customer is the recorded card holder. This is likely to require the customer to provide details that correspond to those on the system (rather than the card). Collection of these details must be such that no other customer could gain access to them.

Collection of Payments

4.3.5.4.12. If authentication is successful then payment details for the customer are presented and encashment is allowed to proceed.

4.3.5.4.13. A receipt and declaration of entitlement are produced for the customer to sign. The cash is then issued and the card returned.

4.3.5.4.14. If the customer has payments for more than one beneficiary (including potentially himself) then it is expected that payments for each must be dealt with separately. Each will require a separate hand-over of cash and signing of a receipt. This facilitates the subsequent transfer of the correct money and receipt to each beneficiary, as appropriate.

Receipts

4.3.5.4.15. The dated receipt will be a multiple copy item, although single ply paper is not ruled out. Each copy will need to be sent to the appropriate destination.

4.3.5.4.16. Subject to the Service Provider's proposals, the signing of the receipt may also be part of the authentication procedure.

Temporary Tokens

4.3.5.4.17. In order to support encashment of urgent payments, the Service Provider may need to support the use of 'one-shot' temporary tokens. Such tokens should be used only once and should be invalidated and impounded at the post office after use.

POL00028135

Encashment Problems

4.3.5.4.18. Encashment problems may arise due to failure of any component of the service, including the card or the POCL infrastructure. Service Providers should indicate how payments could be made under such circumstances.

4.3.5.4.19. A number of other problems may occur at the post office counter during encashment, such as:

- attempt to use an invalid or suspended card;
- authentication failure;
- attempt to make an invalid foreign encashment;
- attempt to collect a restricted payment at a post office other than the one to which the customer or payment has been restricted.

4.3.5.4.20. These are described in more detail in sections 4.3.6.1. 'Encashment Problems'.

Related Customer Services

4.3.5.4.21. Other services, related to benefit payment, may be offered to customers at post offices.

4.3.5.4.22. Customers can currently report changes to their nominated post office at post offices. It is thought desirable that the Service Provider should offer some form of automated process to support reporting of these changes. See section 4.3.5.7 for further details.

4.3.5.4.23. It is currently envisaged that a statement of account may be provided by the DSS to benefit customers on request. This statement may indicate all payments issued to the customer since the last statement (the exact nature and format is still under consideration).

4.3.5.4.24. It is expected that the statement will be produced and distributed by the DSS although it may be desirable for a customer to request the statement while at a post office. Service Providers should note that this feature may not be required initially at 'go-live' of the service. However, provision should be made for it in the design of the service. If this feature is introduced as part of the service, it should only be possible to request a DSS statement as part of a payment collection transaction and not as a separate counter transaction.

4.3.5.4.25. Such a request would be transmitted, via the POCL Infrastructure and PAS, to CAPS.

4.3.5.4.26. A customer's eligibility for milk tokens and the number to be issued is currently stated on the order book or Girocheque. Service Providers are asked to consider how their proposed system design/service might allow for the entitlement to be flagged to the counter clerk. The Contracting Authorities will confirm their requirements at a later date.

POL00028135

4.3.5.4.27. POCL are considering the provision of a saving/budget account facility which would be available to all customers, including benefit recipients. Subject to agreement with the BA and the Service Provider, this may involve limited use of the benefit payment card.

4.3.5.5 CMS Customer Services

4.3.5.5.1. It is expected that the responsibility for dealing with the majority of reports and queries from the public about cards (along with other services provided by the Service Provider) will lie with the Service Provider. The Service Provider should propose both the form that this public interface may take (for example, a 24 hour *freephone* help line) and how they will promote its use by the card using public.

4.3.5.5.2. It is accepted that benefit staff should, subject to business process design, also be capable of dealing with such queries (although it should not be the favoured mechanism). To this end, the Service Provider should demonstrate how they can provide benefit delivery staff with secure and auditable access to CMS.

4.3.5.5.3. The Service Provider should propose ways to reduce the extent to which benefit staff have to deal directly with card related enquiries while still providing customers with a seamless, *one stop* service. Where benefit staff need to be involved in the process of handling card related enquiries, even if this involvement is limited to transferring a telephone call or letter, the Service Provider should propose ways in which they could facilitate the necessary staff training.

4.3.5.6 Financial Reconciliation

4.3.5.6.1. The required service must allow BA to reconcile fully (at an individual transaction level if desired) the statements it receives from POCL in respect of benefit payments and any associated handling fees.

4.3.5.6.2. Every payment made (also stopped payments and expired payments) will be confirmed on CAPS with a message sent from PAS. Therefore, the BA will have an accurate record of its benefit expenditure.

4.3.5.6.3. The service design should minimise the potential for disputes to arise between the Contracting Authorities and the Service Provider regarding responsibility for errant transactions.

4.3.5.7 Nominated Post Offices

4.3.5.7.1. When a customer elects to receive benefit payments at the post office, he currently selects the post office at which he will normally encash his payments. This is termed the 'nominated' post office and encashments at any other post office are called 'foreign' encashments ("temporary change of post office" - "holiday" - encashments). The assignment of a nominated post office has various advantages. These include support for encashment restrictions (the customer is currently limited to two foreign encashments in any one order book); the monitoring of potentially fraudulent benefit encashment; the

POL00028135

management of cash provision; and the links which POCL's agents develop with local customers.

4.3.5.7.2. Certain payments made by girocheque do not require a post office to be nominated. Customers may encash such payments at any post office without restriction

4.3.5.7.3. Service Providers are encouraged to suggest alternatives to the present nominated post office procedures detailing the implications operationally and for the customers.

Changes to "Nominated" Post Offices

4.3.5.7.4. Whilst in receipt of benefit payments the customer may currently change their nominated post office using a special procedure. This procedure involves completing a form (P80MA) at either the post office or the benefit office. The BA can then either accept the change (entering details separately into the benefit systems) or, in unusual circumstances, the change may be refused.

4.3.5.7.5. If nominated post offices continue the current procedure could remain. However, the Service Provider is encouraged to propose an alternative mechanism; preferably one that captures the change of nominated post office in the post office and reports the change (via the POCL Strategic Infrastructure) to CAPS, and one that does not involve clerical intervention by BA staff other than by exception. Such a mechanism must not allow changes of nominated post office where the customer is currently restricted to their nominated post office (this can only be lifted under control of benefit staff).

4.3.5.8 Customer Education and Marketing

4.3.5.8.1. Order books, the most widely used current method of payment, have been in use in the UK for over 40 years and are familiar to over 20 million people. The problems in changing to a new method of payment are therefore very significant. The Service Provider will be required to submit detailed proposals as to how they can achieve the education programme, implied through *welcome packs*, other collateral and other media, and how they will monitor its effectiveness.

4.3.5.8.2. In any case, card customers should be encouraged to value the card; i.e. they should store it safely even during periods between benefit claims (note that certain client groups drop into and out of benefit on a cyclical basis).

4.3.5.8.3. Although market research into the potential use of cards to pay Social Security benefits shows that the majority of benefit customers would be in favour, concern over the use of this MOP has been expressed by some special interest groups, including those representing the elderly and the disabled. The Service Provider should therefore propose ways in which the new method of payment can be designed and marketed in order to allay any public concerns. These proposals should be illustrated with any Service Provider specific experience in related payments projects. All or part of this marketing and customer education effort may be contracted for from the Service Provider.

POL00028135

4.3.5.9 Functional Qualities

Reliability

4.3.5.9.1. In common with all system interfaces dealing with financial authorisation and associated personal identification and authentication, those between CAPS and PAS / CMS must be reliable in terms of both assuring secure data transmission and maintaining the integrity of that data. This reliability is particularly important in the context of benefit payments since the customer base includes some of the most vulnerable in society who rely heavily on the accurate and timely availability of their payments.

Auditability

4.3.5.9.2. All data transmission across the DSS / Service Provider boundary, and any related actions taken by the Service Provider, must be fully auditable both to enable resolution of any disputes that may arise and to support external scrutiny. In particular, the Service Provider should note that, in addition to tracking the movement of cards and receipts, payment transaction details and any collateral forms (such as may be required to support casual agent encashment) will also need to be tracked and stored for audit purposes and possibly for use as evidence in court in fraud cases.

4.3.5.9.3. The Service Provider's design should allow for non-availability of infrastructure services to the post office such as mains electricity and communications networks (including the Public Switched Telephone Network).

Data Sensitivity

4.3.5.9.4. Certain cases (such as those for VIPs) are maintained as 'nationally sensitive' within the DSS. Access to any details on such cases is limited and, in some cases, to very small numbers of DSS staff. In addition, cases which relate to 'locally sensitive' individuals (for example, local councillors or relatives of benefit delivery staff) are also marked and access limited in the corresponding locations. The Service Provider will need to demonstrate the ability to place similar access restrictions on the data supplied to them.

4.3.5.9.5. More generally the Service Provider must describe how they intend to provide security control across their proposed services including (and for example):

- physical storage and transmission of data;
- physical access to hardware infrastructure;
- authentication of users;
- data and function access control;
- auditing accesses and changes to the data.

POL00028135

Configuration Management

4.3.5.9.6. It is anticipated that the Benefit Payment Service will give rise to a number of specific configuration management issues in addition to the general requirements covered in Chapter 5, such as:

- the management of distributed cryptographic keys for card or user authentication;
- synchronisation of time based events (such as payment stop request and response) across physically discrete systems, so that sequencing of transactions between systems can be guaranteed and overall data integrity maintained.

4.3.5.9.7. The Service Provider must indicate how such issues will be addressed, both within the procured service and across the BPS as a whole. Solutions must take into account required business processes as well as any proposed system components.

Scalability

4.3.5.9.8. The DSS, in common with other governmental and private sector bodies, is subject to frequent and sometimes rapid changes in its core business. The Service Provider should anticipate a degree of volatility and, to support such changes, should be able to demonstrate scalability of their solution to cope with wide-ranging benefit changes such as the introduction of new benefits and withdrawal of current ones.

4.3.6 Payment Authorisation Service

4.3.6.1 Functional Properties

General

4.3.6.1.1. CAPS will receive card payments both for benefits which are currently computerised and those which are paid currently via a clerical process. It will forward them to PAS which will be responsible for managing the payment process from that point. Such payments may include both cash entitlement and various tokens. They will only be valid from a due date for a defined period after which time the payment expires. Although milk tokens (of two types — one for ordinary milk and the other for dried) are the only form of token in use at present, the service should provide the flexibility to deal with multiple token types if needed.

4.3.6.1.2. To support PAS in controlling payments, CAPS could supply PAS with a range of personal details consisting of the client's name together with any authentication data that has been agreed.

4.3.6.1.3. Payment details must not be alterable by any unauthorised body during their passage through the end-to-end benefit payment service.

POL00028135

Urgent Payments

4.3.6.1.4. Normally payments will be passed to PAS before their due date. However, support must be provided for urgent issue of payments for encashment at a post office (nominated or otherwise). It is anticipated that a likely target time for making an urgent payment available for collection in the post office is 30 minutes from its award by the benefit system. Depending on the circumstances, such transactions may necessitate the use of temporary tokens and authentication procedures.

4.3.6.1.5. Urgent payments are likely to have a short period of validity, as specified on the payment data sent from CAPS to PAS.

Foreign ('Holiday') Encashments

4.3.6.1.6. It is envisaged that if 'nominated post office' remains, the restrictions, which currently apply to order book encashments at 'foreign post offices' (i.e. post offices other than the nominated post office), will continue to apply for card payments. Encashments at a foreign post office will only be allowed for a specified number of times within a specified period (currently 2 weeks within a 20 week period). The DSS will retain the flexibility to change these two parameters. In some circumstances, foreign encashments may not be allowed at all (see Restricted Encashment below). In other cases foreign encashments may be unlimited.

4.3.6.1.7. The card method of payment may, dependent upon the Service Provider's proposals, be the subject of a phased roll-out. During any such period, the Service Provider would need to propose ways in which foreign encashments can still be made, using the card, at post offices which are not equipped with the POCL Strategic Infrastructure. It is anticipated that the solution to this problem could also be used, even after roll-out, to continue to pay via card where the equipment in the post office is faulty, unavailable or unable to connect to the POCL Strategic Infrastructure.

Restricted Encashment

4.3.6.1.8. PAS must allow encashments to be restricted to a specific post office for either a specific customer or a specific payment. If the restriction is placed on the customer then the restriction applies to all payments they have entitlement to. Where this customer has a proxy (appointee, agent or alternative payee) then the restriction also applies to the proxy in respect of payments collected for the restricted customer. Restrictions for a specific payment would apply to that payment only (irrespective of the customer collecting it).

Authorisation

4.3.6.1.9. Authorisation for card-based payments is the transmission of the payment by CAPS into PAS. Payments will be authorised in sufficient time for PAS to make the payment available (but not earlier so as to minimise the number of revisions across the CAPS / PAS boundary). The payment data will include the allowed payees together with any post office restriction applicable.

POL00028135

Expiry

4.3.6.1.10. All authorised payments will have an associated expiry date which is the last day upon which they can be encashed in the post office. Payments which have passed their expiry date must be made void in PAS and a confirmation returned to CAPS.

4.3.6.1.11. The payment expiry date may vary with benefit or transaction type. It is passed to PAS with the payment data.

4.3.6.1.12. Currently, order book foils have 3 month validity and Girocheques 1 month: a recent sample of order book foil encashments showed that the vast majority were encashed within the first week. Service Providers are invited to give their views on the benefits or costs of reducing the validity period of all payments to 4 or 5 weeks.

Stopped Payments

4.3.6.1.13. It must be possible to stop previously authorised payments which (as far as CAPS is aware) have not yet expired, been encashed or stopped. The response from PAS, indicating success or failure, must be returned to CAPS immediately. Failure implies that the payment has already been encashed and therefore could not be stopped. In the case of failure, it is desirable that PAS returns the relevant encashment details to CAPS immediately instead of waiting for the encashment confirmation to return via the normal path (see 4.3.6.2. 'Stopped Payments').

Customer Identification

4.3.6.1.14. PAS must provide the facility for the post office clerk to check the validity of a card presented for payment encashment and (if valid) to identify the customer presenting the card.

Authentication

4.3.6.1.15. Having established that the card is valid, PAS will need to support whatever authentication process is specified by the Service Provider.

Collection of Payments

4.3.6.1.16. Having successfully authenticated a customer, PAS must allow collection all payments the customer is entitled to collect (both as a customer in his own right and, where authorised to do so, on other people's behalf). PAS must enforce the following restrictions in respect of collection of payments:

- each payment can only be encashed once and only for the amount authorised by the DSS;
- payments of a given type (i.e. relating to a specific payment *string* from the benefit system) must be encashed in date sequence. CAPS will provide PAS with the relevant sequence information;

POL00028135

- partial encashment of an individual payment will not be allowed.

4.3.6.1.17. PAS will, via the POCL Strategic Infrastructure, present all payments available for collection to the post office counter clerk who may communicate this information to the customer. For reasons of confidentiality this information should not be disclosed (either visibly or so that it can be overheard) to any other customer except the one involved in the transaction.

4.3.6.1.18. Where a payee is collecting benefits for more than one customer, it is anticipated that they encash payments for each separately. PAS will therefore allow selection of the beneficiary for whom the payee wants to collect benefits first; this transaction continues until completion (including printing and signing of the receipt). PAS must then allow the payee to select the next beneficiary for whom they want to collect, then continue the encashment process for that beneficiary. PAS will repeat the encashment procedure until the list of available customers is exhausted. For example, if a payee collects benefit for three benefit customers then three receipts will be printed. Note that the customer should only be required to complete the authentication procedure once at the beginning of the whole process.

4.3.6.1.19. PAS should provide the facility to display, at the time of encashment, specific messages to the clerk, relating to the collection of a specific payment, which the clerk may then act upon. These messages will be supplied to PAS via CAPS.

Receipts

4.3.6.1.20. PAS must support the production of receipts with the following attributes:

- audit information for the transaction (e.g. transaction ID, when and where the transaction has taken place, post office clerk identifier);
- optional messages intended for the recipient, under instructions received from CAPS (subject to the physical constraints of the receipt);
- one or more legal declarations that the payee acknowledges entitlement to and receipt of the payment, each of which is signed by the payee;
- a description of each of the payments encashed;
- total amount encashed;
- predicted date and amount of the next payment (of the same type) for each payment type.

4.3.6.1.21. When the new service starts, the current working assumption is that the top copy of the signed receipt is initially retained by the post office clerk and is eventually stored at the DSS facility at Lisahally in Northern Ireland (the exact arrangements for handling receipts is a matter to be agreed between POCL and BA). The Service Provider should suggest how best receipts might be handled to permit the rapid location, recovery and

POL00028135

provision of an original receipt whilst overall providing a lower cost process compared with present arrangements.

4.3.6.1.22. The Service Provider should note that they will be required to provide Police and Criminal Evidence Act certification that their services were working normally at the time of any alleged offence.

4.3.6.1.23. A copy of the receipt will be retained by the customer.

4.3.6.1.24. The Service Provider should state any restrictions that their solution imposes with respect to receipts (such as languages/character sets supported, number and length of messages, etc.).

Encashment Confirmation

4.3.6.1.25. Having completed the encashment procedure and confirmed it to PAS via POCL Strategic Infrastructure, PAS should report details of the encashment to CAPS. One encashment confirmation is required for each receipt signed (and, hence, for each quantity of cash given out). The encashment confirmation should include details of location, time, amounts and to which payments the encashment relates.

Encashment Problems

4.3.6.1.26. In order to maintain high levels of customer service, the Service Provider's proposals should minimise the frequency of card read failure. However, where the card fails to read at the post office, it must be possible to proceed with the encashment although this may involve, subject to Service Provider's detailed proposals, additional customer identity verification. The reference number shown on the card may need to be keyed in to allow PAS to access the authentication details associated with the card holder. In their proposals, the Service Provider should state how incorrect keying of card numbers will be detected — for example using check digits within the card number. The Service Provider's proposals are invited regarding the extent to which card replacement should be automatic upon read failure.

4.3.6.1.27. The Service Provider must consider and describe how his proposed solution will provide measures both to prevent and to detect fraud, but due regard should be given to the customer service requirements discussed in this document. Furthermore, the proposed system should be designed to minimise *false negatives*; i.e. the possibility of a legitimate card holder failing an authentication check.

4.3.6.1.28. An attempt to use a card which is not valid will be recognised by PAS and indicated to the post office counter clerk. The clerk should be prompted to impound the card and inform the customer that it is no longer valid.

4.3.6.1.29. If a suspended card is presented, the post office clerk will be informed by PAS and a message displayed advising the customer to contact his benefit office. The card should be returned to the customer. Card suspension is explained in more detail in section 4.3.7.1.

POL00028135

4.3.6.1.30. The Service Provider may consider ways in which card payments made under duress could be flagged in PAS and, potentially, in the encashment confirmation sent back to CAPS.

4.3.6.1.31. Where the card payee fails the authentication check defined by the Service Provider it is desirable that the post office retains the card (which should now have been invalidated by the authentication failure) for potential examination by POCL or BA security staff. Again, the Service Provider's proposals regarding the handling of these items are invited.

4.3.6.1.32. If the customer attempts to use the card when he is restricted to a specific post office, and the post office in which he presents is not the one to which he is restricted, the post office clerk will have an appropriate message displayed which informs him of the restriction. The message will not include the name of the restricted post office — if the customer is uncertain he will be referred to the BA.

Encashment Monitoring

4.3.6.1.33. The service should be able to record, summarise and report details of all transactions made, in particular providing the following information:

- amounts paid;
- methods of payment;
- due dates;
- encashment dates;
- benefit type;
- payments to agents;
- payments to appointees;
- number of items impounded.

4.3.6.1.34. Encashments will also need to be monitored to detect suspicious conditions. It is desirable that such conditions do not always have to be pre-programmed into the monitoring system; i.e. the monitoring system should be capable of *learning* what exceptional encashment patterns look like using some form of artificial intelligence. For illustration, the following indicators of potential fraud could be detected and reported via PAS to authorised BA and POCL staff:

- multiple encashments on the same day;
- repeated keyed access;
- delays in collecting payments (for some benefits);

POL00028135

- repeated use of casual agents (more than twice a month, say);
- repeated use of temporary tokens;
- repeated foreign encashments.

4.3.6.1.35. In addition, it is desirable to be able to monitor usage of both all cards ever issued to a specific customer and a specific card for detection and prevention of abuses to the benefit system.

Payment Enquiries

4.3.6.1.36. The ability to support benefit payment enquiries on CAPS is one of the main business drivers behind this programme. Access will be required for all DSS benefit processing staff, particularly in response to customer queries. It will be possible to show the existence and status of all card-based payments passed to CAPS from the benefit systems (both automated and clerical). Payment status will be one of the following:

- part of payment *string* received from benefit system and awaiting authorisation;
- payment authorised (passed to PAS) and awaiting collection;
- payment encashed;
- payment stopped;
- payment expired (past expiry date without collection).

4.3.6.1.37. To support these facilities, PAS will report encashments, expiries and stop status back to CAPS as previously described. However, the ability for CAPS to determine up to date payment status on PAS for a particular payment will be required. Therefore, PAS will need to respond immediately to CAPS requests for encashment status on particular payments responding with either the relevant encashment data or with an indicator that the payment has not yet been encashed.

Payment Monitoring

4.3.6.1.38. End-to-end service monitoring to DSS customers is required in addition to any that may be required to support contractual monitoring between the POCL, DSS, and the Service Provider. Possible metrics include:

- payments not available for collection on due date;
- urgent payments not available for collection within specified time (e.g. 30 minutes).

POL00028135

4.3.6.2 CAPS to PAS Interface

4.3.6.2.1. This section describes the specific transactions required between CAPS and PAS, in terms of data content and service levels. Service levels are described in terms of the time constraints of each transaction. The Service Provider should regard these as guidelines only and should, themselves, consider what will be necessary in the light of the requirements defined elsewhere in this SSR.

4.3.6.2.2. In general, all specified transaction data required from PAS and detailed below should be available for use by the DSS at the start of the working day following the transaction.

Payment

4.3.6.2.3. The data required for this transaction is as follows:

	For each authorised payment:
1.	Payment Reference identifier
2.	Prior Payment Reference ID (required to support encashment in sequence)
3.	Beneficiary NINO
4.	Payee List (NINO, Payee Role, Declaration Type, Message to the payee)
5.	Originating benefit office
6.	Payment Description Code (expands to description of each payment for recognition by the customer in the PO – printed on the receipt)
7.	Net Amount to be paid
8.	Token List (Token Type, Number of Tokens)
9.	Due date for payment
10.	Payment Expiry date
11	Nominated post office (if appropriate)
12.	Restricted post office indicator
13.	Optional instruction code to the clerk
14.	Next Payment Due Date (if available)
15.	Next Payment Predicted Amount (if available)

4.3.6.2.4. The Token List identifies one or more token payments required (such as milk tokens).

POL00028135

4.3.6.2.5. The Payee List is a list of allowed payees for this payment. This will consist of one or more of the following:

- beneficiary;
- appointee;
- permanent agent;
- alternative payee.

4.3.6.2.6. The declaration to be printed on the receipt (along with any optional message) will vary with payee and will be specified for each (see section 4.3.6.1 'receipts').

4.3.6.2.7. Note that the data content is the same for urgent and non-urgent payments.

Service Level

4.3.6.2.8. Each payment passed to PAS will have a due date from which the payment must be available for collection.

4.3.6.2.9. It is expected that payments will normally be passed from CAPS into PAS just before they are due for collection by the customer. Typically, the lead time might be 48 hours although instructions to pay may arrive later (for example, during the night for the start of the next day). More notice could be provided for most payments although the number of payment stops experienced in the system would be likely to increase as a result.

4.3.6.2.10. Urgent payments will be subject to a very short lead time (of the order of 30 minutes from transmission by the benefit system). Such payments must be available for collection within this time.

Stopped Payments

4.3.6.2.11. BA staff may wish to stop payments that have already been passed to PAS for a variety of reasons such as change of circumstances or suspected fraud. In such cases, CAPS will send a stop request to PAS, containing the following data:

	For each stop request:
1.	Beneficiary NINO
2.	Payment Reference identifier of payment to be stopped

POL00028135

4.3.6.2.12. The response from PAS, indicating success or failure should be returned to CAPS immediately. It will contain the following data:

	For each stop confirmation:
1.	Beneficiary NINO
2.	Payment Reference identifier of payment to be stopped
3.	Amount (for audit/reconciliation)
4.	Stop Result (Success/Failure)

4.3.6.2.13. In the case of failure, it is desirable that PAS will also return immediately to CAPS the relevant encashment details instead of waiting for the encashment confirmation to return via the normal path.

Service Level

4.3.6.2.14. Stops must be effected immediately. The request may be part of an on-line dialogue and so the response must also be returned immediately.

Expiries

4.3.6.2.15. Confirmation of each payment that expires must be sent back to CAPS as a positive confirmation (even though the expiry can, of course, be inferred from the expiry date). The expiry confirmation will contain the following data:

	For each expiry:
1.	Beneficiary NINO
2.	Payment Reference identifier of authorised payment
3.	Amount (for audit/reconciliation)
4.	Expiry date

Service Level

4.3.6.2.16. Payments will expire when the last post office closes on the date of expiry. PAS must confirm this (and therefore that the payment has been made void) to CAPS before any enquiries are made on this payment (probably before 9 am the next business day).

POL00028135

Encashments

4.3.6.2.17. A confirmation of the encashment must be automatically sent back to CAPS. The data contained within the confirmation will include:

	For each encashment:
1.	post office ID.
2.	post office clerk ID.
3.	Total amount encashed
4.	Token List (Token Type, Number of Tokens taken)
5.	Encashment date and time
6.	Payee National Insurance Number (including casual agent National Insurance Number, if obtained)
7.	Casual Agent Flag (set if encashment made by casual agent)
8.	Keyed flag (implies that the card could not be machine read)
9.	List of payments encashed (payment reference, Beneficiary NINO)

4.3.6.2.18. If the Service Provider's Casual Agent procedures include the production of some form of non-card identification, the form of identification used may also need to be recorded in the encashment transaction.

Service Level

4.3.6.2.19. When a stop is issued it is important (as part of the stop processing) to determine an accurate, up-to-the-minute encashment status for any payment and to make this available to CAPS at the same time. For normal purposes, it is desirable that the encashment confirmations from PAS to CAPS are passed continuously, but asynchronously, to reduce the need to access PAS to answer routine payment enquiries. In designing this component of their solution, the Service Provider should ensure that no particular hours of working are enforced. In particular, the solution should allow the flexibility for varying the length of the business day.

POL00028135

Personal Details

4.3.6.2.20. CAPS will inform PAS of personal details required to make payments. This will consist of the following:

	For each customer:
1.	NINO
2.	Requested Name
3.	Nominated post office (if appropriate)
4.	Restricted post office indicator
5.	Monitor usage flag (indicates that PAS should tell CAPS when any card held by this customer is used)
6	National Sensitivity indicator

4.3.6.2.21. CAPS will pass this data initially and whenever it changes. CAPS will also indicate when the details no longer need to be held:

	For each notification:
1.	National Insurance Number

4.3.6.2.22. Additional data items to support authentication may also be supplied by CAPS.

4.3.6.2.23. Any personal details required to support authentication, or for other purposes, must be specified by the Service Provider in their proposal and agreed with the BA. Information regarding proxies may also be supplied via this route.

Service Level

4.3.6.2.24. Any new or changed personal details must take effect within PAS in time for them to be taken into account in any subsequent encashment or enquiry.

Encashment Problems

4.3.6.2.25. A number of encashment problems will require PAS / CAPS interaction, as described below (this list should not be considered exhaustive).

4.3.6.2.26. The Service Provider may consider ways in which card payments made while the post office counter clerk was under duress could be flagged in PAS and potentially in the encashment confirmation sent back to CAPS, for which an extra flag may be provided, as follows:

	For each encashment:
10.	Duress flag

POL00028135

4.3.6.2.27. When these transactions are alerted by PAS they may need to trigger additional action by POCL.

4.3.6.2.28. The Service Provider should also provide the facility to trigger an alarm in PAS system when a specified card is used (this feature would be used for security monitoring). If this is passed back to CAPS the following transaction will be required:

	For each use of the specified card:
1.	Card holder's NINO
2.	post office ID
3.	post office clerk ID
4.	Date and time

4.3.6.2.29. The need to monitor a specified card would be indicated by a flag on the personal details data sent from CAPS to PAS.

4.3.6.2.30. PAS will also need to inform CAPS if an encashment is attempted which would infringe a post office restriction, passing the following data:

	For each attempted 'restricted PO' infringement:
1.	Customer NINO
2.	Restricted post office ID
3.	Actual post office ID
4.	post office clerk ID
5.	Date and time

Service Level

4.3.6.2.31. Each encashment problem must be notified to CAPS as soon as possible (probably within 1 hour of the encashment).

Payment Enquiries

4.3.6.2.32. The data flows from CAPS to PAS will consist of:

	For each payment enquiry:
1.	Beneficiary NINO
2.	Payment Reference identifier

POL00028135

4.3.6.2.33. The response from PAS to CAPS will consist of:

	For each payment enquiry:
1.	Beneficiary NINO
2.	Payment Reference identifier
3.	Payment Status (unencashed / encashed)

4.3.6.2.34. In the case of the payment already having been encashed, it is desirable that PAS will also return immediately to CAPS the relevant encashment details instead of waiting for the encashment confirmation to return via the normal path.

Service Level

4.3.6.2.35. Such enquiries are likely to form part of an on-line dialogue. Consequently, the response should be provided immediately.

Change of Nominated Post Office (Requested at Post Office)

4.3.6.2.36. This would require the following information to be passed from PAS back to CAPS:

	For each change of Nominated post office:
1.	Customer NINO
2.	Former Nominated post office
3.	New Nominated post office
4.	New Address details (if appropriate)

Service Level

4.3.6.2.37. If required, changes to nominated post office should be reported back to CAPS in sufficient time to allow the DSS to accept the change before the customers next payment is due. Therefore return within a working day is likely to be acceptable.

Request for Customer Statement (at Post Office)

4.3.6.2.38. If this feature is utilised it will require the following information to be passed from PAS back to CAPS:

	For each Customer Statement Request:
1.	Customer NINO

POL00028135

Service Level

4.3.6.2.39. To maintain high levels of customer service, the DSS would wish to post the customer's statement of account by the start of the working day after its request. Therefore such transactions should be passed to CAPS on the same working day as they are generated.

4.3.6.3 POCL Strategic Infrastructure to PAS Interface

4.3.6.3.1. The Service Provider should maintain a logical separation between the POCL Strategic Infrastructure and PAS and define a detailed interface specification to support this. The exact flows across this boundary will vary to some extent depending on the Service Provider's proposals but would need to support such areas as:

- customer identification (via token);
- customer authentication;
- payment availability;
- encashment;
- invalid card use;
- card alerts;
- encashment exceptions;
- temporary token use;
- changes to nominated post office (if appropriate);
- enquiries regarding next payment(s);
- requests for DSS Statement of Account.

4.3.7 Card Management Services – CMS

4.3.7.1 Functional Requirements

General

4.3.7.1.1. The card services provided by the Service Provider should span the whole range from card production and issue through to resolving DSS card related customer queries. The following sections enumerate the core set of such functions.

4.3.7.1.2. The Service Provider should note the requirement that the primary point of customer service for card related services is within their domain but, additionally, benefit delivery

POL00028135

and post office counter staff must be able to deliver a high level of service in response to any reports and enquiries directed at them.

4.3.7.1.3. The Service Provider should also consider the needs of the elderly and disabled customer groups in their proposals. For example, it may be that alternative card issue and authentication procedures are desirable for these groups. However, in this and any other aspects of the service, any differential procedures must not be discriminatory on other grounds and must be subject to the approval of the Secretary of State for Social Security.

4.3.7.1.4. The production, storage, delivery and destruction of cards should be both secure and auditable. The Service Provider should, at any time, be able to produce an audit trail of all cards and associated collateral documents.

New Card Issue

4.3.7.1.5. CMS will issue a card to a customer when:

- the customer is entitled to collect a card-based payment but has no current card;
- a specific request is made to issue a card to the customer.

4.3.7.1.6. The service should issue cards, to customers or proxies authorised by the DSS, with minimal delay (and with due regard to cost constraints and the need for personal authentication measures) when instructed to do so by the DSS.

4.3.7.1.7. CAPS will deliver the initial set of customer details to CMS to enable card issue; CAPS will also inform CMS of any revisions to personal details that may affect later card issues.

Card Replacement

4.3.7.1.8. CMS will need to replace cards for customers who report their existing card:

- lost;
- stolen;
- damaged.

4.3.7.1.9. In all the above cases, the previous card should be invalidated automatically and immediately.

POL00028135

Card Renewal

4.3.7.1.10. CMS will renew a card when either:

- the card has been in use for a pre-determined period of time and should be replaced (for wear and tear reasons, for fraud reduction reasons, or to make the normal lapsing of card simple); or
- the customer changes any detail in use on the card (e.g. name).

4.3.7.1.11. In both cases a new card will be issued automatically by CMS. Such renewal must occur if card payments are still being made to the customer in question (it is possible that customers no longer in receipt of card-based benefit payments will not have their cards renewed). The service should accept a notification from the DSS when a customer no longer requires a card and send no further cards to that customer.

4.3.7.1.12. When a card is renewed in this way, CMS will invalidate the previous card either when it expires or when the new one is collected (whichever occurs first).

4.3.7.1.13. To negate the need for unnecessary card issues, the service should be capable of updating any chosen security verification details or procedures without affecting the customer's ability to collect authorised payments.

4.3.7.1.14. The Service Provider's proposals on the normal handling and frequency of card renewal, based on best industry practice, are invited.

Card Supply and Collection

4.3.7.1.15. When a payee needs a card for the first time CAPS will send a notification to CMS along with the necessary personal details (CAPS also informs CMS of any subsequent changes to these details). This notification implies the customer has an immediate need for a card. CMS will send a new card to the customer. The method of distribution — and the risk therein — is a matter for the Service Provider. However, the network of post offices is available for this purpose; the Service Provider should consider sending the card to the customer's nominated post office and the 'pick up notice' (PUN) to his correspondence address when the card is available. The card would be collected by the customer at the post office in return for the PUN. Other delivery mechanisms proposed by the Service Provider will be considered on their merits although it is desirable that benefit offices are not normally used in the card supply process.

4.3.7.1.16. Where the customer has no fixed abode for correspondence purposes, the current arrangement for distributing order books is to send them to either the post office or the DSS office where they are collected by the customer. While it may be possible to use the DSS office or the post office for distributing cards and their collateral material, the Service Provider is encouraged to propose an alternative solution that achieves the same level of customer service without exposing a security risk. The Service Provider should make clear in their proposals how the risk of internal fraud is countered, be it DSS, POCL, Service Provider or sub-contractor.

POL00028135

4.3.7.1.17. Note that the card distribution procedures can also be triggered by CMS (rather than via CAPS) for normal card renewal cycles, lost/stolen reports or damaged cards.

4.3.7.1.18. In general, CMS must be able to track the life history of each card in order to both validate changes in its state and to trap events which may be invalid or exceptional for a card given its state at any point in time. Therefore, as the card is issued this change in state must be recorded by CMS.

4.3.7.1.19. Upon receipt of the card at the post office (assuming distribution of cards via post offices, discussed above) it may be desirable to read the card through the reader. This will prove that the card can be read and will inform CMS, via the POCL Strategic Infrastructure, that it has been received (so that CMS can maintain the card life history).

4.3.7.1.20. Again assuming card distribution via post offices, the post office will hold cards for collection by customers for a specified period of time. Upon presentation of the PUN (and any required authentication of the individual) the post office will hand over the card to the customer in return for the PUN and inform CMS accordingly. The Service Provider should give thought to ensuring that the PUN is forgery resistant and is in some way uniquely coupled — possibly by printing the unique card ID on the PUN — to the card to which it relates.

4.3.7.1.21. At this point, the card is considered valid for use (i.e. 'activated').

4.3.7.1.22. CMS will identify any cards that are not collected from the post office within a time specified by the Service Provider. CMS will inform the post office holding the card, via the POCL Strategic Infrastructure, and the post office should then destroy it in a way specified by the Service Provider and agreed with the Contracting Authorities. CMS will invalidate this card and will retain a record of the event for BA and POCL audit and fraud investigation purposes.

Invalidation and Suspension

4.3.7.1.23. Invalidation of a card permanently prevents it being used for encashment of any payment at any post office; suspension is under the control of BA staff and temporarily prevents a card being used for encashment.

4.3.7.1.24. Two different categories of invalid card are possible:

- cards which are known to CMS but that have been explicitly invalidated;
- cards which are not known to CMS (such as counterfeit cards).

4.3.7.1.25. The Service Provider should, as part of their proposed exception handling processes, define ways in which the two categories should be treated.

POL00028135

4.3.7.1.26. In general, CMS will invalidate a known card when it expires and whenever an event occurs against it which is regarded as exceptional. Specific examples of this are:

- when CMS is informed of an irregular card movement (e.g. card issued by CMS but not received by the nominated post office within a specified time limit);
- when a card has not been collected by the customer from the nominated post office within a specified time period (any previously valid cards must also be invalidated);
- by direct user action (when reported lost/stolen/damaged, on recovery of card, on suspicion of fraudulent use).

4.3.7.1.27. Furthermore, it may be desirable to allow a card to be suspended on CMS, under control of benefit staff. This would bar payments being made with that card until the suspension was lifted. When such a card is presented in the post office a message would be displayed for the clerk asking them to direct the customer to a local benefit office.

4.3.7.1.28. Notification of invalidation, suspension and lifting of suspension of cards must be made available from CMS to PAS as soon as they are received by CMS.

4.3.7.1.29. If an invalid card is presented for encashment, the post office will retain the card.

4.3.7.1.30. If a suspended card is presented, the post office clerk will be informed by their system and a message displayed directing the customer enquiry to benefit offices.

4.3.7.1.31. The Service Provider needs to cater for the situation where the customer arrives at the post office (assuming distribution of cards via post offices) with a valid PUN and for some reason the card is not available for collection (e.g. the card could not be read when it first arrived at the post office).

Temporary Tokens

4.3.7.1.32. Some benefit payments need to be made very quickly, for example in the case of crisis loans. Where the customer already has a card it must be possible to route the payment authorisation through CAPS and PAS within a specified time limit allowing encashment via the normal process. However, if the customer does not have a card, it will be necessary to issue some form of temporary token which can be used to unlock the payment in the post office. It is anticipated that this form of temporary token can only be used for a single encashment and will be retained by the post office. It is for the Service Provider to define mechanisms for the control of all tokens and documentation relating to the Benefit Payment Service and, hence, they are invited to make specific proposals relating to 'one-shot' temporary tokens (including format, production, distribution, use and retention). However, one solution could be for CMS to supply a unique number to the local office printed on a paper notice. Upon presentation in the post office, the number would be keyed into the counter system to initiate any required authentication and hence unlock any payments.

POL00028135

4.3.7.1.33. The Service Provider should propose the kind of authentication procedures which would be appropriate in this circumstance. They should also ensure that whatever mechanisms are put in place are 'fraud resistant', for example, that the tokens should not be easily forged.

4.3.7.1.34. Where such urgent payments need to be made outside normal post office hours, BA currently has the facility to pay directly in cash. If there is an opportunity to avoid making such direct 'out of hours' payments this should be proposed by the Service Provider.

4.3.7.1.35. In addition to the 'one shot' temporary token it may be necessary for the Service Provider to make exceptional arrangements to supply cards that are required more quickly than their normal delivery cycle. This may happen in circumstances such as replacement of lost / stolen cards.

4.3.7.1.36. The service should treat a temporary token in the same way as a permanent card – that is, as a means of identifying the customer prior to any authentication checks.

4.3.7.1.37. Issue of a temporary token (that is not of the 'one-shot' variety) should automatically trigger the issue of a permanent token to replace it when it expires, assuming it has different physical attributes from a permanent token (this will be subject to the Service Provider's proposals).

4.3.7.1.38. In general, the service should minimise the use of temporary tokens.

Card Return

4.3.7.1.39. Any card returned (at post offices, BA offices or directly to CMS) should be notified on CMS and invalidated. Under certain circumstances it should be retained for investigation purposes.

Card Enquiries

4.3.7.1.40. CMS should support enquiries regarding card status and history (including temporary tokens as applicable). Such enquiries will be required for BA investigations as well as to answer customers' queries and should be provided to all DSS benefit-processing staff in addition to the Service Provider's own customer service staff. For example, the enquiry response should show the following card states (with date and time at which each status change occurred):

- card issued to post office (if appropriate);
- card received at post office (if appropriate);
- card issued to customer;
- card activated;
- card expired;

POL00028135

- card return notified to CMS;
- card invalidated (with reason).

4.3.7.1.41. Note that card invalidation may occur at any stage in the above process in response to reports of loss, theft, suspected fraudulent use etc.

4.3.7.1.42. The service should provide the facility to allow customers to have more than one valid card (although it is expected that one card to one customer will be the objective).

4.3.7.1.43. Exception conditions should also be shown, such as:

- card not received by the customer or post office (if appropriate);
- card uncollected within the specified time;
- card reported lost / stolen / damaged;
- card found;
- card suspended (with reason);
- card impounded at the post office (with reason).

4.3.7.1.44. State changes must always be positively confirmed to CMS rather than inferred.

4.3.7.1.45. It should be possible to obtain details for previous cards issued to a customer as well as the current one. It should also be possible to identify payments that have been encashed using a given card.

4.3.7.1.46. An enquiry to determine the customer of a card, given the card reference, may also be required (for instance, when cards are recovered/handed in or damaged). If the customer's National Insurance Number is visible on the card then such a need may be reduced.

Card Monitoring

4.3.7.1.47. The movement and use of cards will need to be monitored to detect exception conditions and possible fraudulent use (see 'Encashment Monitoring').

4.3.7.1.48. A facility to tag cards which, upon presentation, trigger an alert message at CMS or PAS is desirable. This is to support both the Service Provider's and Contracting Authorities' security control and fraud detection. Such an alert would not be visible at the post office counter.

POL00028135

4.3.7.1.49. End-to-end service monitoring to DSS customers is required in addition to any that may be required to support contractual monitoring between the DSS, POCL and the Service Provider. Possible metrics include:

- time taken from initial issue of card request to CMS until receipt of card at post office;
- mean time between failure for card (card read failure).

4.3.7.2 CAPS to CMS Interface

4.3.7.2.1. This section describes the specific transactions required between CAPS and CMS, in terms of data content and service levels. Service levels are described in terms of the time constraints of each transaction. The Service Provider should regard these as guidelines only and should, themselves, consider what will be necessary in the light of the requirements defined elsewhere in this SSR.

Initial Card Issue Request

4.3.7.2.2. The following data is contained within the initial issue card request sent from CAPS to CMS:

	For each initial issue card request:
1.	Customer National Insurance Number
2.	Customer Name (as requested by the customer to be displayed on the card)
3.	Correspondence Address
4.	Nominated Post Office ID (if appropriate)
5.	Card Type (e.g. WPA card)
6	National Sensitivity Indicator

Service Level

4.3.7.2.3. Any validation or integrity problems arising from this request must be returned immediately (since the request may be part of an on-line dialogue). In general, the actual time taken to issue the card must be as short as possible, with the objective being to make the card available to the customer in time for any subsequent payments to be collected. The Service Provider must balance this against the need to issue temporary tokens (when such a deadline cannot be met) and the subsequent increase in security risk that such tokens may entail.

POL00028135

Change to Personal Details

4.3.7.2.4. The following data is contained within the change to personal details sent from CAPS to CMS:

	For each change to personal details:
1.	Customer National Insurance Number
2.	Customer Name (as requested by the customer to be displayed on the card)
3.	Correspondence Address
4.	Nominated Post Office ID (if appropriate)
5.	Card Type (e.g. WPA card)
6	National Sensitivity Indicator

Service Level

4.3.7.2.5. If a new card is required as a result of this transaction, the same service levels as for card issue will apply.

Customer No Longer Maintained

4.3.7.2.6. The following data is contained within the 'customer no longer maintained' notifications sent from CAPS to CMS:

	For each notification :
1.	Customer National Insurance Number

Service Level

4.3.7.2.7. This change should take effect as soon as possible.

4.3.7.3 Benefit staff to CMS Interface

4.3.7.3.1. The following sections summarise the interface that benefit delivery staff will need to support card related business processes. The volumes associated with this interface are almost entirely dependent on:

- total number of customers;
- the Service Provider's approach to and effectiveness in managing cards.

POL00028135

4.3.7.3.2. This interface, as with all interfaces provided to DSS staff, should be consistent for all users.

Card Enquiries

4.3.7.3.3. The data flows will consist of the input of either a card number or National Insurance Number with output of related card status. If a customer has more than one card, details (as below) must be displayed for each:

	For each card:
1.	Customer National Insurance Number
2.	Card ID
3.	Card Status
4.	Previous Card States (status, date changed)

Service Level

4.3.7.3.4. Since this is likely to be an on-line dialogue, details should be displayed immediately.

Temporary Token Issue

4.3.7.3.5. The data flow will consist of the input of details required to issue a temporary token. The Service Provider must consider what data will be required. Possible details required may include those for card issue (see above).

Service Level

4.3.7.3.6. Since this is likely to be an on-line dialogue, confirmation of token issue should be immediate. Actual issue of the token must occur in time for the next payment encashment required.

Card Control Transactions

4.3.7.3.7. The data flows will consist of the input of either:

- a customer National Insurance Number, followed by selection of a card from a list displayed, or
- a card ID;

followed by the relevant event identification.

4.3.7.3.8. The events will include:

- card loss;

POL00028135

- card theft;
- card damage;
- card return;
- card invalidation;
- card suspension and removal of suspension;
- setting and removal of card 'alerts';
- etc.

	For each card control transaction :
1.	Customer National Insurance Number
2.	Card ID
3.	Status Change
4.	Date and Time
5.	Reason

Service Level

4.3.7.3.9. Since this is likely to be an on-line dialogue, confirmation of the status change should be immediate. Any control information that leads to a restriction in the use of the card (invalidation as a result of card theft, for example) must, ideally, take effect immediately and certainly before any further use of the card.

4.3.7.4 POCL Strategic Infrastructure to CMS Interface

4.3.7.4.1. The Service Provider should maintain a logical separation between the POCL Strategic Infrastructure and CMS and define a detailed interface specification to support this. The exact flows across this boundary will vary to some extent depending on the Service Provider's proposals but would need to support such areas as:

- card receipt at post office (if appropriate);
- card collected from post office (if appropriate);
- card uncollected and destroyed (if appropriate);
- card returned to post office;
- Temporary token ('one-shot') used and retained.

4.3.7.4.2. The volumes of such interaction will be heavily dependent on the detail of the Service Provider's proposals.

POL00028135

4.3.7.4.3. In their proposals, the Service Provider should describe how their proposed POCL Infrastructure could interface to (or migrate to) other Card Management / Authentication services if, for example, there is a Government smart card in the future (see 4.3.5.1).

4.3.7.5 PAS to CMS Interface

4.3.7.5.1. The Service Provider should maintain a logical separation between PAS and CMS and define a detailed interface specification to support this. The exact flows across this boundary will vary to some extent depending on the Service Provider's proposals but will need to support two way provision of information.

4.3.7.5.2. From CMS to PAS:

- current card status (valid, invalid or suspended);
- temporary token issue;
- card alerts.

4.3.7.5.3. From PAS to CMS:

- exceptional card use that may require Service Provider defined exception processing (such as authentication failure, card read failure, attempted use of invalid card);
- use of 'one-shot' temporary token.

4.3.7.5.4. Further / different flows may be needed to support other Service Provider's proposals (for example revised "change of nominated post office" (P80MA) procedures).

Service Level

4.3.7.5.5. Service levels for PAS-CMS interactions are not specified as part of this requirement. The Service Provider should, however, indicate how any other service levels impact on this interface and design it accordingly.

POL00028135

4.4 POCL DATA FLOWS

4.4.1. The above sections have described the overall process for benefit payments. This includes activities in post offices and the following exemplar data flow diagrams show how these might be implemented using the five generic functions described in section 4.2. These diagrams are:

- Figure 4-9 Using the Token Management Generic Transaction to issue first Benefit Card
- Figure 4-10 Using the Outpay Generic Transaction to issue Benefit Payment
- Figure 4-11 Using the Outpay Generic Transaction to perform Girobank Withdrawal
- Figure 4-12 Using the Inpay Generic Transaction to Pay a Telephone Bill
- Figure 4-13 Using the Personal Details Capture Generic Transaction to Change Beneficiary Address
- Figure 4-14 Using the EPOS transaction to Pay Benefit
- Figure 4-15 Using the EPOS transaction to sell Stamps

4.4.2. Further diagrams of exemplar transaction data flows are provided in appendix 4-10.

POL00028135

Token Management

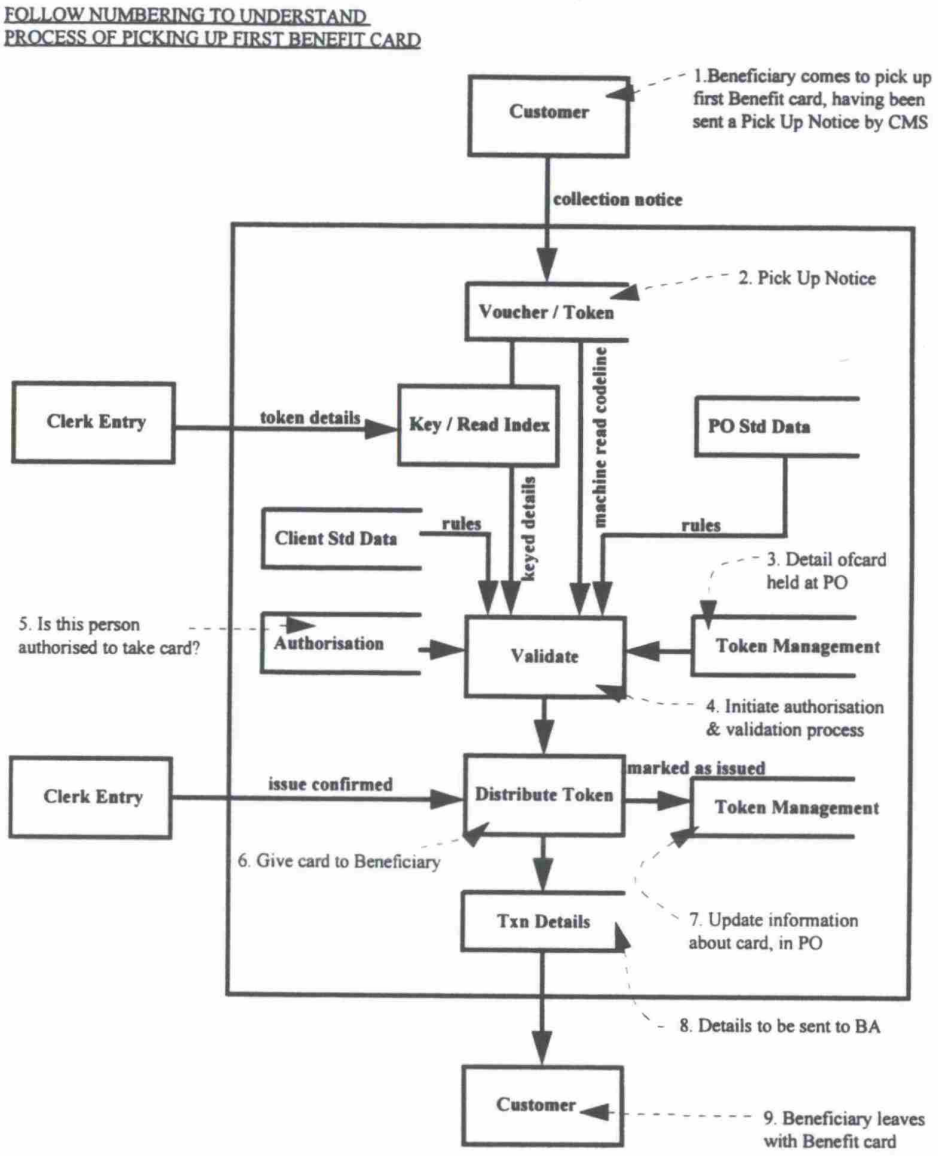


Figure 4-9 Using the Token Management Generic Transaction to issue first Benefit Card

POL00028135

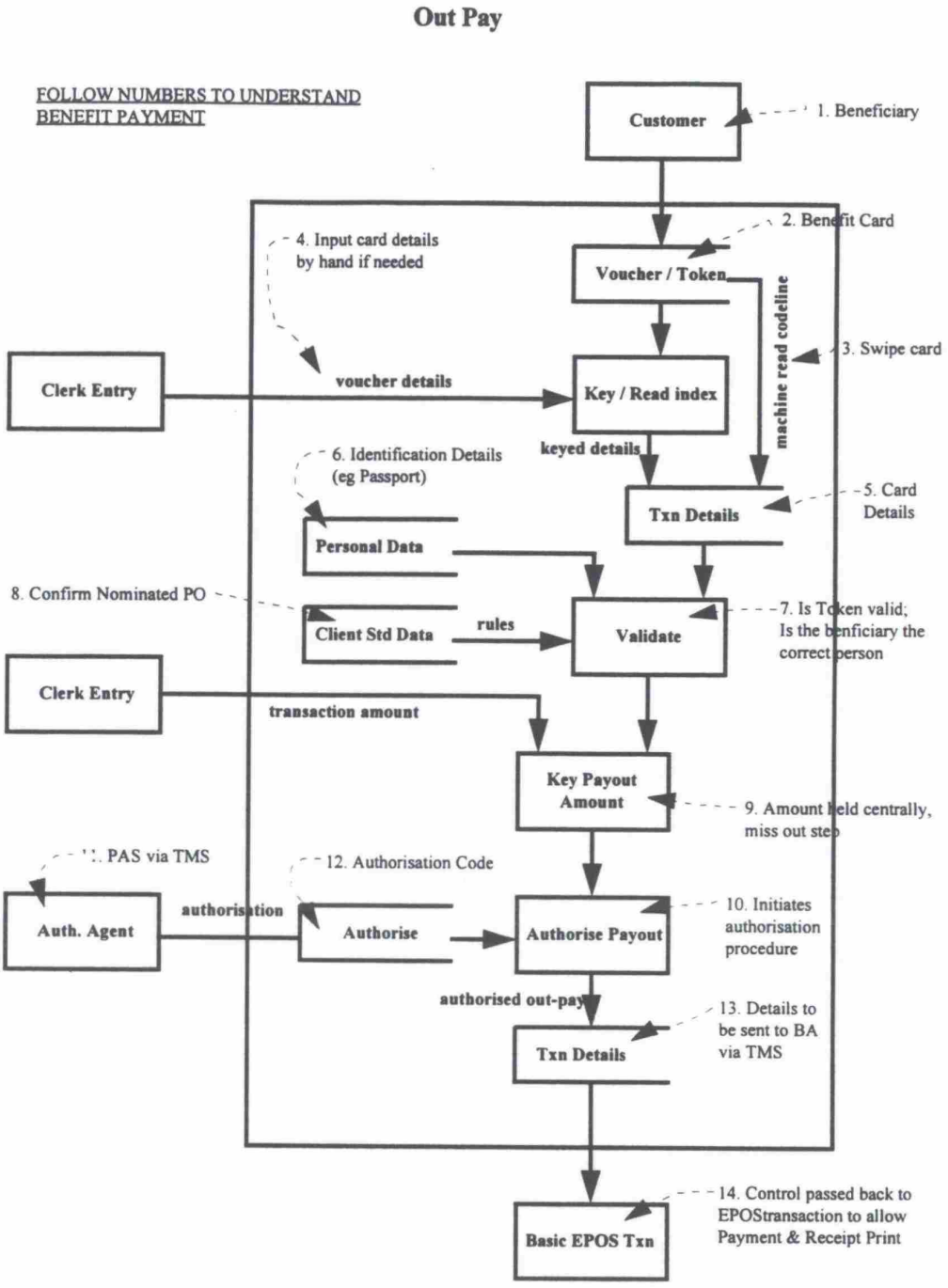


Figure 4-10 Using the Outpay Generic Transaction to issue Benefit Payment

POL00028135

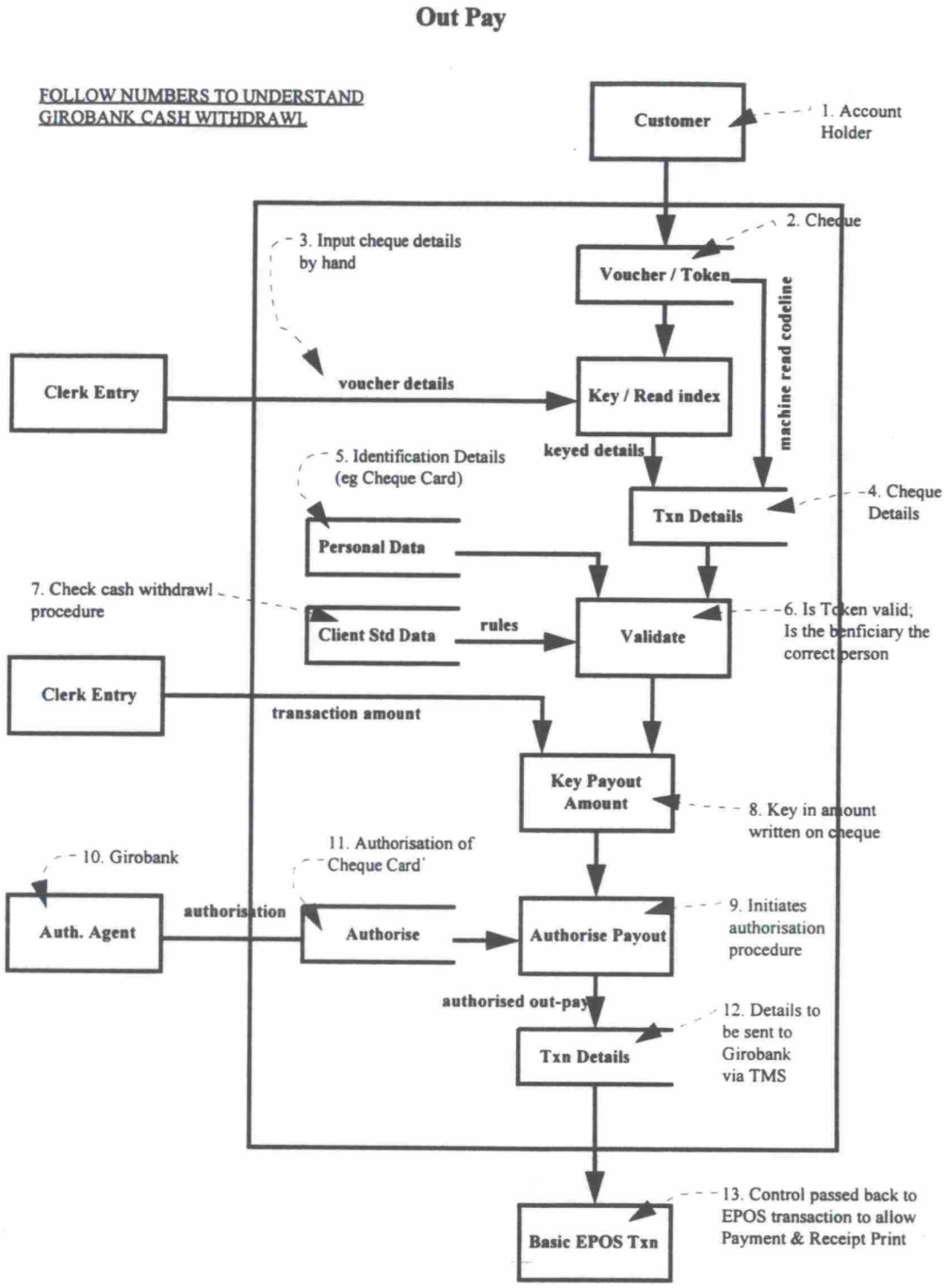


Figure 4-11 Using the Outpay Generic Transaction to perform Girobank Withdrawal

POL00028135

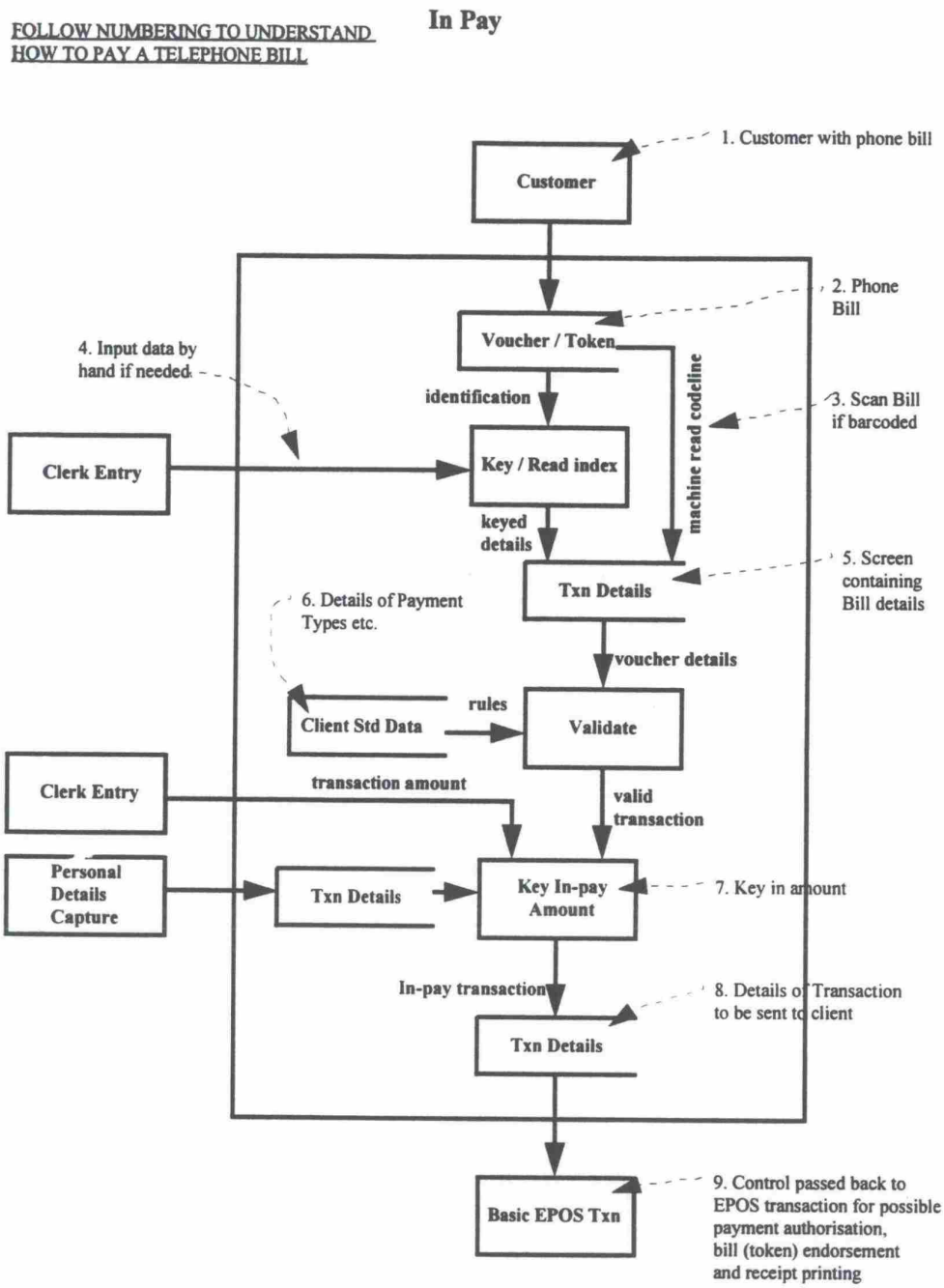


Figure 4-12 Using the Inpay Generic Transaction to Pay a Telephone Bill

POL00028135

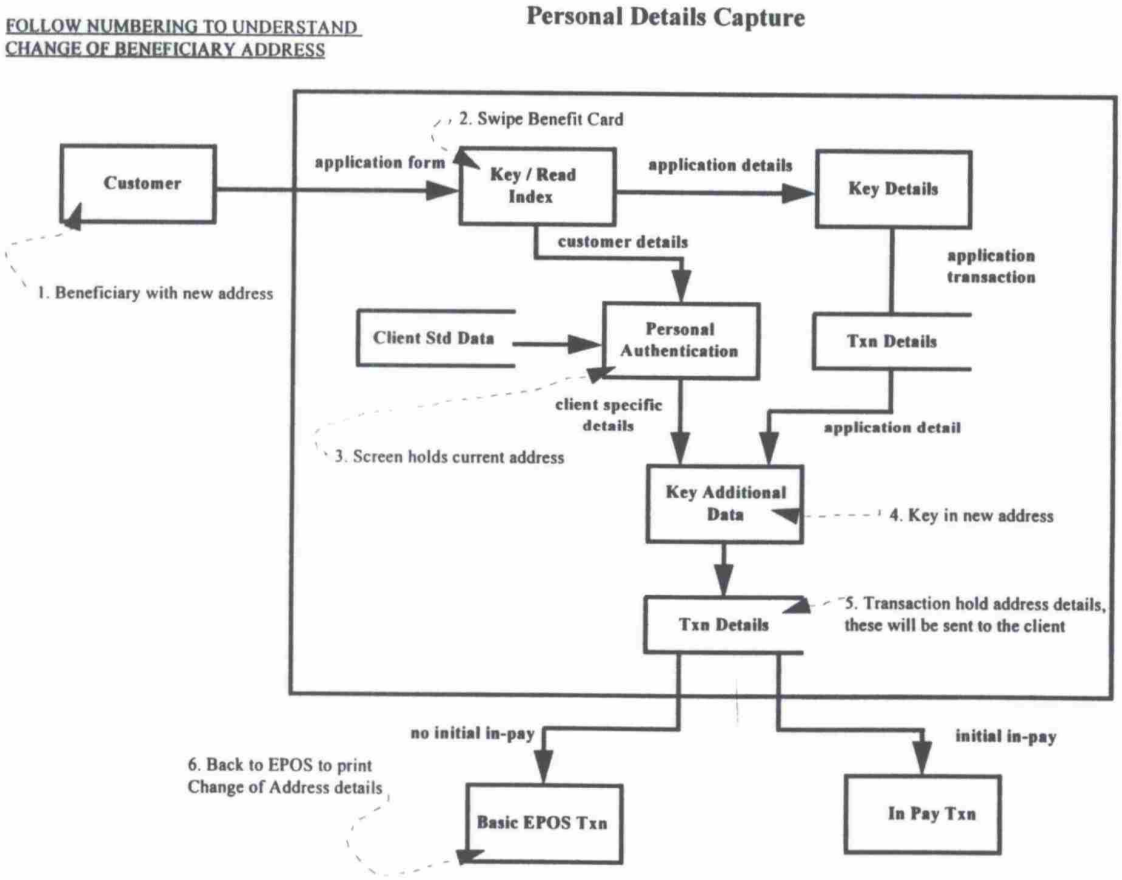


Figure 4-13 Using the Personal Details Capture Generic Transaction to Change Beneficiary Address

POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

Basic EPOS Transaction

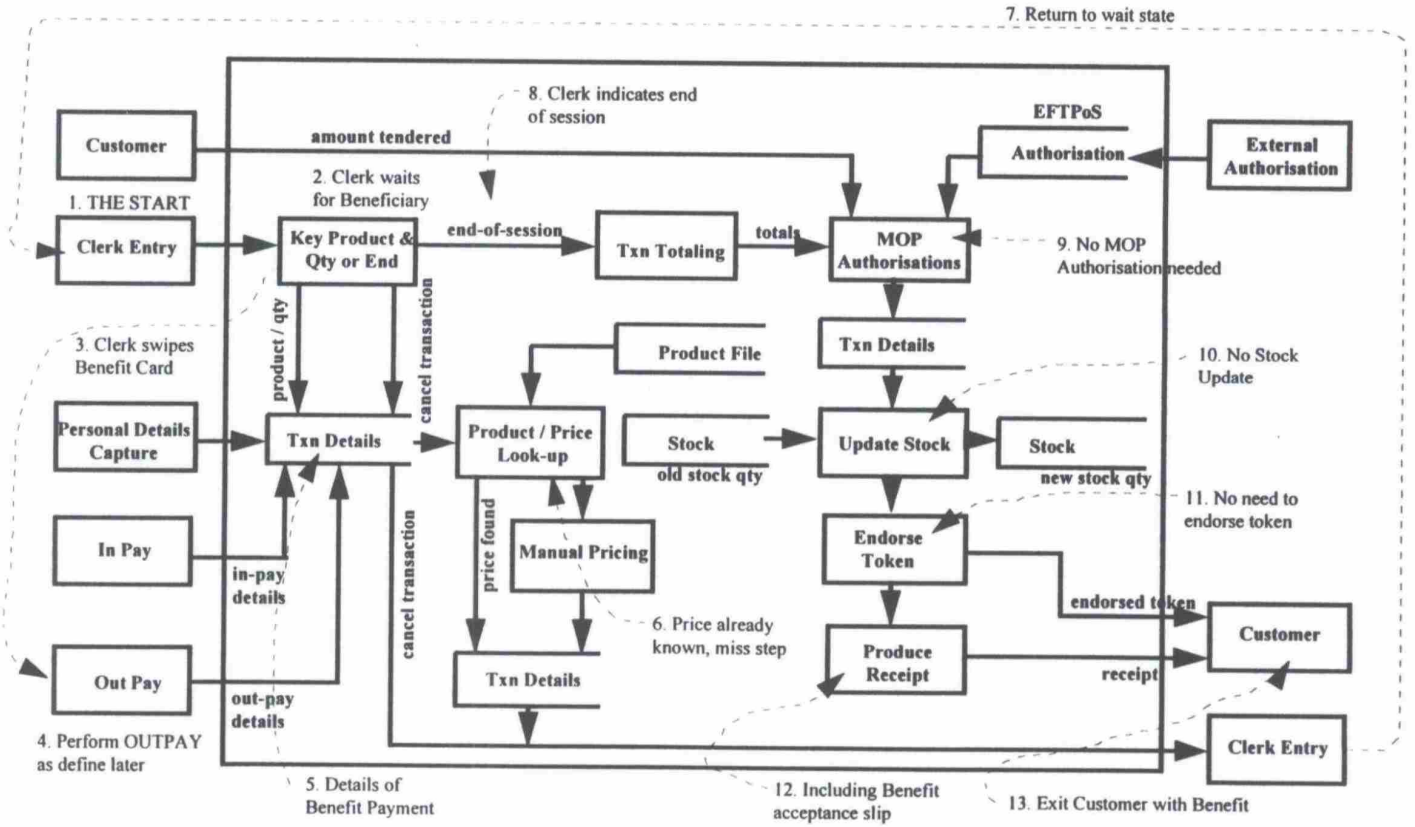


Figure 4-14 Using the EPOS transaction to Pay Benefit

POL00028135

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE

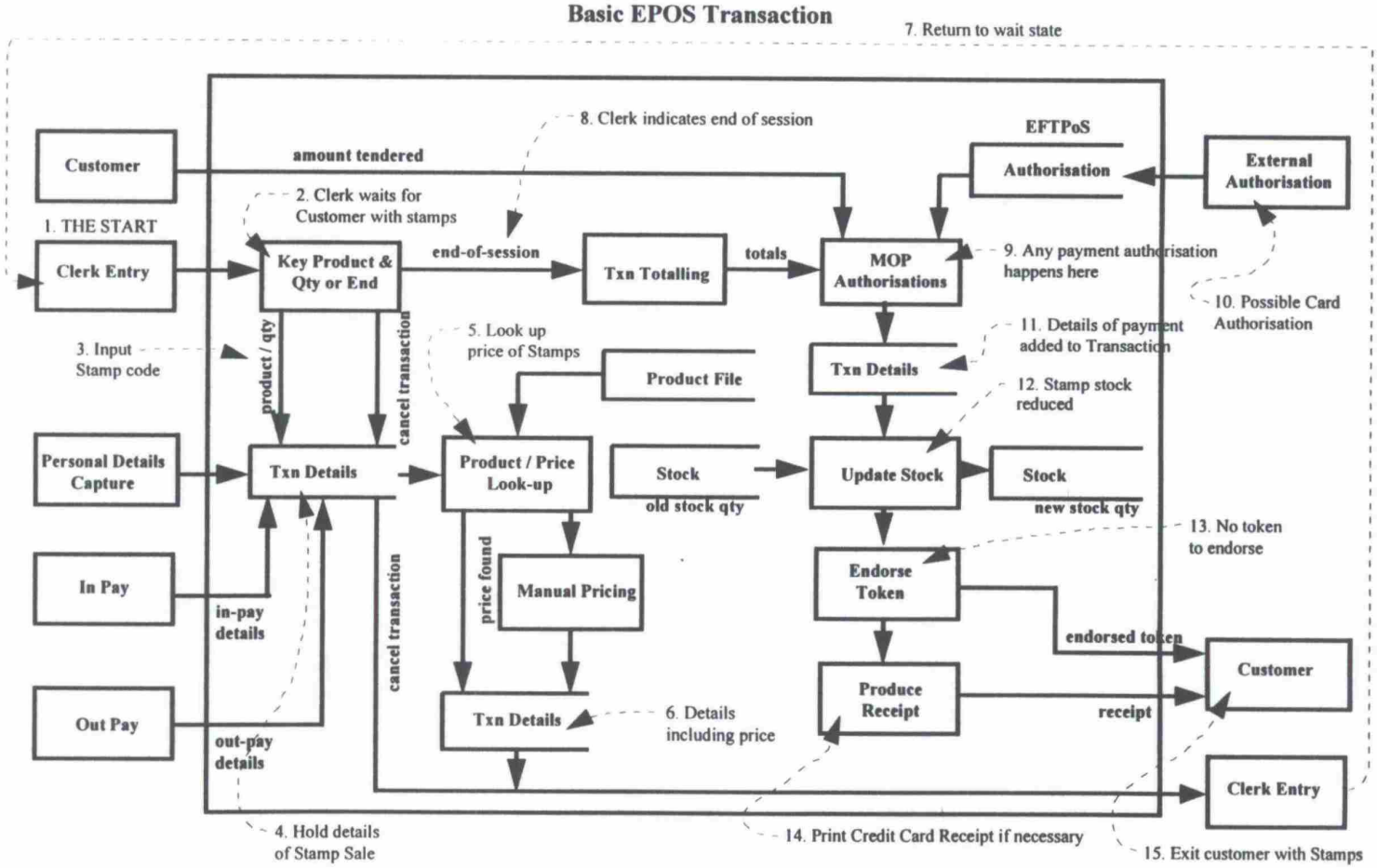


Figure 4-15 Using the EPOS transaction to sell Stamps

POL00028135

4.5 SERVICE PROVIDER'S RESPONSE

4.5.1 Proposal Content

4.5.1.1. This chapter has set out the service architecture and the main functional requirements. Throughout, a number of areas are specifically indicated where the Service Providers are required to make detailed proposals, and offer alternative solutions if appropriate. For guidance, Service Providers should structure their proposal in three separate sections under the headings of:

- Service Architecture;
- POCL Strategic Infrastructure Service;
- Benefit Payment Service.

4.5.1.2. In particular, as well as responding to specific requests within this chapter, Service Providers should ensure that the following information is provided.

Service Architecture

4.5.1.3. A target service architecture was set out in section 4.1 for consideration by Service Providers. Service Providers are invited to confirm that this architecture is the basis of their proposal, or offer modifications providing justification of their alternative. In particular, an explanation of the alternative service boundaries and implications for both BA and POCL are requested.

4.5.1.4. For their proposed service architecture Service Providers should describe the main functional attributes of each service element, e.g. the Card Management System (CMS), together with performance characteristics and any constraints and dependencies on either the BA or POCL. With regard to the service boundaries between the POCL Strategic Infrastructure Service and PAS, Service Providers are requested to consider whether this could be generic interface common to all types of POCL clients providing both batch and real time capability.

POCL Strategic Infrastructure

4.5.1.5. Service Providers are requested to set out their approach to the design and development of the POCL Strategic Infrastructure Service elements.

4.5.1.6. In particular, Service Providers should advise on the feasibility and implications of adopting the generic approach to the counter interface discussed in this chapter. Service Providers should consider whether their approach is equally applicable to the Benefit Payment Service at the counter, and indicate if there would be any effect on timescales or cost.

POL00028135

4.5.1.7. Details showing the split of functionality between the TMS and Counter Interface Service are required.

4.5.1.8. In particular details should be provided which describe:

(a) the approach to design and development of the counter interface and TMS;

(b) software approach and whether based on off the shelf product or bespoke development;

(c) physical hardware attributes e.g. size, reliability, environmental constraints;

(d) HCI approach and why it will be suitable for a wide range of users;

(e) how the design will have the ability to meet the wide range of applications and transaction volumes envisaged;

(f) timescales for development;

(g) how the overall approach to design will provide for migration of current counter services, including interfaces to client systems where appropriate;

(h) how it will provide for rapid adoption of new client services.

Benefit Payment Service

4.5.1.9. Service Providers are required to set out their overall approach to the design and development of the Benefit Payment Service, in particular explaining:

(a) how much development is bespoke and how much is package adaptation;

(b) timescales for development;

(c) relationship to and dependencies on the generic approach to the POCL Strategic Service Architecture;

(d) the physical attributes of the systems e.g. the hardware upon which the service is based.

4.5.1.10. For each of the Payment Authorisation Service and the Card Management Service, or your equivalent, describe:

(a) the detailed functionality;

(b) the interface with CAPS and the POCL Strategic Infrastructure and any other proposed interface;

(c) any constraints you are imposing on CAPS or the POCL Strategic Infrastructure;

(d) the service levels you offer;

POL00028135

(e) the ability of the designs and service to cope with change e.g. volumes and different benefits.

4.5.2 Specific Responses

General

C SR4.1 Can the Service Provider confirm that the service will comply at all times with all relevant legislation?

C SR4.2 Can the Service Provider confirm that it will be possible to prove that the service was operating without defect in evidential support of any appropriate prosecutions in court?

I SR4.3 State how the service will provide the office polling and real time authorisation; elements of the applications portfolio for value added processing.

I SR4.4 Service Providers should indicate their interest in utilising the existing POCL data capture and document processing services.

I SR4.5 Service Providers should state the design methodology(ies) which will be/were used to produce the software components. They should also indicate the language/tools used and suggest how small, medium and major enhancements to software might be incorporated.

I SR4.6 Service Providers should state the capacity limitations (minimum and maximum) of each component of in their proposed service, identifying areas of overlap between component capabilities.

I SR4.7 Service Providers should state how potential customer acceptability issues will be identified and customer acceptability assessed, both prior to roll-out and once the service is in operation.

I SR4.8 Service Providers should state the scalability of the service (both up and down) to allow changes in business volumes to be readily accommodated.

Equipment Considerations

C SR4.9 The Service Provider is aware of his obligations under the emerging EC directives on Visual Display Screen Equipment 90/270/EEC and on Electromagnetic Compatibility (EMC) 89/336/EEC. Can the Service Provider confirm that all products used in the provision of the service, after implementation dates, will conform to these standards?

C SR4.10 The standards which come under the scope of Decision 87/95/EEC and of the Directive 77/62/EEC, will apply to the Services provided under any Contracts arising from this procurement. Can the Service Provider confirm that all products used in the provision of the service, after implementation dates, will conform to these standards?

POL00028135

C SR4.11 Can the Service Provider confirm that any equipment, installed for operation, will not significantly contribute to the ambient noise level in the office?. As a guide, the acoustic noise emission of any item of equipment should be less than 60 dB(A), measured at a distance of 1 metre.

C SR4.12 Can the Service Provider confirm that all equipment is capability of withstanding (without degradation in performance) impacts, shock and vibration, which may occur when in normal use?

C SR4.13 Can the Service Provider confirm that any electronic emissions from equipment will not interfere with other systems in offices?

C SR4.14 Can the Service Provider confirm that provision will be made for logic ground and mains safety earth to be connected or separated at each counter terminal supplied and peripheral supplied?

C SR4.15 Can the Service Provider confirm that equipment shall not interfere with the health, comfort or normal pattern of work of staff as a result of emission of acoustic noise, vibrations, heat fumes or other radiation, or as a result of its construction?

C SR4.16 The Service Provider to confirm the temperature range which the equipment can operate in without degradation in performance?

C SR4.17 The Service Provider to confirm the temperature range which the equipment can withstand without degradation in a storage environment?

Benefits Payments System General

I SR4.18 State how the service will prohibit fraudulent attacks (both internal and external) with particular reference to attempted fraudulent payment transactions.

Benefits Payments should be made to the right person

I SR4.19 Service providers should state how their proposed receipting procedure would operate, including details of any additional messages or information which could be incorporated on the receipt.

I SR4.20 Service Providers should state how and in what circumstances the service will support and enable payments away from a nominated post office (if appropriate).

I SR4.21 Service Providers should state how they intend to support and enable customer changes of nominated post office (if appropriate) and how the DSS will be informed of such changes.

Token Production, Issue and Replacement

C SR4.22 Can the Service Provider confirm that any card produced, or used by him, in the provision of the service will conform to all relevant British, European or International ISO (or equivalent) standards?

POL00028135

I SR4.23 Service Providers should state the maximum time for the production of a card and its delivery.

I SR4.24 The Service Provider should state how they intend to issue cards to authorised customers.

Security

I SR4.25 The Service Provider should state how he will ensure that all data (electronic or paper-based and including stored data) is secure against unauthorised access and that the service is protected against internal fraud and counterfeiting.

I SR4.26 The Service Provider should state how case sensitivity will be applied in the service domain (as described in Section 4.3).

Authentication

I SR4.27 The Service Provider should state how authentication data would be collected, both initially and on a regular or continuing basis.

I SR4.28 The Service Provider should provide any background information and research that may support their proposed method of authentication.

POL00028135

CONTENTS

5. STEADY STATE SERVICES

POL00028135

CHAPTER 5. STEADY STATE SERVICES

5.1 INTRODUCTION

5.1.1. This chapter specifies the high level business requirements for the actual provision of the "business as usual" or "steady state" services both during and after roll-out. The duration of the roll-out programme is not yet defined but may take several years (see chapter 7) and thus the boundary between roll-out and steady-state will be complex. Some of the associated detailed service levels specific to the applications are given in chapter 4, others will need to be developed during the contract negotiation stage, referred to as stage 3, see chapter 9. Service Providers are asked to confirm that they can meet the service performance criteria or to propose viable alternatives, and to provide a detailed explanation of their approach to management of these services.

5.1.2. The steady state services have been broken down into four types. These can be defined as:

(a) the **operational** services defined in chapter 4 e.g. the POCL Strategic Infrastructure Service or the Card Management Service (CMS);

(b) the **support** services required by the operational services e.g. the help desk service, the primary route for requesting any service or problem support;

(c) the **contract management** service e.g. the monitoring and review of service levels for the operational and support services;

(d) and **contract transfer**.

5.1.3. High level performance criteria have been identified and should be applied to the services where appropriate. These are:

(a) **hours of cover**, which identifies the period during which the Service Provider should provide the service;

(b) **availability**, which identifies the minimum percentage of the hours of cover that the service should be operationally available;

(c) **response times**, which identifies the speed of response required to any operational or user request;

(d) **counter transaction times**, which identifies the time the customer is at the counter, measured from the moment eye contact is established between the customer and the clerk to the moment the customer walks away.

POL00028135

5.2 OPERATIONAL SERVICES

5.2.1 Introduction

5.2.1.1. The complete operational service for an application will be achieved by a combination of the appropriate service elements, for example the Benefit Payment Service (BPS) requires the POCL Strategic Infrastructure Service, the Card Management Service (CMS) and the Payment Authorisation Service (PAS). This is best illustrated by reference to the Service Architecture diagram given in chapter 4, figure 4-1.

5.2.1.2. For the BPS, the requirement is to achieve a consistent end to end service from the input service boundary, i.e. the interface with the CAPS system to the PAS and CMS, through to the counter clerk at the post office counter and back to PAS and the CAPS interface. Hence the service performance criteria for the BPS and other applications, are defined on this end to end basis since this is consistent with the overall business objectives. However, it is likely that the contract for each discrete service element and the associated performance criteria will be specifically agreed with only one organisation, either POCL or BA.

5.2.1.3. The specification of the overall customer service interface, including that for BA customers is outside the scope of this procurement. However the services provided by the Service Provider must enable POCL to deliver the appropriate level of service and not adversely impact on quality standards or customer perceptions.

5.2.1.4. The Contracting Authorities will require the ability to add further applications to the service. The Service Provider should be willing to integrate and operate these via the service agreement, provided that there are no valid technical reasons that preclude their inclusion in the service.

5.2.1.5. The following sections summarise some of the business performance criteria for the end-to-end operational service as required to be delivered at the customer interface by the counter clerk. All payments to the customer should be 100% accurate.

5.2.2 Counter Interface Service

5.2.2.1. The performance criteria below are based on post office counter transactions and include payment of a benefit as a result of a customer submitting a card. Service Providers should note that the service levels should not be compromised.

Hours of Cover

5.2.2.2. Service availability will need to be agreed with POCL and would include opening hours and use of the service for any additional requirements e.g. audit, accounting, training. The majority of post offices are currently open 09.00 - 17.30 (Mon-Fri) and 09.00 - 13.00 (Sat), but there are significant variations: National Lottery offices are open until 19.00 on Saturday, and offices in supermarkets can be open 08.00 to 21.00, and any 6 hours on a Sunday. Opening hours are subject to change and revision and this needs to

POL00028135

be reflected in any proposals. Service Providers are invited to put forward proposals for further discussion.

Availability

5.2.2.3. A customer expects to receive a payment 100% of the time even when the computer service is unavailable or partially available. Service Providers are invited to propose their availability for the computer supported counter interface service, indicating various levels of manual or partial computer service fall-back, and the implications in terms of responsiveness of the service when in fall-back mode. Service Providers must describe the fall-back process they suggest for the counter clerk experiencing both full or partial system failure and the steps needed for recovery. In certain circumstances, the normal service will not be available, due to situations beyond the control of the Service Provider, such as fire and flood. The Service Provider should indicate when these circumstances would apply and how they would support the post offices and set up alternative arrangements.

Counter Transaction Times

5.2.2.4. Service Providers should seek to improve on the current counter transaction times. The current average counter transaction time for a customer benefit payment, dependent on the type of benefit is from 22 to 32 seconds. Service Providers will be required to work with POCL to facilitate improvement in counter transaction times and to agree detailed performance criteria and measurement methods. Service Providers should indicate typical response times from the request to the central system to a response on the screen for the benefit payment processing.

5.2.3 Card Management Service

5.2.3.1. The CMS will issue new and replacement cards and will process the blocking of lost and stolen cards.

Hours of Cover

5.2.3.2. the service for the notification of lost and stolen cards should be available 24 hours a day, 7 days a week. The hours of cover for issuing new or replacement cards should reflect those to be agreed for CAPS transfers.

Response Times

5.2.3.3. Lost or stolen cards should be blocked immediately and under certain agreed circumstances a replacement card issued. A new or replacement card should be received at its nominated destination within 2 working days of a request from BA. Service Providers should propose alternative response times for the normal bulk issue of cards but must include an option for cards reaching their nominated destination within five working days and they should clearly indicate any financial implications against each option. It is vitally important that cards arrive by the expected date to avoid unnecessary

POL00028135

and costly time and effort in making follow-up enquiries . Currently it is envisaged that BA will distribute any emergency cards and the Service Provider may be required to issue these cards to BA offices within 24 hours.

5.2.4 Transaction Management Service

5.2.4.1. The TMS will interface with other POCL systems and service performance criteria will need to be agreed that are no worse than current levels. Service performance criteria already exist for the host polling and control service (appendix 4-8) in respect of POCL and client interfaces. POCL are looking to the Service Provider to agree standards and criteria which maintain or improve current or agreed levels.

5.2.5 Payment Authorisation Service (PAS)

5.2.5.1. The performance criteria for PAS need to reflect those of the counter interface service.

5.3 SUPPORT SERVICES

5.3.1 Introduction

5.3.1.1. All services must be fully supported from end-to-end by the Service Provider. It is expected that the focus for all enquiries or problems will be the help desk service and these services are described in this section together with their performance criteria. Enquiries may cover requests for a range of supporting services that the Service Provider will need to provide e.g. training, software support and security management.

Help Desk Support Services

5.3.1.2. The help desk support services are logically defined in relation to the type of end-user of the service. Support services can therefore be categorised under the following headings. The physical design will be for the Service Provider to determine.

5.3.1.3. This structure of help desks is not mandatory, Service Providers are invited to propose alternatives where they believe this will be beneficial to the Contracting Authorities, their clients and customers. It is important to ensure that any help desk receiving an enquiry will re-route it to the appropriate help desk, if it is outside the scope of its service responsibilities. Service Providers are asked to consider this issue and suggestions as to how this might be achieved bearing in mind that problem ownership and resolution are essential.

5.3.2 The Help Desk for Customer Enquiries

5.3.2.1. The Contracting Authorities envisage that this service will be a direct line 'freephone' help desk for customers who have a query regarding any card based services e.g. lost or stolen cards. The Service Provider should also accept local calls that have been re-routed from POCL's 7 regional helplines, or BA customer helplines. The Service Provider is reminded that non English speaking customers will also require help.

POL00028135

5.3.3 The Help Desk for BA Enquiries

5.3.3.1. This help desk is the primary BA interface for any problems, advice or action to second line support services from BA staff or the ITSA help desk. Fault reporting may be via the ITSA Service Delivery function.

5.3.4 The Help Desk for POCL Infrastructure Enquiries

5.3.4.1. This help desk is the primary interface for any problems related to the POCL infrastructure. Post office staff and agents will use this service either to seek advice or to action second line support services such as system maintenance for faults and system upgrade for changes to the service. Counter clerks and agents will continue to pass any other queries to regional helplines.

5.3.5 Underlying Support Services

5.3.5.1. The Service Provider will need to consider and define a range of underlying services which can be accessed by a help desk and will cover aspects such as:

(a) software support service;

(b) service upgrade;

(c) training;

(d) service administration and maintenance;

(e) supply of documentation;

(f) configuration management;

(g) security management, for example requirements for new agents;

(h) counter equipment relocation and network changes;

(i) counter equipment removal;

(j) change management;

(k) incident and problem management;

(l) fault diagnosis and resolution;

(m) customer education and marketing;

(n) reference data management.

5.3.5.2. While not all of these services will be visible to the users of the services, they will be fundamental to contract transfer e.g. configuration management.

POL00028135

5.3.6 Performance Criteria

5.3.6.1. The performance targets for help desks are specified below:

(a) **Hours of Cover**

The Customer Help Desk — should be operational 24 hours a day, 7 days a week for the reporting of stolen or lost cards.

Service Providers should propose cost effective and efficient hours of cover for the BA and POCL help desks.

(b) **Response Times** — all help desks should normally respond to calls within 3 rings (ten seconds). Where an immediate problem resolution is not achievable, the enquiry should be categorised and prioritised so that it can be actioned and completed within a standard timescale. Service Providers are asked to propose categories, priorities and associated timescales for agreement with the Contracting Authorities.

5.4 CONTRACT MANAGEMENT SERVICE

5.4.1 Introduction

5.4.1.1. This section outlines the anticipated scope for the contract management service. The shape of the contract(s) will be agreed during the contract negotiation stage described in chapter 9, and the exact number of Contracting Authorities will be decided then. However, the Service Provider is required to provide a single point of contact for all contract management issues for each contract. The scope of the contract management function will include:

(a) monitoring service performance statistics e.g. help desk service performance statistics;

(b) contract authority/service contractor reviews;

(c) escalation procedures;

(d) charges authorisation;

(e) contract change management;

(f) service change management e.g. ordering procedures;

(g) audit control and access;

(h) security;

(i) quality management;

POL00028135

(j) monitoring of complaints from customers.

5.4.1.2. Service Providers are invited to consider the above, define their overall approach and make any proposals for additional areas which from their experience should be included within the Contract Management Service.

5.4.2 Service Code of Practice

5.4.2.1. The Contracting Authorities wish to manage the contract both in terms of monitoring the service actually received and by inspecting how the service is provided. It is expected that the Service Provider will need to develop a range of procedures and practices that defines in detail the day to day service, the operational and management interfaces and the relationships between the Contracting Authorities and the Service Provider. This set of procedures will be referred to as "The Service Code of Practice" (SCOP) and they are to be developed by the Service Provider during the operational trial period, and formally accepted as part of the operational trial process. The Service Provider will also be required to develop customer charters for those services which are provided directly to customers and these should be in line with those already produced by the Contracting Authorities.

5.4.2.2. Service Providers are invited to outline the scope of such a Service Code of Practice and indicate whether they agree with this approach, or propose an alternative. Evidence of how they have established day to day operational and management interfaces and procedures for other major service contracts and the success of employing those procedures is requested. References should be proposed.

5.5 CONTRACT TRANSFER

5.5.1. Service Providers will understand that at the appropriate time the service contract(s) is likely to be re-competed and this may result in the need to transfer the service in part or whole to another party. This must be achieved without disruption to the services and within a reasonable time period. The Contracting Authorities consider this to be a critical requirement and one for which the proposal will need to be convincing and practical.

5.5.2. Service Providers are invited to consider from an operational perspective (financial and commercial perspectives to be covered in chapter 8) how the service would be provided and managed during the transfer period. Also how the transfer of the following elements would be achieved if appropriate or contractually required, while still achieving the contracted performance criteria:

(a) assets;

(b) staff;

(c) third party software;

(d) own software, including bespoke and/or packages;

POL00028135

(e) documentation and procedures;

(f) other sub-contract activity;

(g) support services, e.g. helplines.

5.5.3. Service Providers should describe in overview the processes and constraints, including timescale, associated with the Contract Transfer Service and should use their past experience to identify risks and issues. Where the Service Provider has been party to such transfer circumstances, they are requested to give reference site details.

5.6 SERVICE PROVIDER'S RESPONSES

5.6.1 Proposal Content

5.6.1.1. This chapter has described the Steady State Service requirements and specifically indicates a number of areas where the Service Providers are required to make detailed proposals, and offer alternative proposals if appropriate. For guidance, Service Providers should structure their proposal as follows.

5.6.1.2. For each of the following services:

- Operational;
- Support (including the underlying Support Services);
- Contract Management;
- Contract Transfer;

the Service Provider's proposal should:

(a) describe how the service would be developed and brought into operation;

(b) describe how it will operate from the user perspective and give the Service Provider's approach to providing the organisation, processes, and resources necessary to provide the service and meet the service criteria;

(c) provide supporting evidence of capability by making reference to past and current experience and, in particular offering hard evidence of capability wherever possible, (e.g. by provision of reference site visits and availability of documentation for inspection);

(d) consider the proposed end to end performance requirements and advise on the feasibility of achieving these requirements (alternatives may be suggested but they should be supported by both a rationale and a cost benefit justification);

POL00028135

(e) for all services, Service Providers should propose performance criteria for the various service elements (e.g. Payment Authorisation Service, which would give the cumulative effect of achieving the overall end to end performance);

(f) for all underlying services, Service Providers should identify the scope of the service, state how the service would be developed, introduced and provided as part of the steady state services (include details of the number of people providing the service, their qualifications and where they will be located);

(g) Service Providers should also identify and justify any specific constraints, that they would wish to impose , and so underpin their commitment to meeting the performance criteria;

(h) consider and confirm the Contracting Authorities responsibilities.

5.6.1.3. In particular, proposals should include details on exemplar potential problem scenarios relevant to the services required, drawing out issues of risk, flexibility, and responsiveness in coping with changing situations. These scenarios should also be used to illustrate how problems will be identified and resolved, and the impact on the service minimised. The Service Provider should included at least one scenario where a post office, data network or central system is in a disaster situation e.g. a fire, and also scenarios where the service is operating in full or partial fall-back.

5.6.2 Specific Responses

I SR5.1 State any perceived dependencies between service levels that can be met by the Service Provider and the service levels of interfacing computer services and/systems (e.g. CAPS).

I SR5.2 State the upgrade paths available for the proposed solution within the proposed operating environment, clearly indicating the current (as at the time of the response) maximum capacity for the service.

I SR5.3 State how upgrades will be undertaken, whether they can be undertaken in the field and the steps in which the upgrade can be made.

I SR5.4 Describe the ongoing development programme to which the service proposed is subject, and state how it will provide an appropriate basis for the addition of new facilities and technologies.

I SR5.5 State the service levels that are proposed for the availability and reliability of the service at post offices; transaction transfer to and from client systems; and for interrogations from BA offices.

I SR5.6 State the service levels that are proposed for transaction response times and demonstrate that these will not adversely impact on current levels of service or business for POCL clients.

POL00028135

I SR5.7 State the service levels that could be attained concerning the following:

(a) call to fix time for equipment failure;

(b) helpline queue times;

(c) any other service.

I SR5.8 State how the service supplied can best be measured to facilitate payment.

I SR5.9 State how the service will enable the post office clerk accurately to pay valid payments even if technical equipment is not working, and to make payments in case of industrial action affecting the Service Provider or its sub-contractors.

I SR5.10 State how the CMS customer services will be provided and promoted.

I SR5.11 State recommendations for the training services that should be available for the steady state operation.

I SR5.12 State recommendations for customer education and marketing.

I SR5.13 State recommendations for the documentation that should be available for the steady state operation.

I SR5.14 State the level of project support that will be provided to support the steady state operations of the service, in terms of the number and qualifications of people assigned to the project, the proportion of their time which will be devoted to the project, and where they will be located.

I SR5.15 Describe the logistics for introducing new, or new versions of, software (including third party products) and in particular state how the following functions would be carried out:

(a) initiating and logistics planning of version change;

(b) testing;

(c) code control;

(d) implementation planning;

(e) authorisation to implement;

(f) implementation;

(g) regression in the event of problems;

(h) training and documentation revision;

(i) configuration management update.

POL00028135

I SR5.16 Describe the field engineering operation and in particular state:

(a) suggested call to fix times including any geographical differences;

(b) escalation levels and procedures;

(c) policies on "swap out" versus "on site repair" of faulty equipment;

(d) involvement, if any, with the recovery of any locally held software or data;

(e) arrangements for ensuring availability and confidentiality of any locally held data on equipment removed from post offices;

(f) involvement, if any, with the introduction of new, or new versions of, applications;

(g) any routine preventive maintenance requirements.

I SR5.17 State what, if any, involvement from Contracting Authorities' staff will be required in the following processes:

(a) introduction of new, or new versions of, applications;

(b) routine backup of any locally held software and/or data;

(c) hardware fault rectification;

(d) software fault rectification;

(e) communications fault rectification.

I SR5.18 State details of the management information to be offered as part of the service.

I SR5.19 Describe the reconciliation process for providing a complete, accurate, automated daily reconciliation between the Service Provider's system and those of the Contracting Authorities and propose methods to resolve discrepancies that do not increase Contracting Authorities costs.

POL00028135

CONTENTS

6. PILOT PROGRAMME

POL00028135

CHAPTER 6. PILOT PROGRAMME

6.1 INTRODUCTION

6.1.1. This chapter outlines the processes that will be used to prove that Service Providers can meet the service requirements. The first phase of the pilot programme, the demonstrator, will be used to satisfy the Contracting Authorities that all the final shortlisted Service Providers have a viable solution and can be invited to submit financial proposals. The second phase of the pilot programme, the operational trial, will be undertaken only with the selected Service Provider as the means to establish readiness for roll-out, and for the Contracting Authorities to test and accept the service.

6.1.2. Service Providers are invited to provide details of their approach to performing the pilot programme. These details should include an outline plan, checkpoints, acceptance points, descriptions of the deliverables and stages involved, and an estimate of any resources needed from the Contracting Authorities. Service Providers will be responsible for their own costs and any associated risks for both phases of the pilot programme.

6.2 THE DEMONSTRATOR PHASE

6.2.1 Objectives

6.2.1.1. The objectives of the demonstrator phase are to reduce the risks to the Contracting Authorities by giving them firm evidence of the Service Provider's capability and an understanding of the underlying technologies of the proposed service. The Service Provider should also give firm evidence during the demonstrator phase that they have a viable roll-out strategy.

6.2.1.2. The demonstrator phase will also provide the Service Provider with the opportunity to discuss and understand the business requirements in detail. The demonstrator will illustrate aspects of the business process and the underlying functional capabilities, the interfaces, (in particular the counter interface) and the technical solutions. The Contracting Authorities will also look to the Service Provider to propose and demonstrate the available options, so that they can provide guidance on their suitability. The demonstrator phase should also be used to show how other POCL requirements could be added to the initial service with minimum disruption and cost.

6.2.1.3. The demonstrator phase also gives an opportunity for the Contracting Authorities to build a working relationship with the Service Provider, and to assess his project management and organisational strengths.

6.2.2 Timescale

6.2.2.1. The demonstrator phase is planned to run in parallel with contract negotiations, stage 3 of the procurement.

POL00028135

6.2.3 The Process

6.2.3.1. The Contracting Authorities' evaluation team will be based in Terminal House, Victoria, London and a separate secure office in this building will be allocated to each Service Provider.

6.2.3.2. The evaluation team will consist of a full time project manager and personnel from POCL and BA with IT and business expertise that will include knowledge of application requirements and the associated audit functions. Additional persons will be drafted into the evaluation team or consulted as necessary, e.g. a training expert, a communications expert and representatives from the user population and customer groups such as Mencap, Aged Concern, the disablement lobby and ethnic groups. The evaluation team project manager will manage the pilot evaluation process for the Contracting Authorities, monitor progress against plans, arrange regular checkpoint meetings with Service Providers, arrange formal reviews of Service Provider deliverables and demonstrations, and manage the evaluation team.

6.2.3.3. The Service Provider will work closely with the evaluation team in an iterative process to assess the different technologies, ranges of platforms and options they propose to meet the requirements. Solutions being demonstrated must not be unduly restrained by the Service Provider's preference for their own product sets, technology or niche expertise. Service Providers are encouraged to provide two or more independent solution variants or options. Service Providers will be expected to design and develop prototype and "mock up" systems to demonstrate the functionality and suitability of their solution, and show that they understand the requirement. These prototypes should, as far as is practicable, simulate the use of the service and the component items in a user environment. Service Providers should note that all demonstrations should normally be held in the UK. The Service Provider will be responsible for the development of test data, but, subject to discussion, the Contracting Authorities will provide some assistance. Where it is not practicable to simulate the use of the service, the Service Provider should propose alternative ways of providing evidence of capability and understanding such as visits by the evaluation team to comparable live services or systems, or the production of paper-based analysis. During the demonstrator phase, the Service Provider will also be expected to present and elaborate upon their proposed exemplar roll-out models.

6.2.3.4. The evaluation team will develop a Risk Register for each Service Provider. The Risk Register will be based initially upon the Service Provider's proposal, and will be given only to the Service Provider to which it relates. During the pilot programme, the evaluation team will update the Risk Register as risks are addressed, or new risks emerge and will regularly review them with each Service Provider.

6.2.4 The Evaluation

6.2.4.1. The evaluation team will perform ongoing assessments of the demonstrations, advising on the suitability of options from those proposed. The evaluation team will use the Risk Register to record any weaknesses found and the Service Provider may also use this process as an opportunity to remove or reduce the classification of any outstanding

POL00028135

risks. At the end of this phase the Service Provider will be required to give a formal demonstration and the evaluation team will produce an evaluation report for senior management. This report, covering ongoing assessments and assessments of the formal demonstrations, and the Risk Register will be a major input into the overall evaluation process which concludes at the end of the draft contract negotiation stage, referred to as stage 3, see chapter 9.

6.3 OPERATIONAL TRIAL

6.3.1 Objectives

6.3.1.1. The objectives of the operational trial are to demonstrate that all aspects of the service are developed, that they have been formally tested, and to achieve final acceptance prior to roll-out and implementation.

6.3.1.2. The scope of the operational trial must be such that the Service Provider is able to demonstrate his ability to start the roll-out programme with the functionality, procedures, and the delivery mechanisms to provide a successful operational service.

6.3.2 Timescale

6.3.2.1. The operational trial is planned to run from January 1996 to May 1996. The Service Provider should confirm the feasibility of this timescale, or make other recommendations bearing in mind the overall timescale of the project given in chapter 9.

6.3.3 The Process

6.3.3.1. The exact nature of this phase of the pilot programme will be agreed during the draft contract negotiation stage, stage 3, see chapter 9. It is envisaged that the operational trial will run primarily in a simulated environment to provide end-to-end and volume testing, and to prove that service performance criteria can be met. At the end of this phase, it is currently envisaged that there will be a limited trial in a live environment to test the full functionality and customer acceptability of the service. It is expected that further refinements to the service will be made during this phase, and that these will be under formal change control. The operational trial will not just focus on the testing of the applications, but will include testing and demonstration of all supporting services such as help desks, training, contract management procedures and roll-out procedures. The Contracting Authorities evaluation team will manage this process, and will involve other interested parties.

6.3.3.2. It is expected that any development undertaken during the demonstrator phase will be used as the starting point for the operational trial.

POL00028135

6.3.4 Evaluation and Final Acceptance

6.3.4.1. A continuous evaluation process similar to that in the demonstrator phase will be undertaken by the evaluation team. The team will also conduct a formal acceptance process, the details of which will be agreed with the Service Provider during draft contract negotiations, stage 3, see chapter 9. The evaluation will cover all aspects of the service and, when completed, will signify the conclusion of the pilot programme.

6.4 THE PILOT PROGRAMME REQUIREMENTS

6.4.1 Introduction

6.4.1.1. An initial indication of the focus for the pilot programme follows. This section is subdivided into the various business needs that are to be addressed, and the particular business requirements for which the Contracting Authorities will require demonstrable evidence. These business requirements are not exclusive, but are to give guidance to Service Providers on the scope needed from their responses.

6.4.1.2. Service Providers should propose how they would prove or demonstrate their solution to the business requirements, and when this could be accomplished during the pilot programme, i.e. demonstrator phase, operational trial phase, or both.

6.4.2 Overall Prime Contractor Capability

6.4.2.1. The Contracting Authorities will be seeking to evaluate the overall prime contractor capability for:

(a) project and service management;

(b) quality of standards and procedures;

(c) understanding of the business and of the service requirements;

(d) cultural and commercial compatibility to work within both the BA and POCL business environments;

(e) flexibility and responsiveness to cope with change and fast roll-out;

(f) technical and logistical competence;

(g) speed of implementation.

POL00028135

6.4.3 POCL Prime Needs

6.4.3.1. POCL will wish to satisfy itself that the Service Provider will provide:

(a) flexible solutions that enable the Service Provider rapidly to take on further applications and / or higher volumes with minimal impact on the counter interface. For example:

i. post office applications, such as stock control,

ii. new business, such as further inpayment and outpayment applications,

iii. the ability to handle post office agents' private business, subject to appropriate security controls that prevent unauthorised access to client data (e.g. benefit payment details),

iv. support systems and reporting;

(b) a service which has the capability of being introduced to all post offices, irrespective of size or type, bearing in mind the current minimal range of automation;

(c) a secure, accurate and auditable accounting and reconciliation service;

(d) compatibility with the existing information systems strategy and interfaces with other POCL systems and methods;

(e) a service that will be easily understood by counter clerks;

(f) an approach that does not undermine customer trust in POCL, and improves on the quality of service to clients and customers;

(g) an approach that allows for the migration of existing systems with the minimum disruption.

6.4.4 Benefits Agency Prime Needs

6.4.4.1. BA will wish to satisfy itself that the Service Provider has:

(a) the ability to provide a reliable and consistent 'end-to-end' service for the payment of benefits via post offices;

(b) the ability to supply and manage a large scale card issue and management operation;

(c) a migration capability, in particular from the current benefit payment service to a card based service;

(d) proven methods for fraud reduction that are practical, politically and publicly acceptable;

POL00028135

(e) a secure, accurate and auditable accounting and reconciliation service.

6.4.5 Customer / Clerk Needs

6.4.5.1. POCL will assess the impact of the service on the counter clerk and the customer. In particular, the Service Provider must demonstrate that:

(a) the solutions will cope with a variety of post office accommodation (for example acknowledging space limitations and environmental conditions current in many small post offices);

(b) the proposed payment method is acceptable to customers, including the elderly, disabled and non English speaking claimants;

(c) the service can cope with a wide range of exception situations (for example lost or stolen, and damaged cards);

(d) there is contingency fall back in the case of full or partial system failures;

(e) the migration options in roll-out are acceptable to customers.

6.4.6 Training and Documentation

6.4.6.1. The Contracting Authorities will assess the Service Provider's training and documentation. In particular, the Service Provider must demonstrate:

(a) its capability for providing effective training for both the Contracting Authorities' staff and agents;

(b) the quality and standards of the documentation that will be provided;

(c) that it can provide effective documentation of the service for users, counter clerks and staff;

(d) its ability to integrate with existing systems and documentation.

6.4.7 Service Delivery

6.4.7.1. The Contracting Authorities will assess the ability of the Service Provider to deliver the service. In particular:

(a) that operational services can meet the full functionality requirements, with particular reference to the availability, audit, and responsiveness requirements;

(b) that the associated roll-out and support services are comprehensive, and that the interfaces are clearly defined and meet the availability and responsiveness requirements;

POL00028135

(c) that there are effective project and contract management procedures, for example change control procedures, service performance monitoring, and planning;

(d) that plans exist for contingency, fall-back and recovery;

(e) that the interfaces to the PAS, CAPS and POCL systems are accurate and auditable;

(f) that procedures exist for developing future requirements into a service;

(g) the Service Providers commitment to quality assurance, both prior to award of business and upon agreement throughout any contract period. In particular they must demonstrate to the Contracting Authorities their commitment relating to the quality of their procedures, processes, controls (including change control and quality control), manpower, software and equipment, e.g. in areas such as production, assembly, final inspection, dispatch/distribution. Contracting Authorities should have the right to conduct reference site visits to Service Provider sites in order to confirm quality assurance procedures.

6.4.8 IT Infrastructure

6.4.8.1. The Contracting Authorities will assess the proposed IT infrastructure. In particular, that:

(a) the technology has the capability to cope with increased volumes or increased functionality, for example adding peripherals such as CD-ROM and OCR;

(b) the solution adheres to industry and Health and Safety standards and is compatible with the Contracting Authorities' IT/IS strategies;

(c) the IT infrastructure can handle technology refresh and change without disruption, for example rate changes, new releases of software, and hardware upgrades;

(d) it has appropriate security;

(e) there is a workable configuration management service;

(f) measures have been taken to ensure data integrity and resilience.

Commercial Aspects

6.4.8.2. The Contracting Authorities will review any changes or options which may occur during the pilot programme that may have commercial implications. All the services that are contracted for must represent optimum value for money.

POL00028135

6.5 SERVICE PROVIDER'S RESPONSE

6.5.1 Proposal Content

6.5.1.1. The Service Provider should describe how he proposes to undertake the pilot programme. In particular, the Service Provider must:

(a) show evidence of ability and willingness to prototype solutions;

(b) define what aspects of the solution will be demonstrated during which phase(s) of the pilot programme;

(c) produce a matrix of the service elements that will be demonstrated during the pilot programme, referenced back to the descriptions of the solution in the other chapters, and referenced, where applicable, to supplementary evidence in the form of reference site visits to other services or like services.

6.5.1.2. The Service Provider must describe any dependencies on the Contracting Authorities actions or resources.

6.5.2 Specific Responses

I SR6.1 State any deviances from the requirements given in chapters 4, 5 and 7 relevant to the services to be used during the pilot programme.

I SR6.2 State the level of project support that will be provided pre-contract-award, in terms of the number and qualifications of people assigned to the project, the proportion of their time which will be devoted to the project, and where they will be located.

I SR6.3 State the service levels that can be attained during the operational trials.

I SR6.4 State any differences between the operational trials and the roll-out in respect of proposals for training, documentation, procedures and other support services.

I SR6.5 State how the Service Provider ideally sees the "Demonstrator" process taking place and in what environment.

I SR6.6 State the Service Provider's view of how the post-award final refinement of the service and "live" testing will take place and how the results will be monitored.

I SR6.7 State the Service Provider's view of how the post-award final refinement of the service and "live" testing will take place and how the results will be monitored.

POL00028135

CONTENTS

7. THE ROLL-OUT PROGRAMME

POL00028135

CHAPTER 7. THE ROLL-OUT PROGRAMME

7.1 INTRODUCTION

7.1.1. This chapter sets out the broad scope of the roll-out programme, identifying the key business imperatives from both the Contracting Authorities' perspectives. Service Providers are invited to propose and describe a number of exemplar roll-out strategies and implementation services, setting out any of their own constraints and dependencies which will impact the roll-out programme. The final roll-out strategy and detailed implementation approach will be decided in discussion with the Service Providers during the negotiation stage of this procurement.

7.2 TIMESCALES

7.2.1. Current plans indicate that the pilot programme should complete with a formal acceptance procedure by May 1996. The Service Provider would then enter the roll-out programme. It will be a formal project-based activity with an agreed final acceptance procedure, but it is accepted that there will be a need for a progressive number of staged acceptances throughout the roll-out programme. The actual priorities for roll-out of service will be agreed with the Service Provider. However it is anticipated that there may be benefits to the Service Provider in separating physical roll-out of infrastructure from that of the operational service. Hence there is scope for the Service Provider to offer to complete early implementation of the physical infrastructure well within 3 years from the successful conclusion of the pilot programme. Service Providers will realise from the objectives below that the Contracting Authorities place considerable potential value on the infrastructure roll-out being completed as early as possible.

7.2.2. Service Providers can assume that sufficient functionality of the CAPS system will be available by May 1996 to provide the primary input to the BPS. However the full range of customer claimant details for all benefits cannot be assumed, and priorities will need to be agreed with the Contracting Authorities.

7.3 OBJECTIVES

7.3.1. The objectives for the roll-out are identical to those given in the introduction, chapter 1 section 1.2. It will also be vitally important that any roll-out programme has the flexibility to cope with change, bearing in mind actual experience, and changing political and market drivers. Having the physical infrastructure in place early could, in itself, help achieve the desired flexibility. The ability of POCL to offer a nationally available and consistent automated network of counters could significantly add to its ability to attract new clients and services. The need for flexibility is further illustrated by the range of business imperatives discussed below. These business imperatives will also shape the roll-out programme.

POL00028135

7.4 CONSIDERATIONS FOR THE ROLL-OUT STRATEGY

7.4.1 The Contracting Authorities' Business Imperatives

7.4.1.1. The business imperatives which must be taken into account in determining the roll-out strategy are summarised below.

POCL Business Imperatives

7.4.1.2. The major business imperatives for POCL are:

(a) the importance of implementation of the infrastructure to all post office outlets (currently over 19,700) and the resultant advantages of being able to offer the benefits of a totally automated counter network to clients;

(b) that the roll-out programme is acceptable and easily understood by POCL staff and agents and is seen to be supporting the government policy of a national network of post offices;

(c) to protect and maintain the security of POCL staff, outlets, cash and value of stock before, during and after roll-out in accordance with agreed standards;

(d) to minimise the length and degree of disruption to current operations, systems, other POCL clients and processes. Account should be taken of the local trading pattern and surveys; equipment installation etc. should try to avoid busy periods such as Christmas and month ends; and installation should be co-ordinated with other initiatives;

(e) the migration or replacement of existing systems such as ALPS, ECCO+, APT, Capture and CRISP; in a way which ensures value for money as far as POCL are concerned;

(f) the success of the early roll-out in the area of customer and client satisfaction and presenting a positive image;

(g) satisfying the requirements of clients including BA and ensuring the appropriate prioritisation and development of other existing and new services;

(h) ensuring that the wide range of agency post offices are taken into consideration in determining roll-out plans;

(i) balancing the geographical implications with all the business imperatives given above;

(j) to ensure that the infrastructure can support the minimum application configuration at each post office (i.e. automated payments (migrated form APT), benefit payments, EPOS (migrated from ECCO+)) and connectivity to the remainder of the requirements;

POL00028135

(k) to ensure no adverse impact on quality of service forecasting or on service standards for clients.

BA Business Imperatives

7.4.1.3. The primary BA business imperatives are:

(a) the fastest possible roll out of BPS consistent with operational reliability and customer acceptability;

(b) the need to consider whether roll-out of the operational service should cover more than one type of benefit, whether it would be confusing for the customer to receive some benefits by an automated payment service and some by existing means and also to consider the advantages of a roll-out plan that converts groups of benefits that are often claimed together by the customer;

(c) consideration of the stability of legislation associated with particular benefits, including the likelihood of changes in legislation having a significant effect on the application, the timing of any such potential change and the ease with which it can be made, as these are obviously critical from both a business and political perspective;

(d) the mobility of customers and the importance of their being able to use more than one post office for claiming benefit will also impact on any decisions on a geographical roll-out plan;

(e) the need to maximise the reduction of fraud, considering which benefits and/or geographical areas are most at risk and the effectiveness of interim measures to combat fraud such as the ALPS project;

(f) the need to minimise duplication of costs during the transitional period by reducing the period:

- when order books for each of the major benefits are in issue i.e. there will be advantage in terminating all order books for a particular benefit;
- between issue of benefit payment cards and commencement of their operational use (thus minimising nugatory work on losses, change of circumstances, etc.).

7.4.2 Service Provider's Business Imperatives

7.4.2.1. It is accepted that Service Providers will also have certain business imperatives and constraints, some of which must be taken into account in developing a feasible low risk roll-out programme. In this context Service Providers are asked to set out their business imperatives and constraints, explaining why they should be taken into account together with those of both Contracting Authorities.

POL00028135

7.5 SERVICE PROVIDER'S RESPONSE

7.5.1 Proposal Content

Roll-Out Programme

7.5.1.1. Having discussed above the business imperatives from all perspectives, Service Providers will now appreciate the flexibility that will be required of a roll-out programme to support the main business drivers.

7.5.1.2. Service Providers are requested to provide an overview of their roll-out strategy and should justify the feasibility of their approach and the timescales. Service Providers should base their proposals on a range of appropriate exemplar roll-out models and plans, identifying the relative benefits, cost implications, risks and constraints associated with each option. In particular, Service Providers should outline the implications for a minimum timescale on the infrastructure roll-out, paying particular attention to their own constraints such as availability of engineering resources. It is important for Service Providers to identify and state all assumed dependencies with regard to both Contracting Authorities for each exemplar put forward within their proposal, particularly as it is envisaged that the Contracting Authorities' and Service Providers' roll-out teams will need to work in a collaborative way.

7.5.1.3. It is not expected, at this stage, that roll-out strategies will be definitive, but offer a basis for evaluation of the Service Providers' capabilities. The strategies will provide a sound framework for more detailed discussions throughout the course of negotiations. During these discussions the assumptions and commitments of both parties will be agreed and a practical roll-out programme and definition of roll-out services will be embodied within the contract.

Roll-Out Services

7.5.1.4. Within the context of the overall roll-out programme it is envisaged that a number of defined services will be required including:

(a) site surveys;

(b) cabling;

(c) installation of hardware;

(d) ordering of infrastructure and operational services;

(e) installation and acceptance of infrastructure and application;

(f) acceptance of new customers and applications onto the help desk service;

(g) management of change services including:

i. training requirements for users, the Contracting Authorities' staff and agents,

POL00028135

ii. customer awareness processes, particularly for special needs customer groups as required by the overall Communications Strategy project,

iii. introduction of new application services,

iv. major change to existing services and infrastructure.

7.5.1.5. Service Providers should define the roll-out programme around a range of discrete but inter-related services. Each service should be described in terms of scope and functional capability.

Experience and Capability

7.5.1.6. Service Providers should provide a description of how they would organise and manage the delivery of such services, explaining the underlying processes of each service. Past and current experience of developing and delivering similar services should be provided, particularly in environments having similar scale and, where possible, in retail or financial services. References should be provided where Service Providers can demonstrate through reference site visits such experience and capability.

7.5.2 Specific Responses

I SR7.1 State any deviances from the requirements given in chapters 4 and 5 relevant to the services to be provided during the roll-out.

I SR7.2 State roll-out arrangements for the provision of benefit payments and other POCL services to customers who may choose to use more than one outlet, some having the service available and some not.

I SR7.3 State roll-out proposals for the provision of training giving details of the types, duration and target audience of the training that Service Providers consider will be needed at each stage of the roll-out.

I SR7.4 State roll-out proposals for the provision of documentation giving details of types, quantities and potential users of the documentation that will be needed at each stage of the roll-out.

I SR7.5 State the level of project support that will be provided during the roll-out period, in terms of the number and qualifications of people assigned to the project, the proportion of their time which will be devoted to the project, and where they will be located.

I SR7.6 State any differences between proposed service levels for the steady state and roll-out period;

I SR7.7 State roll-out proposals for post offices.

POL00028135

CONTENTS

8. COMMERCIAL POLICIES AND RELATIONSHIPS

POL00028135

CHAPTER 8. COMMERCIAL POLICIES AND RELATIONSHIPS

8.1 INTRODUCTION

8.1.1. This chapter sets out the Contracting Authorities' approach to the development of the commercial relationship with the Service Provider. It describes models which would meet the Contracting Authorities' requirements and in addition invites Service Providers to suggest other options. It is expected that extensive discussions will be required between BA, POCL and the Service Provider to develop appropriate commercial frameworks.

8.2 COMMERCIAL PRINCIPLES

8.2.1. The following principles will be applied by the Contracting Authorities in assessing proposals from potential Service Providers and in helping to prepare business cases. They are in no particular order and the list is not exhaustive.

8.2.2. A main objective of the development is to minimise the overall cost to the public sector as a whole, taking an end-to-end view and assessing the impact on public expenditure.

8.2.3. The service must offer the Contracting Authorities, and also allow POCL to offer all its business partners (clients, agents and franchisees), a high degree of integrity, probity, financial control and confidentiality for both clients and customers.

8.2.4. The Service Provider's charges must be reconcilable to the services provided, so that POCL can take this into account when pricing particular products and client services, and so that BA can fully account for expenditure and price their services. The Contracting Authorities will require a mechanism for ensuring that agreed pricing formulae for the contract(s) are being correctly applied; and that there is no cross-subsidy between different elements of the service.

8.2.5. The Contracting Authorities will require the ability to add further applications to the service. These may be sourced from third parties or from the Service Provider. The Service Provider must be willing to integrate and operate these via the original service contract(s).

8.2.6. Without prejudice to BA's right to market the benefit payment service at post offices, POCL will control the rights for using and marketing the services offered through the facilities provided by the Service Provider in post offices, i.e. the Service Provider will not contract directly with agents or other third parties for use of these facilities. It is expected that the Service Provider will assist in identifying, suggesting and helping develop new services to use these facilities. POCL must be free to use the service to transact business for any existing or future client (even if that client is a competitor to the Service Provider or to a member of a supplying consortium), subject to full security and service delivery safeguards for existing clients.

POL00028135

8.2.7. It is Government policy to:

- provide choice in the method by which customers can receive their Social Security payments; namely through the banking system, or by collection from a post office;
- maintain a nationwide network of post offices.

8.2.8. Contract(s) under this procurement will not be written so as to constrain development of government policies in respect of payment or a nationwide network of post offices.

8.3 CONTRACTUAL MODELS

8.3.1 Introduction

8.3.1.1. The Contracting Authorities wish to consider options under which their business requirements can be met by a service contract or contracts which conform to the requirements of the Private Finance Initiative (PFI). In addition, the Contracting Authorities wish to obtain sufficient information in response to this SSR to enable them to compare any privately financed procurement option with more conventional public sector procurement alternatives and have the option to contract for some or all of the services on these alternative bases. Comparison of all such options will be on the basis of the overall economic advantage of the total package, taking account of costs, benefits, and the extent to which risk is reduced and transferred to the Service Provider.

8.3.1.2. Accordingly, the Service Provider must submit proposals on the basis of a privately financed contractual model, and must show these separately for the various components of the system, e.g. CMS / PAS / Counters Infrastructure, on the following lines:

- the Service Provider will buy the assets required to provide the service using private capital and will own and operate them, charging the Contracting Authorities fees, related to the usage of the service, for the services they each receive;
- other privately financed contractual models might be suggested also. See sections 8.3.3 to 8.3.6 below.

8.3.1.3. In addition, the Service Provider must indicate the financial and other implications of alternative proposals on the basis of a more conventional public sector contractual model, and must show these separately for the various components of the services e.g. CMS/PAS/Counters Infrastructure on the lines of:

- The Service Provider will design, build and operate the service. The capital assets required to provide the service will be funded and owned by the Contracting Authorities for their respective requirements. The Service Provider will then charge an operating fee for running and maintaining the service;
- See sections 8.3.7 and 8.3.8 for further discussion of this non-PFI approach.

POL00028135

8.3.1.4. The Service Provider may also offer hybrid proposals in which different parts of the service are provided on different bases of financing. In evaluating such hybrid proposals, the Contracting Authorities will look at the economic advantage of the overall package.

8.3.2 Contract Structures

8.3.2.1. Elements of the service may be contracted with either Contracting Authority or both at the discretion of the Contracting Authorities.

8.3.3 Supply of Services under the PFI

8.3.3.1. Service Providers are reminded of the principles of the PFI which were set out in Chapter 6 of the prospectus issued to them on 5 October 1994.

8.3.3.2. The Service Provider must put forward a proposal to meet all requirements under the SSR. That is, where the Service Provider designs, develops, implements and subsequently enhances, operates and maintains, the respective parts of the service for the sole use of the Contracting Authorities. Under such contract(s), the Contracting Authorities would pay to use the service according to a pre-determined tariff, with payments largely based on usage but which may also include other elements such as service performance related payments or payments related to growth.

8.3.3.3. Under such a service supply arrangement, POCL would lead in developing new business to utilise the infrastructure and counter service facilities provided, developing a number of "partnerships", possibly taking the form of joint ventures, with existing and new clients. POCL may also invite the Service Provider or individual members of a service- providing consortium to take part in some of these business development partnerships, and proposals should indicate whether or not, and on what basis, the Service Provider would wish to participate. In developing the use of the service, POCL will wish to use the best products available from the market place and will want to ensure that the service supply contract(s) facilitates this, including cases where the solution for a particular application involves a different supplier being used. Thus adherence to open technical standards and a corresponding contractual framework are both highly desirable.

8.3.3.4. The Service Provider is also invited to propose arrangements under which it and POCL jointly market products using elements of the infrastructure and counter service and share the profits from this. The Service Provider may wish to consider such arrangements, including joint ventures, which cover the whole service to POCL (i.e. provision and operation of the service and its further commercial exploitation).

8.3.3.5. The Service Provider may also propose arrangements under which it retains the rights to use and market hardware or software or facilities developed for this service for other applications. Such proposals should show whether this would result in lower prices for services to the Contracting Authorities, either through an initial lower price or via agreed formulae for price reductions related to such other uses. In considering such proposals, the Contracting Authorities will require safeguards to ensure that their

POL00028135

commercial and operational interests are not damaged. These safeguards may take the form of contractual terms based on Intellectual Property Rights, which define the geographical areas and markets in which the Service Provider may do this, and/or by the Contracting Authorities having the right to vet individual cases.

8.3.3.6. The Service Provider may also propose any other commercial structure which it considers may be of benefit to all parties.

8.3.4 Funding of Services Provided

8.3.4.1. The Service Provider must set out its preferred approach to funding the services within the terms of the PFI. The proposal must indicate whether the Service Provider will fund them from its own resources. If the Service Provider proposes using an external source of finance the proposal must set out how this will be arranged and the contractual relationships which are envisaged between the Service Provider, the capital funder and the Contracting Authorities.

8.3.5 Charges for Services Provided under Privately Financed Options

8.3.5.1. The proposal must explain the charging structure which the Service Provider envisages for each of the contractual models included in the proposal. Service Providers may present options, but must include at least one charging structure with volume/usage-related prices as its major element for each component of the service (e.g. CMS/PAS/Counter Infrastructure). Responses should include the Service Provider's approach to pricing for the development and operation of additional services which either or both of the Contracting Authorities may wish to add to the service, as described at section 8.3.3 above. This should take account of the need to allow for future implementation of requirements which are not part of the initial go-live service requirement, but which are currently known, and also the need to accommodate new requirements which are identified during the course of the contract(s).

8.3.5.2. The Service Provider may propose other charging mechanisms.

8.3.6 Risks Transferred to the Private Sector under Privately Financed Options

8.3.6.1. In procuring this service under the PFI, the aim will be to minimise risk and place it where it can most effectively be managed. This means that the total risk left with the Contracting Authorities must be at a minimum commensurate with value for money, and that significant risks must be borne by the Service Provider. Such risks could include:

- cost and timescale of service development and delivery;
- operating cost and service performance;
- consequential costs of service performance.

POL00028135

8.3.6.2. The payments to the Service Provider must, to a large part, depend on the usage of the service. Proposals must demonstrate how charging mechanisms for each major component of the service depend on throughput (service providers to define their throughput metrics) and must indicate the nature of minimum volumes required, if any.

8.3.6.3. Proposals must show how the service will eliminate fraud and how the Service Provider would take responsibility for this being achieved. Service Providers must undertake responsibility for fraud losses which result from errors in their design, implementation or operation of the service, including unauthorised actions by their staff or sub-contractors.

8.3.6.4. Proposals should include the extent to which Service Providers will accept the transfer of risks associated with the Contracting Authorities' operation of the service, risks associated with the copying, forging or alteration of cards, and risks associated with "hacking".

8.3.6.5. Where the Service Provider is proposing a joint venture approach for part or all of the service to POCL (as in section 8.3.3 above), its proposals should show the extent to which the commercial risks of such a joint venture lie with the Service Provider.

8.3.6.6. Proposals should show any other areas in which the Service Provider would accept risks currently managed and borne by the public sector.

8.3.6.7. Proposals must show the Service Provider's approach to managing the risks for which it is undertaking responsibility. This must include contingency plans and must demonstrate that the Service Provider has the financial resources available (in-house or through an insurance arrangement) to meet any resulting liabilities.

8.3.6.8. Proposals should set out a number of options for the level of risk which the Service Provider would accept and the effect of these on costs. Each option should show the risks for which the Service Provider would accept responsibility and their approach to risk management.

8.3.7 Development and Operation of a Publicly Owned Service

8.3.7.1. In addition to their privately financed options, Service Providers must set out their approach to publicly funded bases for each component of the service, e.g. CMS/PAS/Counters Infrastructure. This would be on the basis of separate but linked arrangements as follows:

(a) The Service Provider designs, supplies and builds a turnkey system(s) (including roll-out) to meet the business requirements, technical standards and policies set out in this document and to be amplified and agreed during subsequent discussions;

(b) The Service Provider runs the service on a facilities-management basis.

8.3.7.2. The Service Provider should set out its approach to charging for the development and operation of the service. This should state whether it is proposing a single

POL00028135

reimbursement of capital costs on delivery and acceptance of a working, turnkey service, or whether it would require any staged payments during development.

8.3.7.3. The Service Provider should set out its approach to charging for facilities management.

8.3.7.4. Responses must include the Service Provider's approach to pricing for the development and operation of additional services which either or both of the Contracting Authorities may wish to add to the service, as described at section 8.3.3 above.

8.3.7.5. The Service Provider may propose other approaches to public-sector owned solutions and their charging mechanisms for them.

8.3.8 Risks Transferred under Publicly Funded Options

8.3.8.1. The Service Provider should set out the extent to which it is prepared to accept the risks associated with the development and operation of the service (as outlined in section 8.3.6). It is required that the Service Provider accept responsibility for risks in all areas under its control.

8.3.8.2. Under the design and build contract, the Service Provider must accept all risks associated with timescale and cost over-run in developing an agreed turnkey service.

8.3.8.3. Under the facilities management approach, the Service Provider must provide guarantees of service performance and indemnify the Contracting Authorities against costs caused by failure to meet agreed service levels.

8.4 INTELLECTUAL PROPERTY RIGHTS (IPR) AND DATA OWNERSHIP

8.4.1. In order to safeguard their services to the public and their commercial interests the Contracting Authorities will require appropriate arrangements with the Service Provider covering IPR and Data Ownership.

8.4.2. Arrangements for the provision of this service will not give the Service Provider rights to ownership or use of the data in other applications except by explicit agreement of the relevant Contracting Authority. In particular the Contracting Authorities will require confidentiality undertakings from the Service Provider both to ensure the confidentiality of personal information about customers and to ensure that the security of the system is not compromised.

8.4.3. The Contracting Authorities will require an agreed framework for Intellectual Property Rights in the systems developed to provide this service, which safeguards both the Contracting Authorities' operational requirements and commercial interests during and after the contract(s).

8.4.4. The Contracting Authorities will require contractual arrangements which safeguard continuity of service, including rights to acquire source code of any licensed software necessary to provide the service and rights to take over licences to any third party software in the event that the Service Provider fails to provide an adequate service.

POL00028135

8.4.5. POCL will require the exclusive right based on IPRs to use the facilities which the Service Provider installs in post offices. In exercising this right, POCL will seek to maximise benefits from the services available from the Service Provider.

8.4.6. Either or both of the Contracting Authorities, as appropriate, require the right to control the use of cards or other tokens issued to the public for benefit payment or other transactions at post offices. In particular, the Service Provider must not itself offer services which would use such cards at other locations. The use of the National Insurance Number will be controlled by the Secretary of State for Social Security.

8.4.7. Either or both of the Contracting Authorities may require the IPR and source code of any bespoke software developed to provide the service. Should the Service Provider wish to market such software, then subject to satisfactory safeguards on system security, the Contracting Authorities would wish to consider this in return for agreed lower costs.

8.4.8. The Service Provider may propose arrangements under which it can exploit software developed for this service in other contexts, to the mutual advantage of the Service Provider and Contracting Authorities. The Contracting Authorities will wish to encourage such arrangements provided that they are compatible with their commercial interests and operational requirements including security.

8.4.9. Either or both of the Contracting Authorities will require Intellectual Property Rights covering the design, branding and procedures associated with the benefit payment process, and POCL (with its other clients in some cases) will require similar rights associated with other products transacted at post offices. Service Providers should note that the Contracting Authorities will not allow any unauthorised use of any POCL or Post Office, nor of any BA, DSS or other government trademarks, brands, logos etc. in any advertising, PR, or promotional material either in the UK or in any other country.

8.4.10. Where the Service Provider proposes developing facilities for the delivery of the system which may be applicable in other contexts and are not specifically related to the BA and/or POCL business requirements, then it would be appropriate for the Service Provider to exploit those facilities for other business and the proposal should state this and indicate the extent to which the Contracting Authorities can expect lower costs as a result of it. This may be expressed as a lower initial price or as an agreed price reduction formula.

8.5 RE-TENDERING, RESIDUAL VALUES, AND TRANSFER OF ASSETS

8.5.1. In order to ensure continuing value for money, the Contracting Authorities may wish to re-tender for the supply of all or part of the service after the initial contract period.

8.5.2. The Service Provider should respond on the basis of a contract(s) lasting five years from the contracted date of completion of the implementation of the service.

8.5.3. In the event that the initial Service Provider did not wish to continue providing the service after the contract period, or was unsuccessful in re-tendering, the Contracting Authorities would wish to ensure the smooth transfer of a "going concern" service to

POL00028135

another operator or operators or in house. The Service Provider must set out its proposals for how this could be achieved from a commercial viewpoint. (See also Chapter 5 which sets out requirements from an operational perspective.)

8.5.4. As a consequence the Service Providers should develop its responses on the basis that it will not recover all its costs from service charges during the initial contract and that residual values will be reflected in a terminal charge dependent on performance. Service Providers' proposals should consider approaches which include pre-determined formulae for calculating the transfer values of assets to a subsequent contractor, or in-house, and approaches under which the assets are vested in a company created for the purpose which could itself be transferred to a subsequent contractor or in-house. Cost areas where full recovery of investment during the initial service period would be inappropriate include, for example:

- major bespoke software development for central services and communications;
- hardware with more than 25% of its expected operational life outstanding at the end of the contract(s);
- new developments and upgrades to the service introduced within 3 years of the end of the contract(s).

8.5.5. For reasons of operational feasibility, the Contracting Authorities will require the right to have all the hardware and licences to use package software in post offices or elsewhere transferred to a subsequent contractor or to the Contracting Authorities themselves at the determination of the contract(s).

8.6 EARLY TERMINATION OF CONTRACT

8.6.1. The Contracting Authorities will require reserved rights so that if the Service Provider fails to provide the contracted service or gives other grounds for early termination of the contract, then the Contracting Authorities will take over the operation of all or part the service, or appoint a third party to operate it on their behalf, including all hardware, software, communications facilities, and infrastructure which they deem necessary for the operation of the service.

POL00028135

8.7 SERVICE PROVIDER'S RESPONSE

8.7.1 Proposal Content

8.7.1.1. The Service Provider's response should adopt the same section headings as 8.1 to 8.6 above.

8.7.2 Financial Information

8.7.2.1. Service Providers are required to provide indicative financial information, but not final prices, in their proposals. Such information will not constitute an offer by the Service Provider but will assist the Contracting Authorities to review thoroughly the investment aspects of their business case(s) and at a later date facilitate further discussion with the Service Providers over the strategic direction of proposed solutions, particularly in relation to the efficiency and overall viability of the project. In the final stages of the procurement, price and overall costs to the Contracting Authorities will be highly relevant factors. Therefore in providing the information Service Providers should take note of the objectives of the programme detailed in Chapter 1, particularly those relating to:

(a) reducing administration costs of the benefit payment system;

(b) eliminating fraud and controlling residual liabilities;

(c) improving overall efficiency and cost effectiveness for POCL and its clients;

(d) at least maintaining, if not improving, overall customer service.

8.7.2.2. The investment appraisal aspects of BA's business case will examine the current administration costs of the end to end system for making payments through post offices against the costs of an automated service through post offices. Savings of Social Security benefit payments arising from the elimination of fraud are unlikely to be included in the basic assessment of net costs or benefits though remaining opportunities for fraud or potential new areas for fraud will be included in the review of risks.

8.7.2.3. Indicative financial information should cover:

(a) proposed approaches to charging structures for components of the service (i.e. CMS / PAS / TMS / Counter Infrastructure), for both private and publicly funded options. Within the response the Service Provider should assume that the Contracting Authority for the CMS will wish to own (i.e. purchase) the benefit payment card, as part of the contract arrangements. If a Service Provider sees any difficulty with this approach the problem(s) should be identified within their response;

POL00028135

(b) differences between a service based around minimum requirements of the BPS, EPOS/ECCO+ and automated payment functionality and a service based on a generic approach. Any additional (costed) alternative approaches would also be welcome;

(c) indicative financial information (one-off and running costs) by major cost element for each component, e.g.:

- hardware;
- software development and licences;
- telecommunications;
- consumables;
- other, e.g. training and help desk facilities;

(d) preferred approach to funding the service;

(e) the financial resources available to meet liabilities for the assumption of risk.

POL00028135

CONTENTS

9. PROCUREMENT REQUIREMENTS

POL00028135

CHAPTER 9. PROCUREMENT REQUIREMENTS

9.1 INTRODUCTION

9.1.1. This chapter sets out the procurement process and describes the actions to be taken by service providers in response to this SSR. The structure of the chapter is as follows:

(a) Administration and Logistics, which describes the contact points for queries and the return address for the SSR, numbers of copies etc.;

(b) Procurement Process and Timetable;

(c) Evaluation, which describes the evaluation approach for proposals in response to this SSR;

(d) Proposal Format and Content.

9.2 ADMINISTRATION AND LOGISTICS

9.2.1 Submission of Proposals

9.2.1.1. Service Providers are to respond to this SSR by preparing a proposal document and submitting it as follows:

(a) prepare the proposal with the structure and content described below in section 9.5. Proposal Format and Content;

(b) provide sixteen copies of the proposal on paper, plus a copy on 3.5" floppy disk in Microsoft Word 6.0 for Windows format;

(c) seal the proposal material in an envelope or package with the reference number (94/S 165-58937/EN) clearly indicated on the back; and

(d) send it to Patrick Sedgwick to be received at the address below by 12.00 noon on 15th May 1995.

9.2.1.2. The only form of response permitted will be in English and delivered to the stated address. Faxed responses will not be permitted. The Contracting Authorities reserve the right to reject responses received after the above deadline or that do not provide the required information.

9.2.1.3. Both the SSR and parts of the Service Provider's proposal may form part of the contract(s) and therefore should be reviewed at appropriate legal and managerial level before submission.

POL00028135

9.2.2 Contacts and Queries

9.2.2.1. All queries with respect to this procurement must be directed to:

Patrick Sedgwick
BA/POCL Response Unit
Third Floor
Terminal House
50 - 52 Grosvenor Gardens
London
SW1W OAB

Telephone: GRO
Facsimile: GRO

9.2.2.2. All contact must be initiated through the authorised individual named above. Informal contacts are not permitted and may lead to disqualification from the procurement. POCL wish to emphasise that any proposed contact with their clients and agents in respect of this procurement must be channelled via the above contact.

9.2.2.3. Service Providers are reminded that any public statements made through the press or elsewhere about this procurement should be cleared with the above contact.

9.3 PROCUREMENT PROCESS AND TIMETABLE

9.3.1 Procurement Process

9.3.1.1. Of the five stages identified for procurement in the Request for Statement of Capability, *Stage 1 Establish Playing Field* is now complete. The remaining stages are set out below with indicative timescales.

Stage 2 - Innovation and Clarification ***(Nov. '94 -May '95)***

9.3.1.2. This is the current stage. Its objective is to assess the viability of Service Providers' approaches by evaluating their detailed proposals for development, technology, service provision, management, resourcing etc. The stage will set the basis for the contract negotiations and involves the issue of this SSR to which Service Providers are to respond with written proposals. This stage will finish with a review of the architecture and standards requirements, taking into account industry input. Shortlisted Service Providers will be invited to enter into contract negotiations in parallel with undertaking their demonstrator programme.

Stage 3 - Contract Negotiation / Pilot Commencement ***(Jun. - Oct. '95)***

9.3.1.3. The objectives of this stage are to agree draft contracts and to develop the tender evaluation model. This stage will involve meetings to discuss the draft contracts and model workloads to be used in the evaluation model. Demonstrations of proposed

POL00028135

solutions based on a Demonstrator programme and reference site visits will occur in parallel with the negotiations. This process is aimed at evaluation and risk assessment of the potential solutions and is part of the overall procurement risk reduction process.

Stage 4 - Evaluation and Selection ***(Nov. - Dec. '95)***

9.3.1.4. During this stage Service Providers will be asked to submit financial proposals on the basis of the agreed draft contracts. These will be evaluated, and at the end of the stage the prime contractor(s) will be selected.

Stage 5 - Operational Trials ***(1996)***

9.3.1.5. Following selection of the prime contractor(s), the operational trials will commence (details of which will have been agreed during Stage 3 Contract Negotiation) to refine and prove the final solution for the service provision, to establish the detail of the roll-out programme and associated change management processes. The timescales are to be agreed during Stage 3 Contract Negotiation.

9.3.2 Timetable

9.3.2.1. The following table provides the indicative timetable following the issue of the SSR. The Contracting Authorities will use all reasonable endeavours to comply with this timetable and with any revision thereof which may subsequently be notified to potential Service Providers during the course of procurement. However, neither this timetable nor any subsequent revision thereof shall be taken as constituting a contract, agreement or representation that the procurement will be conducted in accordance therewith, and the Contracting Authorities accept no responsibility for any delay in meeting this timetable (or any subsequent revision thereof) or for any costs that may be incurred by potential Service Providers as a result of such delay or otherwise.

	Activity	Week
i.	Issue SSR	1
ii.	Receipt of Service Providers' proposals	8
iii.	Proposal evaluation	9 to 15
iv.	Service Providers shortlisted for negotiations	15
v.	Negotiation of draft contracts and schedules, plus Demonstrators and risk assessment	16 to 37
vi.	Complete Demonstrators and risk assessment	34
vii.	Agree draft contracts	38
viii.	Invitation to submit financial proposals	39
ix.	Receipt of financial proposals	41
x.	Select intended prime contractor(s)	46

POL00028135

9.3.2.2. The above timetable covers the activities up to the end of Stage 4. Following this, the selected prime contractor(s) will then undertake Stage 5 Operational Trials in accordance with the timescales agreed during the negotiations, the basis for which is set out in chapter 6.

9.4 EVALUATION

9.4.1 Evaluation Approach

9.4.1.1. This section describes the evaluation approach for Service Providers' proposals and the implications for their content. The approach is based on the use of predetermined formal evaluation criteria against which each proposal will be scored. These scores will then be combined by a pre-specified formula to position the proposals on an evaluation grid, in a similar way to the Statement of Capabilities, and the results used for the shortlisting decision. The grid and the evaluation criteria are described further after the next sub-section which discusses the three types of information required in proposals.

9.4.1.2. The proposal evaluation will be based upon the written responses from Service Providers. While some minor clarification may be undertaken following receipt of proposals, failure by the Service Provider to document his proposal clearly is likely to result in a poor rating in the evaluation.

9.4.2 Information in Proposals

9.4.2.1. The evaluation will be looking for three types of information in Service Providers' proposals. These are:

- "what"
- "how" — Characteristics as seen by service users
- "proof" — Evidence of viability as seen by experts

9.4.2.2. It is important that the Service Providers understand the distinction between these types of information and how they support each other, so that they are included in the proposals. Hence these are explained further below.

"What" and "How"

9.4.2.3. Information about the "what" and "how" relates to the service boundary as shown in Figure 9-1 The Service Boundary.

POL00028135

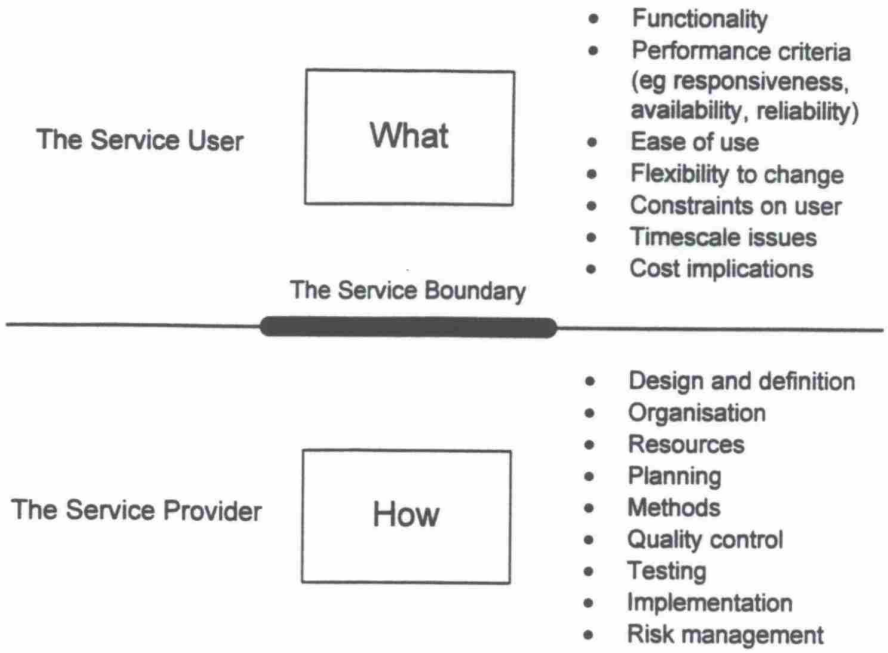


Figure 9-1 The Service Boundary

9.4.2.4. Information about the "what" is above the service boundary and describes what services are to be delivered by the Service Provider from the perspective of the user of the services and the Contracting Authorities. Information about the "how" is below the service boundary and describes "how" the service provider will undertake the development and provision of the services.

9.4.2.5. Following the award of any service contract(s), "how" the Service Provider undertakes the service provision and his internal management and control processes should be a matter for the Service Provider's management team. This is on the basis that "what" services are delivered meet the contracted specifications. However it is important for the Contracting Authorities to understand "how" Service Providers propose to develop and deliver their services to enable proposals to be evaluated and for possible inclusion in any contract(s).

"Proof"

9.4.2.6. In addition to information about "what" services are to be delivered and "how" they are to be provided, it is important that Service Providers provide "proof" that their proposals are feasible. In the evaluation of Statement of Capabilities, the "proof" focused primarily upon track record. For the proposal evaluation, "proof" is extended to consider the overall feasibility of the proposal which will not only consider relevant track record, but also factors such as relevant references, examples of where similar approaches have been successful before, formal certifications and approvals.

POL00028135

9.4.3 Evaluation Selection

9.4.3.1. While the preceding sub-section covered the type of information required in proposals, this one addresses how the shortlist is to be identified. As mentioned above, the proposals will be scored against formal evaluation criteria and the results plotted on an evaluation grid. To do this, the evaluation criteria are divided into two categories:

- Characteristics, and
- Viability.

9.4.3.2. The "characteristics" of a proposal will be assessed on "what" services are proposed (e.g. their structure, content and performance criteria) and certain aspects of "how" these are to be provided. The relevant aspects of "how" will be those where the Service Provider has explained the implications of a particular approach or solution for the service users (e.g. implied functionality and flexibility, speed of implementation).

9.4.3.3. The "viability" of a proposal will be assessed on the evidence that the Service Provider provides to prove that his proposal is feasible and his proposed services can be provided as he has described them. This category will be assessed on the "proof" type information in the proposal (e.g. evidence of having done it before) and certain aspects of "how". In this case, the relevant aspects of "how" will be those where it provides a logical explanation underpinning the services to be delivered, such that this would be convincing to an expert. For example: describing the design approaches to show how aspects of functionality and flexibility would be achieved; offering exemplar plans illustrating resources and timescales to achieve specific deliverables; describing the processes and organisation that would be used to manage and deliver service. Where "viability" cannot be fully shown in writing, then the Service Provider will need to explain what actions would be taken to prove his approach following shortlisting (e.g. by references and demonstrations).

9.4.3.4. The scores for each evaluation criteria will be combined by pre-specified formulae and weights into a score for "characteristics" and a score for "viability" for each proposal. These scores will then be used to plot the position of each proposal on a proposal evaluation grid. An example of this is shown in Figure 9-2 Proposal Evaluation Grid.

POL00028135

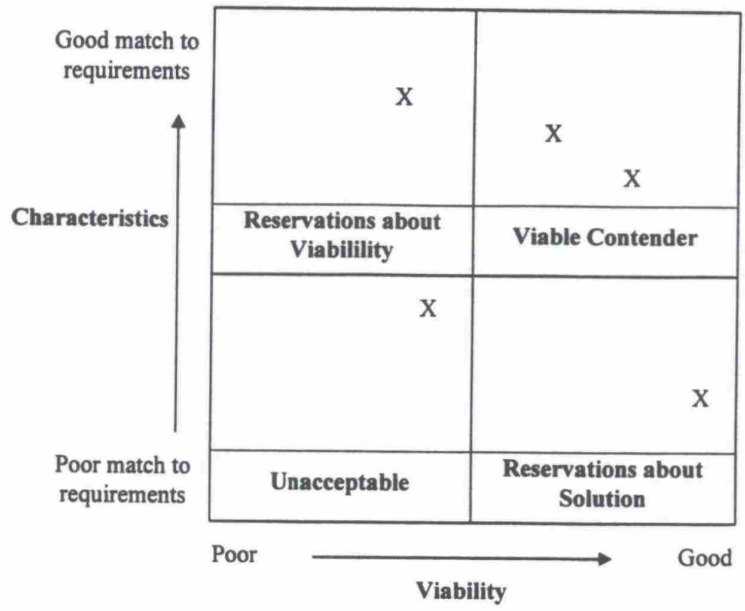


Figure 9-2 Proposal Evaluation Grid

9.4.3.5. A proposal may fall into one of the four boxes as follows:

(a) Reservations about Viability

This indicates the proposal, while overall a good fit to the requirements, has insufficient evidence to substantiate the proposed solution (or that the services could not be implemented as described).

(b) Reservations about Solution

This indicates the proposal document has been well constructed and the proposed services shown to be viable; however the proposed services do not provide a good fit to the requirements.

(c) Viable Contender

This indicates the proposed services both provide a good fit to the requirements and are shown in the proposal to be a viable option.

(d) Unacceptable

This indicates an unacceptable set of services not properly substantiated in the proposal.

9.4.3.6. The natural choice for the negotiation shortlist is for Service Providers whose proposals fall into the "Viable Contender" box. However there are associated factors that will be taken into consideration, for instance the number on the shortlist (if too many or too few Service Providers fall into this area), and the specific strengths and weaknesses of each proposal.

POL00028135

9.4.3.7. In addition, a separate evaluation of the Service Provider's commercial response to chapter 8 will be undertaken to assess whether his initial proposals offer a reasonable basis for further discussion. Any costs provided in response to the SSR will be treated as indicative and will be used for budgetary and business case purposes only.

9.4.4 Evaluation Criteria

9.4.4.1 Throughout the procurement, the Service Providers and their proposals will be assessed against objective evaluation criteria to select the most economically advantageous solution. These evaluation criteria relate to how well these proposals support the business objectives for the overall programme. These were introduced in the prospectus and the Request for Statement of Capability, and a comprehensive set of objectives is provided in chapter 1.

9.4.4.2 The evaluation criteria for proposals are based upon the requirements set out in chapters 4 to 8. These reflect the business objectives which are also used to set the relative importance of the criteria. The generic headings under which evaluation shall take place include, but are not limited to, the bullet points shown in Figure 9-1 The Service Boundary. The Contracting Authorities will also have regard to all other shortlisting criteria to which reference is permitted under EC/GATT procurement rules.

9.5 PROPOSAL FORMAT AND CONTENT

9.5.1 Proposal Structure

9.5.1.1. This section describes the required format and content for the Service Provider's proposal.

9.5.1.2. The overall structure of the proposal shall be as follows:

		Indicative size (A4 sides)
1. Management Summary		10
2. Introduction		5
3. The Service Provider		15
4. Services and Systems Architecture	(response to chapter 4)	150
5. Steady State Services	(response to chapter 5)	50
6. Pilot Programme	(response to chapter 6)	50
7. Roll-out and Implementation	(response to chapter 7)	50
8. Commercial	(response to chapter 8)	50
Annexes		--
	(contingency on size)	50
TOTAL		430

9.5.1.3. The indicative sizes shown for proposal sections are not expected to vary by more than about 10%, and the overall length of the proposal should not exceed 430 sides of A4 paper. The sizes of the annexes are not included within the indicative page count;

POL00028135

however the Contracting Authorities cannot undertake to read all annex material for the proposal evaluation.

9.5.1.4. The proposal sections 1 to 3 are explained in 9.5.2 to 9.5.4 respectively.

9.5.1.5. Proposal sections 4 to 8 (the responses to Chapters 4 to 8) are explained in 9.5.5 below.

9.5.1.6. The annexes are explained in section 9.5.6 below.

General Points

9.5.1.7. Each section of the proposal should start on a new page and the proposal should be constructed so that, if necessary, any section can be separated from the body of the proposal and given to specific readers.

9.5.1.8. Section 8 containing the commercial information must be bound separately from the other sections for reasons of confidentiality. Any indicative cost information should be provided separately from the main body and section 8 of proposals, and will not be used in the proposal evaluation.

9.5.1.9. Proposals should include financial implications for proposed options where this helps explain the Service Provider's proposal. The Service Provider may describe any innovative or other options in addition to the Service Provider's main proposal, provided these are justified.

9.5.1.10. The Service Provider is requested to use any estimates, assumptions and volumetrics shown in the SSR. The Service Provider may present additional sizings/costings based on alternate methods, estimates, assumptions and volumetrics if he can justify doing so.

9.5.1.11. Whilst every endeavour has been made to give Service Providers an accurate description of the requirements, Service Providers should form their own conclusions about the methods and resources needed to meet those requirements. The Contracting Authorities cannot accept responsibility for the Service Provider's assessment of the services.

9.5.2 Proposal: Management Summary

9.5.2.1. The Service Provider should present the main points of his proposals and recommendations in no more than ten sides of A4 paper. This must be capable of being read independently of the body of the proposal.

9.5.3 Proposal: Introduction

9.5.3.1. The Service Provider should provide a brief introduction to his proposal.

9.5.3.2. The Service Provider must identify a single contact point, and deputy, for procurement issues and queries about his proposal.

POL00028135

9.5.4 Proposal: The Service Provider

The Service Provider should explain the make-up of his consortium, how it would provide the range of proposed services and provide for a stable long-term business relationship. This description must clearly identify the separate contributions and responsibilities of each organisation.

The Service Provider must provide the financial information requested in the Request for Statement of Capability, where organisations are proposed as consortium members or major sub-contractors and this information has not been provided before.

9.5.5 Proposal: Responses to SSR Chapters

9.5.5.1. Sections 4 to 8 of the proposal will respond to chapters 4 to 8 of the SSR respectively. Each section shall have a similar structure as described below.

9.5.5.2. Each section shall provide the information as requested at the end of the respective chapter under the heading "Service Provider's Response". These ask for a narrative description of the Service Provider's approach taking full account of the information within the main body of the respective SSR chapter (particularly where the Service Provider is asked to provide specific comments).

9.5.5.3. Many of the chapters also ask for "Specific Responses" set out in a sub-section within that for "The Service Provider's Response". These responses should be provided with the respective proposal sections following the narrative description. The format for these responses is described below.

Format of Specific Responses

9.5.5.4. Where a chapter includes a sub-section at the end titled "Specific Responses", a series of paragraphs are set out for response by the Service Provider. These are categorised as:

"C" for standards conformance; or

"I" for request for information.

9.5.5.5. Service Providers are to respond to each paragraph and reproduce the paragraph reference and text (e.g. in italics) before the response.

9.5.5.6. A simple statement that the request will be met is not sufficient. For each paragraph the Service Provider should:

- provide the information requested (in response to "I") or describe what applicability the standards identified have to the proposal (in response to "C");
- describe any options available and state the implications.

9.5.5.7. Responses must be limited to providing information which is directly relevant.

POL00028135

9.5.6 Proposal: Annexes

9.5.6.1. The Service Provider may provide a further additional information if this is considered by the Service Provider to be relevant to this procurement.

POL00028135

Appendix 1-1

GLOSSARY

POL00028135

APPENDIX 1-1 GLOSSARY

1.1 Terms

Accounting Officer	Named individuals who are accountable to Parliament for the use of money voted to departments.
Agency	An abbreviation for Executive Agency, which is a semi-independent public body reporting to a government minister (e.g. Benefits Agency).
Agent	*1. BA usage*: person appointed by the customer to act on his or her behalf, and to receive and deal on his or her behalf with any sums payable to him or her. *2. POCL usage*: person in charge of any post office except a directly managed office (i.e. except post offices owned and staffed by POCL).
Availability	The minimum percentage of the hours of cover that the service should be operationally available.
Benefit Office	A location from which benefits are administered.
Benefit Payment Service	The service that ensures that benefits are paid to customers.
Benefit Agency	An executive agency of the DSS.
Client	Body whose business POCL transacts
Card Management Service	A service which manages the distribution and monitoring of benefit payment cards to benefit customers.
Common Audit Trail Model	Defines the minimum requirement for data retention and retrieval issues for the DSS.
Contract	A legally binding agreement that concerns the services between the Contracting Authorities and the Service Provider.
Contracting Authorities	The Department of Social Security and Post Office Counters Limited.
Contract Transfer Service	The service that provides for the transfer of the services to a new Service Provider or reversion to the Contracting Authorities.
Counter Clerk	A member of staff at a post office who serves customers. The term does not apply just to POCL staff, but also agents and assistants.
Counter Interface Service	The service provided by the Service Provider that supports counter clerks in providing counter services. The service boundary for the Counter Interface Service is expected to be between the service provided by the Service Provider and counter clerks.
Counter Services	Counter services are those services provided by post offices to their customers at the counter. The service boundary for Counter Services is expected to be between counter clerks and customers.

POL00028135

Customer	*1. BA usage*: person who has applied for or claim benefit, or his agent or appointee. *2. POCL usage*: person coming into a post office to transact business.
Demonstrator Phase	The first phase of the pilot programme where each shortlisted Service Provider is given the opportunity to demonstrate their solutions and options.
Draft Contract Negotiation Stage	The stage of the procurement process during which the Contracting Authorities and the Service Provider negotiate the terms of the final contract(s).
Electronic Stop Notice System	Electronic notification to post offices of lost, stolen, or recalled IOPs.
Evaluation Team	The Contracting Authorities' personnel who are involved in the pilot programme, and who evaluate the competing offerings from the Service Providers.
FAD code	A numeric code which uniquely identifies a post office. (While the term "FAD code" is still used, the Finance Accounting Division no longer exists by this name.)
Hours of Cover	The period of the working day during which the Service Provider should provide the service.
Operational Trial	The second phase of the pilot programme where the selected Service Provider further develops the solutions and selected options, and develops the SCOP.
Pilot Programme	That part of the procurement process that will be used to prove that the Service Provider can meet the service requirements.
Post Office Counters Ltd (POCL)	Part of the Post Office Group. One of the two Contracting Authorities for the services described in this document.
Risk Register	A log of the risks associated with each Service Provider that is compiled by the evaluation team during the pilot programme.
Roll-out Service	The service that implements the operational services in a planned and progressive manner.
Service Code of Practice (SCOP)	The procedures written by the Service Provider, and agreed by the Contracting Authorities, that will be used by the Service Provider and the Contracting Authorities during the duration of the contracts.
Service Provider	A person or body that expressed interest in being considered for the award of a public services contract as advertised in the Official Journal of the European Communities (reference 94/S 165-58937/EN) and was subsequently shortlisted following appraisal of their statement of capability.
Steady State Services	Those services that the Service Provider will provide in the "business as usual situation" following roll-out.
Support Services	Any of the services that are provided to support the operational services, e.g. Help Desk Service.
Voucher	Document on which an individual transaction is based

POL00028135

1.2 Abbreviations

AA65	Attendance Allowance computer system
AAB	Administration and Accounting Branch
ACC	Area Computer Centre
ACT	Automated Credit Transfer
ALPS	Automation of London Post Offices
APPU	Automated Payments Peripheral Unit
APT	Automated Payments Terminal
BA	Benefits Agency
BACS	Bankers Automated Clearing System
BAS	Benefit Apportionment System
BED	British Excursion Document
BPS	Benefit Payment Service
BVP	British Visitor's Passport
CAPS	Customer Accounting and Payments System
CHB	Child Benefit computer system
CLASS	Client Ledgering and Settlement System
CMS	Card Management Service
COD	Cash on Delivery
CPP	Common Payments Package
CRISP	Counters Retail Information Systems in Post Shops
CRU	Counters Remittance Unit
CSA	Child Support Agency
DE	Department of Employment
DHSS NI	Department of Health and Social Security (Northern Ireland)
DLA	Disability Living Allowance
DLO	Dead Letter Office
DSS	Department of Social Security
DVLA	Driver and Vehicle Licensing Agency
DWA	Disability Working Allowance system
ECCO+	Electronic Cash Registers at Counters
EFL	External Financing Limit
EFTPOS	Electronic Funds Transfer at Point of Sale
EIS	Executive Information System
EPOS	Electronic Point of Sale
ES	Employment Service
ESNS	Electronic Stop Notice System
FA	Financial Administration
FAMC	Family Credit computer system

POL00028135

GDN	Government Data Network
GIREC	Girocheque Reconciliation system
HCI	Human Computer Interface
HMG	Her Majesty's Government
ID	Identity
INCAP	Incapacity benefits computer system
IOP	Instrument of Payment
IPR	Intellectual Property Rights
IS	Information System or Income Support, depending upon context
ISCS	Income Support Computer System
IT	Information Technology
ITSA	Information Technology Services Agency
ITT	Invitation to Tender
JSA	Job Seekers Allowance
LAN	Local Area Network
MIS	Management Information System
MOP	Method of Payment
NI	National Insurance, or Northern Ireland, depending upon the context.
NINO	National Insurance Number
NIRS	National Insurance Recording System
NSB	National Savings Bank
NUBS2	National Unemployment Benefit System
OBS	Other Benefit Systems
OCR	Optical Character Recognition
OPSTRAT	Operational Strategy
PAC	Public Accounts Committee
PACE	Police and Criminal Evidence Act
PAG	Programme Accounting Group
PAGL	Programme Accounting General Ledger
PAO	Principal Accounting Officer
PAS	Payment Authorisation Service
PC	Personal Computer
PFI	Private Finance Initiative
PIN	Personal Identification Number
POCL	Post Office Counters Limited
POU	Paid Order Unit
PR	Public Relations
PSCS	Pensions Strategy Computer System
PUN	Pick-up Notice
ROCE	Return On Capital Employed
RUC	Real Unit Costs

POL00028135

SFCS	Social Fund Computer System
SMART	Salient Multi Attribute Research Technique
SSA	Social Security Agency
SSADM	Structured Systems Analysis and Design Method
SSA (NI)	Social Security Agency (Northern Ireland)
SSR	Statement of Service Requirements
TMS	Transaction Management Service
UK	United Kingdom of Great Britain and Northern Ireland
UKPA	United Kingdom Passport Agency
VAP	Value Added Processing
VIP	Very Important Person
WPA	War Pensions Agency
WPENS	War Pensions computer system

POL00028135

Appendix 2-3

Departmental IT Security Standards of the DSS

POL00028135

APPENDIX 2-3

DEPARTMENTAL IT SECURITY STANDARDS OF THE DSS

1. INTRODUCTION

This appendix provides an overview of the DSS IT Security Standards. These standards cover such topics adhering to legislation, implementing adequate audit trails (also see Appendix 2-8), adequate user access controls, standards to be adhered to in the design and development of application services, report production, checks to be implemented, testing and contingency plans. The full standards are available, from ITSA, on request.

2. POLICY AND LEGAL REQUIREMENTS

2.1 Objectives

The Departmental Security Policy is based on Her Majesty's Government Security Policy. The Departmental Security Policy requires organisations to:

(a) ensure that all actions by computer services or individuals using computer resources conform to Departmental policy, standards and legal requirements;

(b) ensure that only authorised persons are allowed access to the computer resources and that such access is limited to their job functions;

(c) ensure that an organised security infrastructure is set-up, trained and maintained to:

i. implement all applicable security standards;

ii. document procedures which satisfy security standards;

iii. monitor and review their security arrangements to ensure that standards and procedures remain relevant and effective;

iv. promote security awareness amongst all staff;

v. provide an annual report on the status of security within their area;

(d) ensure that data designated as 'restricted', including personnel data, is handled in accordance with Departmental instructions: sensitive data not carrying the designation should be protected from public release;

(e) ensure that users are responsible for their interaction with the Department's computer resources and that such actions are recorded and monitored and security breaches are investigated and reported to the Departmental IT Security Group (DITSG). A copy of the Security Breach Guide, which will clarify what constitutes a security breach, is available upon request;

(f) ensure that security procedures and controls are installed, managed and maintained effectively in all computer services and environments which must also provide accurate and adequate monitoring and reporting facilities;

(g) ensure that data is protected during processing, transmission and storage;

POL00028135

(h) ensure that contingency and recovery procedures which ensure acceptable levels of service and control are provided, tested and maintained.

2.2 Legislation

Security related legislation includes:

- Data Protection Act, 1984;
- Copyright, Design and Patents Act, 1988;
- Official Secrets Act, 1989;
- Computer Misuse Act, 1990;
- Social Security Administration Act, 1992;
- EC Directive on Legal Protection of Databases, 1993.

3. DEPARTMENTAL SECURITY STANDARDS

3.1 Objectives

Departmental security standards, which the Department and its agents are obliged to observe, ensure compliance with Departmental security policy by ensuring the confidentiality, integrity and availability of Departmental data and services by minimising the risks of:

- unauthorised access/disclosure

  the unauthorised access to or disclosure of information;

- modification

  the unauthorised amendment by update, addition or deletion of information;

- denial of service

  unauthorised withholding of information or resources, i.e. the failure of service whether by accident or design;

- theft/destruction

  permanent non-availability of information or other assets.

3.2 Standards Publications

There are two sets of security standards:

POL00028135

(a) The Departmental Security Instructions (DSI) covering personnel, document and physical security, which are the responsibility of the Departmental Security Officer (DSO);

(b) The Departmental IT Security Standards (ITSS) covering IT security, which are the responsibility of the Departmental IT Security Officer (DITSO).

The Service Provider will be expected to:

(a) comply with all applicable standards defined in current and future DSI and ITSS requiring positive action on its part, except where agreement to the contrary has been reached with the DITSO in accordance with this provision in the ITSS;

(b) cooperate with the Department, as required, in order to assist the Department in complying with those applicable standards, which are not complied with at the time of the awarding of contract;

(c) not knowingly do anything that would prevent or hinder the Department in complying with standards.

Relevant extracts of the DSI and ITSS will be made available upon request. Both are evolving documents and whilst revisions are planned, major change is not envisaged. Changes to ITSS are approved by the Departmental Change Control Board.

Departmental security standards will apply to services and data provided outside Departmental premises.

Throughout the term of any contract with the Service Provider, and afterwards, all information relating to the Department's services will remain the property of the Department and its successors. The Department's information must be classified in accordance with security standards and must not be disclosed by the Service Provider to a third party without prior written consent of the DSO or the DITSO.

4. ACCESS

The Service Providers, and any of their sub-contractors, will be expected to grant DSS and its authorised agents access to staff, data, and installations at all reasonable times, and to inspect and take copies from all documentation relevant to the service provision. All reasonable assistance should be provided at no extra cost for the purposes of allowing DSS to obtain such information as is necessary to:

(a) fulfil DSS's obligations to supply information for parliamentary, governmental, judicial or other administrative purposes;

(b) carry out an audit of the providers compliance with the obligations with respect to the security and confidentiality of data, computer integrity and other security requirements;

(c) investigate any suspected impropriety if the DSS has a reasonable suspicion that the impropriety has taken place.

POL00028135

Appendix 2-5

Benefit Payments
-Emergency Procedures

POL00028135

APPENDIX 2 - 5

BENEFIT PAYMENTS - EMERGENCY PROCEDURES

1. INTRODUCTION

Under the provisions of the Social Security Administration Act 1992, regulations (Claims and Payment regulations) provide that benefit shall be paid in accordance with an award as soon as is reasonably practicable after the award has been made.

In order to ensure that payments are made when required the Benefits Agency (BA) has evolved a series of procedures designed to enable the continuation of payments of benefit during a period in which normal procedures are not available.

1.1 Emergency Situations

There are six main emergency situations identified by BA:

1.	local disasters;
2.	disruption of a benefit computer system;
3.	disruption to Postal delivery/collection services;
4.	disruption to the Crown Post Office network;
5.	failure of the Departmental Central Index;
6.	failure of Area Computer Centre (ACC) computer systems.

2. LOCAL DISASTERS

A local disaster occurs when all ACCs and postal delivery services are functioning normally but a single or number of District Offices (DOs) are unable to provide a normal service. In each case the initial action is to undertake an assessment of the nature and scale of the problem. Table 1 below indicates the assessment of the impact on the service which is undertaken (with reference to each disaster type). Table 2 indicates the contingency options open to DSS staff to ensure the continuing provision of a payment service.

Table 1 Nature and impact assessment of disaster on service

	Nature of Disaster	Assessment of Impact on Service
1.	BA staff unable to use normal office premises due to fire, flooding, power supply failure etc.	Damage is assessed to establish: a) whether the building is in a habitable condition; b) how soon damage can be rectified; c) whether alternative local accommodation is immediately available
2.	Operational Strategy computer system equipment rendered inoperable due to theft or malicious damage.	Damage is assessed to establish: a) the amount of equipment still usable b) can the damaged equipment be repaired or replaced c) when is it likely to be fully operational again.
3.	Industrial action taken by BA staff.	An assessment is made to establish: a) the number of staff still working

POL00028135

	Nature of Disaster	Assessment of Impact on Service
		b) the number of staff required to run essential (e.g. Finance) sections. c) the prospects resolving the dispute. d) whether staff are available from other sites to maintain a service.

Following the above actions a further assessment is made to determine how soon:

(a) the office can be opened to the public;

(b) a telephone service can be provided;

a payment service can be provided.

Table 2 Options available in the event of a local disaster

1.	Interim payments of any benefit can be made via an automated "Emergency Payment Dialogue" within the Income Support Computer System (ISCS).
2.	Within a cluster of offices it is possible for casework to be accessed remotely by means of a District Processing Facility, thereby allowing payment award details from a closed office to be processed at another.
3.	Introduction of a Local Emergency Centre which may cater for the making of clerical payments.
4.	Where one or more offices are unable to process work an Emergency Processing Centre may be established.
5.	Interim awards of benefit, using clerically issued Instruments of Payment (IOP), may be made to customers.
6.	In cases of extreme urgency, cash payments may be made to customers.
7.	Arrangements can be made for a local authority to make interim payments to BA customers on behalf of the BA.

2.1 Emergency Payment Dialogue

ISCS contains a dialogue (IS 899) which can be used in emergency situations to make payments by girocheque via the ACCs.

2.1.1 Payment

Although using ISCS to generate the payment award, payments made in this dialogue are intended (and classified) as interim payments only. They are made as the result of an entitlement to any benefit requiring payment.

This dialogue generates payments by girocheque, made as normal through the ACCs. Payments may be for amounts between £1.00 and £999.99. The amount to be paid is calculated off-line using either an interim or emergency rate or the actual amount due for payment where this is known/accessible.

The serial number imprinted on the girocheque is taken from the batch of numbers allocated to the host office.

Additionally a customer notification is produced via the Common Payments Package (CPP).

Computer systems are not automatically updated with the information concerning payments made via this procedure. The process has therefore to be repeated either weekly or fortnightly, dependent on payment period, until the emergency has ended.

POL00028135

2.1.2 Returned Girocheques

If a girocheque issued in accordance with this procedure IS 899 is returned (either cashed or uncashed) to the office, it is treated in the same way as a clerical girocheque which has not been recorded on the system.

2.1.3 Reconciliation

Following the issue of interim or emergency payments using this procedure there is a reconciliation between the amount of benefit paid during the period of the emergency and the entitlement. It is established whether an over or under payment has occurred. Balances due to the customer are paid, accompanied by a notification advising the customer on how payment has been calculated. Overpayments of benefit are calculated and consideration given to their recovery from benefit payable.

2.2 District Processing Facility

The District Processing Facility allows staff at any site within a district to process work from other sites, without moving location or having to transfer ownership of a case. This enables work to be processed as normal without the need to make interim payments or take any necessary subsequent recovery action. A District Processing Facility can also be used to process recovery work if interim payments were made during the emergency period.

2.3 Local Emergency Centre (LEC)

If an office becomes unusable or is only able to provide a limited service as a result of the disaster, it may be necessary to set up a Local Emergency Centre (LEC). This is a centre set up to provide clerical payments, and/or caller facilities for BA customers. Its availability would be dependent on the availability of suitable accommodation and staffing.

The LEC may be set up within the affected office itself, (if still usable) or in temporary premises in the location. The LEC may be used:

1.	throughout the emergency period;
2.	until alternative system processing arrangements can be made from an Emergency Processing Centre (EPC - see 2.4);
3.	in conjunction with an EPC.

An LEC can be used to perform a number of different business functions. Its actual functionality is a management decision which must take into account a number of factors, the major ones being listed below:

1.	the nature and severity of the disaster affecting the office i.e. the extent to which computer systems can be accessed and the availability of accommodation/staff;
2.	whether the business has to be conducted at temporary accommodation - in this case factors such as transportation of necessary staff/equipment and security of the premises has to be taken account of;
3.	whether the LEC is being used in conjunction with the affected office and/or an EPC.

2.3.1 Service Levels Offered by an LEC

The level of service offered by an LEC is individually determined by the tasks it is able to carry out (having taken the above factors into consideration), this can vary considerably, however examples of services which may be provided are:

POL00028135

1.	until system processing can be arranged from an EPC, all essential business can be carried out using the emergency clerical instructions. If the LEC is not in the office itself, this may require essential items such as stationery, files etc. and post to be transported to the LEC for the duration of the emergency;
2.	the LEC could be used as a customer caller point and advisory centre only;
3.	clerical payments could be made from the LEC, requiring additional stationery stocks, security arrangements, finance stocks etc.
4.	the centre could deal only with certain types of work, more suited to clerical procedures, e.g.: • new and repeat claims which can be transferred onto the system later; • residual clerical cases which are not dealt with on-line.

2.3.2 Customer Information

It is essential that customers are kept informed during a period when normal procedures are disrupted by the need to take emergency action. A number of methods are used to inform customers of contingency procedures including the following:

1.	neighbouring DSS offices are advised of the situation and emergency procedures in operation;
2.	if an office is unmanned arrangements are made for the diversion of telephone calls either to a working office or to a recorded informative message;
3.	local statutory and voluntary organisations are informed;
4.	local media are informed;
5.	explanatory notices are positioned at public entrances to the stricken office and in other suitable locations in the vicinity.

2.4 Emergency Processing Centre (EPC)

An Emergency Processing Centre (EPC) is a facility that can be used when one or more offices are unable to process work. The EPC becomes the link to the computer systems and processes work on behalf of the offices.

An EPC is established by connecting a communications controller (at a designated site) to the required computer service or services. Other essential requirements (e.g. staff, budgetary control) are also decided and provided. Payments are generated through the computer systems and issued as normal. The work to be undertaken by the EPC is decided at the outset of the emergency. This is dependent on the nature of the damage to the affected office(s), and whether any work can be undertaken at LECs. Options available are:

1.	all work to be generated through the computer systems sent to the EPC for processing;
2.	only urgent work sent to and processed at the EPC;
3.	all work sifted and classified at the EPC with non-urgent work being returned to the office or LEC for eventual processing;
4.	work of a certain type, generally that requiring payments to be awarded, is selected for processing at the EPC (e.g. new or repeat claims, change of circumstances.

2.4.1 Returned IOPs

Where IOPs are returned to the EPC and it is unable to cater for the receipt, storage or disposal of the IOP. The EPC issued with clerical forms enabling the returned IOP to be recorded and destroyed.

Where IOPs are returned to the office and it still has access to computer systems normal procedures for returned IOPs apply.

POL00028135

If the office has no system access or post is being diverted to an LEC, arrangements are made to record returned IOPs on an appropriate system which is developed by SIS in any emergency. Detailed arrangements depend on the availability of secure accommodation at both the Emergency Caller Centre and the EPC.

2.5 Interim Awards

An interim award of benefit can be made during an emergency. Such an interim award is a payment, which would normally have been via one of the computer systems, made clerically during an emergency. There are several means by which interim payments may be made:

1.	a girocheque locally produced and issued at an office site (either office, LEC or EPC);
2.	cash;
3.	a payment made through a post office based on an expired order book;
4.	a payment made by a local authority on behalf of BA.

The person making a claim for an interim award need not be an existing customer, however in this instance a new claim must be made before payment can be considered.

2.5.1 Interim Payments

Interim payments:

1.	are not payments of a specific benefit, but are made on account of an entitlement to that benefit;
2.	carry no right of appeal against; the basis of the decision to make payment, the rate of payment or a decision not to pay;
3.	can be for any reasonable amount which any authorised agent of the Secretary of State considers appropriate. This may be for the exact entitlement to benefit (where this is known) or can be for a reasonable amount to cover the customer's immediate needs;
4.	can be offset or recovered if the customer is given notification that the payment is recoverable before or at the same time as payment is made.

If the entitlement to benefit is exceeded during the emergency period the excess can be recovered from most benefits as overpayments.

2.5.2 Methods of Payment

Once an interim award of payment has been confirmed and calculated there are a number of methods by which payment may be made.

Payments by Girocheque

Girocheques will be issued as normal through the computer systems where this is possible (e.g. where access to the systems is still obtainable or through an EPC). Where it is not possible, they will be issued clerically from the issue point (office or LEC). Where a customer is in receipt of benefit, payments are made on their normal pay-day if possible. Payments in respect of new claims are paid on their future pay-day if this can be established.

A central control record of all payments is kept to help:

1.	respond to enquiries either during the emergency or concerning payments made during the emergency;
2.	with recovery action in the event of any overpayments of benefit.

POL00028135

Cash Payments

In certain circumstances it may be possible to make emergency payments to customers in cash. There is a regular 'out of hours' service run by officers of the DSS and accessible to customers outside of business hours in an emergency from whom small amounts of cash may be obtained. Designated emergency offices are able to obtain cash outside normal banking hours and certain nominated officers can draw up to £5,000 in cash from banks in an emergency. Cash payments are primarily made in the following emergency situations:

1.	following the non-delivery of a large number of giros;
2.	in a large scale emergency that the 'Out of Hours' service can not adequately handle;
3.	cash payments may be made at the beginning of an emergency period until other arrangements have been made.

The amount payable is at the discretion of management who can determine it by using either a set amount for all customers or by paying on a sliding scale according to numbers of dependants etc.

The "out of hours" service is provided by BA to customers who need money urgently outside normal office hours. Emergency telephone numbers are provided for the Police, Social Services etc. to provide a contact point within BA. The service is operated by BA staff.

The call is initially answered by a BA officer who makes a decision as to whether to visit the customer. If a visit is suitable, a visiting officer is sent to the address. The second officer makes a discretionary decision as to whether a payment should be made. Most payments are made in cash, and all are recoverable.

Order Book Based Payment

In an emergency it is possible to use expired order book covers and payment foil counterfoil stubs to make payments of benefit to those customers currently paid by book. To assist in such a procedure the back cover of an order book is printed with ten boxes. Post office clerks use these to record any emergency payments made.

Should BA (in agreement with POCL) authorise payment to be made in this way, customers are advised to continue attending post offices for payment of benefit following the encashment of the last payment foil in their book.

(a) Periodicity of payment

Where possible the customer will continue to be paid at the usual frequency i.e. at the rate (generally weekly or four weekly) shown on the order book. The paying clerk stamps one box for each payment made, with the customer being required to confirm receipt of the payment by signing a schedule.

(b) Rate of Payment

Where possible the customer will continue to receive their correct entitlement to benefit. The normal amount paid is ascertainable from information printed on the front cover of the order book. The rate of benefit payable may however be adjusted by authorised staff at a BA office with the adjusted rate being marked in an 'adjustment box on the back cover'

(c) Receipt of renewal book

When a renewal order book is received at a post office it is issued to the customer in exchange for the expired order book. The details of payments made during the emergency period are examined

POL00028135

and any relevant payment foils (those which would duplicate payments already made under this procedure) are extracted.

Payments by a Local Authority

There are arrangements with local authorities which enable them to make interim payments to BA customers in an emergency. This is expected to provide a short-term solution in cases of real need pending BA bringing its own emergency payment arrangements into action. The authority claims reimbursement by forwarding completed application forms which act as the customer's acknowledgement of receipt of the payment.

The batch of applications is checked to ensure that the amount claimed is the total of the payments made. The application forms are then filed and retained for eighteen months and where necessary overpayments are considered for recovery.

3. BENEFIT SYSTEM DISRUPTION

3.1 Income Support System

In the event of a short term loss of access to the ISCS the following action is taken:

1.	clerical payments are made in hardship cases only;
2.	normal off-line activities continue;
3.	other work is stockpiled in order of priority.

A long term loss would require:

1.	utilisation of the interim payment procedures previously described clerical, primarily this would comprise clerical payments for new and repeat claims or weekly paid customers);
2.	existing work would be prioritised and stockpiled.

3.2 Pensions Strategy Computer System

In the event of a short term loss of access to this system the following action is taken:

1.	interim or clerical payments are authorised for urgent cases;
2.	off-line action continued;
3.	on-line cases are prioritised and stockpiled.

A long term loss would require:

1.	clerical payments to be made to customers primarily those with new or repeat claims or who were weekly paid customers;
2.	clerical action would be required to be taken on on-line cases;
3.	cases would be prioritised and stockpiled where possible.

3.3 Social Fund System

A short term loss of access to this system requires that:

1.	a customer's budget status can be established;
2.	clerical decisions and payments are made only if there is a health or safety risk to the

POL00028135

	customer or their household;
3.	an up to date budget record must be kept;
4.	work which cannot be cleared is prioritised and stockpiled.

A long term loss of access to this system action will be the same as above except that staff are not advised to resist making payment unless serious risk will occur.

3.4 Area Computer Centres (ACC)

The complete long term loss of a system is an extremely remote because benefit applications are housed between the 4 ACCs. If an application fails within one ACC then that system's backup tapes are sent to an alternative ACC until necessary repairs have been made.

It is more likely that local access to an application may be lost and in this event measures are taken to establish the cause of the loss. Local office management then refer to the options available to them and detailed within section 2 (Local Disasters).

4. DISRUPTION TO POSTAL DELIVERY AND COLLECTION SERVICES

A disruption to Royal Mail delivery and collection services will have a substantial effect primarily on the IOP issuing centres i.e. the ACCs.

4.1 Areas of Impact

4.1.1 Payment Issuing Offices

The collection of outgoing girocheques, order books and customer notifications from ACCs, and payable orders from NFCO and their subsequent delivery to customers will be affected. Additionally, dependent on the nature and scale of the disruption, all mail normally issued from a local office may be affected.

The courier services which normally operate between ACCs, local offices and ES offices will however continue. This service can be used to send outgoing mail, which would normally be sent through the postal system, from the ACCs and NFCO to the local offices.

Output Handling

The ACCs and NFCO have three main options available for handling their output in the event of any disruption in the postal service:

1.	retention of output on the premises until it can be delivered normally;
2.	delivery of output by alternative means;
3.	a combination of the above, retaining some output and delivering that with priority status by alternative means.

Usually ACCs are directed to retain output during the initial stages of any disruption, pending alternative means of delivery being found for (in order of priority):

1.	IOPs;
2.	payment stop and cancellation notices;
3.	other customer notifications.

POL00028135

4.1.2 Local Offices (LO)

The impact on local offices is felt in numerous areas. In order to maintain a reasonable level of customer service local offices may do all or some of the following:

1.	extend public opening hours;
2.	provide secure collection points for IOPs within the office;
3.	arrange for staff deliveries of IOPs to those customers who are unable to collect them;
4.	ensure that customers are informed of the revised services and procedures through local publicity;
5.	where appropriate arrange for the delivery and collection of mail to and from any unaffected sorting offices;
6.	maintain communication with other local government departments and agencies;
7.	where appropriate consider the issue of clerically produced payments as per section 2.5.

5. CROWN POST OFFICE DISRUPTION

If the service provided by a Crown post office is disrupted customers are advised to use a nearby sub post office.

5.1 Post Office Action

POCL will immediately arrange for:

1.	customers to have the facility to cash order books normally payable at Crown offices at specified sub-offices, without going through normal change of office procedures;
2.	all girocheques normally cashed at a Crown office to be encashable at specified sub offices;
3.	all alternative service arrangements to be widely advertised to customers.

BA customers will be informed which sub-office will hold any order books awaiting collection during the dispute, and which offices they may use for encashment purposes. Initially customers are able to cash their books at any of the specified sub-offices without being required to follow the normal change of office procedures. This position may change if the disruption at the Crown office is long-term. Any change in procedures is determined by agreement between POCL and BA.

5.1.1 Order Books Issued During the Disruption

At the outset of the dispute the BA Emergency Co-ordination Team liaises with POCL and the local office to establish which sub-office is to receive the redirected order books. When this has been agreed, BA advises the relevant ACCs so that any new order books may be redirected to the specified sub-office.

POCL is responsible for ensuring that if any mail has been sent from the ACCs (before the above decision has been made or communicated) to the affected Crown offices during the dispute it is retrieved and redirected to either:

1.	the specified sub post office for collection and encashment;
2.	returned to the appropriate local DSS office;
3.	returned to the appropriate Central Benefit Unit (which issues order books relating to centrally administered benefits e.g. Child Benefit).

POL00028135

5..2 **Local Office Action**

Should an order book become 'trapped' at a Crown post office the local office is responsible for issuing a replacement order book to the customer at a specified sub post office. If the customer is unable to get to this office then four options are open to the local office:

1.	to agree with the customer that payment can wait until the conclusion of the disruption;
2.	to arrange for an alternative payee to collect the payment;
3.	to arrange for payment either by girocheque (which can be paid into a bank or building society) or Automated Credit Transfer;
4.	in an exceptional situation to arrange for encashment to be made at the local office.

6. FAILURE OF DEPARTMENTAL CENTRAL INDEX

The Departmental Central Index (DCI) is a national computer system which stores certain personal and benefit related information of UK residents who have been allocated a National Insurance number.

If DCI fails payment of benefit is not affected immediately, however after a short period of time benefit payment related problems emerge.

To avoid this situation a contingency plan is in existence. In summary this entails a standby backup DCI system at a remote location which is updated with daily live journals from the main DCI system. In the event of the main system failing, the standby system is upgraded so that the information contained on it is that which was on the main system at the time of failure. Once updated, the network connections are enabled and all user access is switched to the standby system. It is required that this transition must be completed within 72 hours, to ensure a continuation of normal service levels.

7. FAILURE OF AREA COMPUTER CENTRE COMPUTER SYSTEMS

In the event of failure at one or more of the 4 ACCs contingency planning switches IOP production to a remote ACC even to the extent that payment requests can be collected from machines in all 4 ACCs and IOPs produced centrally at one.

POL00028135

Appendix 2-6

Benefits Agency Security Strategy

POL00028135

APPENDIX 2 - 6

BENEFITS AGENCY SECURITY STRATEGY

1. INTRODUCTION

In common with BA's IS/IT strategy the aim of the Security Strategy is to deliver good customer service alongside value for money by supporting the BA's core business aim of paying the right benefit to the right customer at the right time. Part of BA's remit therefore is to detect, investigate and stop fraud and abuse of the benefit process and payment systems.

2. CURRENT BENEFIT SERVICE FRAUD RISK

The DSS employs a number of staff engaged in formulating security policy and strategy. Additionally numbers of operational investigators conduct the investigation of suspected fraud and (together with Solicitors Branch) any subsequent prosecution of offenders. Despite the success enjoyed by these staff, the mainly tactical, reactive and organisational measures carried out by the investigators currently perform a containment function only.

Fraudulent attacks on the benefit system can be categorised into four types and relative magnitudes attributed from the current estimated total stock of fraud - illustrated in the table below. Additionally, this table shows the areas in which future risk, subject to negotiation, may be transferred to the Service Provider.

Figure 1. Categories of existing fraud risk

Type of Fraud Risk	Percentage of Total Fraud Risk
Identity - customers registering as benefit claimants using an incorrect or assumed identity.	up to 5%
Misrepresentation of domestic circumstances - customers misrepresenting their domestic circumstances, either at the point of an initial or repeat claim, or by failing to notify a change of relevant circumstances during the life of a claim.	between 20% & 30%
Misrepresentation of financial circumstances - customers misrepresenting their financial circumstances either at the point of an initial or repeat claim, or by failing to notify a change of relevant circumstances during the life of a claim	between 55% & 60%
Security of Payments - the theft, manipulation or counterfeiting of IOPs and subsequent obtaining of payment where there is no entitlement.	10%

2.1 Definition of Fraud

Within each type of fraud risk outlined above, there may be areas of greyness relating to the definition of an act as fraudulent. There are primarily four definitions covering acts which have resulted in the obtaining of a benefit payment to which there is no entitlement:

1.	**Fraud**	an act motivated by a deliberate intent to obtain benefit to which the customer knows they are not entitled. In this category benefit is generally obtained through a misrepresentation of facts which may be: (a) premeditated or planned fraud on a large or small scale; (b) opportunistic fraud resulting from an unreported change in personal circumstances.

POL00028135

2.	**Inadvertent Fraud**	fraud perpetrated through a lack of clarity on entitlement; or by a failure to recognise the individual's responsibility to report changes in personal circumstances.
3.	**Abuse**	a deliberate intent to obtain benefit through creative but inappropriate use of the rules, or the accessing of confidential data by BA staff for unauthorised purposes.
4.	**Incorrectness**	Whilst the main losses within the benefit system occur through fraud the strategy looks to address all areas where programme losses occur.

3. VISION

The vision for the future is of a secure benefit delivery system, administered by staff for whom security consciousness is an integral part of their work and behaviour, on behalf of an organisation for which security is a central focus, for customers who understand and accept their rights and responsibilities.

In order to attain this objective the following need to be achieved:

(a) security has to be integrated within the wider context of the BA operation, enabling and supporting better customer service and value for money;

(b) the end-to-end benefit delivery processes have to be made secure at all points so that, in the future, the security focus shifts from detection to prevention and deterrence; and

(c) three distinct groups of people;

- Staff;
- Customers; and
- Business Partners

must have confidence in the integrity of the benefit system.

A key factor in the achievement of the above objectives relates to the behaviour of the three groups identified above, so that:

(a) **staff** have the motivation and possess the skills to identify, prevent and pursue fraud, whilst maintaining and developing a professional service to customers;

(b) **customers** are confident that benefits are going to the right people at the right time, in the right amounts; accept that they must comply with existing regulations in their applications for benefit, recognising equally their rights and responsibilities; and

(c) **business partners** of BA are identified, and co-operative partnerships developed.

4. STRATEGY

The Security strategy encompasses a series of integrated but distinct projects which over a period of five years will move BA significantly closer to achieving the vision and a reduction in losses through fraud. The five year programme will encompass:

1.	design and development of integrated IT systems to: a. support investigative staff; b. detect fraud within the benefit process; c. prevent fraud;

POL00028135

2.	the implementation of the automation of benefit payments at post office counters;
3.	detection work, peaking in the first half of the Strategy period (in line with IT development) and moving towards prevention;
4.	work to move the cultural focus, continuing throughout the Strategy period;
5.	the design of benefit reviews, targeted at testing the changing shape of fraud over time, has started and will continue throughout the period;
6.	the establishment and continuation of programme control and performance management, with the objective of demonstrating progress and accounting for allocated money.

The programme will be:

1.	comprehensive - covering all types of fraud and anti-fraud activity;
2.	cost-effective - maximising value for money;
3.	sustained - weaving together a programme of change, over 5 years, across people, processes and supporting technology;
4.	demonstrable - describing the changes, monitoring and measuring the success of projects and showing tangible improvements;
5.	pragmatic - taking account of political and financial constraints, and allowing for prioritisation and adjustment during the strategy programme;
6.	significant - achieving a substantial change in the level of fraud in the system, and shifting the focus from detection to prevention.

POL00028135

Appendix 2-7

BA IS/IT Strategy

POL00028135

APPENDIX 2 - 7

BA IS/IT STRATEGY

THE INFORMATION SYSTEMS/INFORMATION TECHNOLOGY STRATEGY STATEMENT OF THE BENEFITS AGENCY

1. INTRODUCTION

1.1 Primary Function

The primary function of BA is to deliver benefits in accordance with the law and to the satisfaction of ministers and customers. The aim of BA is to fulfil this function economically, efficiently and effectively with due regard to the varying needs of its customers.

1.2 Objective

The objective of the IS/IT Strategy is to provide the framework for planning the enhancement and development of information systems to support BA's business aims, objectives and core values for the next 10 years or more.

1.3 Content

This appendix provides a high level and concise statement of the BA's business vision, strategic aims and objectives, and show how they in turn define the IS Strategy and the necessary IT support.

2. BUSINESS VISION

2.1 One Stop Service

BA's vision is to provide an efficient "one stop" benefit service that offers reliable advice and pays the right money to the right person at the right time. The vision will be delivered in accordance with the four core values:

(a) customer service;

(b) value for money;

(c) bias for action;

(d) caring for staff.

BA seeks to achieve this by providing a customer centred service delivered in an environment which encourages innovation and excellence and is administered in an accurate, secure and cost effective way.

Customers will be provided with more choice: BA will offer flexibility in how, where and when customers make contact; customers will have the choice of how they are paid and how they make their claims.

POL00028135

This choice will be given by motivated, well trained and skilled staff through processes that allow flexibility but ensure that security, accuracy and integrity of information are maintained.

2.2 Strategic Business Objectives

This Business Vision defines a number of strategic business aims and objectives, which are summarised as:

(a) deliver benefits promptly and accurately;

(b) deter, prevent, detect and investigate internal and external fraud;

(c) improve customer service by the successful delivery of a One Stop Service;

(d) improve quality by getting payments right first time and asking for information from customers only once;

(e) develop systems with the flexibility to support local needs; ministerial and policy requirements; and changing work patterns and organisational structures;

(f) provide staff with the tools, training, support and motivation to achieve a recognised standard of excellence in a demanding but satisfying environment;

(g) provide best value for money and drive out inefficiencies in both administrative and programme expenditure.

3. IS/IT STRATEGY

Information Systems and the supporting Information Technology are key enablers to the achievement of BA's business aims and objectives.

3.1 Strategy

The strategy recognises that there will be a continuing need to enhance existing systems and respond to legislative and ministerial requirements. Changes to support the future business of BA must therefore be evolutionary, rather than revolutionary.

Set in the context of Agency business strategies such as the Security Strategy, Market Testing and Personnel, the IS/IT strategy seeks to move BA forward by providing IS/IT support that:

(a) makes advice and information more readily accessible to staff and customers;

(b) moves towards more consistent benefit processing systems;

(c) exploits more modern and secure methods of payment;

(d) bears down on fraud and abuse;

(e) improves financial controls and management information;

(f) provides the services and tools that staff need to support them.

POL00028135

3.1.1 Advice and Information

Systems will be implemented which provide benefit advice and information. Initially available to staff to support them in their contact with customers, some of the functionality, such as data input and advice seeking, may over time become directly available to customers themselves. *This supports the customer service core value, and the business objectives of improved customer service and support for staff.*

3.1.2 Common Information

Separate benefit systems will gradually be migrated to benefit processing systems built with generic modules which can be easily replicated. They will be built on a common repository for all customer information, and a common repository for all payment details. *This supports customer service, bias for action, and value for money core values, and the business objectives of improved customer service, flexible systems, value for money, and fraud prevention and detection.*

3.1.3 Methods of Payment

New methods of payment will be introduced, which provide more modern and secure instruments of payment than existing paper based systems, offering benefits to both customers and BA. *This supports the customer service core value, and the business objectives of improved customer service, prompt and accurate benefit payment, and fraud prevention and detection.*

3.1.4 Fraud and Abuse

Existing systems to detect and prevent fraud and abuse will be extended, and focus on allowing BA to be more proactive in recognising patterns of fraud and effectively targeting resources to combat it. *This supports the value for money core value, and the business objective of fraud prevention and detection.*

3.1.5 Management Information

Management information will be enhanced and systems will be developed to improve financial control, accountability and resource management. *This supports the bias for action core value, and the value for money core value and business objective.*

3.1.6 Communications

A range of communications, administrative, and support systems will be introduced to increase the efficiency and effectiveness of all staff. *This supports the value for money, bias for action, and caring for staff core values, and the business objectives of flexible systems, support for staff, and value for money.*

3.1.7 Common Infrastructure

These systems will be supported by a common infrastructure and, eventually, a single workstation per desk which will also provide the platform for enhanced local services, including personal productivity tools. *This supports the value for money and caring for staff core objectives, and the business objectives of system flexibility, support for staff, and value for money.*

POL00028135

3.1.8 Secure Accountable Framework

This must all be achieved within a framework that ensures systems are secure, maximise the detection and prevention of fraud, provide full benefit accounting information, and provide a common look and feel through the use of uniform screens and dialogues. *This supports the value for money and caring for staff core objectives, and the business objectives of flexible systems, staff support, and value for money.*

3.2 The IS/IT Strategy Framework

The IS/IT Strategy sets out the business, technical and managerial framework to achieve these objectives. The main elements of the framework are as set out below:

(a) all IS developments will be business driven, will be determined by the business strategy and will fit with the BA strategic direction;

(b) developments will build upon the existing systems and consist of an evolutionary approach to change;

(c) all developments will be built in a secure manner, ensure secure benefit delivery, contain comprehensive audit trails, and ensure full administrative and programme accountability;

(d) developments will conform to agreed technical standards, and run on a common infrastructure built of strategic components;

(e) IT developments will comply with common data standards, be built with generic components and have a common look and feel;

(f) all investment in IT systems will be spent in accordance with this strategic framework;

(g) the management and control of the IS/IT Strategy and the consequent work programme will be by a series of processes and procedures owned by BA Management Team (BAMT) and agreed and operated through its sub-committee BASCIS and the business areas concerned.

3.3 Implementation of the IS/IT Strategy

The delivery of the IS/IT Strategy will be by the implementation of an agreed and co-ordinated work programme, which integrates the IS/IT requirements of BA business strategies and encompasses all IS/IT projects within BA.

A 10 year programme sets out the IT developments needed to achieve the strategic aims and objectives. This long term programme and associated strategic business case are supplemented by a detailed 1-3 year implementation plan and business case that are rolled forward on an annual basis. These also inform the current years work programme, at any given time, feed into the strategic planning process, and act as the base environment for negotiating resources with Treasury through the PES process.

The programme will be implemented and adapted within the constraints of:

(a) the need to provide a continuous uninterrupted service;

(b) the need and desire to conform to legal obligations;

(c) the availability of resources;

(d) operational priorities.

POL00028135

The strategy, associated business case and work programme will be continuously co-ordinated with the strategies of other stakeholders within the Departmental Strategy to ensure that value for money and maximum cost effectiveness and flexibility are maintained.

POL00028135

Appendix 2-8

DSS Common Audit Trail Model

POL00028135

APPENDIX 2 - 8

DSS COMMON AUDIT TRAIL MODEL

1. INTRODUCTION

The DSS has in place an agreed Common Audit Trail model. The standards imposed by this model are controlled by the Departmental IT Security Group.

The DSS IT Security Standards (ITSS) require IT systems to provide an audit trail. It is a requirement that the service operate in conformance with these standards which are reinforced by the legislative requirement imposed by:

- The Data Protection Act 1984; and
- The Computer Misuse Act 1990.

1.1 Audit Trail Objectives

The primary purpose for maintaining audit trails is one of accountability. Agencies must be able to show that their business is conducted with fiscal propriety and in conformance with the law and relevant Government policies. In the case of IT applications this requirement is reinforced by: the Departmental IT Security Standards (DITSS) and the legal requirements contained in relevant legislation (e.g. Data Protection and Computer Misuse Acts).

1.1.1 IT Transactions

IT transactions are of a transitory nature and the IT audit trail may be the only way open to agencies to demonstrate propriety, conformance to the law and to police its operations. The audit trail should provide the means to establish the event or events which have led to questions arising as to the propriety or legality of a transaction, or the compromising of the integrity or confidentiality of any system or data. It should also be the means by which an agency can prove that it has performed certain specific transactions. (The word transaction as used here means a set of consecutive actions, normally between a user and the IT system, which results in access or a change to data held on the system).

1.1.2 Retention and Retrieval of data

The Common Audit Trail Model defines the minimum requirement for data retention and retrieval issues. This requirement applies to all systems which hold, process or provide access to personal data or which issue payments of benefit.

1.1.3 Management Information

There may be other uses for the data collected in connection with audit trail purposes. It may be used to provide management information statistics or to collect or substantiate financial control data.

1.2 Audit Trail Policies

POL00028135

1.2.1 Agency Tasks

The objectives defined in chapter 1.1 map onto identifiable tasks which the agencies either must, or may be required, to perform. They include:

(a) identification of a user who has carried out a suspect transaction (i.e. one suspected of breaching confidentiality or integrity;

(b) examination of transactions carried out by a specified user;

(c) examination of all transactions carried out on individual accounts;

(d) provision of supporting evidence in relation to criminal or civil proceedings;

(e) provision and support (through security checking and other forms of analysis of audit trails) of a means of detecting and deterring internal fraud or abuse, or of providing assurance in relation to levels of internal fraud or abuse;

(f) provision of protection to individual users (i.e. the identification of one officer breaching confidentiality or integrity rules in a case where another officer has prima facie responsibility);

(g) provision of information to assist in the resolution of administrative queries relating to an individual customers account and ensure that proper action has been taken.

Where developments involve direct customer interface with systems, audit trails take on a greater significance.

1.2.2 Relevant Transactions

The requirement for audit trails is to retain details of user and other transactions necessary to support the tasks outlined in section 1.2.1. Relevant transactions comprise user activity leading to any of the following:

(a) a change to personal data;

(b) access to personal data;

(c) access to records held for security management purposes;

(d) the issue or prevention of issue of a payment;

(e) the recording of a returned payment;

(f) the issue, or suppression of the issue, of a notification to a customer;

(g) the setting-up or deletion of customer accounts.

A user transaction with one system may result in changes to data held on another system or involve access to data held on another system. The requirement is that the causes and effects of a suspected breach of system integrity or confidentiality can be established with certainty even where these take place through different systems which interface with one another.

POL00028135

1.2.3 System Output (excluding payments)

In addition to output to a user's VDU, system output may be: by printed report, electronically to other systems or by other means. Where this output contains customer related information, or data produced for the purposes of controlling system security, the circumstances surrounding its production (or in certain circumstances, suppression) must be written to the audit trail. This requirement may be modified in the case of routinely generated reports.

1.2.4 System Output: Payments

There is a general need, consistent with an agency's accountability objectives, to prove (or refute) the issue of specific payments or instructions to pay. An agency may also routinely provide witness statements relating to the issue of payments for use in prosecution cases.

1.2.5 Data Retrieval

Retrieval of audit trail data (or sets of data) must be in an agreed format and context. This format should be consistent with supporting the various uses to which audit trails may be put.

1.2.6 Audit Trail Integrity

The integrity of audit trails must be assured. This requirement follows from the overall accountability objective and from the implications for individual system users of the various uses to which audit trails may be put.

2. SCOPE

This model applies to all IT systems holding or processing customer information or issuing benefit payments.

3. RELEVANT TRANSACTIONS

3.1 Transactions

The audit trail must record all transactions leading to:

1.	output of all or part of a customer record (this does not include the output of routine reports, such as reports for management information);
2.	change to a customer record (particularly creations and deletions);
3.	issue of a payment;
4.	the return and recording of a returned payment and its' replacement;
5.	the issue or user suppression of a notification to a customer;
6.	access to user or security related records;
7.	local authorised user activity.

3.1.1 Users

This must include all transactions between the system generating the audit trail and:

1.	internal system users;

POL00028135

2.	external users (e.g. Agency customers);
3.	other systems.

3.1.2 Payments

NB. The issue of a payment is itself a transaction which must be recorded whether or not directly prompted by user action.

4. INFORMATION TO BE RECORDED

4.1 User Transactions

The information required from the audit trail in respect of each relevant user transaction is:

1.	log-on and log-off times for each user;		
2.	date and time of user activity;		
3.	user identity;		
4.	identity of terminal where user activity took place;		
5.	system or systems involved in the transaction;		
6.	record identifier (NINO);		
7.	field identifier (where data is changed);		
8.	dialogue activity identifier;		
9.	where data is changed :	a.	new state of field;
		b.	old state of field;
		c.	the start and end dates of the data.;
10.	where data is accessed :	a.	location and date of data output where this is other than directly to the user's VDU;
		b.	where the data was output (e.g. local printer).

4.2 Payment Transactions

In the case of payment transactions, the information required is as described above together with any additional data which may be defined subsequent to any changes in the current method of payment and thereby benefit payment transactions.

4.3 Card Management

In the case of card management transactions, the information required is as described above together with any additional data which may be defined subsequent to any changes in the current method of payment and thereby benefit payment transactions including any card identification code selected by the Service Provider.

5. RETENTION PERIODS

Audit trails should be retained for a period of at least 18 months (as specified by the National Audit Office (NAO). They may be retained for longer at the instigation of an individual agency. There must also be a facility available to retain selected data from the audit trail for a longer period if this is required i.e. for legal proceedings.

POL00028135

6. RETRIEVAL

Audit trails should always be accessible, by designated users, as printed output. It is also necessary to have automated access to an audit trail to allow local interrogation (via PC) and printing. This output may be limited to a period or periods within the 18 month retention span where this is specified by the user accessing the audit trail. To support the requirements of both security checking and investigation, data should be available by NINO, by user ID, by terminal ID and by office ID. The requirement is that the user of audit trail data can either:

- start with a specific record (normally defined by NINO) and establish which user action created or changed a given data item within that record or conversely;
- establish which data items were input by a particular user, or which records or dialogues a user had accessed.

This requirement applies equally where more than one system is involved. For example, access may be through one system to data held on another, or a change to data on one system may affect data or generate output on others.

7. AUDIT TRAIL SECURITY

Audit trails in themselves must be secure and should remain inviolate at all times. Information written to an audit trail must have a level of security such that it cannot be altered or deleted by **anyone** with access to the system.

POL00028135

Appendix 3-1

POCL Existing Services

POL00028135

POCL EXISTING SERVICES

1.1 Postal Orders

Postal orders are sold by POCL as a convenient way of sending money by post. They are issued and can be cashed at all post offices in the UK, and in some countries overseas.

At nominated post offices, sealed packages of postal orders (and/or international money orders) are accepted under the 'central payment to banks scheme'. The packages are accepted from banks and passed to an accounting branch of the Post Office at Chesterfield.

Payment can be made by cash or cheque (if supported by a valid guarantee card).

1.2 International Money Orders

International money orders issued in Canada and the United States may be cashed at post offices, provided that a sterling equivalent is shown on the order.

1.3 Cashing Other Banks' Cheques

This service allows account holders of many banks, building societies and other financial organisations to cash a cheque at most post offices (approximately 17,000) provided that the conditions under which payment can be made are met.

1.4 Post Shops

Post Shops are separate units within directly managed outlets retailing greeting cards, stationery, packaging materials and office sundries. A small number of Post Shops also retail philatelic and small gift items. There are approximately 200 Post Shops and experiments are underway to offer the Post Shop format as a franchise offer to POCL's Agents.

1.5 Browser units

A browser unit is either a 1 metre or 2 metre single sided or double sided unit displaying over 100 stationery products for re-sale. There are approximately 280 browser units in branches.

1.6 Bureau De Change

POCL in partnership with First Rate (a wholly owned subsidiary of the Bank of Ireland) presently offers Bureau de Change services at 4300 post offices. There are two elements sold:

(a) Foreign Currency;

(b) Travellers Cheques.

300 post offices offer an on demand (buy/sell) service and 4000 post offices offer a pre order service. At present POCL do not offer a buy back service.POCL'sintention is to extend Bureau de Change to 600 post offices offering the on demand (buy/sell) service and the remainder of the network offering the pre order service. POCL intend to enhance further the pre-order service with a buy back facility. Payment can be made by cash or cheque (if supported by a valid guarantee card). POCL intend to accept credit cards for this range of transactions.

POL00028135

1.7 Active Life

Active Life is a "lifestyle" magazine aimed at the 55+ age group. Membership brings various benefits and discount offers. First applications can be made at post offices and renewals can either be done directly or via post offices.

1.8 Photobooths

Where there is surplus space Photobooths are installed in directly managed outlets providing customers with facilities for passport photos.

1.9 Telephones

Where there is space and a suitable environment public telephones are provided by both British Telecom and Mercury Communications.

1.10 Media

POCL offers three advertising channels for clients and other companies to their customers.

- Direct Response Television

  A television at the head of a queue, with response leaflet dispensers, in directly managed outlets, plays a loop of adverts for a variety of products (not necessarily linked to post offices)to customers.

- Post Office Point of Sale

  In all directly managed outlets and a large number of agency outlets display boards ranging from A1 to A4 are available for advertising. The majority of this advertising space is taken up by POCL's major clients. Leaflet dispensers are also available.

- Counterpoint

  This service allows clients to bring their services directly to the attention of targeted customers. The counter clerk hands out a leaflet on behalf of the client or company with a targeted range of transactions. This is popular with local traders.

1.11 Savings

POCL provides a range of savings and investment services on behalf of the Department for National Savings. Briefly these are:

- National Savings Bank Ordinary Account

  The National Savings Bank Ordinary Account offers a simple method of saving money via a pass book through the Post Office. The amount saved may be withdrawn on demand subject to maximum withdrawals and other such conditions on the account..

- National Savings Bank Investment Account

  The National Savings Bank Investment Account offers savers a higher rate of interest than the ordinary account. The customer may withdraw money from an investment account but must give one month's notice to National Savings Bank of the amount to be withdrawn.

POL00028135

- National Savings Certificates

  Savings Certificates provide savers with a tax free rate of interest. For ordinary certificates the rate is guaranteed over five years. The rate of interest payable on index linked certificates is determined by the Retail Prices Index and they may attract a bonus rate above this rate if held for a set period.

- Premium Savings Bonds

  "Premium Bonds" offer the investor a secure capital investment with a chance to win monthly and weekly prizes.

- Capital Bonds

  Capital Bonds are a savings scheme which offers a guaranteed rate of interest over a full five year savings period.

- Children's Bonus Bond

  Children's Bonus Bond is a specially designed savings scheme for parents, relations and friends to save money for children under sixteen.

- Income Bonds(Repayments only)

  Income Bonds are a method of saving a lump sum which provides a monthly income.

- Government Stock (repayments only)

  Government Stocks (also known as "gilts") are Stock Exchange securities issued by the government which pay a guaranteed rate of interest (unless index linked).

1.12 Travel Permits And Tickets

POCL issues concessionary travel permits for participating local authorities typically free of charge to customers.

POCL also retails travel tickets on behalf of participating travel companies. These can be simple scratch cards which customers validate for a period of travel themselves or they can be strips or books of tickets sold at a discount from the full fare to customers.

1.13 E111

POCL issue, and validate, form E111 on behalf of the Department of Health. An E111 enables a person from a European Community member country, when visiting another member country, to obtain urgent medical treatment as if he/she were a national of that country. E111s are available from all post offices. No fee is charged to customers for this service.

1.14 TV Licences

POCL issues television licences and sells television licence savings stamps on behalf of the British Broadcasting Corporation (BBC). Television licences are available from all post offices. £1 television licence savings stamps are available enabling customers to save towards the payment of a new licence. Two licences are available:

- monochrome (also known as 'black and white');

POL00028135

- monochrome and colour (also known as 'colour').

Payment can be made by cash, cheque or savings stamps at the counter on production of either a reminder letter and application form from TV Licensing, Bristol or by completing an application form available at the post office. Unused portions of monochrome licences can be refunded against a first application for a full monochrome and colour television licence.

1.15 Motor Vehicle Licences

POCL issues motor vehicle renewal licences and sells motor vehicle licence savings stamps on behalf of the Department of Transport Driver and Vehicle Licensing Agency (DVLA). Motor vehicle licences are available from approximately 4000 outlets. Customers apply for a vehicle licence either on a reminder letter (V11) sent directly to them by DVLA or by completing an application form (V10) available at post offices. Customers must produce a valid insurance document and, if the vehicle requires one, a MOT certificate. Applications on form V10 must also be supported by the vehicle registration document (V5) issued by DVLA to the keeper of the vehicle. If any details on the V5 have changed (e.g. change of owner) or are incorrect, the V5 form is retained with the application form and dispatched to DVLA for amendments.

£5 vehicle licence saving stamps are available enabling customers to save towards the payment of a new licence.

Payment can be made by cash, cheque or saving stamps at the counter. Refunds for unused portions of vehicle licences are not available at the Post Office but the application form to apply for refunds from DVLA or local vehicle registration offices is.

1.16 Rod Licences

POCL issues Rod Licences on behalf of the National Rivers Authority (NRA). There are two types of licence :

- Salmon and migratory trout;
- Non migratory trout and other coarse species.

Rod Licences are issued at approximately 17,000 post office outlets. Payment can be made by cash or cheque.

1.17 Passports

POCL acts as agent for the United Kingdom Passport Agency, an agency of the Home Office, in issuing British Visitors' Passports (BVP) and the British Excursion Document (BED). They are available from main post offices only (approximately 1500 outlets).

BVPs are valid for one year, cannot be renewed and can only be used for short visits for pleasure, education or social purposes to the countries listed in the notes on the application form. They will cease to exist as a valid passport from 1 January 1996.

BEDs are short stay passports valid for one month which may be used for trips of up to 60 hours duration to France. Ceasing 1 March 1995.

After these dates customers will have to use 10 year standard passports. The UKPA are likely to be looking for a partnership with post offices, travel agents, banks and building societies to accept applications for 10 year passports.

POL00028135

1.18 Game Licences

POCL issues game licences on behalf of the Department of Environment in Great Britain (administered by local authorities) and on behalf of the Department of Health and Social Security in Northern Ireland. Game licences are available from selected post offices.

There are 3 types of licence:

- Game Keeper;
- Game Dealer;
- To Kill Game.

The licence to kill game is available in four different validity periods matching different game seasons.

1.19 Banking

POCL provides banking services on behalf of Girobank. Briefly these are:

- Transcash

  Transcash allows Girobank and non Girobank customers to pay bills and make payments to other Girobank account holders - for instance to local electricity companies, mail order firms and water authorities.

  Cheques may be accepted if the Transcash slip states a cheque is acceptable.

  For some of these transactions a fee may be payable.

- Personal Deposits

  Deposits to Girobank personal accounts may be made by cash over the post office counter. Cheque deposits may also be accepted in sealed envelopes. (A cheque will be credited to a customer's account once it reaches Girobank).

  Deposits to Girobank business customers' accounts may be made by cash. Cheques may also be accepted in sealed envelopes. (Cheques will be credited to a customer's account once they reach Girobank).

- Business Deposits

  Deposits can be made either personally by the business customer (or an employee), or made via a security carrier (e.g. Securicor).

- Merchant Voucher Deposits

  This facility allows Girobank business customers to make merchant voucher (credit card slip) deposits into their accounts.

  Merchant voucher deposits are made in sealed envelopes. (Deposits will be credited to a customer's account once they reach Girobank).

- Change Giving

  This facility allows Girobank business customers to exchange cash (and cheques if agreed) for coins.

POL00028135

- Rent Schemes

  Girobank operates two schemes which allow local authority tenants and tenants of some large housing associations to pay their rent using either rent cards or rent vouchers.

- Building Society Deposits

  Deposits can be made into either Alliance and Leicester or Swindon building society accounts, provided that the customer has arranged this facility with the building society concerned.

- Personal Withdrawals

  A Girobank personal account holder may make a cash withdrawal at a post office provided that the Girobank card produced allows him/her to make a withdrawal at that particular office.

- Business Cash

  Girobank business customers may, with prior arrangement, withdraw cash up to £5000 at a nominated post office.

- Cashcheques

  Some business customers use cashcheques to make payments to people who do not have a Girobank account.

  Payment can either be made by cash, or the cashcheque may be crossed and paid through a bank account.

- Building Society Withdrawals

  Withdrawals can be made from either Alliance and Leicester or Swindon building society accounts, provided that the customer has arranged this facility with the building society concerned.

- Sending Money Abroad

  This service allows customers to make payments to people in other countries, either by cash, cheque or Giro transfer.

- Post Cheques

  Post cheques from certain European countries may be cashed at selected post offices.

- Girobank Transfer

  Girobank transfers are a means of moving money between Girobank accounts to pay for goods and services only. Girobank transfers are acceptable at all post offices under the same regulations as cheques issued by Girobank and other financial institutions e.g. cheques and Girobank transfers are acceptable for:

  - ◊ TV Licences;
  - ◊ Motor Vehicle Licences;
  - ◊ British Visitor Passports;
  - ◊ Department of National Savings products;
  - ◊ Girobank "Cheque Acceptable" transcash transactions;
  - ◊ Redirection of mail;
  - ◊ Cash on delivery - fees paid in by Royal Mail staff as a transcash "Cheque Acceptable" item;

POL00028135

- ◊ Franking machine setting;
- ◊ Any transactions for a recoverable service undertaken on behalf of a client.

1.20 British Telecom Telephone Bills

POCL accepts payment for British Telecom (BT) telephone bills and sells telephone savings stamps on behalf of British Telecom PLC at all post offices. Only full payments of BT bills are accepted. Payment can be by cash, cheque or saving stamps in any combination.

1.21 BT Phonecards

BT phonecards in £2, £4, £5 £10 and £20 denominations are available from all main post offices and agency offices where there is an identifiable demand. Cards can be purchased with cash and/or a cheque (if supported by a valid guarantee card).

1.22 Mercurycards

POCL sells phonecards (Mercurycards) on behalf of Mercury Communications in £2, £5 and £20 denominations at all main offices (approximately 1500 outlets) and agency outlets where there is an identifiable demand. Cards can be purchased with cash and/or a cheque (if supported by a valid guarantee card).

1.23 Water Authority Saving Stamps

Water Authority saving stamps are on sale at a value of £2 at post offices within the operating areas of participating water companies. The stamps are used only for saving towards the payment or part payment of water service bills under the Girobank Transcash system.

1.24 British Gas Meter Tokens

British Gas meter tokens are used by British Gas customers who have specially designed meters installed in their homes. (Meter tokens allow the customer to pay for gas as it is used.) British Gas tokens are sold at selected post offices in England and Wales. In order to purchase a token each customer must present:

- payment;
- a British Gas payment record book containing details of:
  - ◊ customers name;
  - ◊ customers address;
  - ◊ customers British Gas reference number.

A voucher must be removed from the book each time tokens are purchased. It is the voucher and not the purchase of the token that is used to credit the customer with a payment for gas consumed.

1.25 British Gas Quantum Card Recharging

British Gas Quantum Cards are smartcards used by British Gas customers who have specially designed meters installed in their homes. Quantum Cards are recharged at selected post offices which have the British Gas Quantum Card Recharging equipment.

POL00028135

1.26 Automated Payments

POCL is installing 8,000 Automated Payment Terminals in some 5,000 post offices to perform a wide variety of bill payment and pre-payment work directly for clients. It has been designed to handle the following transaction types:

- Magnetic Stripe Cards;
- Smart Card Recharging;
- Smart Key Recharging.

The terminal captures data relating to a customer transaction and transmits this data overnight to a "host" computer. The "host" computer then transmits the data to the appropriate client.

Amongst those utilising the new system are:

- South Wales Electricity (SWALEC);
- Scottish Power;
- Hydro Electric;
- Yorkshire Electricity;
- Severn Trent Water;
- Northern Ireland Electric;
- British Gas (all regions by May 1995);
- South West Water;
- Eastern Electricity;
- Northern Electricity;
- East Midlands Electricity;
- Knowsley Borough Council.

1.27 National Lottery

POCL sells National Lottery products on behalf of Camelot, the national lottery operator. There are two types of product:

- on line weekly jackpot lottery draw;
- Scratch card instant win prizes (not available yet).

Plans are in place to roll out the on-line game to 4000 post offices and the scratch card game to an additional 6000 post offices. Post offices also pay out prizes up to the value of £10,000.

National Lottery tickets and scratch cards can be purchased by cash.

POL00028135

1.28 Royal Mail

POCL offers a range of postal services on behalf of Royal Mail (a business of the Post Office). Advice and information on all Royal Mail services is provided. There are rules and regulations covering the post which must be met e.g. perishable items, size limits and proper packaging.

Payment can be made by cash or cheque (if supported by a valid guarantee card). Cheques can also be accepted if supported by a Post Office Authority card. This card is only issued to solvent, bona fide companies and organisations that regularly make large purchases of stamps.

Briefly the services offered on behalf of Royal Mail are:

- Inland Letter Services

  First and second class mail to all addresses in Great Britain and Northern Ireland is accepted at all post office outlets. Post offices sell a range of postage stamps for affixing to letters and letter packets. The rate of postage is determined by the weight of the item and service(s) used.

- Philatelic Products

  A wide range of stamp related products are offered as gifts and souvenirs such as:

  ◊ First Day Covers;

  ◊ Presentation Packs;

  ◊ Collectors Packs.

- Redirection

  Applications to have mail redirected can be accepted in the first instance at all post office outlets.

- Priority Services

  The following services are offered in addition to the inland first class letter rate:

  ◊ Special Delivery: A guaranteed next day delivery by 12.30 pm to addresses in Great Britain and Northern Ireland (except Channel Islands and the Isle Of Man).

  ◊ Express Delivery: A supplementary service which is available to Channel Islands or the Isle of Man.

  ◊ Recorded Delivery: Ensures a signature on delivery.

  ◊ Registered Delivery: A guaranteed next day delivery by 12.30 pm with compensation for value of goods sent and signature on delivery.

  ◊ Consequential Loss: An additional insurance for use with registered mail where an item is worth more than its material value.

  ◊ Advice of Delivery: Used in conjunction with other priority services for proof of delivery.

  ◊ Cash on Delivery: Used in conjunction with registered mail, money is collected by Royal Mail from the addressee and paid to the sender in the form of a Girobank cashcheque.

- Poste Restante

POL00028135

Poste Restante is a facility provided for the convenience of travellers, which allows them to collect mail from a post office.

- Discount Wholesale Stamps For Retailers

  Many retailers now sell books of first and second class stamps. POCL offers a service arrangement which allows authorised retailers to purchase in bulk a range of stamp books at a discount. This is available at selected outlets as local demand warrants.

- Pre-Paid Mail

  The postage pre-paid (letters) service enables customers posting a minimum of 500 letters, to have their letters franked by Royal Mail instead of affixing postage stamps. This service is available at main post offices and authorised sub post offices.

- Articles For The Blind

  The inland articles for the blind service is a special service for transmission of articles which have been specially produced or adapted for use by the blind or visually handicapped. Items up to 7Kg are free of charge and treated as first class letters.

- Stamped Stationery

  Pre-paid envelopes for posting ordinary letters, and registered letter envelopes are available for sale at all post office.

- Undelivered Mail

  Letters may be undelivered because:

  ◊ Premises temporarily unoccupied and there is no letter box;

  ◊ Letter requires a signature;

  ◊ Postage is due;

  ◊ Item may be too large for delivery into the letter box.

  In such cases the postman/postwoman leaves an advice at the address informing the customer what has been done with the letter. In some localities these undelivered items are left for collection at post offices.

- Faxmail

  Faxmail is a high-speed facsimile service for transmission of documents between faxmail centres. The service is available at nominated main post offices (Faxmail centres) only. It offers same day delivery from the destination centre by messenger, or counter collection following telephone advice of receipt to addressee, or normal first class postal delivery. Customers may also send documents from a Faxmail centre direct to contacts with fax machines, provided that the customer can provide the appropriate fax number.

- Franking Machines

  Franking Machines are manufactured by a number of companies for sale or hire to firms or individuals wishing to pay the postage on letters and parcels by means of self-franked impressions rather than by the use of postage stamps or the postage pre-paid service.

  Each franking machine user operates such machines under licence from the Post Office.

POL00028135

The resetting (recharging) of machines to keep them in credit, thereby enabling their continued use, and the inspection of the machines to prevent their misuse is undertaken at nominated post offices or by Royal Mail staff on the customer's or Royal Mail premises.

1.29 International Letter Services

International letters can be accepted at all post offices. With a few exceptions, virtually anything which can normally be sent by post can be sent by one of the international letter services. There are two main classes of international letter service, Airmail (for speed) and Surface Mail (for economy). The rate of postage is determined by the weight of the item and service(s) used. Customs forms need to be completed by the customer when sending goods abroad or to the Channel Islands.

- Priority Services

  The following services are offered in addition to the main class of letter service:

  ◊ International Recorded: Available to all countries and ensures a signature on delivery.

  ◊ International Registered: Available to most countries with different levels of compensation available for value of goods sent and ensures signature on delivery.

  ◊ Swiftair: An express airmail service available to every country.

  ◊ Advice of Delivery: Used in conjunction with international recorded or international registered for proof of delivery.

- International Reply Coupon

  International Reply Coupons are sold at all post offices and are exchangeable in all countries in the world (except South Africa and Taiwan) for a stamp or stamps to the value of the minimum international airmail postage for a letter sent from the country of exchange.

- Postcards

  Postcards can be sent anywhere in the world by airmail or by surface mail to countries outside Europe.

- Aerogrammes

  Aerogrammes are available at post offices and can be sent anywhere in the world by airmail. An aerogramme is a prepaid airmail letter which contains no other items.

- Small Packets

  The Small Packet service is designed for the transmission of goods, gifts and trade samples to international destinations. Although these items can be sent by the letter service, small packet offers cheaper airmail and surface mail rates.

- Air Packs

  Airpacks are padded envelopes with postage prepaid up to 560 grammes which are designed for sending gifts and merchandise by the airmail packet service. The airpack also includes a pre-printed C1 customs form and an airmail label.

POL00028135

- Printed Papers

  The Printed Papers service is designed for the transmission of books, newspapers and other non-personalised printed items to international destinations. It is the cheapest of the Royal Mail International services.

- Articles For The Blind (International Service)

  The International Articles for the Blind service is a special Royal Mail International letter service for transmission of articles which have been specially produced or adapted for use by the blind or visually handicapped. Surface mail up to 7kg is free and airmail rates are very cheap.

- Postage Prepaid

  In the same manner as for inland mail, the postage prepaid service enables customers posting a minimum of 500 items to have the mail franked by Royal Mail. It is accepted at all main post offices and sub post offices where local demand warrants the service.

1.30 Parcelforce

POCL offers parcel services to all inland (Great Britain and Northern Ireland and Isle of Man) and international destinations on behalf of Parcelforce, (a business of the Post Office). Advice and information on all Parcelforce services is available. There are rules and restrictions covering the posting of parcels (e.g. flammable liquids, size restrictions, alcohol may not be sent to Moslem countries). The price of each service varies with the weight of the item (and country of destination for international postings). Payment can be made by cash, cheque (if supported by a valid cheque guarantee card or Post Office Authority Card).

Briefly the parcel services offered are:

- Parcelforce Standard

  A basic, reliable, but not guaranteed delivery service within Great Britain, Northern Ireland, and Isle of Man. Maximum compensation of £20 per parcel.

- Compensation Fee Service

  Used in conjunction with Parcelforce standard offers two levels of cover against loss or damage up to £500.

- Parcelforce 24 and Parcelforce 48

  Provides a guaranteed next day and two day delivery service to over 95% of all Great Britain, Northern Ireland, and Isle of Man. Includes pro-rata cover for delay and cover for loss or damage up to £500 per parcel.

- Parcelforce Datapost

  A premium service providing a guaranteed next morning delivery service to all main business centres in Great Britain and Northern Ireland - either by 10am or by noon. Offers compensation cover for delay (on a pro-rata basis), loss or damage up to £500 per parcel and consequential loss up to £5,000 per consignment within a single fee.

- International standard service

  An international standard service for delivery to over 200 destinations worldwide with exclusive compensation cover of up to £250 for loss or damage.

POL00028135

- International Economy Service

  A basic international delivery to almost anywhere in the world. Compensation for loss or damage is paid at the discretion of Parcelforce.

- International Euro 48*

  Offers guaranteed delivery, within 2/3 days to countries within Europe with inclusive compensation cover, loss or damage up to £1,000 and for delay a refund of the fee. It does not offer consequential loss.

- International Datapost

  Offers an express, guaranteed delivery service to 200 countries and territories world-wide. For a single all inclusive fee compensation cover for loss or damage up to £5,000 per parcel, consequential loss up to £10,000 per parcel and delay in delivering a full refund of the initial fee.

  All international items and postings to the Channel Islands require customs declaration forms to be completed and affixed to the parcel.

[* This service is presently only offered by Parcelforce direct to contract and business customers. POCL are jointly planning with Parcelforce to offer these services at post offices from summer 1995.]

This section has provided a snapshot of the main services offered through POCL as of December 1994. It is in the nature of the retail offer that services change. Due to the government's commitment to Commercial Freedom POCL hope to offer new services not listed here but POCL also realise in the modern competitive market place that some services may cease to be offered in time. Prospective service providers should understand that in Spring 1996 (estimated start of roll out of automation) there will inevitably be changes to the services provided on behalf of clients by POCL.

POL00028135

Appendix 3-2

POCL IS Strategy

POL00028135

POST OFFICE COUNTERS Ltd

INFORMATION SYSTEMS STRATEGY

Section I: Information Systems Strategy Context

1. The Information Systems Strategy of Post Office Counters Ltd is made up of 2 main components:

   - the Technical Infrastructure, which describes ***how*** various pieces of technology fit together.
   - the Applications Portfolio, which describes ***what*** systems are required to support the mission and vision of the business.

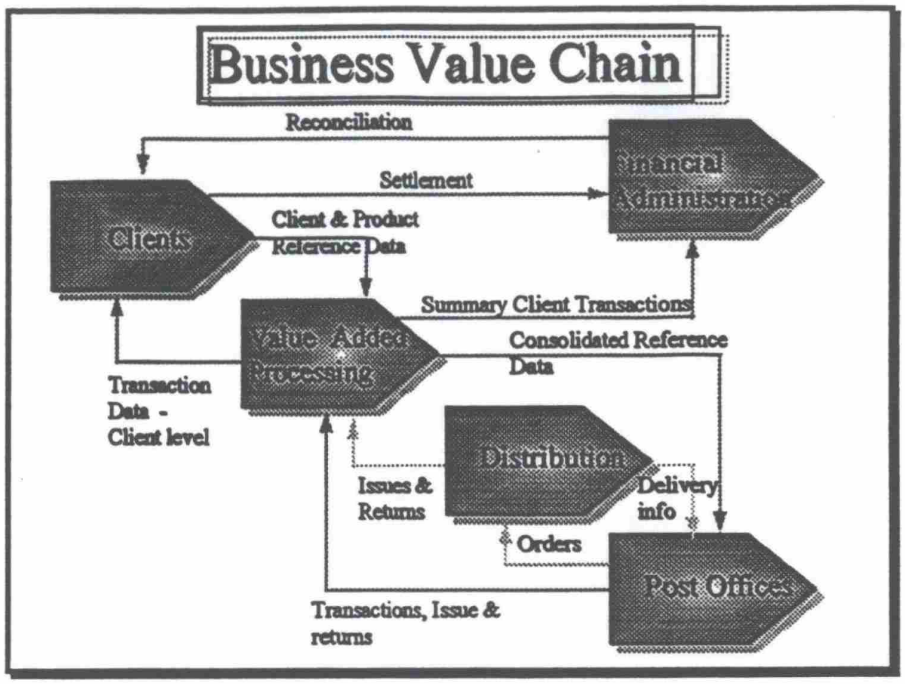
2. The Technical Infrastructure is described in a separate document held by the Information Systems Strategy Unit.

3. The Applications Portfolio for Post Office Counters Ltd focuses on the underlying business processes which will continue to support the operation of our business, irrespective of organisational or product detail changes. There are 5 key processing areas which make up the core business of Post Office Counters Ltd., known as the 'Business Value Chain'. They are shown in Diagram I below, together with the key data flows that link them together, and comprise:

   - Clients: who influence the shape of the transaction
   - Post Offices: which deliver client transactions to customers
   - Value Added Processing: which allows a small number of clients (< 200) to communicate with a large number of Post Offices (> 19 000), and in turn, allows the Post Offices to send relevant transaction information back to them.
   - Distribution: this includes the planning and physical distribution of cash and stock across the business, and the balancing of the 'pipeline'.
   - Financial Administration: which is concerned with the reconciliation of client transactions and the settlement of client monies, as well as statutory accounting and treasury functions.

POL00028135

Diagram I : The Business Value Chain



POL00028135

Section II: Post Office Counters Applications Architecture

1. This document describes the applications architecture which has been adopted for use in Post Offices and devised by the Information Systems Strategy Unit of Post Office Counters Ltd. It forms part of a set of documentation which together describe the overall Information Systems Strategy for Post Office Counters Ltd. All future systems work in Post Offices will comply with the principles outlined in this document.

2. In addition to this section, the document comprises of the following:

   - *Section III:* Sets out the objective of the applications architecture, and describes the scope and boundaries of the applications for Post Offices, and summarises the applications architecture.

   - *Section IV:* Outlines the process that has been adopted in defining the architecture

3. These sections are supported by annexes which hold more detailed information about the activities undertaken by Post Offices, high level data entities which need to be supported, application descriptions, and data flow diagrams to support them.

POL00028135

Section III: The Applications Portfolio for Post Offices

1. The applications portfolio for Post Offices describes all of the systems which should be found in an automated Post Office, together with their key data flows and interfaces.

2. The Applications Portfolio has been designed to:

   - Support the existing lines of business performed by the Post Office, future lines of business as identified by the Commercial Strategy of Post Office Counters Ltd., and the sub-postmasters private business.
   - Encourage the use of standard, packaged software wherever appropriate, and discourages tightly integrated and inflexible solutions.
   - Be implemented on industry standard, 'open', hardware and software platforms.

3. The applications within the portfolio have been summarised into three groupings (or tiers) based upon the function that they provide within the Post Office. The three tiers are:

   - Basic Trading Systems: These are the applications which are needed in order to transact Post Office business. The Basic Trading Systems are represented by the middle tier on the model which can be found in Annex I.
   - Back Office Processing: These are applications which give administrative efficiency to Post Offices. These applications are represented by the top tier on the model which can be found in Annex I.
   - Reporting & M.I.S : These are applications which are needed to report back to the Post Office hierarchy (and in some cases Clients), and which enable Post Office staff to identify business improvement opportunities. These applications are represented by the bottom tier on the model which can be found in Annex I.

4. The model in Annex I gives a complete picture of all the applications that are ultimately required to support a Post Office, together with an indication of the way in which they interface with each other. Those applications which require greater definition have been amplified in the schedules which appear in Annex II. These include:

   - Personal Details Capture
   - In-Pay
   - Out-Pay
   - Basic EPOS transaction
   - Token Management
   - Purchase Order Management
   - Information Provision
   - Stock Management
   - Staffing
   - Financial Accounting

POL00028135

5. In addition, the Reporting and M.I.S applications are likely to be delivered through a set of data delivery, or EIS tools which cover:

   - Regular reporting: These are reports that will be delivered through standard screen or paper based reporting tools which give the user a limited set of parameters to report by.
   - Story-book reporting: These are screen based reporting tools which generate updated information on a regular basis (in text and graphical format), but the sequence of the 'reporting pack' is fixed.
   - 'Slice & Dice' reporting: These are screen based reporting tools which allow users to view data, or summarise it, in a user definable flexible way.
   - Data Driven reporting: These are screen based reporting tools within which there is a set of rules, such that the system analyses the data and only reports on data which meets the user defined rules (e.g. exception reporting, Top 20, changes in contribution etc.)

6. Finally, the applications portfolio is a dynamic tool, and will be updated to reflect additions, as they become known.

7.

Section IV: Outline of the process used to define the architecture

1. The process used to define the applications architecture for post offices included the following steps:

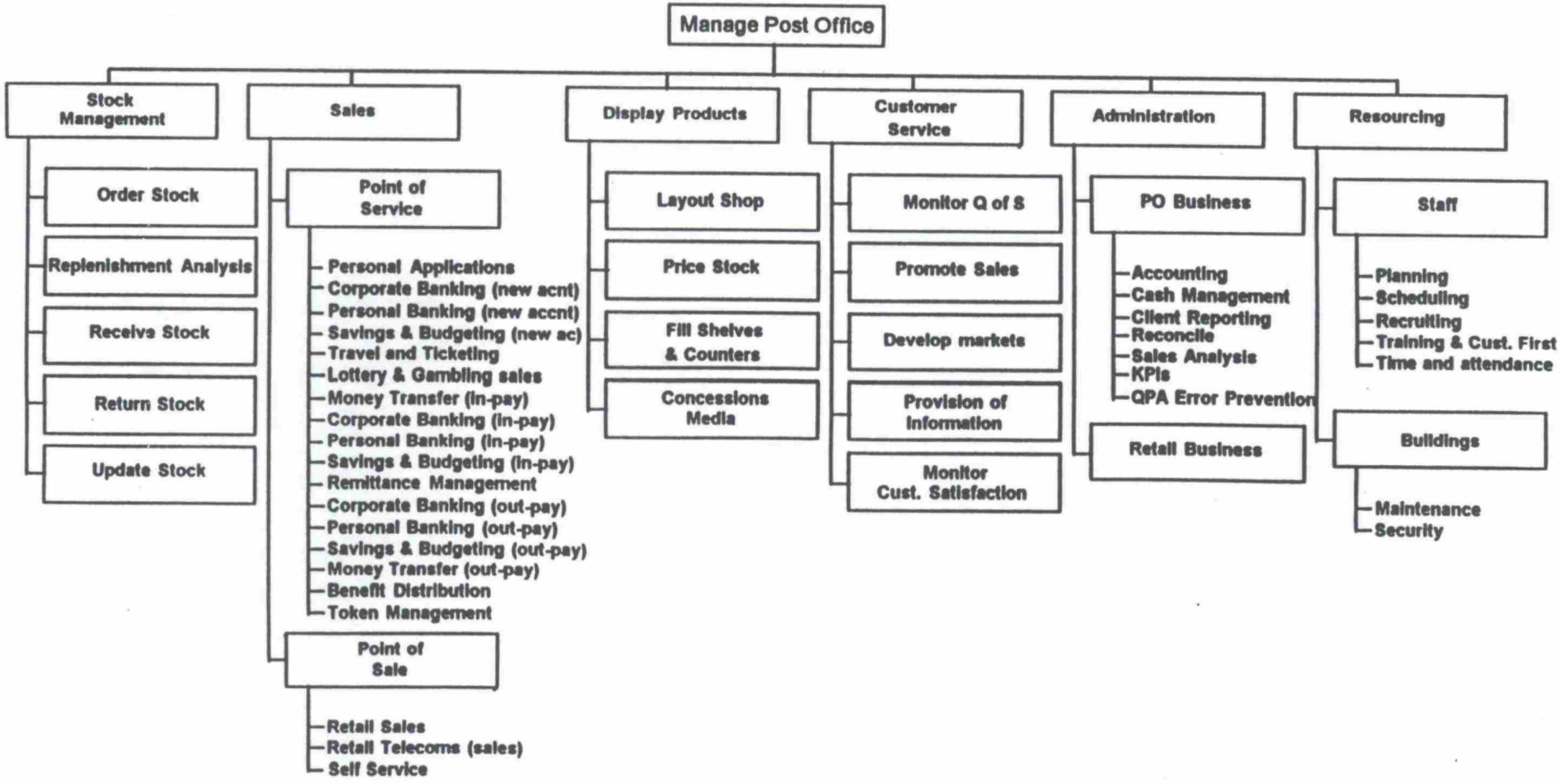
Process	Output	Reference
1. Define the Activity Model for Post Office	Activity Model to cover existing lines of business, future lines of business, and the sub-postmasters private business	Annex I
2. Define the key data elements required by the Post Office function	Process/Entity Matrix and associated data definitions	Annex II
3. Document the key data flows/applications	Application descriptions for key applications, including associated business processes supported, systems processes, data flows, interfaces, and technologies used.	Annex III
4. Prepare the applications portfolio for Post Office	Applications Portfolio map	Annex IV

POL00028135

Annex I: Activity Model for Post Offices

POL00028135

ACTIVITY MODEL for POST OFFICES



POL00028135

Annex II: Process / Entity Matrix

POL00028135

Process / Entity Matrix

	PROCESS \ ENTITY	Supplier Details	Stock item standing data	Product cross reference	Purchase Order	Supplier dispatch note	PO (returns) dispatch note	Transfer docket	PO standing data	Stock	Receipt	Client Standing Data	Voucher / Token details	Transaction details	Tender Type	Tender type authorisations	Customer Personal Details	Cash withdrawals	Pricing Look-up Table	Authorisations	Sales History	Ledgers	PO Encyclopedia	Quality of Service data	Employee Standing Data	Staff records	Token Management	In-pay	Out-pay	Token in	Token out
STOCK CONTROL																															
	Order Stock	X	X	X	X				X																						
	Replenishment Analysis		X							X											X										
	Receive Stock				X	X		X																							
	Return Stock	X			X	X	X	X																							
	Update Stock					X	X	X		X												X									
SALES																															
Personal Details Capture	Point of Services																														
	Personal Applications									X	X	X	X	X	O	O	X		X									O			X
	Corporate Banking (new accnt)									X	O	X	X	X	O	O	X											O			X
	Personal Banking (new accnt)									X	O	X	X	X	O	O	X											O			X
	Savings & Budgeting (new accnt)									X	O	X	X	X	O	O	X											O			X
	Travel & Ticketing									X	X	X	X	X	X	X	X		X									X			X
	Lottery/Gambling (sale of)									X	X	X	X	X	X	X	X											X			X
	Money transfer (in-pay)								X	X	X	X	X	X	X	X	X		X									X			X
In-pay	Corporate Banking (in-pay)									X	X	X	X	X	X	X												X		X	
	Personal Banking (in-pay)									X	X	X	X	X	X	X												X		X	
	Savings & Budgeting (in-pay)									X	X	X	X	X	X	X												X		X	
	Remittance Management									X	X	X	X	X	X	X												X		X	
Out-pay	Corporate Banking (out-pay)									X	X	X	X	X				X		X								X	X	X	
	Personal Banking (out-pay)									X	X	X	X	X				X		X								X	X	X	
	Savings & Budgeting (out-pay)									X	X	X	X	X				X		X								X	X	X	
	Money transfer (out-pay)									X	X	X	X	X				X		X									X	X	
	Benefits Distribution									X	X	X	X	X				X		X									X	X	
	Token Management								X			X	X	X						X							X				X

O = optional

POL00028135

Process / Entity Matrix

	Point of Sale																										
	Retail Sales									X	X			X	X	X			X								
	Retail Telecoms (sales)	X								X	X			X	X	X	X		X								
CUSTOMER SERVICE																											
	Monitor Q of S								X															X			
	Analyse Sales																										
	Promote Products																										
	Develop Markets																										
DISPLAY PRODUCTS																											
	Layout Shop																										
	Price Products																										
	Fill Shelves & Counters																										
	Concessions/Media																					X					
	Information provision								X					X									X					
ADMINISTRATION																											
	PO Business																										
	Accounting					X	X	X	X	X				X	X			X				X				X	
	Cash Management					X		X	X	X					X			X				X					
	Client Reporting								X			X		X	X	X				X	X				X		
	Reconcile														X			X									
	Sales Analysis													X							X						
	Retail Business																										
RESOURCING																											
	Staff																										
	Scheduling								X															X	X		
	Recruitment																										
	Training								X															X	X		
	Time and attendance								X															X	X		
	Buildings																										
	Maintenance																										
	Security																										

O = optional

POL00028135

Entity Definitions

Supplier Details

Standing details of all internal and external suppliers.
This will cover common data such as name address and could include lists of products, discount rates, payment terms etc.

Stock Standing Data

General description of stock item including re-order levels.

Product Cross Reference

Cross reference of stock items with similar attributes.

Purchase Order

Official Post Office order for the supply of stock items.

Suppliers Dispatch Note

List of stock items accompanying any delivery of such items to a Post office

PO Return Note

List of items being returned to a supplier. This includes transfer of stock to other Post Offices

Transfer Docket

Internal Post Office equivalent of a supplier dispatch note.

Post Office Standing Data

Address and reference number of Post office outlet. Might also include manager's name, number of staff etc.

Stock

This is split between valued and non-value stock.
Value stock are items for which the counter clerk must account. e.g. Stamps, electricity token.
Non-value stock are items which clerks require in the performance of their duty but for which no accounting is required. e.g. Forms, leaflets.
see also Token management

Receipt

Printed receipt prepared at the time of the transaction.

Client Standing Data

Standing details of all clients.
This will cover common data such as name address and could include lists of products / services performed for that client.

POL00028135

Vouchers / Tokens

This covers both physical and electronic vouchers and tokens. Examples are, electricity pre-payment tokens, postal orders, passports, plastic cards, DSS instructions-to-pay.

Transaction Details

Record of each counter transaction for which the clerk is accountable.

Tender Type

This involves in-pay and out-pay. For in-pay, this is the method-of-payment . e.g. cash, cheque, postal orders. For out-pay, these are the vouchers / tokens against which the out-pay is made.

Tender Type Authorisation

This covers the authorisation of non-cash methods of payment. These range from "stop lists" through guarantee cards to on-line confirmation of funds availability.

Customer Personal Details

Details of a customer such as name and address which must be captured, electronically or in writing as part of the transaction. e.g. passports, bus passes, money transfers.

Cash Withdrawal

Cash out-payments.

Product and price look-up

Manual or electronic reference to a price list for transactions which are priced according to variables such as weight , destination.

Authorisations

Validation of the voucher / token being submitted against which the counter clerk will make payment. e.g. Money transfer, DSS benefit foil or instruction-to-pay..

Sales History

Daily, weekly, annual history of all sales transactions against which analysis can be performed.

Ledgers

Post Office accounts. General ledger, purchase ledger, cash book etc.

PO Encyclopaedia

Reference manual for the operation of a Post Office. This covers standing PO instructions and special client instructions

Quality of Service Data

All information gathered in respect to the measurement and provision of a quality service at Post offices.

POL00028135

Employee Standing Data

Standing details of all employees.
This will cover common data such as name, address, PO grade, etc.

Staff Records

Attendance records, shift patterns etc. for each employee.

Token Management

Items of value for which the Post Office provides a secure distribution service but which is not regarded as stock.

POL00028135

Annex III: Application Descriptions

POL00028135

Application Description

Application Name	Personal Details Capture
Package / Bespoke	Bespoke

Objectives

Record pertinent / relevant customer details against the transaction

Business Processes

1 Clerk accepts application form and supporting documentation as appropriate. e.g. driver's licence, passport, authenticated photograph.

2 Clerk has ability to capture customer's name, address and other pertinent details.

note Applications involving an initial deposit (not payment) continue through In-Pay Transaction. Where no deposit is involved, process continues with Basic EPOS Transaction.

System Processes

1 Accept transaction identifier and paint appropriate data entry screen.

2 Accept data entry from keyboard or other input device (bar code reader etc.)

3 Retrieve data held by system and / or paint screen for further keyboard entry

4 Store all transaction details as temporary subject to end-of-session confirmation.

5 If transaction involves customer making initial deposit (not payment), pass control to In-Pay Transaction.

6 If no initial deposit to be made, pass control to Basic EPOS Transaction.

Key Data Flows

Customer Details
Client Standing Data
Transaction Details

POL00028135

Key Interfaces

Internal

Transaction Process Shell
In-Pay Transaction
Basic EPOS Transaction

External

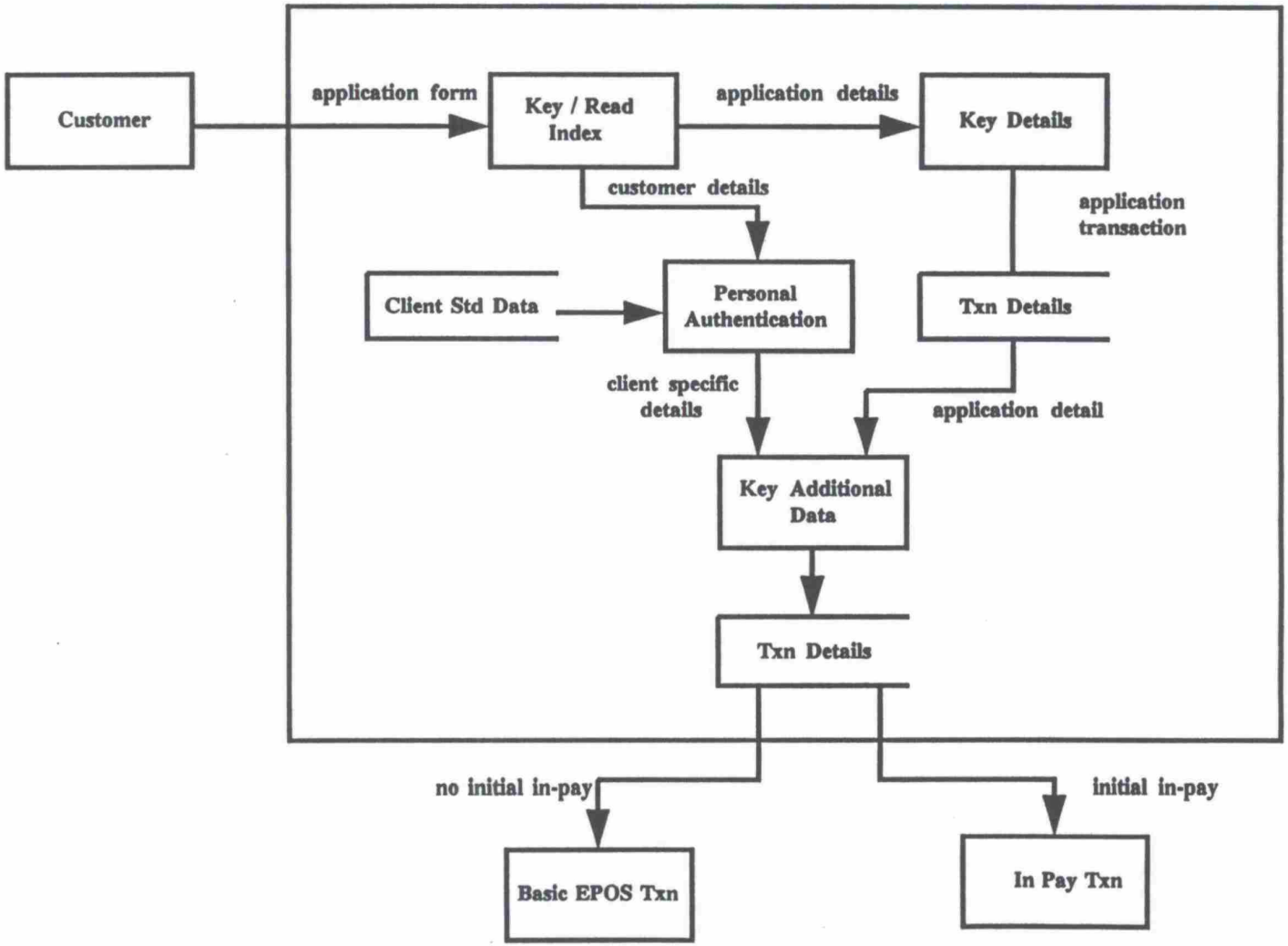
Customer Application Form

Technology Types

Bar code readers

POL00028135

Personal Details Capture



POL00028135

Application Description

Application Name	In-pay
Package / Bespoke	Bespoke

Objectives

To record the receipt of in-payments for deposit to customer's accounts or bill payments

Business Processes

1 Clerk accepts remittance advice, deposit slip or other voucher / token and tender(s).

2 Clerk has ability to key or machine read in-pay details from remittance advice, deposit slip or other voucher / token.

3 Clerk has ability to key in-pay amount if not part of machine read codeline.

note transaction continues through Basic EPOS Transaction.

System Processes

1 Accept transaction identifier from keyboard, other input device or other (Point of Service) transaction and paint appropriate data entry screen.

2 Accept data entry from keyboard or other input device (card swipe, bar code reader etc.)

3 Retrieve data held by system and / or paint screen for further keyboard entry

4 Store all transaction details as temporary subject to end-of-session confirmation.

5 Validate voucher / token data to client rules. If valid, paint screen for entry of amount to be paid in.

6 Accept data entry from keyboard or other input device.

7 Pass control to Basic EPOS Transaction.

Key Data Flows

Customer Details
Client Standing Data
Transaction Details

POL00028135

Key Interfaces

Internal

Transaction Process Shell
Basic EPOS Transaction

External

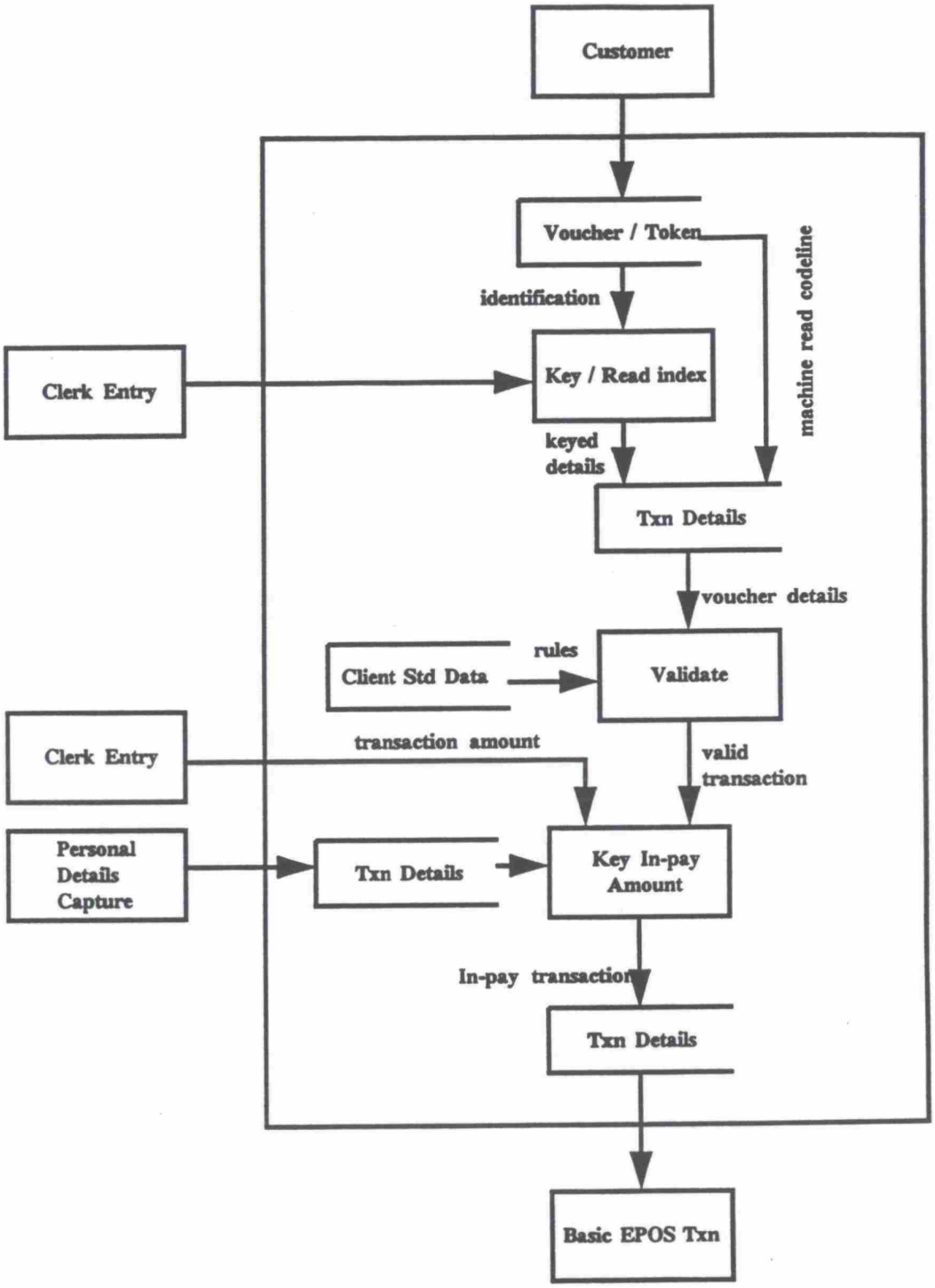
Customer voucher / token

Technology Types

Bar code readers
Magnetic stripe readers
Smart card

POL00028135

In Pay



POL00028135

Application Description

Application Name	Out-pay
Package / Bespoke	Bespoke

Objectives

To record the out-payments to customers from their accounts or on behalf of a client.

Business Processes

1 Clerk accepts customer's voucher / token.

2 Clerk has ability to key or machine read in-pay details from voucher / token.

3 Clerk has ability to key out-pay amount if not part of machine read codeline.

note *transaction continues through Basic EPOS Transaction.*

System Processes

1 Accept transaction identifier from keyboard, other input device and paint appropriate data entry screen.

2 Accept data entry from keyboard or other input device (card swipe, bar code reader etc.)

3 Retrieve data held by system and / or paint screen for further keyboard entry

4 Store all transaction details as temporary subject to end-of-session confirmation.

5 Validate voucher / token data to client rules. If valid, paint screen for entry of amount to be paid out.

6 Accept data entry from keyboard or other input device.

7 Establish authorisation for pay-out.

8 Pass control to Basic EPOS Transaction.

Key Data Flows

Customer Details
Client Standing Data
Transaction Details

POL00028135

Key Interfaces

Internal

Transaction Process Shell
Basic EPOS Transaction

External

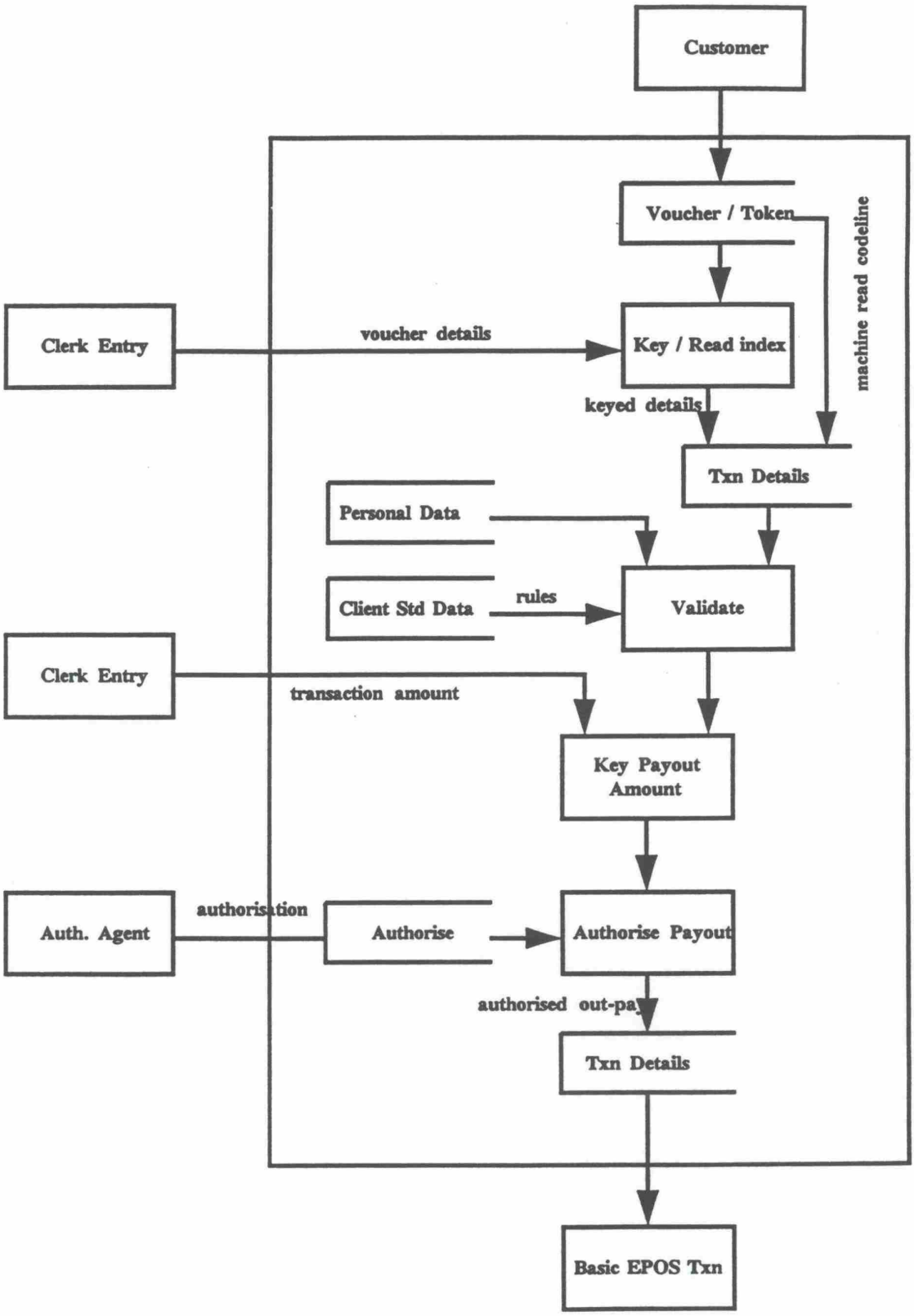
Customer voucher / token

Technology Types

Bar code readers
Magnetic stripe readers
Smart card

POL00028135

Out Pay



POL00028135

Application Description

Application Name	Basic EPOS Transaction
Package / Bespoke	ARTS compliant package

Objectives

To manage all common Point of Sale transaction activities and complement the Point of Service transactions. Features include:

- Product and price look-up
- Receipt production
- Method of payment and authorisation
- Stock update
- Token endorsement

Business Processes

1 Clerk will have the ability to select from a menu of processes:

- In pay transaction
- Out pay transaction
- Personal Details Capture
- End-of-session

or invoke:

- standard EPOS transaction of Product code, quantity

2 Clerk will follow system prompts as appropriate to selection made.

3 When end-of-session selected, clerk will have ability to record tender type(s) and amount(s). This could involve use of keyboard or machine readable medium.

4 Where appropriate, clerk will have the ability to endorse a customer voucher / token.

System Processes

1 Accept transaction identifier from keyboard, other input device or other (Point of Service) transaction and paint appropriate data entry screen.

2 Accept data entry from keyboard. This may be:

- Product code and quantity.
- Request to enter further Point of Service transaction.
- End-of-session confirmation.

3 Where appropriate, perform product / price look-up. If no price found, prompt and accept keyboard input

4 Store all transaction details as temporary subject to end-of-session confirmation.

POL00028135

5 When end-of-session is confirmed, perform totalling and displays session totals and requests input of tender type(s) and amount(s).

6 Where tender type requires authorisation, system invokes authorisation as appropriate. (Debit card cheque guarantee etc.)

7 Update stock holding of products sold.

8 Endorse token, if appropriate.

9 Produce receipt.

10 Record transaction details as permanent.

11 Pass control to Transaction Process Shell.

Key Data Entities

Product / price Look-up File
Tender Type Authorisation.
Stock File
Transaction Details

Key Interfaces

Internal

Transaction Process Shell
In-pay Transaction
Out-pay Transaction
Personal Details Capture

External

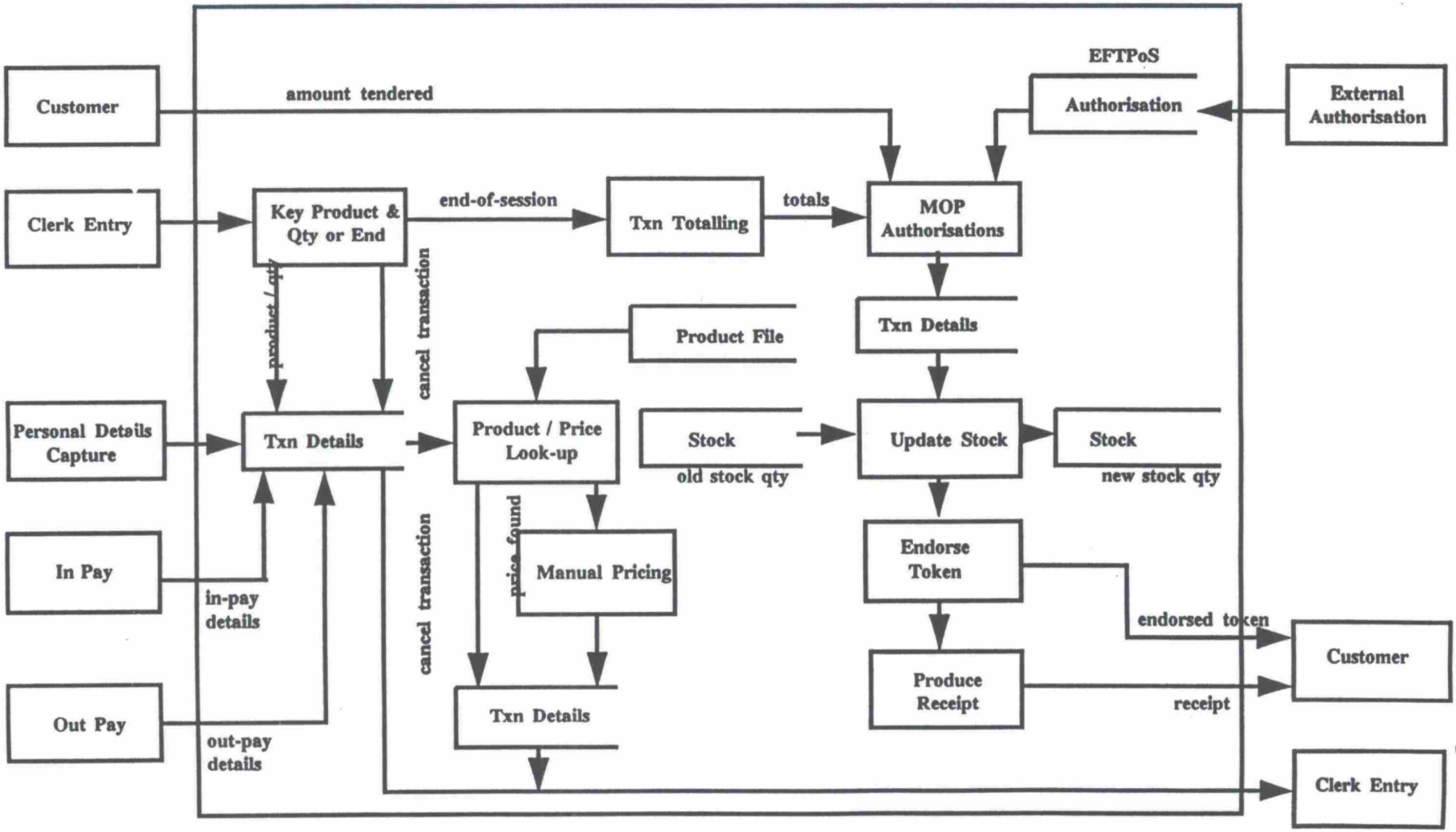
Client / Bank authorisation system.

Technology Types

Bar code readers
Magnetic stripe readers
Smart card reader/writers

POL00028135

Basic EPOS Transaction



POL00028135

Application Description

Application Name	Token Management
Package / Bespoke	Bespoke

Objectives

Manage the distribution of client tokens as a service. These tokens do not form part of Post Office stock but are "valuable".

Business Processes

1 Clerk accepts collection notice or other form of personal identification. e.g. expired benefit book.

2 Clerk has ability to validate (authenticate) the collection notice or other form of identification.

3 Clerk has the ability to record the issue of the token.

System Processes

1 Accept transaction identifier and paint appropriate data entry screen.

2 Accept data entry from keyboard or other input device (card swipe, bar code reader etc.)

3 Retrieve data held by system and / or paint screen for further keyboard entry

4 Accept confirmation of issue from keyboard or other input device.

5 Update token management files.

Key Data Flows

Customer Identification
Collection notice
Client Standing Data
Transaction Details

Key Interfaces

Internal

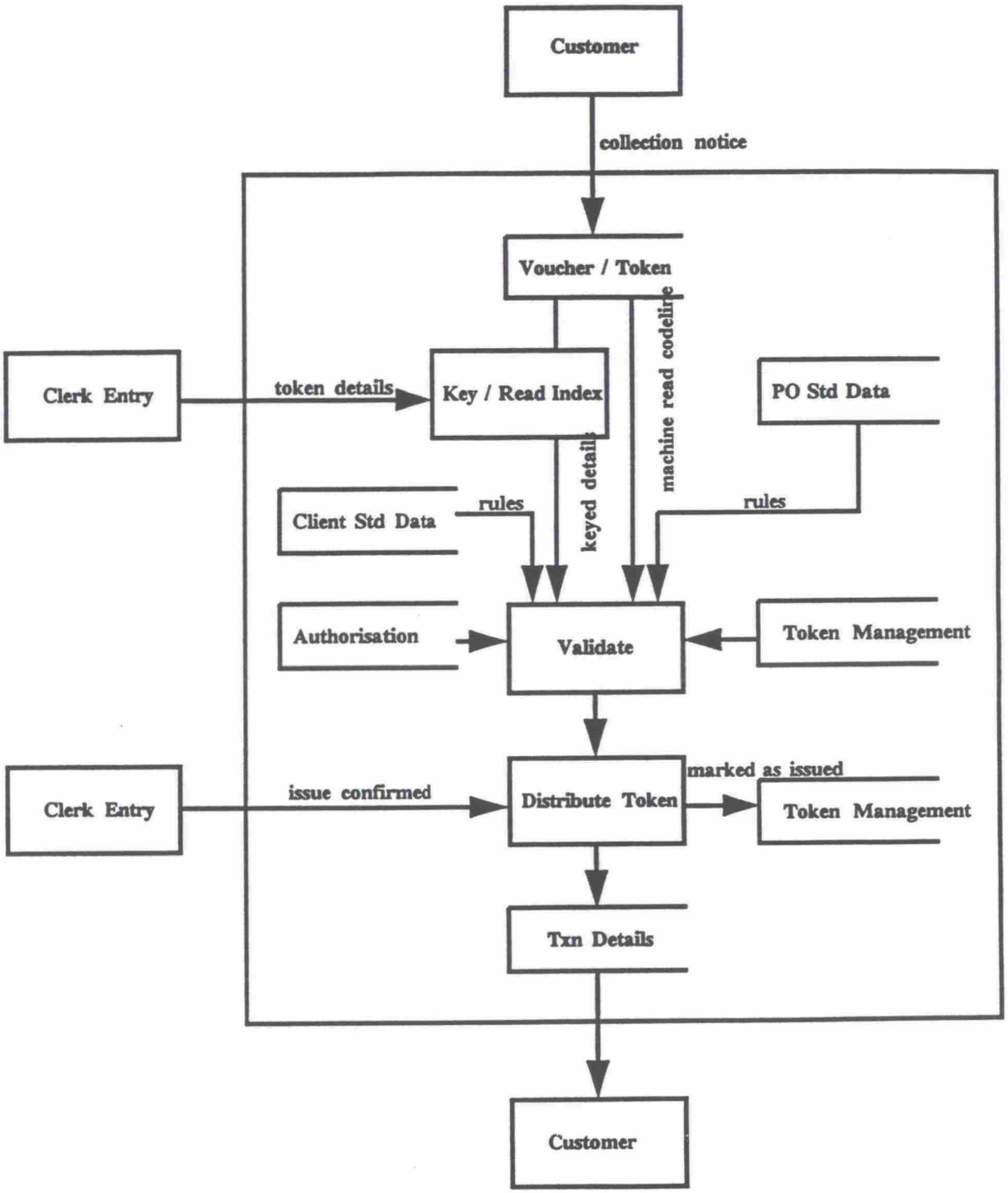
Transaction Process Shell

External

Collection notice

POL00028135

Token Management



POL00028135

Application Description

Application Name	Purchase Order Management
Package / Bespoke	Package

Objectives

Control the purchase and return of stock from / to suppliers (including other Post Offices).

Business Processes

1 User will have the ability to enter for each stock item;
- supplier reference
- product code
- quantity
- price quoted (optional)

2 User will have the ability to interrogate status of outstanding orders.

3 User will have the ability to mark stock items received as return-to-supplier.

System Processes

1 Accept data entry from keyboard. This may be

- goods in data
- goods to be returned data
- enquiry on status of stock item

2 Accept data entry from keyboard additional data as appropriate

3 Print order on supplier or return dispatch note.

Key Data Flows

PO Standing Data
Supplier Standing Data
Stock item Standing Data
Purchase Order Details
Product Cross Reference

Key Interfaces

Internal

Stock Control
Financial Accounting

External

PO Purchase Order

POL00028135

Technology Types

Local Area Network (LANs)

POL00028135

Application Description

Application Name	Information Provision
Package / Bespoke	Package

Objectives

To provide both "active" and "passive" information to customers regarding products and services available from Post offices and clients.

Business Processes

Active

1 Customers will have the ability to interact with the information provision medium.

2 Customers will have the ability to "print" selected information to take away.

3 Customers will have the ability to request further information to be sent directly to them (at home).

4 Customers will have the ability to discuss information with "provider" via video links.

5 Customer will have the ability to pay for selected items of information.

Passive

6 Information is on continuous "loop" and screened / available at strategic positions within the office. Information may be up-to-the-minute but customer plays no direct part in the type or frequency of screening.

System Processes

Active

1 Accept data entry from keyboard (or touch sensitive screens) and paint information screens or further data entry screens as appropriate.

2 Where necessary, perform product / price look-up.

3 Accept data entry from keyboard and save data for down-loading to centre for further processing by client.

4 When required, print details of information selected by customer.

5 Accept payment details from credit / debit cards where appropriate.

Passive

6 System will have the facility for keeping the information current.

7 Frequency of individual topics will be selectable. This could be central or transactional based.

POL00028135

Key Data Entities

Product / price Look-up File
Tender Type
Tender Type Authorisation.
Transaction Details

Key Interfaces

Internal

External

Bank authorisation system.

Technology Types

Magnetic stripe readers
Smart card reader/writers

POL00028135

Application Description

Application Name	Stock Management
Package / Bespoke	Package

Objectives

Accurate recording of stock levels (stock keeping) and the reporting of re-order requirements (replenishment analysis).

Business Processes

Replenishment Analysis

1 This is an automatic process invoked at periodical intervals, by users or time scheduled event.

Stock Keeping

2 Clerk has the ability to record the arrival of stock from supplier or "other" Post Office.

3 Clerk has the ability to "transfer" stock to "other" Post Office at the request of that Post Office.

4 Clerk has the ability to record "sales" of stock. (This may be automatic if links to transaction details logs are available).

System Processes

Replenishment Analysis

1 Build "sales" profile for period leading up to analysis.

2 Adjust profile to cater for forecasted "sales".

3 Compare profile to current stock levels and delivery lead times.

4 Reports recommended re-order quantities.

Stock Keeping

5 Accept transaction identifier and paint appropriate data entry screen

6 Accept data entry from keyboard or other input device.

7 Retrieve stock record for product identified.

8 Apply changes (increases / decreases) to current stock level.

9 Record transaction on transaction log

POL00028135

Key Data Flows

Supplier Dispatch Note Details
PO Transfer Docket Details
PO Dispatch Note Details (returns)
Transaction Details

Key Interfaces

Internal

Purchase Order System.
Transaction Details Log

External

Supplier Dispatch Note
PO Transfer Docket
PO Dispatch Note

Technology Types

Bar code readers
Local Area Network (LANs)

POL00028135

Application Description

Application Name	Staffing
Package / Bespoke	Package

Objectives

To record (time and attendance) and manage the availability (scheduling) of staff to ensure standards of service are maintained:

Business Processes

Scheduling

1 Manager will have the ability to record planned periods of absence.

2 Manager will have ability to invoke scheduling algorithm.

3 Manager will have ability to accept or modify schedule proposed by algorithm.

Time and Attendance

4 Manager / clerk(s) will have the ability to record start and end of each period of work.

System Processes

Scheduling

1 Accept data entry from keyboard. This may be:

Add new staff members
Delete staff members no longer employed
Record periods staff will not be available for work

3 Using known staff numbers, staff availability and recent working schedules, propose schedule for forthcoming period.

4 Accept, through keyboard, modifications to proposed schedule.

5 Re-work schedule for forthcoming period based on modifications input.

Time and Attendance

6 Accept data entry from keyboard or other input device (smart card reader)

7 Retrieve staff record and record time and date of entry.

POL00028135

Key Data Entities

PO standing data
Employee standing data
Staff records

Key Interfaces

Internal

Financial Accounting

External

Technology Types

Bar code readers
Smart card reader/writers
Local Area Network (LANs)

POL00028135

Application Description

Application Name	Financial Accounting
Package / Bespoke	Package / Bespoke

Objectives

To maintain the financial records of the post office

Business Processes

1 These provide all the "standard" features and functionality of:

Sales ledger
Purchase ledger
General ledger
Fixed Assets register

and

Outlet Remuneration and Reconciliation

System Processes

Ledgers and Asset Register

1 Systems process will be as per "standard" package offering but will be "configurable".

Remuneration and Reconciliation

2 System will take copy of daily transaction details log and update history

3 Transaction are sorted by client and reconciliation reports produced periodically

4 Transactions are analysed by type and post master remuneration report produced.

Key Data Flows

PO standing Data
Client Standing Data
Transaction Details
Purchase Order Details

Key Interfaces

Internal

Transaction Details Log

External

POL00028135

Technology Types

Local Area Network (LANs)

POL00028135

Application Description

Application Name	Administrative Support
Package / Bespoke	Package

Objectives

To provide administrative support to post office management and staff.

Business Processes

1 These provide all the "standard" features and functionality of:

Word Processing	MS Word
Spread Sheets	MS Excel
Graphics / presentations	MS Powerpoint
Database	MS Access
Electronic Mail	MS cc Mail

System Processes

1 Systems processes will be as per "standard" package offerings.

Key Data Flows

Key Interfaces

Internal

External

Technology Types

Local Area Network (LANs)

POL00028135

Application Description

Application Name Sales Analysis

Package / Bespoke Report Writing Package

Objectives

To analyse product sales by volume, value and time

Business Processes

1 User will have the ability to "construct" Sales reports to a standard style from data held by office, region and company

Key Data Flows

Transaction Details

Key Interfaces

Internal

Transaction Details Log

External

Head Office
Regions
Clients

Technology Types

Local Area Network (LANs)

POL00028135

Application Description

Application Name	Contribution Analysis
Package / Bespoke	Report Writing Package

Objectives

To report on Business Performance for individual post offices.

Business Processes

1 User will have the ability to "construct" Contribution Analysis reports to a standard style from data held by office, region and company

Key Data Flows

Transaction Details

Key Interfaces

Internal

Transaction Details Log

External

Head Office
Regions

Technology Types

Local Area Network (LANs)

POL00028135

Application Description

Application Name	Quality of Service
Package / Bespoke	Report Writing Package

Objectives

Analyse the Waiting Time and perform Customer Counting for individual post offices from transaction details.

Business Processes

1 User will have the ability to "construct" Quality of Service reports to a standard style from data held by office, region and company

Key Data Flows

Transaction Details

Key Interfaces

Internal

Transaction Details Log

External

Head Office
Regions
Clients

Technology Types

Local Area Network (LANs)

Technology Types

Bar code readers
Magnetic card reader

POL00028135

Annex IV: Applications Portfolio for Post Offices

POL00028135

2.4 Balancing and accounting

CRISP provides the following functionality:

- For each cash account week end, a printed report is generated along with a transmission file for all transactions occurring during the week. This file must is retained and accessible for the following cash account week. The summary file which is printed at the site is be produced at a departmental level. The transmission file is at item level.
- Weekly sales levels and till uploads
- Weekly sales and goods movement reports
- Reports from PostShops to a central location
- Cash and stock transfers to/from main counter and other PostShops
- deliveries from suppliers, returns to suppliers
- facilities to count and check stock

2.5 General

The system is designed to be capable of accepting all types of required payment methods

Reference data is maintained centrally

Reference data maintenance is password protected and an audit trail of all changes is maintained.

Promotions and item discounts are catered for.

2.6 Volumes

The PostShop network is currently 209 with forecast growth of 30 new sites per year. Current total forecast is approximately 350 sites by 1999/2000. The HP3000 processes an average of 150,000 records from PostShops daily. There are currently around 150 suppliers offering c. 9,000 products.

3. New Software Distribution

Updates are provided by RIVA and downloaded to the outlets from Chesterfield.

4 Help Desk Facility

POCL operates a central help desk facility, located in Chesterfield for all hardware and software calls.

5 Training

There is no official training course for retail assistants using the system.

6 Intellectual Property Rights

The software is effectively an off-the-shelf package, albeit with a few reports customised for POCL. The IPR resides with Riva Systems Ltd.

POL00028135

Applications Architecture for Value Added Processing

Section I: Purpose of the document

1. This document describes the applications architecture which has been adopted for the Value Added Processing functions of Post Office Counters Ltd as devised by the information Systems Strategy Unit. It forms part of a set of documentation which together describe the overall Information Systems Strategy for Post Office Counters Ltd. All future systems work in Value Added Processing area will comply with the principles outlined in this document.

2. In addition to this introductory section, the document comprises of the following:

   - *Section II:* Sets out the objective of the applications architecture, and describes the scope and boundaries of the applications for Value Added Processing, and summarises the applications architecture.

   - *Section III:* Outlines the process that has been adopted in defining the architecture

3. These sections are supported by appendices, which hold more detailed information about the activities undertaken by the Value Added Processing function, high level data entities which need to be supported, application descriptions, and data flow diagrams to support them.

POL00028135

Section II: The Applications Portfolio for Value Added Processing

1. The applications portfolio for the value added processing function describes all of the systems which should be found in the function which enables a small number of clients to send data to post offices, and in turn passes relevant information from post offices to clients. It also describes their key data flows and interfaces.

2. The Applications Portfolio has been designed to:

   - Support the primary process of turning post office data into accurate and consistent information which can be used to meet the financial, costing, marketing, and client requirements of Post Office Counters Ltd.
   - Ensure that where particular functions are not directly managed by Post Office Counters Ltd., adequate controls are highlighted and put in place.
   - Encourage the use of standard, packaged software wherever appropriate, and discourage tightly integrated and inflexible solutions.
   - Be implemented on industry standard, 'open', hardware and software platforms.

3. We have separated the applications contained in the Applications Portfolio into three tiers:

   - Basic Operational Systems - these are the systems that that will perform the day-to-day processing and include:
     - i) the data collection systems (such as polling, real time data capture, data keying, and document processing)
     - ii) the data flow matching systems (which ensure that supporting documents and complementary data items are properly matched)
     - iii) data reconciliation systems (such as stock balancing and 'cash account balancing')
     - iv) data delivery systems (which pass the data to internal management information databases, client host systems, and internal accounting systems)
   - Operational Support Processing - these are the systems which support basic operational systems by taking clerical and semi-automated activities out of the fully automated cycle. They include systems to assist in :
     - i) The maintenance of the standing and reference data
     - ii) The investigation and resolution of errors
     - iii) Calculation of sub-postmasters remuneration
     - iv) Preparation of ledger postings

POL00028135

v) Management of company resources

- Reporting and Management information systems - these systems will use the operational data to support internal sales, marketing, and quality of service reports.

4. The model in Appendix I gives a complete picture of all the applications that are required to support the Value Added Processing function, together with an indication of the way in which they interface with each other. Those applications which require greater definition have been amplified in the schedules which appear in Appendix II. These include:

- Perform Data Collection
- Perform Data Flow Matching
- Perform Reconciliation
- Perform Data Delivery
- Maintain Standing Data
- Error Correction
- Perform Postmaster Remuneration
- Prepare Ledger Postings
- Quality of Service
- Sales and Marketing
- Value Added Reporting

5. In addition, the Reporting and MIS applications are likely to be delivered through a set of data delivery or EIS tools which cover:

6. Regular reporting: These are reports that will be delivered through standard screen- or paper-based reporting tools which give the user a limited set of parameters to report by.

- Story-book reporting: These are screen-based reporting tools which generate updated information on a regular basis (in text and graphical format), but the sequence of the 'reporting pack' is fixed.
- 'Slice and Dice' reporting: These are screen-based reporting tools which allow users to view data, or summarise it, in a user-definable flexible way.
- Data Driven Reporting: These are screen-based reporting tools within which there is a set of rules, such that the system analyses the data and only reports on data which meets the user defined rules (e.g. exception reporting, Top 20, changes in contribution etc.)

7. Finally, the applications portfolio is a dynamic tool, and will be updated to reflect additions as they become known.

POL00028135

Section III: Outline of the process used to define the architecture

1. The process used to define the applications architecture for post offices included the following steps:

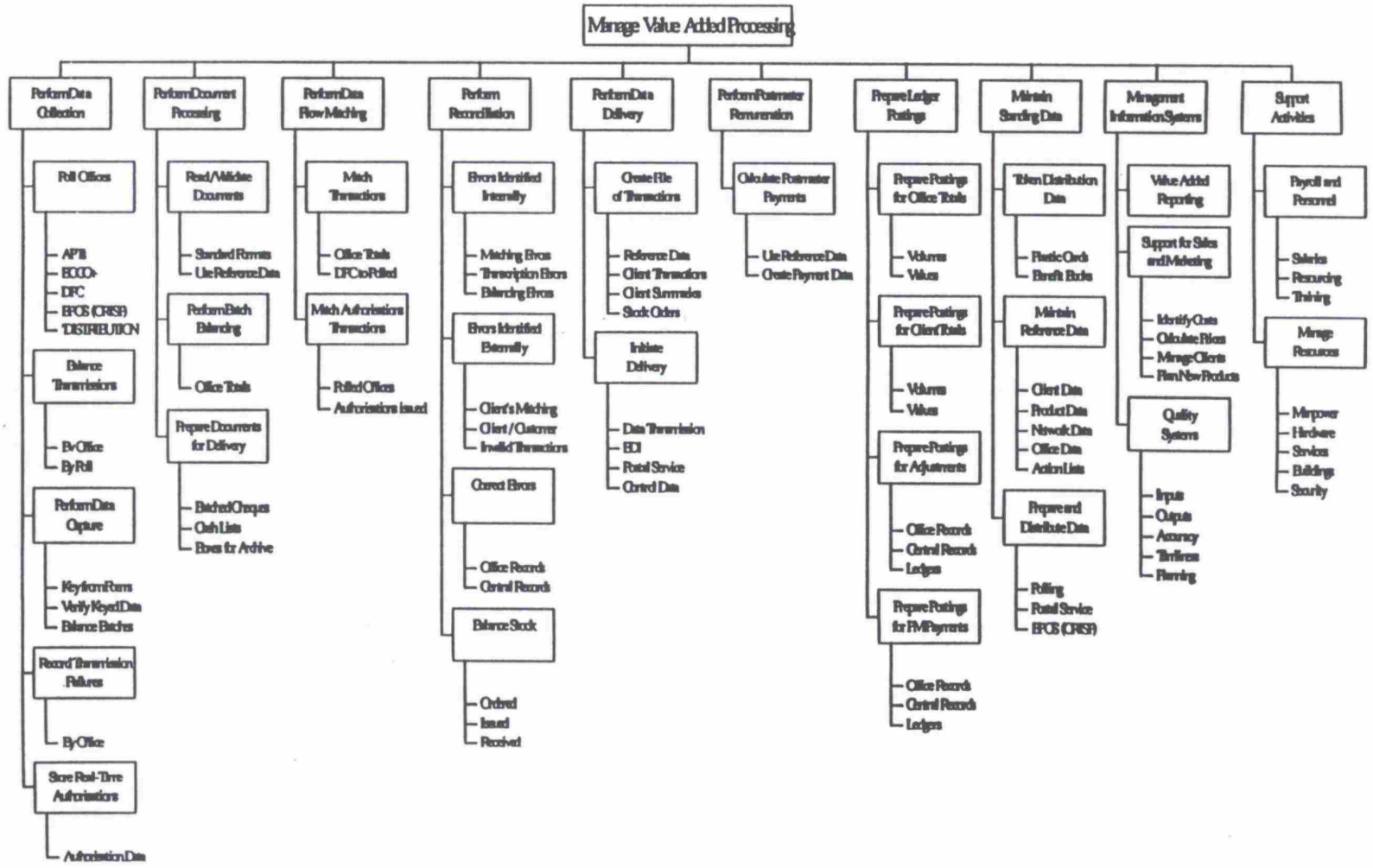
Process	Output	Reference
1. Define the Activity Model for Value Added Processing	Activity Model to cover existing and future processes	Annex I
2. Define the key data elements required by the Value Added Processing function	Process/Entity Matrix and associated data definitions	Annex II
3. Document the key data flows/applications	Application descriptions for key applications, including associated business processes supported, systems processes, data flows, interfaces, and technologies used.	Annex III
4. Prepare the applications portfolio for Value Added Processing	Applications Portfolio map	Annex IV

POL00028135

Annex I: Activity Model for Value Added Processing

POL00028135

ACTIVITY MODEL for VALUE ADDED PROCESSING



POL00028135

Annex II: Process / Entity Matrix

POL00028135

Process / Entity Matrix

PROCESS \ ENTITY	Network Std Data	Transaction Details (raw)	Transaction Header	Transmission Controls	Transaction Error Log	Transaction Details (accepted)	DPC accepted transactions	Distribution movements	Transaction Details (matched)	Batch Headers	Forms	Authorisation Request	Client Authorisation	Documents (OCR)	Document Summaries	Stock Balances	Error Record	Error Correction	Client Std Data	Client Transaction Record	Client Summary	Control Data	Ledger Postings	PO Std Data	Product Std Data	Action Lists	Stock Movement History	Quality of Service Data	Employee Std Data	Plant & Equipment Std Data	Token Distribution Data
PERFORM DATA COLLECTION																															
Poll Offices	X	X	X	X			X	X								X															
Record Transmission Failures	X			X																											
Balance Transmissions Received		X	X		X	X																									
Perform Data Capture					X	X				X	X					X															
Store Real-time Authorisations												X	X																		
PERFORM DOCUMENT PROCESSING																															
Read / validate Documents		X	X											X	X										X						
Perform Batch Balancing		X	X		X		X																								
Prepare Documents for Delivery														X	X				X												
PERFORM DATA FLOW MATCHING																															
Match Transactions					X	X	X	X	X																						
Match Transactions to Authorisations					X	X			X				X																		
PERFORM RECONCILIATION																															
Errors Identified Internally					X												X														
Errors Identified Externally																	X														
Balance Stock						X	X	X								X	X														
Correct Errors																	X	X													

POL00028135

Process / Entity Matrix

PROCESS / ENTITY	Network Std Data	Transaction Details (raw)	Transaction Header	Transmission Controls	Transaction Error Log	Transaction Details (accepted)	DPC accepted transactions	Distribution movements	Transaction Details (matched)	Batch Headers	Forms	Authorisation Request	Client Authorisation	Documents (OCR)	Document Summaries	Stock Balances	Error Record	Error Correction	Client Std Data	Client Transaction Record	Client Summary	Control Data	Ledger Postings	PO Std Data	Product Std Data	Action Lists	Stock Movement History	Quality of Service Data	Employee Std Data	Plant & Equipment Std Data	Token Distribution Data
PERFORM DATA DELIVERY																															
Create Transaction File						X	X												X	X	X										
Initiate Delivery	X																			X	X	X									
PREPARE POSTMASTER REMUNERATION																															
Calculate Postmaster Remuneration									X															X	X						
PREPARE LEDGER POSTINGS																															
Prepare Postings for Office Totals									X														X								
Prepare Postings for Client Totals																					X		X								
Prepare Postings for Adjustments																		X					X								
Prepare Postings for Postmaster Payments																							X								
MAINTAIN REFERENCE DATA																															
Maintain Data	X																		X					X	X	X			X	X	
Prepare and Distribute Data	X																		X			X		X	X	X					X
MANAGEMENT INFORMATION SYSTEMS																															
Sales & Marketing		X				X	X	X	X				X			X	X										X	X			X
Quality Systems		X				X	X	X	X				X			X	X										X	X			X
Value Added Reporting		X				X	X	X	X			X	X			X	X											X	X			X
SUPPORT ACTIVITIES																															
Payroll & Personnel																														X	
Resource Management																															X

POL00028135

Annex III: Application Descriptions

POL00028135

Process Description

Process Name	Perform Data Collection
Package / Bespoke	Bespoke

Objectives

To collect data, resulting from Post Office counter activity, document processing, distribution system processing and data keyed from forms.

Processes

1. Offices and central locations are polled via telecommunications, under the control of network standing data and transmission controls, to collect transaction data. Transmission failures are identified and the corrective action, required to collect the data, is reported. Received transmissions are batch balanced and validated
2. Forms are delivered for central processing where they are keyed and validated.
3. Authorisation requests and client responses are intercepted as they occur and copies stored for later processing.
4. Machine readable documents are sent to the document processing centre where they are captured, batch balanced and validated..

Key Data Flows

1. Network standing data
2. Client standing data
3. Product standing data
4. DPC transactions
5. Transaction Details
6. Transaction Header
7. Distribution Movements
8. Transmission Controls
9. Authorisation Requests
10. Client Authorisation
11. Stock Balances
12. Batch Headers
13. Forms
14. Machine readable documents
15. Transaction Error Log

Key Interfaces

Internal

- Data Flow Matching
- Data Delivery

External

- POCL Locations
- Distribution Function
- Clients

POL00028135

Technology Types

- Telecommunications
- Data base management
- OCR and Image processing

Notes:

Within the definition of 'office', Post Office Counters Ltd. includes their own Document Processing Centre, their own Data Preparation Centre, and their own distribution centres which send data to the Value Added Processing function

The list of offices to be polled, together with an indication of the type of data to be moved, and an approximate sizing of the data will be provided to the private sector contractor, through the standing data function which will remain within POCL's direct control.

(Document Processing Centre and Data Prep Centres will need to be polled to pull in the transactions read from machine readable code lines, or keyed in, and which complement the transactions from post offices and distribution centres).

The private sector operator may be required to send data polled from the offices directly to clients, in addition to sending it to Post Office Counters Ltd. for further processing. This requirement will be confirmed on a client by client basis.

A. Real Time Authorisation: We would expect the design of the authorisation system to be sufficiently flexible to support:

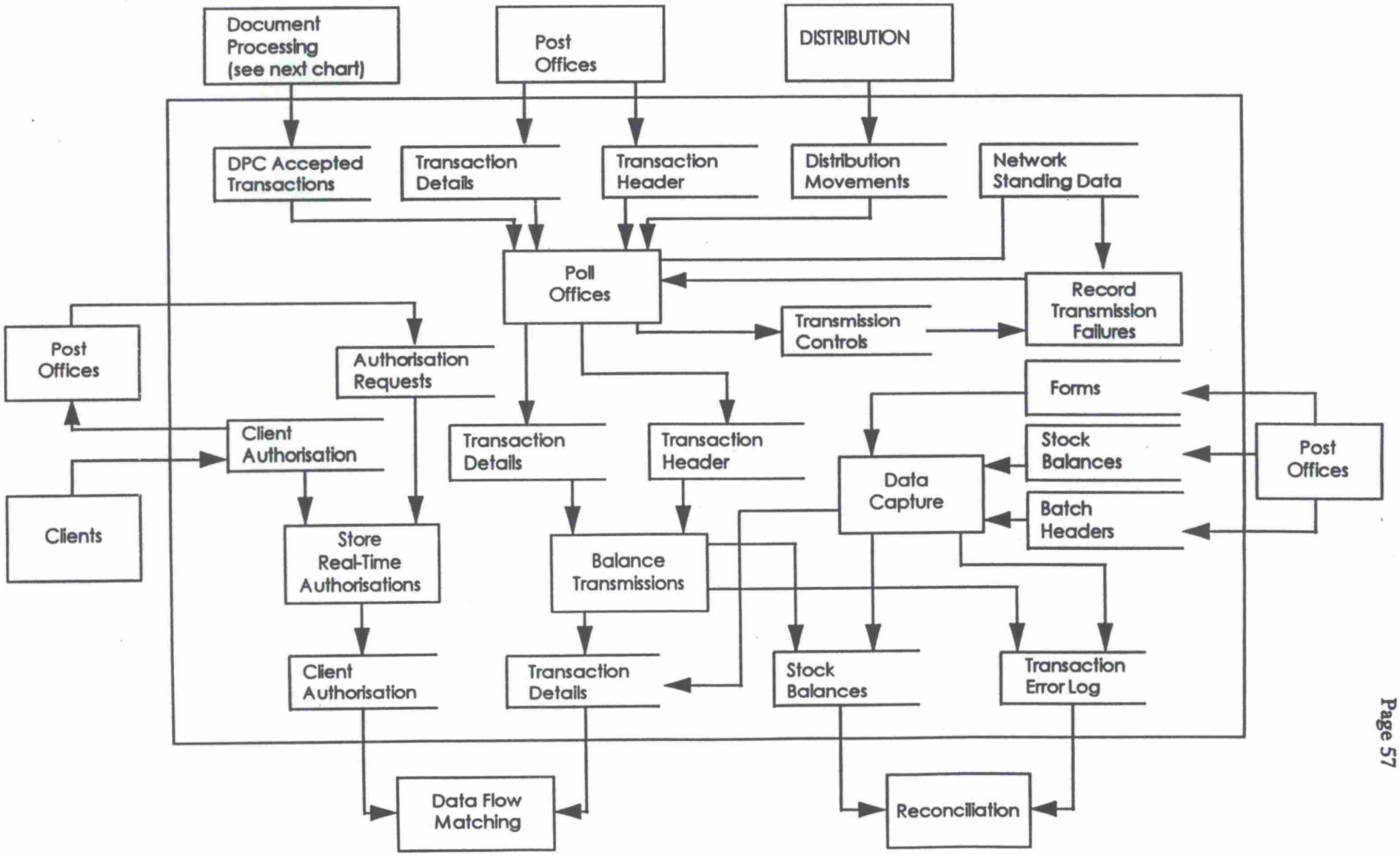
1. Batched authorisations being held at nominated post offices, or
2. Batched authorisations being held centrally within the operators polling system, or
3. Batched authorisations being held centrally within Post Office Counters Ltd's Value Added Processing Systems, or
4. Authorisations being held in the Client Host Systems.

The authorisation system must be able to support all of the authorisation methods mentioned above. The exact method used for a particular client will be confirmed on a client by client basis. However, it must be possible to change the authorisation approach merely by changing the location of the authorisation files (and system parameters) but without re-writing the systems.

B. Data Capture and Document Processing: At present, it is not envisaged that the private sector operator will take on the work currently done by POCL's Data Capture or Document Processing units. However, the operator may decide that he requires similar functions to provide contingency, resilience, and migration opportunities.

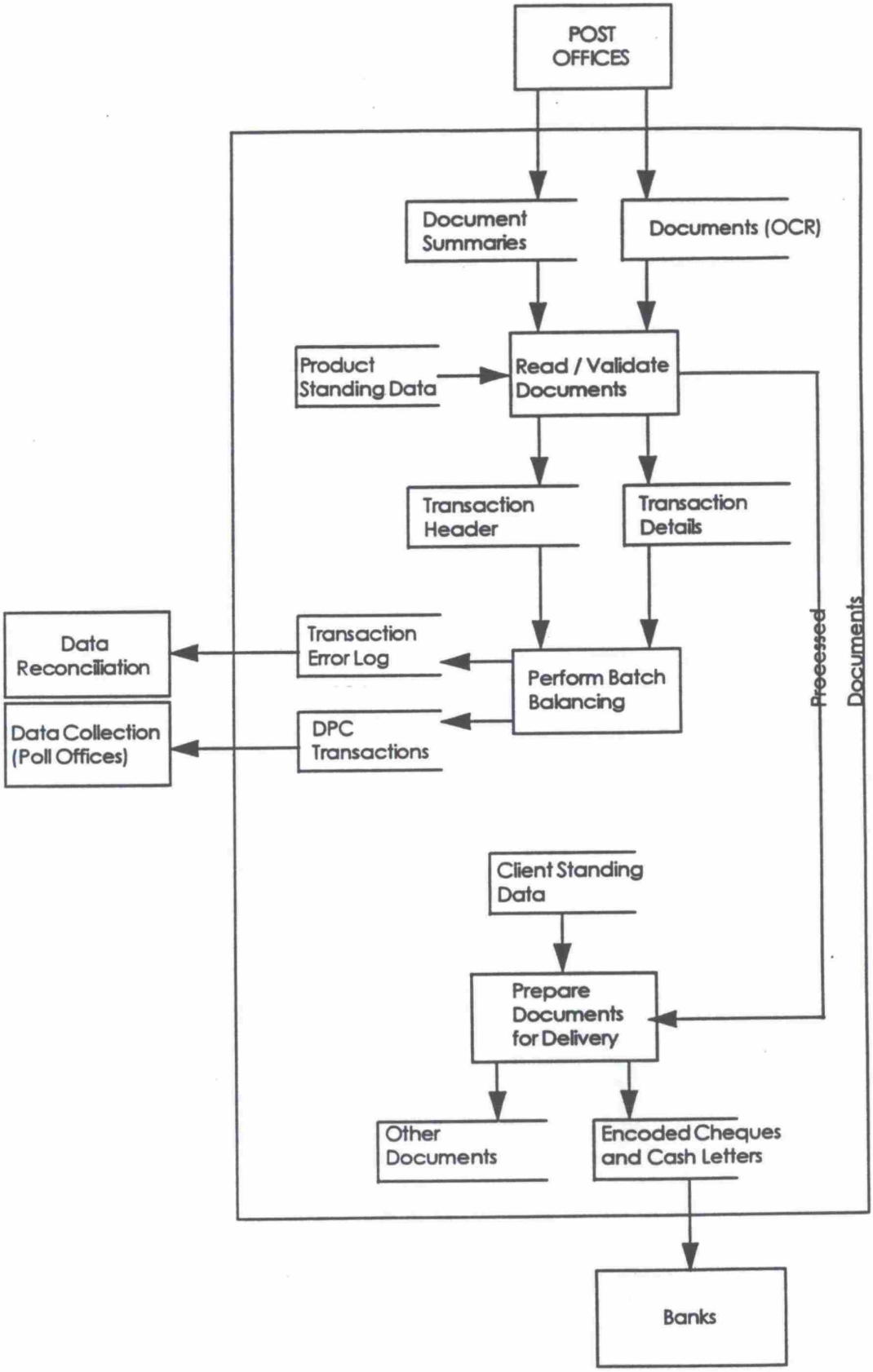
POL00028135

Perform Data Collection



POL00028135

Perform Document Processing



POL00028135

Process Description

Process Name	Perform Data Flow Matching
Package / Bespoke	Bespoke

Objectives

To match transactions details obtained from the outlets to relevant data gathered from other sources and to prepare data into a matched form for ledger posting purposes.

Processes

1. Transactions, Cash and Stock accepted from outlets are input to the matching process.
2. The following are matched and errors logged :

- Outlet transactions are compared to other data streams, i.e. Document Processing centre and Data Processing Unit
- Client authorisations stored at the time of the transaction are retrieved and matched against the appropriate transaction detail supplied by the outlet

3. A file of successfully matched transactions and transactions not requiring a match is created and this is delivered to the Prepare Ledger Postings process.
4. Mismatched transactions are delivered to the error reconciliation process.
5. Unmatched items are held over so that a further attempt at matching can be made when more data is available.

Key Data Flows

1. Transaction Details
2. Distribution movements
3. DPC transactions
4. Client Authorisations
5. Transaction Error Log

POL00028135

Interfaces

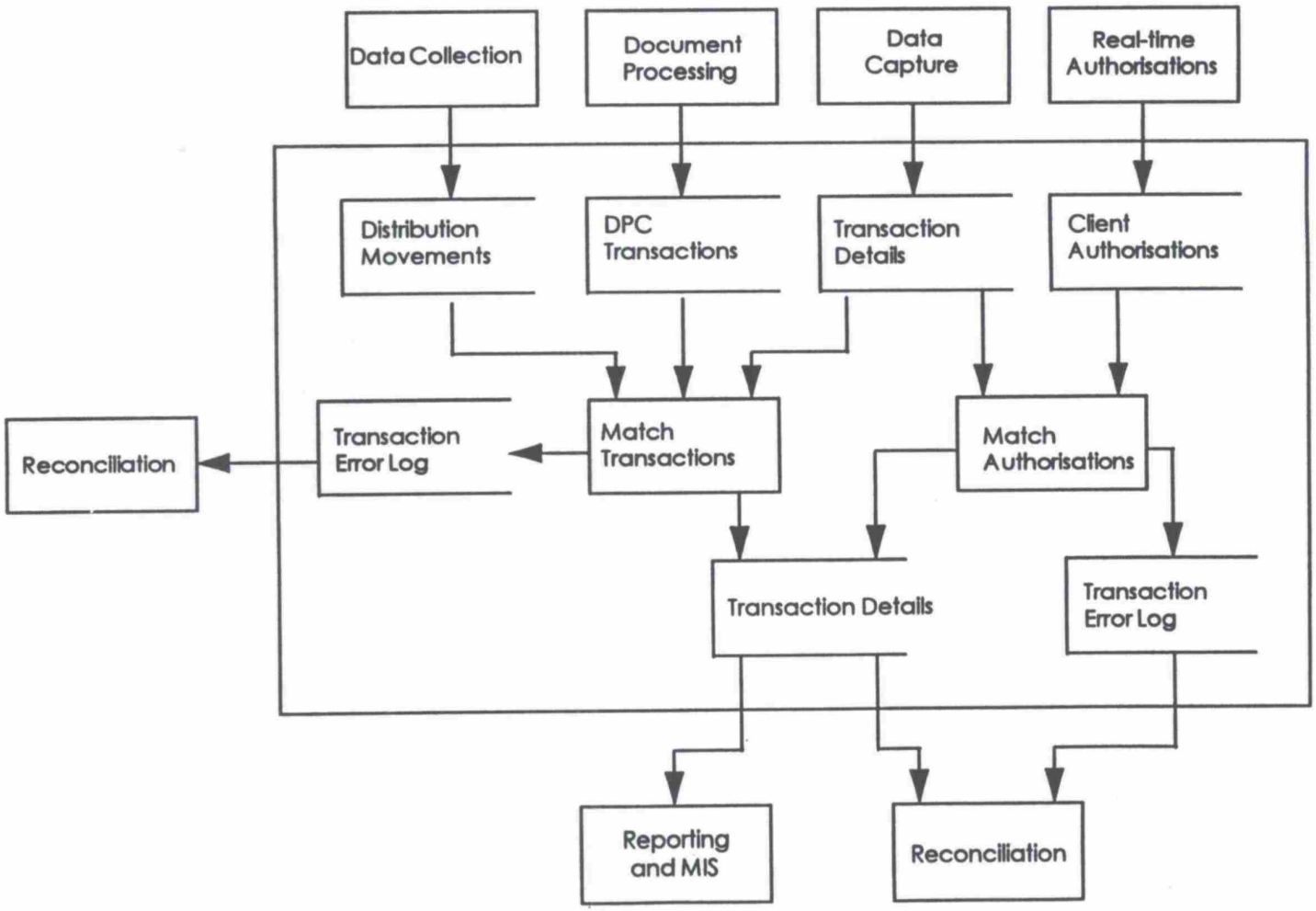
Internal

- **Data Collection**
- **Data Reconciliation**

Technology

POL00028135

Perform Data Flow Matching



POL00028135

Process Description

Application Name Perform Reconciliation

Package / Bespoke Bespoke

Objectives

To identify transaction errors, not already corrected by individual processes, and maintain an accurate stock balance.

Processes

1. The daily transaction files, having been batch balanced and matched, are validated against client, post office and product files. Errors are outsorted for investigation.

2. Stock balances are maintained by valid transactions.

Key Data Flows

1. Transaction Error Log
2. Distribution Movements
3. Stock Balances
4. Error Correction
5. Error Record
6. Transaction Details

Key Interfaces

Internal

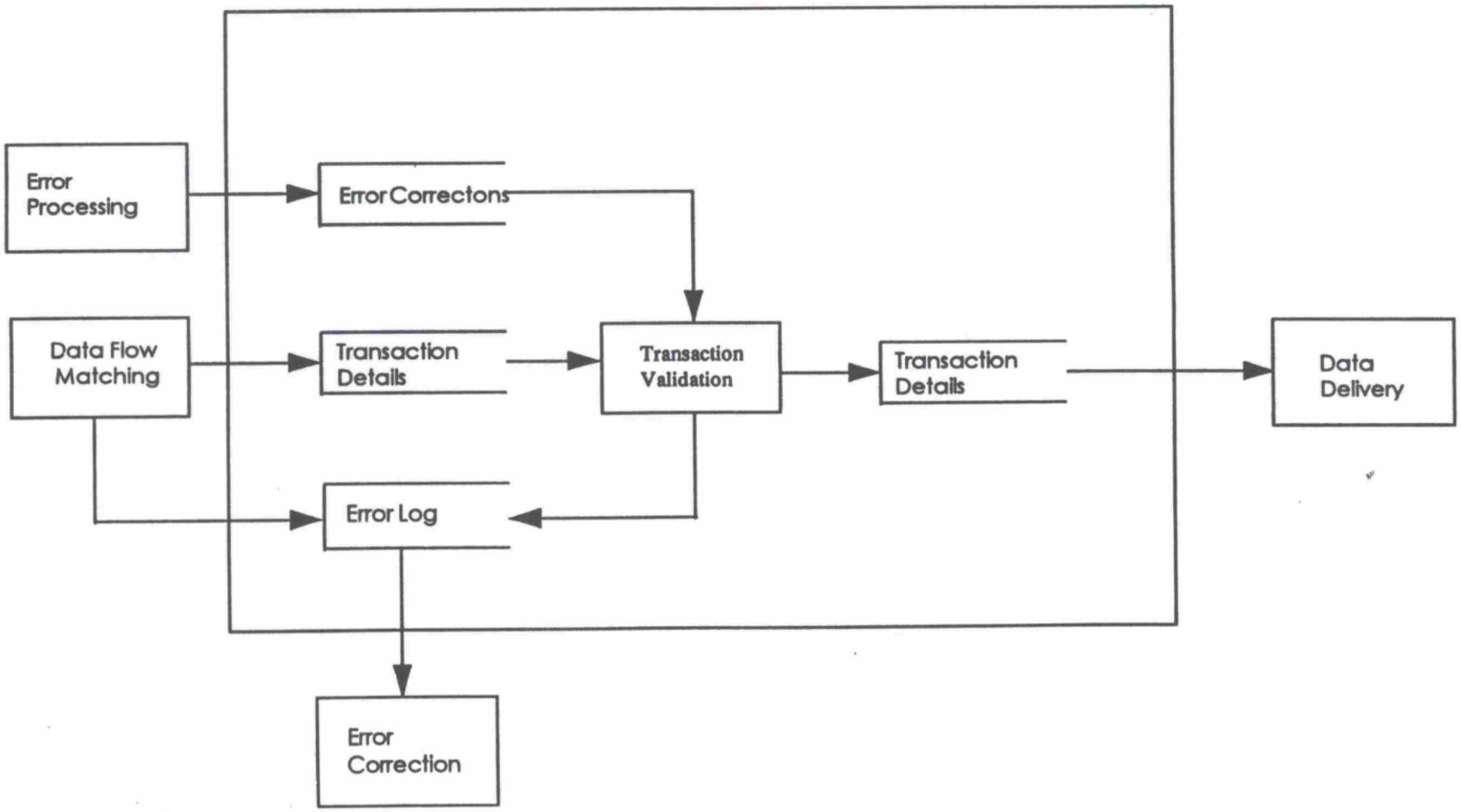
- Data Flow Matching
- Data Delivery
  Error Processing

External

Technology Types

POL00028135

Perform Reconciliation



POL00028135

Process Description

Application Name Perform Data Delivery

Package / Bespoke Bespoke

Objectives

To create Client transaction data and summary files from the transactions and deliver these to the Clients.

Processes

1. Using the Client Standing data file to govern the timing and format, the Client transaction records and summaries are created.

2. Transaction records and summaries are delivered to Clients either electronically by data comms or other magnetic medium. Control data is created to ensure successful delivery.

Key Data Flows

1. Transaction Details
2. Client Std Data
3. Client Transaction Record
4. Client Summary
5. Control Data
6. Network Std Data

Key Interfaces

Internal

- Data Reconciliation
- Ledger Postings
- Postmaster Remuneration

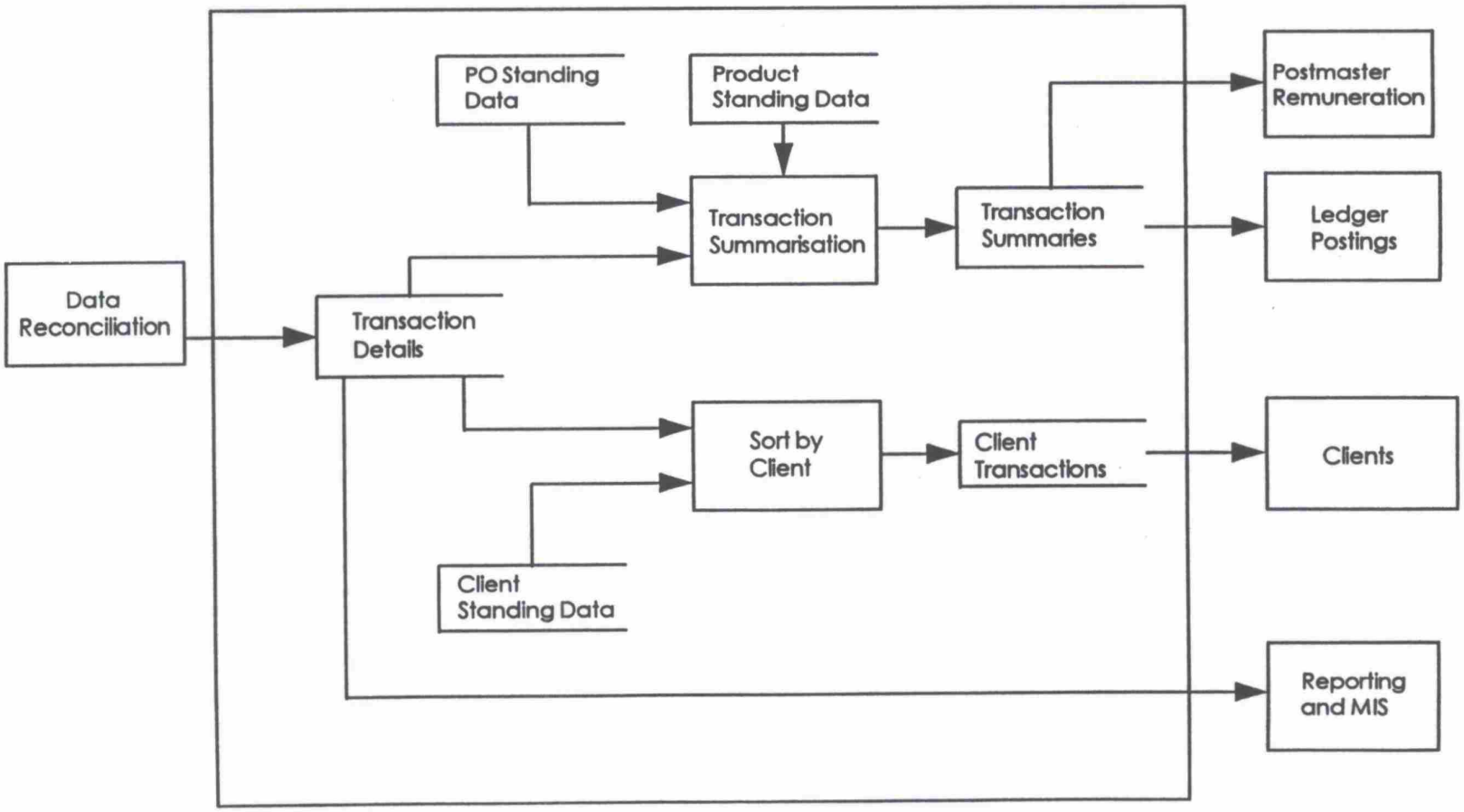
External

- Client

Technology Types

POL00028135

Data Delivery



POL00028135

Process Description

Process Name	Maintain Standing Data
Package / Bespoke	Bespoke

Objectives

To maintain files of standing data, from information supplied by Clients or POCL, and to prepare subsets of the data for distribution to those locations which require them.

Processes

1. Data files or documents, relating to process control parameters and token distribution instructions, are received from Clients or POCL at a central processing site where they are validated and used to update the standing data files.
2. Subsets of the standing data are created for distribution to central and office locations, and control data is created to ensure successful delivery.

Key Data Flows

1. Reference Data Changes
2. Network Standing Data
3. Client Standing Data
4. Product Standing Data
5. Post Office Standing Data
6. Action Lists
7. Token Distribution Data
8. Employee Standing Data
9. Plant and Equipment Standing Data
10. Control Data

Key Interfaces

Internal

- All internal systems

External

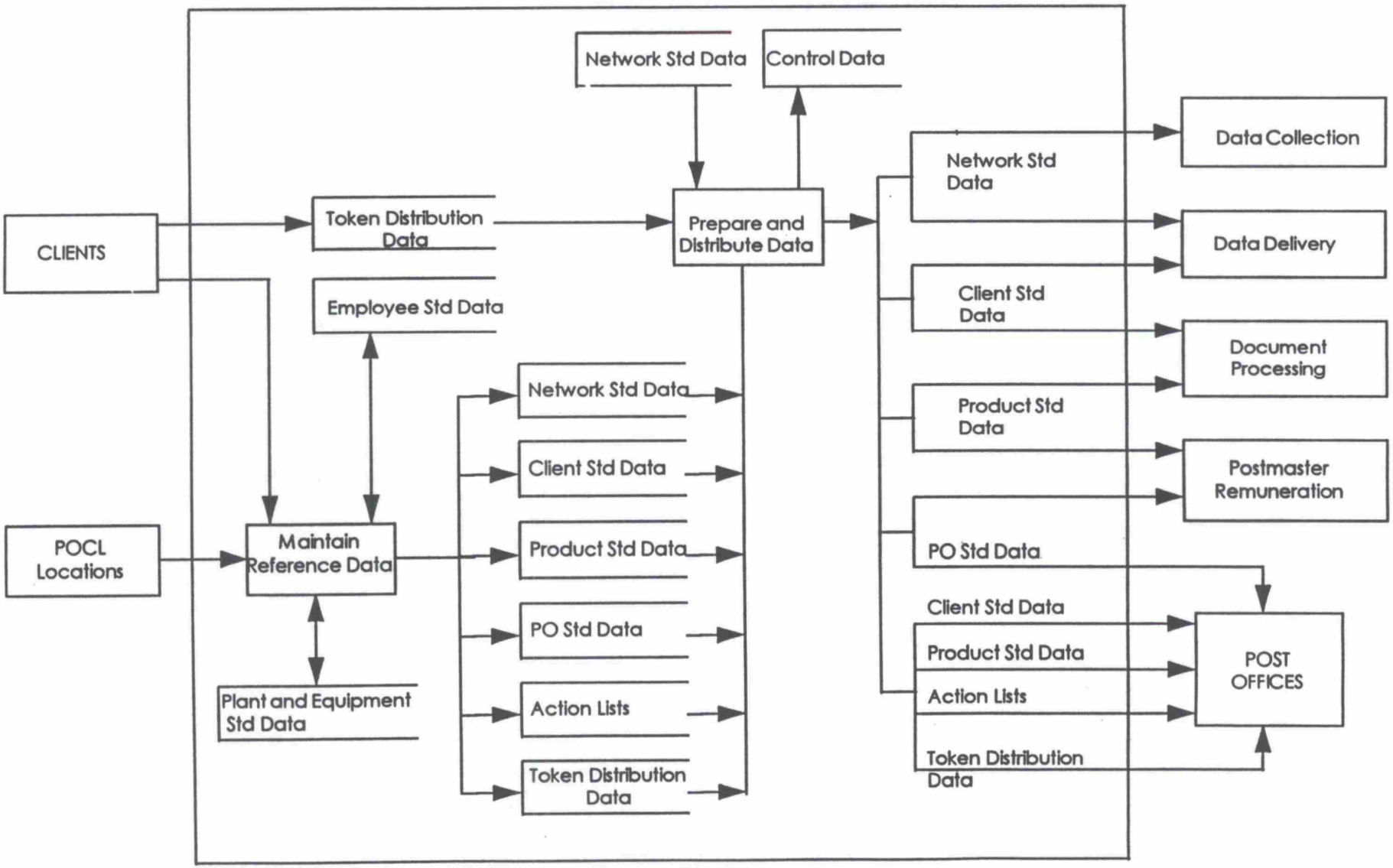
- Clients
- Post Offices

Technology Types

- Data base management

POL00028135

Maintain Standing Data



POL00028135

Process Description

Application Name Error Correction

Package / Bespoke Bespoke

Objectives

To investigate and correct errors identified internally by the data reconciliation process or externally by clients.

Processes

1. Transaction errors are identified at various stages, i.e. whilst polling offices, as part of data capture, document processing, during matching against other documents and authorisations; and are also reported by customers or clients.

2. Errors will be investigated and corrected and correction records created for posting to ledgers and clients.

Key Data Flows

1. Transaction Error Log
2. Distribution Movements
3. Stock Balances
4. Error Correction
5. Error Record
6. Transaction Details (Accepted)
7. DPC Accepted Transactions

Key Interfaces

Internal

- Data Collection
- Document Processing
- Data Flow Matching
- Ledger Postings

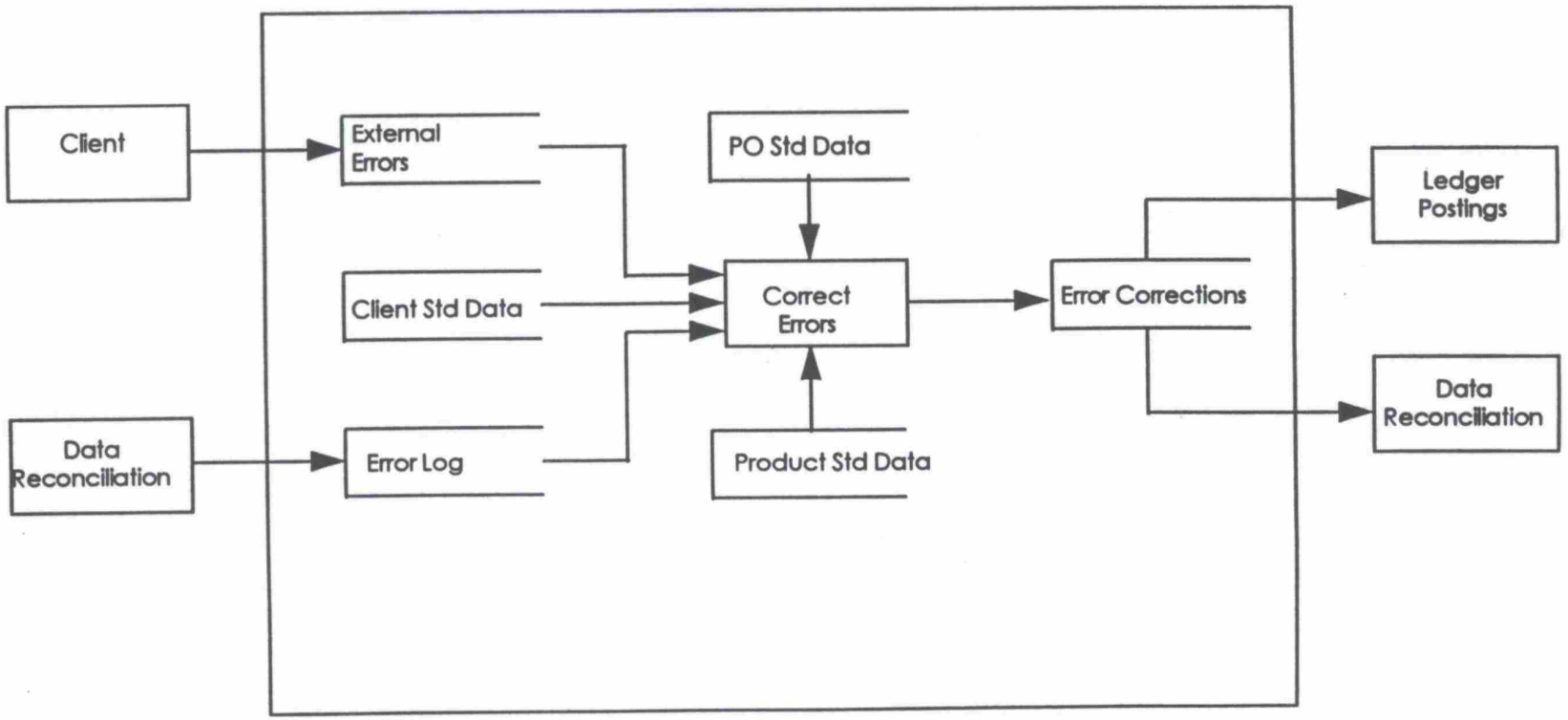
External

- Distribution
- Client/Customer

Technology Types

POL00028135

Error Correction



POL00028135

Process Description

Process Name	Perform Postmaster Remuneration
Package / Bespoke	Bespoke

Objectives

To calculate monthly postmaster remuneration.

Processes

1. Transactions, successfully passing the various validation processes, are used in the remuneration calculations.

2. Remuneration is calculated in accordance with contractual rules. This might be based on either, the volume or value of transactions carried out at the outlet or the fixed rate for the outlet.

Key Data Flows

1. Transaction Details
2. Product Std Data
3. P O Std Data
4. Remuneration figures

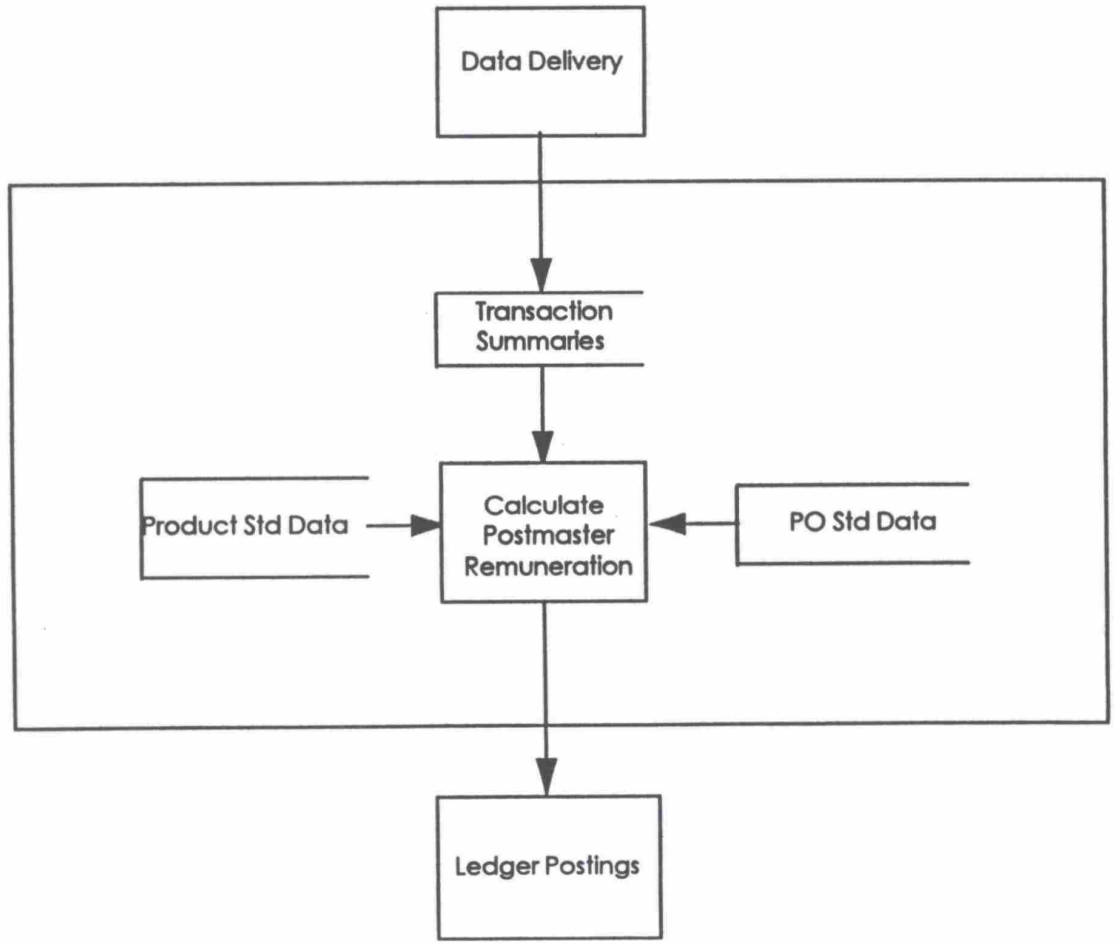
Interfaces

- Data Delivery
- Ledger Postings

Technology

POL00028135

Prepare Postmaster Remuneration



POL00028135

Process Description

Application Name Prepare Ledger Postings

Package / Bespoke Bespoke

Objectives

To prepare ledger postings using outlet transaction data in the form of office totals, client totals and adjustments together with postmaster payments for subsequent processing by Financial Administration

Processes

1. Ledger postings are created for the following situations
   - Office postings using information from transactions
   - Client postings using client summary data
   - Adjustments for error correction
   - Postmaster postings from remuneration calculations.
2. All ledger postings are passed to Financial Administration.

Key Data Flows

1. Client Summary
2. Transaction Details
3. Error Correction
4. Ledger Postings
5. Remuneration Figures

Key Interfaces

Internal

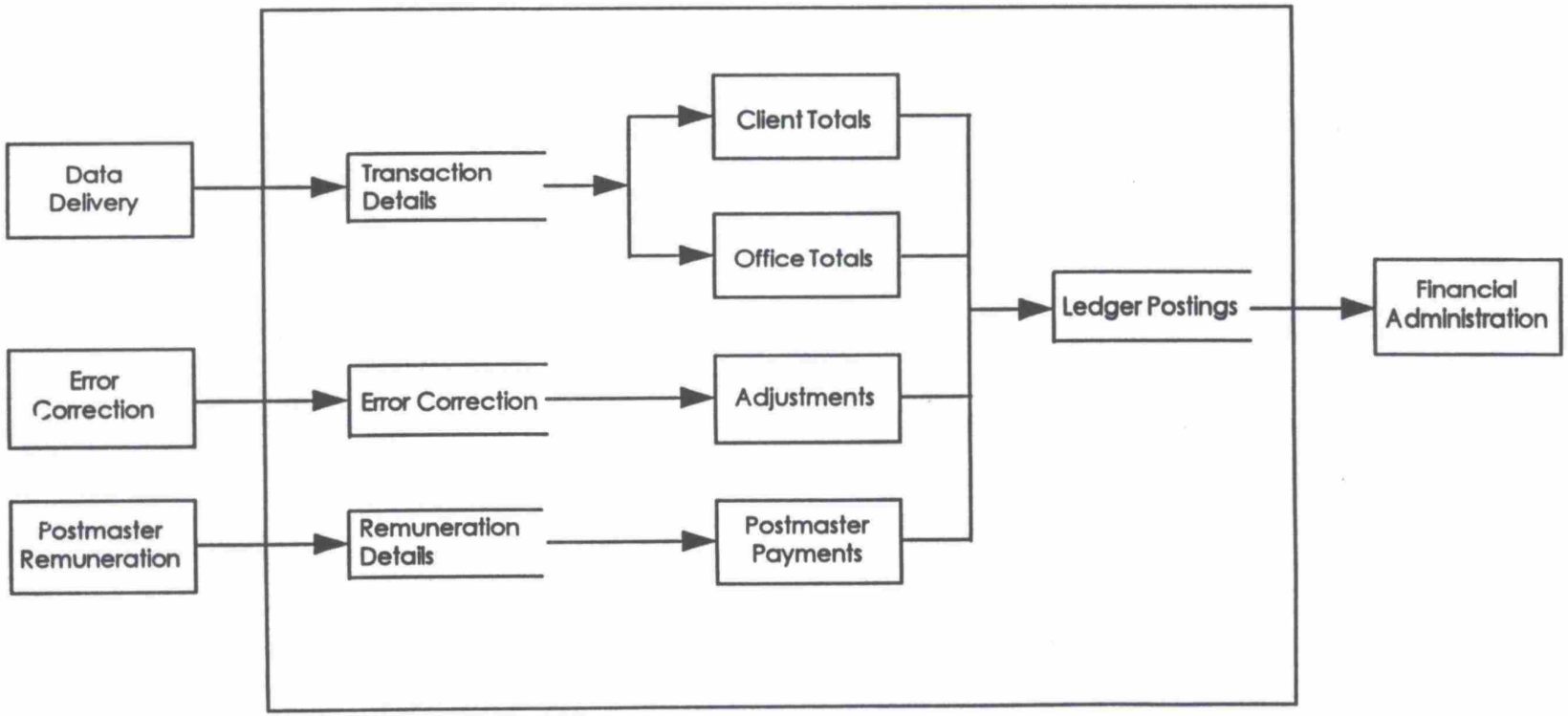
- Data Delivery
- Error Processing
- Postmaster Remuneration

External

- Financial Administration

POL00028135

Perform Ledger Postings



POL00028135

Application Description

Application Name	Quality of Service
Package / Bespoke	Report Writing Package

Objectives

Analyse the system performance in terms of quality and timeliness of deliverables to clients

Business Processes

1. User will have the ability to "construct" Quality of Service reports to a standard style from data held by office, region and company

Key Data Flows

- Transaction Details

Key Interfaces

Internal

- Transaction Details

External

- Head Office
- Regions
- Clients

Technology Types

POL00028135

Application Description

Application Name Sales and Marketing

Package / Bespoke Report Writing Package

Objectives

To analyse product sales by volume, value and time

Business Processes

1. User will have the ability to "construct" Sales reports to a standard style from data held by office, region and company

Key Data Flows

- Transaction Details

Key Interfaces

Internal

- Transaction Details

External

- Head Office
- Regions
- Clients

Technology Types

POL00028135

Application Description

Application Name	Value Added Reporting
Package / Bespoke	Report Writing Package

Objectives

To analyse and report on client transactions which would "add value" to the normal delivery of transaction data.

Business Processes

1. User will have the ability to "construct" reports to a standard style from data held by office, region and company

Key Data Flows

- Transaction Details

Key Interfaces

Internal

- Transaction Details

External

- Head Office
- Regions

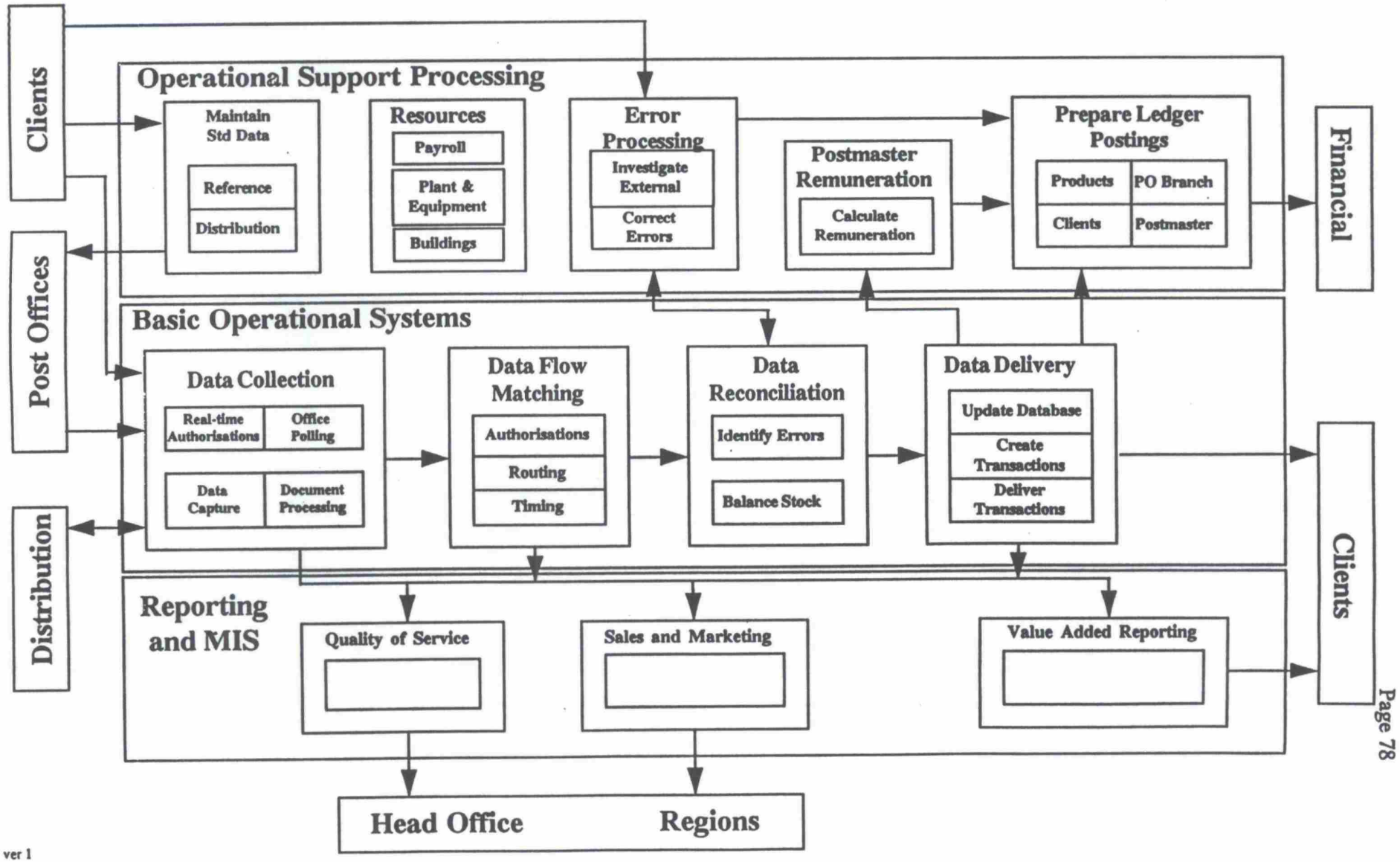
Technology Types

POL00028135

Annex IV: Applications Portfolio for Value Added Processing

POL00028135

Applications Portfolio for Value Added Processes



ver 1

POL00028135

Appendix 3-3

CRISP technical description

POL00028135

CRISP TECHNICAL DESCRIPTION

1. Background

CRISP (Counters Retail Information Systems Project) was launched in late 1992 to provide better data capture and transmission from PostShops. The software is designed and maintained by RIVA Systems Ltd.

2. Overview of the Requirement

2.1 Objectives

The objectives of the CRISP system are to:

a) automate the capture of sales and stock movement data
b) permit local processing of this data
c) provide electronic data transfer to a central location

2.2 Current Hardware

The CRISP system has the following hardware components:

- Hewlett Packard HP3000 937LX
- 120Mb memory
- 2 x 1.35GB discs
- 1 x 2 GB disc in an external peripheral tray
- 1 x 2 GB DDS DAT tape drive
- 1 x 2.8 GB DDS compression DAT
- 2 x peripheral trays
- DTC 48
- C001G console
- 6 x RIVA Black box modems (using 6 external telephone lines)
- RIVA 6900 EPOS Terminal

2.3 Data Entry / Key Features

Data is captured by the use of standard retail peripheral units such as bar-code readers or by data entry by the operator.

The system is designed to ensure that:

a) data entry can be made with the minimum number of keystrokes.

b) operators are able to verify any input they have made

c) for any transaction entered into the system the operator is able to:

- suspend input before completion without losing any data already captured
- resume input to a previously suspended transaction set from the point where it was left
- review any input made previously, whether partially or fully completed
- correct any previous input at any stage prior to the generation of the weekly office summary
- cancel an individual transaction within a transaction set
- access data for the previous week on screen or to print, without the ability to amend

POL00028135

Appendix 3-4

"Capture" technical description

POL00028135

CAPTURE TECHNICAL DESCRIPTION

1. Background

Capture is a cash accounting package currently sold by POCL to Agency offices. The first offices went live in June 1992. It is a back office, not an EPOS, system and data is not captured in real time.

2. Overview of the Requirement

2.1 Objectives

The requirement which Capture was developed to meet is for a summarisation and balancing facility where transaction data can be entered either individually or in bulk to allow production of a cash account and associated client summaries. The objectives of the system are to:

a) Improve the speed of cash account and summary production.

b) Improve accuracy.

c) Offer office and management information with facilities for password entry, hot lists, reconciliation and remuneration calculation.

d) Be easy to use by a combination of menus and hot keys.

e) Allow users to customise the system where applicable and change prices when required to.

2.2 Current Hardware

Capture runs on any standard PC with the following minimum specification :

- IBM compatible
- 386 processor
- 4 Megabytes of RAM
- 100 megabyte hard disc
- High density 3.5 inch floppy drive
- DOS 6 plus windows
- XT keyboard

Hardware supplied by POCL is specified as 486SX, 33Mhz, or 66 MHZ with 210 or 270 Mbyte hard disk options.

The program has been designed to be compatible with the star LC24 - 200 or 300 dot matrix printers and selected ink jets.

2.3 Data Entry / Key Features

All transactions are entered subsequent to the transaction taking place and can be entered at any time during the week to which they relate for the current or previous days.

Transactions can be entered in individual detail or bulk.

Keystrokes are minimised by the use of hot keys to move between common transactions or options.

POL00028135

Where possible the system provides the price of an item.

There is a maintenance function to allow price changes and product insertion/deletion.

There is a facility to allow data re-entry for checking purposes.

Data entry for the production of the cash account is automatically reported to a management information facility to calculate volumes of transactions converted by multipliers into units for agents to calculate their remuneration.

There are a maximum of 99 stock units allowed with selection of the actual number at the discretion of the outlet and available as an option.

Speed of data entry and associated processing maximised.

Data can be entered on days prior to the current working day.

A transaction log facility is available for the current week and the previous 8 weeks.

2.4 Client Summaries

Capture prints on to preprinted client summary forms (eg. DVLA / Girobank / DNS).

Other summaries are printed on plain paper and sent to client.

2.5 Balancing and Cash Account

Balance can be produced at any time during the week.

Processing time is minimal.

Daily cash book and stock and reconciliation reports are available.

2.6 General

All databases are parameter driven to enhance ease and speed of change.

Maintenance functions to allow user driven changes are available for both prices and products.

Management and office Information facilities are available for (but not exclusively) : Hot lists, passwords ,stock units, cash targets, remuneration.

2.7 Volumes

There are 1600 capture offices forecast to rise to 2000 by March 1996. There are no available figures for transaction volumes going through the system, but our system test criteria specifies weekly volumes of 10,000 transactions being entered (4,000 of them pensions and allowances).

3 New Software Distribution

New versions of the software are developed to POCL specifications, by the software supplier and handed to POCL for user acceptance testing. There are an average of 2-3 new versions per year. These are distributed on disc (currently one disc per site).

POL00028135

4 Help Desk Facility

POCL operates a central help desk facility, located at Farnborough, which provides the first line of support to outlets for all education, hardware and software problems.

There are around 1500 - 1600 calls per month, around 1300 - 1400 of which would be educational. The calls are to an 0345 number and each call should be answered within 30 seconds. All calls are logged on a fault management system.

5 Training

One day on site training is provided to each new user of the system. The training is provided by a fully trained agency trainer and comprises installation of the hardware and software, basic training in the use of a PC and intensive training on the functions of the program itself.

6 Intellectual Property Rights

The application has been developed for POCL by Unisys Ltd using their own 4GL development application (generic postal architecture). The IPR in the development tool resides with Unisys but the capture application itself is "owned" by POCL

POL00028135

Appendix 3-5

Benefit Payment Procedures
(Payment to Proxies and "Foreign Encashments)

POL00028135

APPENDIX 3 - 5

BENEFIT PAYMENT PROCEDURES (PAYMENT TO PROXIES AND "FOREIGN ENCASHMENTS")

1. INTRODUCTION

There are instances within current standard benefit payment procedures where payments of benefit can be authorised to be made to proxies appointed either by the DSS or the customer. This appendix deals with some of these situations and highlights the existing procedures used to deal with them.

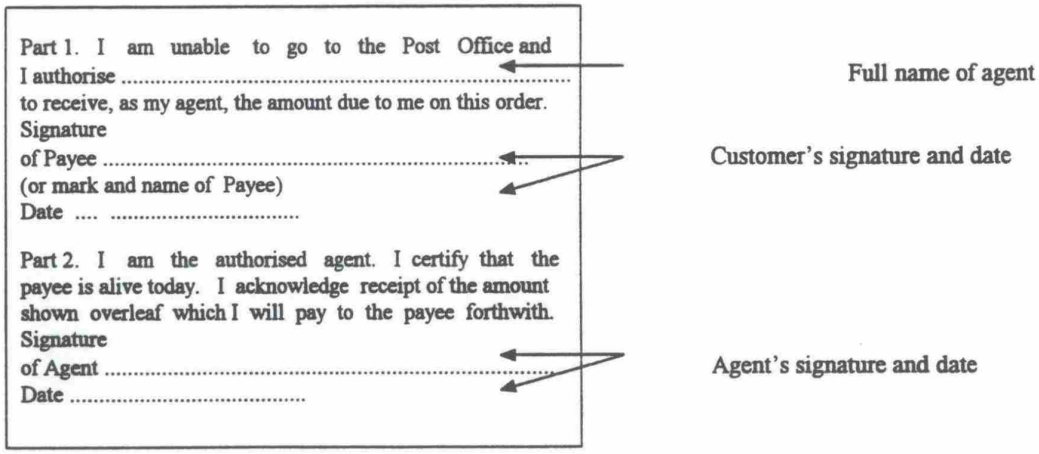
2. AGENT/APPOINTEE PROCEDURES

A customer currently has the option to arrange for their payments of benefit to be collected by a third party (an appointee or agent). This option may be exercised through customer choice, or, if for example the customer is no longer able to act for themselves, on their behalf by someone authorised to act for them. Additionally in some circumstances the DSS can appoint an agent or appointee to act on behalf of a customer.

2.1 Casual Agents

Casual agents are appointed on an ad hoc basis, their identity may differ from week to week. BA is not informed in advance of when this facility is used nor the identity of the person authorised by the customer to receive their payment. The customer authorises a casual agent to act on his behalf by completing the relevant sections on the reverse of the payment foil or girocheque to be presented, and due, for payment. The wording on both foil and girocheque is similar and an example is shown below

Figure 1 Agency authorisation section contained on the reverse of a payment foil



2.2 Casual Agent Procedures

When a casual agent presents an order book for payment, the standard payment procedures (outlined in appendix 3-6 are followed with the following additional checks being made:

POL00028135

1.	on the front of the payment foil	a.) confirmation that the customer has signed the payment foil;
		b.) in some instances the customers may have deleted the line in which, by signing, they confirm receipt of the sum detailed on the foil;
2.	on the reverse of the payment foil	a.) confirmation that the agent's full name is shown;
		b.) confirmation that the customer has signed and dated the order;
		c.) confirmation that the agent has signed and dated the order.

Circumstances in which evidence of identity may be required to support an encashment are agreed between DSS and POCL. Should these circumstances apply to a casual agent encashment the agent is required to produce identity relating both to themselves and the customer appointing them.

2.3 Permanent Agent Procedures

A permanent agent has been authorised by the BA to receive payments of benefit on behalf of a customer. In order to confirm their status to the counter clerk they may produce either:

1.	the order book only, in which case their name and address will be clearly imprinted on the front by the DSS;
2.	an order book accompanied by a form BF74 Payment to an Agent - Standing Authority (see figure 2) or written authority from the issuing office.

Figure 2. Payment to an Agent - Standing Authority Form

Payment to an agent - Standing Authority

To the postmaster

.....Post Office

We have authorised this person to act as this payee's agent. Please pay the payee's money to agent. Details of the payee and the agent are on the right.

Details of agent

Name .....

Address .....

.....

.....

Details of payee

Name .....

Pension No, Allowance No or NI No

.....

Form BF 74

2.3.1 Order Book Only Produced

When the permanent agent produces an order book only, the standard payment procedures are followed accompanied by the following additional check:

1.	confirmation that both the customer's and the agent's names appear on the front cover of the order book (either the customer or the agent may sign the payment foil).

2.3.2 Order Book and Authority Produced

When the permanent agent produces an order book together with a form BF74 or written authority, standard payment procedures are followed accompanied by the following additional check:

1.	confirmation that the details shown on the written authority correspond with those printed on the front of the order book.

POL00028135

2.4 Appointees

Persons may be appointed either on a temporary or (as is more usual) a permanent basis to act as an appointee for a customer. This appointment may be made at the behest of the customer, the DSS, a person authorised to act on behalf of the customer or a person granted power of attorney over a customer's affairs.

In this circumstance the entitlement to benefit is based on the customer's personal circumstances but for all benefit payment intents and purposes the appointee becomes that customer. All IOPs are issued to the appointee. They bear their name and address details and are encashed by them, they also bear the customer's name and National Insurance Number.

3. FOREIGN ENCASHMENT PROCEDURES

"Foreign encashments" are those which are made at post offices other than the one a customer has nominated for the encashment of their IOPs (their "home" post office). Customers inform the DSS at the start of any claim to benefit of the post office at which they wish to receive payment of that particular benefit. The nomination of post office is per benefit, customers receiving more than one benefit currently have the option to nominate different post offices. IOPs subsequently issued to customers will be made payable at the post office so nominated. In the case of order books the vast majority are actually issued to that post office for customer collection.

3.1 Temporary Change of Post Office

Customers are currently given the facility to make up to two encashments during the life of any individual order book at a post office other than their home post office. This service is offered primarily to cater for periods when customers may be away from home for short periods e.g. when they are on holiday.

3.2 Permanent Change of Post Office

Customers also have the facility to permanently change the post office at which they wish to receive payments of benefit:

1.	during the life of a claim there is a mechanism referred to as a P80MA procedure by which the post office of payment can be changed;
2.	at the initial stages of a repeat claim to benefit customers can elect to have their benefit paid at a different post office to the one used by them in a previous claim.

POL00028135

3.3 Post Office Counter Procedures

Figure 3 - Order Book cover

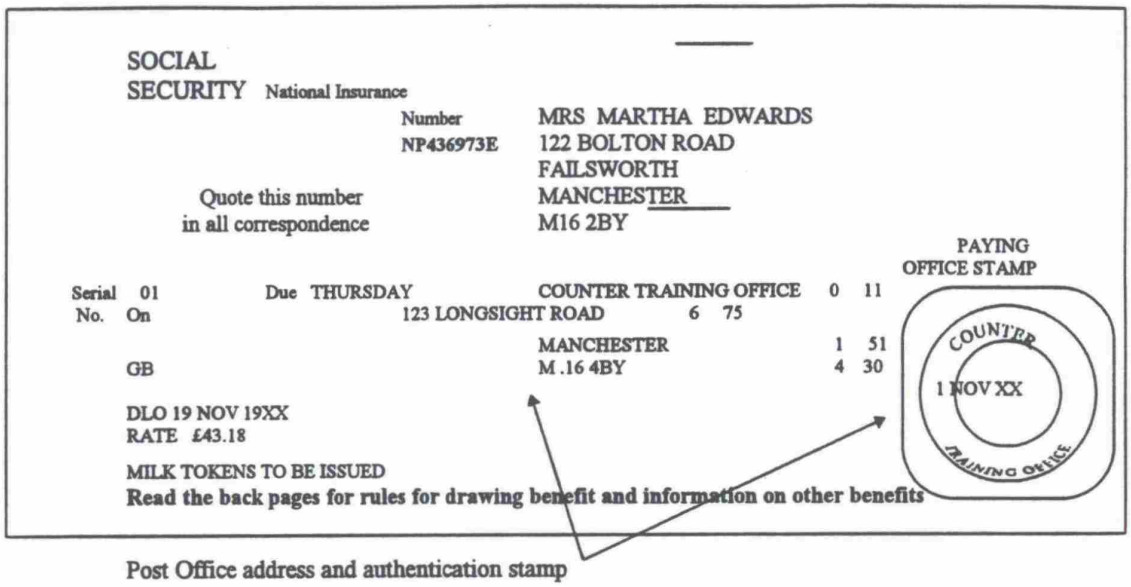


Figure 1 illustrates the existing layout and information displayed on the front cover of an order book. Counter clerks are able to confirm that customers are presenting their books for payment at their home post office as the post office address is printed on the front cover of the order book. As Figure 1 shows the front cover of the book also contains a post office authentication stamp, which is printed on it by post office staff when it is delivered to their office for customer collection.

POL00028135

3.3.1 Temporary Change of Post Office

Customers are able to receive two payments of benefit away from their home post office. Counter clerks at the foreign post office, on realising that the book presented is not normally cashed at their office, examine the inside front cover of the book. In particular they examine the boxes (a) and (b) to see if the temporary agent procedure has already been used. If one or both of these boxes are empty then this facility is still available to the customer. Standard procedures are followed and in addition the counter clerk imprints the post office authentication stamp in box (a) or (b).

CHANGE OF POST OFFICE OF PAYMENT

See M2 BOO21 for full instructions re change of office procedure if required		COMPLETE SPACES BELOW IN P80 CASES ONLY	
		New office of payment not valid until (d)is stamped	Date stamp of new office
Payment without P80 (FIRST ORDER) (a)	Payment without P80 (SECOND ORDER) (b)	(c)	(d)
Not to be encashed outside Great Britain unless authorised on the front cover by Issuing Authority			
Proof of identity is required for each order exceeding £50 when presented at other than the nominated Post Office			
Not more than two orders maybe cashed on any one day if the value of each exceeds £50			

Figure 4 - Inside front cover of order book showing temporary change of post office mechanism.

Once all the above checks have been made the standard payment procedure is followed. If boxes (a) and (b) have both been date stamped and the customer still requires payment they must request a permanent change of post office.

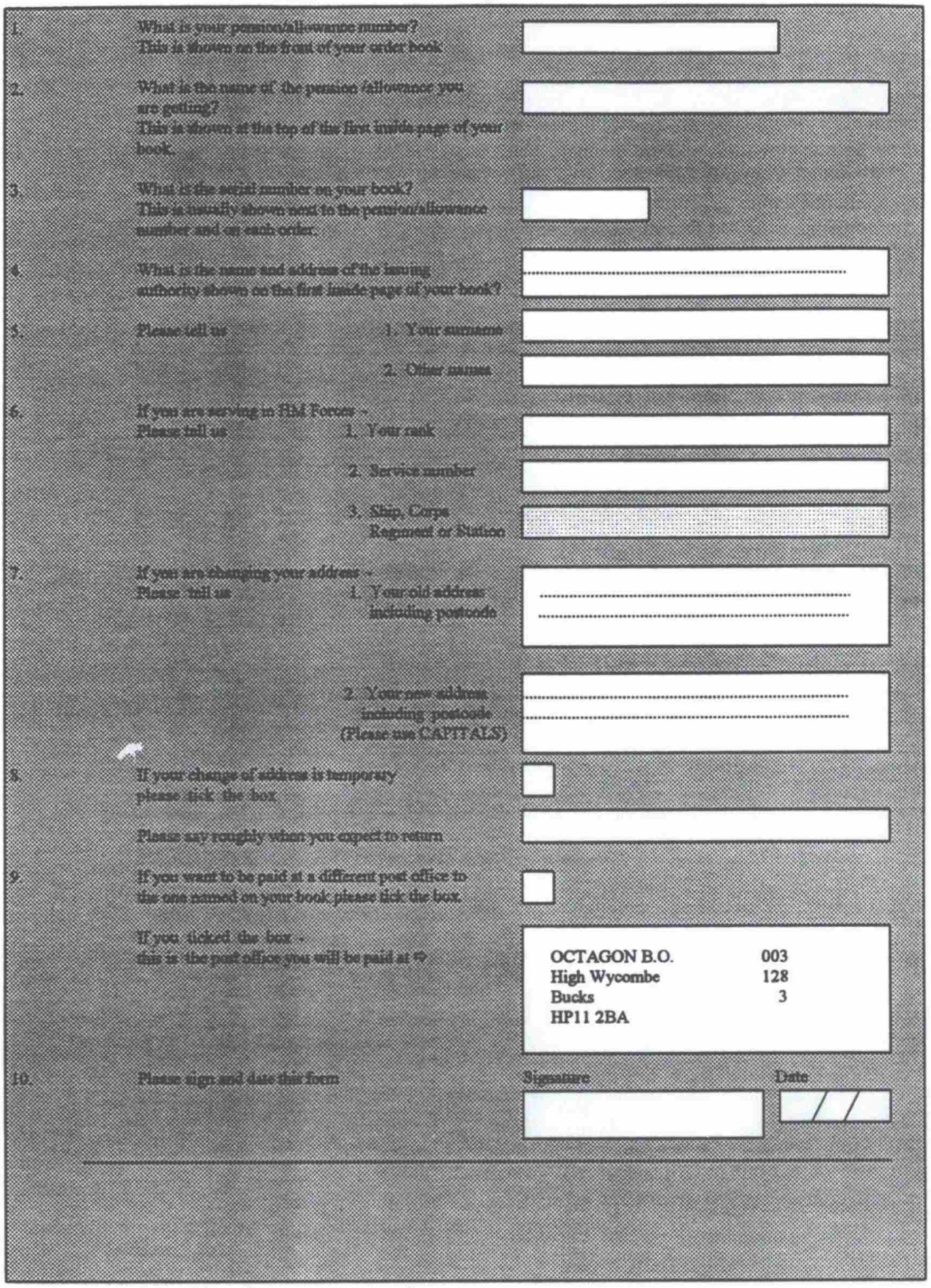
3.3.2 Permanent Change of Post Office

In order to achieve a permanent change of post office of encashment the customer must follow a defined procedure. They are required to complete a form P80MA, an example of which is shown at figure 5:. The DSS may, for security or administrative reasons choose to restrict the customer's ability to encash their book at one post office only. All restricted order books are endorsed on the front cover with "No change of Post Office allowed".

This form is obtained from the 'new' post office, completed by the customer and returned to the DSS, via the post office, for their information. Counter clerks then complete the post office address details in manuscript in box (c) of the inside front cover of the order book (see Figure 4) and in confirmation of the change of post office imprints his authentication stamp in box (d) of the inside front cover (see Figure 4). Additionally the counter clerk amends the post office and, if appropriate, the customer address details on the front cover (see Figure 3).

POL00028135

Figure 5 Form P80MA - used to effect a permanent change of post office of encashment.



1. What is your pension/allowance number?
This is shown on the front of your order book

2. What is the name of the pension /allowance you are getting?
This is shown at the top of the first inside page of your book.

3. What is the serial number on your book?
This is usually shown next to the pension/allowance number and on each order.

4. What is the name and address of the issuing authority shown on the first inside page of your book?

5. Please tell us
1. Your surname
2. Other names

6. If you are serving in HM Forces -
Please tell us
1. Your rank
2. Service number
3. Ship, Corps Regiment or Station

7. If you are changing your address -
Please tell us
1. Your old address including postcode
2. Your new address including postcode (Please use CAPITALS)

8. If your change of address is temporary please tick the box

Please say roughly when you expect to return

9. If you want to be paid at a different post office to the one named on your book please tick the box.

If you ticked the box -
this is the post office you will be paid at ⇨

OCTAGON B.O. 003
High Wycombe 128
Bucks 3
HP11 2BA

10. Please sign and date this form
Signature
Date

POL00028135

Appendix 3-6

Encashment at a Post Office
Existing Service Levels and Standards and Standard Payment Procedure

POL00028135

APPENDIX 3 - 6

ENCASHMENT AT A POST OFFICE

EXISTING SERVICE LEVELS AND STANDARDS AND STANDARD PAYMENT PROCEDURE

1. INTRODUCTION

The following service levels are those which currently apply for encashment of benefit transactions conducted at post offices. They have been agreed between BA and POCL. The standard agreed payment procedure is charted at Figure 1.

2. SERVICE AVAILABILITY

2.1 Hours of Business

No restriction shall be placed on serving BA's customers at any post office during the normal hours of business of that post office.

3. SERVICE PRINCIPLES

3.1 Office and Staff Appearance

Post offices should offer surroundings commensurate with POCL's required image of a modern retail organisation, and POCL's staff, agents and their staff project a professional image.

3.2 Privacy

All staff of POCL, its agents and their staff shall be conscious in dealing with BA's customers that many matters which may be raised are of a private and confidential nature. Staff shall keep confidential any information received in the course of a transaction. All POCL's staff and agents shall be bound by the Official Secrets Act.

4 SERVICE LEVELS

4.1 Speed of Service

96% of BA's customers to be served within 5 minutes of joining the queue at any post office.

[N.B. 1993/94 waiting times sampled each month peaked at 98.2%.]

100% of BA's customers to be served within 10 minutes of joining the queue at any post office.

POL00028135

4.2 **Payment Accuracy**

100% of cash payments made to the BA's customers to be accurate and in accordance with the value shown on the payment order.

4.3 **Advice**

On request, advice will be available to the BA's customers, which includes procedures for reporting lost or stolen order books and acceptable means of identification.

4.4 **Identification of Staff**

All staff of POCL and its agents and their staff shall give their names and title and the address and telephone number of their Helpline Unit if requested to do so by a customer of the BA. POCL shall encourage staff likely to come into contact with customers to wear name badges at all times except where they feel personal safety is at risk.

4.5 **Availability of Leaflets and Forms**

95% of requests for any leaflets or form stocked by POCL at post offices should be fulfilled immediately. 100% of requests should be fulfilled within five working days.

4.6 **Post Office Point of Sale Displays**

POCL will aim to display an average of 95% of the items specified by BA and maintain the displays in a tidy condition throughout normal hours of business.

4.7 **Facilities for Disabled Customers**

POCL shall wherever possible, provide easy access and adequate facilities for disabled customers to use the post office of their choice. Disabled customers shall be afforded the same range and standard of service provided to other customers.

4.8 **Complaints About Service at the Counter**

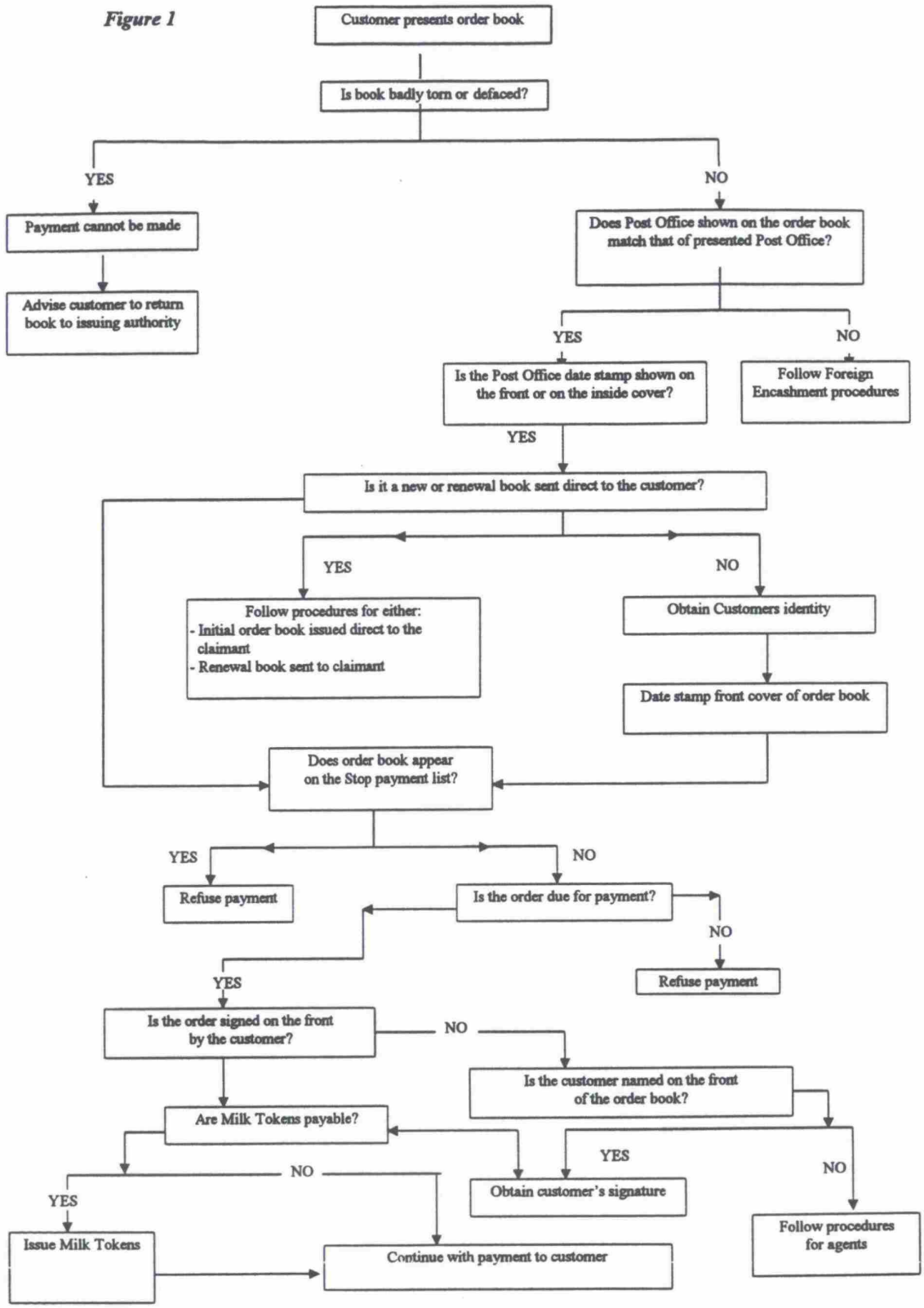
Complaints procedures include the following:

- complaints in post offices must be referred without delay to a member of staff qualified to deal with the complaint;
- telephone complaints should receive an acknowledgement within one working day;
- written complaints should receive an initial answer within seven working days.

POL00028135

Encashment at a Post Office

Figure 1



POL00028135

Appendix 3-7

Existing Output Handling Deadlines

POL00028135

APPENDIX 3 - 7

EXISTING OUTPUT HANDLING DEADLINES

1. INTRODUCTION

The majority of Instruments of Payment (IOP) and customer notifications (including order book pick-up notices) are currently produced at four Area Computer Centres (ACC) located throughout the UK. These are presently managed by the Service Delivery element of ITSA (this function is currently the subject of an outsourcing exercise ["FOCUS 95"]). Generally each ACC houses a number of benefit applications and provides a service for a number of specified DSS local offices. Some benefit applications (e.g. Child Benefit) are however currently housed in their entirety at one ACC. The negotiated output handling deadlines apply to each benefit application no matter where it is housed. These deadlines differ both between and within applications the reason for these differences are dependent primarily on:

1.	the benefit application;
2.	the IOP type (i.e. order book, girocheque, payable order or ACT);
3.	the urgency of the payment (i.e. a new book has greater priority than a renewal book and girocheques are always treated as urgent);
4.	the method of distribution.

1.1 Deadlines

The tables below show, by benefit application, the relevant existing agreed output handling deadlines. Each of which are the subject of audit trails and management information. The tables show the following information:

1.	**Output type** - a description of the media on which the output is stored;
2.	**Service Category** - a description of the particular service being provided;
3.	**Frequency** - the frequency with which the output is to be collected;
4.	**Collection method** - a description of the method of dispatch/carrier of the output;
5..	**Deadline for Collection** - the agreed service levels for provision of the particular service.

1.2 Delivery Addresses for Order Books and Girocheques

There are three types of address to which ACCs may issue order books or girocheques:

(a) a post office nominated by the customer at which the IOP is held for their collection (this option is available only for Order Books)

(b) the customers home address

(c) a DSS District Office for collection by or onward issue to the customer.

Each payment award notified to the ACC by the Benefit Systems contains a dispatch code which dictates the address to which the IOP is dispatched. The decision as to the choice of the delivery address is primarily the customer's, however in some instances (for security or administrative reasons) the DSS can dictate to which address IOPs will be issued.

POL00028135

2. INCOME SUPPORT COMPUTER SYSTEM (ISCS)

This application deals primarily with the payment of Income Support, which may be made via; order book, girocheque, automated credit transfer or payable order. Payments generated by this application are currently produced at all four ACCs.

Table 2.1

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Printed	Early Girocheques and Accompanying Notifications	Daily	Royal Mail	To be ready for the last scheduled 1st class collection on the same day as input to the system; to be delivered by 1st class post.
Printed	Other Girocheques and Accompanying Notifications	Daily	Royal Mail	To be ready for the last scheduled 1st class collection one working day after input to the system; to be delivered by 1st class post.
Printed	1st Class Order Books	Daily	Royal Mail	To be ready for the last scheduled 1st class collection on the working day immediately following commencement of the batch run; to be delivered by 1st class post.
Printed	2nd Class Order Books	Daily	Royal Mail	To be ready for collection within three working days of the commencement of the batch run; to be delivered by 2nd class post.
Printed	B2s and D2s	Daily	Courier	To be ready for collection one working day after input to the system.
Printed	All Urgent Notifications	Daily	Royal Mail	To be ready for the last scheduled 1st class collection on the working day immediately following commencement of the batch run; to be delivered by 1st class post.
Printed	Customer Notifications (1st class Letters)	Daily	Royal Mail	To be ready for the last scheduled 2nd class collection three working days following commencement of the batch run; to be delivered by 2nd class post.
Printed	Customer Notifications (Direct Payment Letters)	Daily	Royal Mail	To be ready for the last scheduled 2nd class collection three working days following commencement of the batch run; to be delivered by 2nd class post.
Printed	Customer Notifications (All other 2nd class letters)	Various	Courier	To be ready for collection on the working day immediately following commencement of the batch run.
Printed	Reports (District Offices Uprating Miscellaneous)	Various	Courier	To be ready for collection on the working day immediately following commencement of the batch run.

POL00028135

Existing Output Handling Deadlines

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Magnetic	National Girobank Tapes BACS Tapes	Various	Courier	As required.
File Transfer	All output designated for PMS to District Offices	Daily	N/A	File(s) to be made available for transfer to destination to allow delivery by 07:00 hours the next working day.
File Transfer	ACT Payment Details Reports	Daily	N/A	File(s) to be made available for transfer to destination to allow delivery by 10:00 hours on the day of production.

POL00028135

3. PENSIONS STRATEGY COMPUTER SYSTEM

This application deals primarily with the payment of Retirement Pensions which may be made via : order book, girocheque, automated credit transfer or payable order . Payments generated by this application are currently produced at all 4 ACCs.

Table 3.1

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Printed	On-Line Girocheques	Daily	Royal Mail and Courier Royal Mail and Courier	As appropriate, to be made ready for courier collection or mailsorted and made ready for collection one working day after input to the system; to be delivered by mailsort class post or by courier to the chosen delivery address. To be mailsorted and made ready, as appropriate, for the last scheduled 1st class collection one working day after the batch run; to be delivered by 1st class post or by courier to the chosen delivery address.
Printed	On-Line Order Books	Daily	Royal Mail and Courier	To be mailsorted and made ready, as appropriate, for the last scheduled 1st class collection or courier collection one working day after input to the system; to be delivered by 1st class post or by courier to the chosen delivery address.
Printed	Renewal Order Books	Daily	Royal Mail and Courier	To be mailsorted and made ready, as appropriate, for the last scheduled 2nd class collection or courier collection within three working days of the commencement of the batch run; to be delivered by 2nd class post or by courier to the chosen delivery address..
Printed	Payable Orders (addressed to payee living in GB and rest of world except NI)	Daily	Royal Mail	To be mailsorted and made ready for the last scheduled 1st class collection one working day before the payable date; to be delivered by 1st class post.
Printed	Claim Packs (Various)	Daily	Royal Mail	To be mailsorted and made ready for the last scheduled 2nd class collection two working days after commencement of the batch run; to be delivered by 2nd class post.
Printed	Customer Notifications (Various)	Various	Various	As required.
Magnetic	ACT (BACS)	Daily	Courier	To be ready for transportation to the relevant bank in time to arrive there four working days before the intended bank entry date.

POL00028135

Existing Output Handling Deadlines

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Magnetic	ACT Transcontinental Automated Payment Service (TAPS)	Daily	Courier	To be ready for collection one working day after requisition or renewal.
Magnetic	ACT (National Girobank and Bank of Scotland)	Various	Courier	As required.
File Transfer	All output designated for FTF to DOs	Daily	N/A	File(s) to be made available for transfer to destination to allow delivery by 07:00 hours the next working day.

POL00028135

4. INCAPACITY BENEFIT COMPUTER SYSTEM

This application deals primarily with the payment of Incapacity Benefits, which may be made via: order book, girocheque, automated credit transfer or payable order. Payments generated by this application are currently produced at all 4 ACCs.

Table 4.1

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Printed	All Girocheques	Daily	Royal Mail and Courier	As appropriate, to be made ready for courier collection or mailsorted and made ready for the last scheduled mailsort class collection one working day after input to the system; to be delivered by mailsort class post or by courier to the chosen delivery address..
Printed	On-Line Order Books	Daily	Royal Mail and Courier	To be mailsorted and made ready, as appropriate, for the last scheduled 1st class collection or courier collection one working day after input to the system; to be delivered by 1st class post or by courier to the chosen delivery address.
Printed	Renewal Order Books	Daily	Royal Mail and Courier	To be mailsorted and made ready, as appropriate, for the last scheduled 2nd class collection or courier collection within three working days of the commencement of the batch run; to be delivered by 2nd class post or by courier to the chosen delivery address
Printed	Payable Orders (Addressed to payee living in GB and Rest of World except NI)	Daily	Royal Mail	As required.
Printed	Recall/Transfer Order Books (Various)	Daily	Royal Mail	To be mailsorted and made ready for the last scheduled 2nd class collection one working day after input to the system; to be delivered by 2nd class post.
Printed	Entitlement Notices (Various)	Daily	Royal Mail	To be mailsorted and made ready for the last scheduled 1st class collection one working day after input to the system; to be delivered by 1st class post.
Printed	Customer Notifications (Various)	Various	Various	As required.

POL00028135

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Magnetic	ACT (Various)	Daily	Courier	To be ready for transportation to the relevant bank in time to arrive there four working days before the intended bank entry date.
File Transfer	All output designated for FTF to DOS.	Daily	N/A	File(s) to be made available for transfer to destination to allow delivery by 07:00 hours the next working day.

POL00028135

5. CHILD SUPPORT COMPUTER SYSTEM

This application deals solely with the payments on behalf of the Child Support Agency which may be made via: girocheques or automated credit transfer. Payments generated by this application are currently produced at one ACC only. .

Table 5.1

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Printed	Girocheques and Priority 1 and 2 Notifications	Daily	Royal Mail	To be made ready for the last scheduled 1st class collection one normal working day after input to the system; to be delivered by 1st class post.
Printed	Priority 3 Reports	Daily	Courier	As required.
Magnetic	"A" Type Girocheque Reconciliation Tape and "Jumbo" Type Girocheque Reconciliation Tape	Weekly	Royal Mail (GB) Courier (NI)	To be ready for the last 1st class collection on the normal working day immediately following input to the system/the batch run; to be delivered by 1st class post. To be ready for collection by 16:00 hours the normal working day immediately following production.
Magnetic	ACT Payment File	Daily	Courier/Air	To be ready for collection by 16:00 hours the normal working day immediately following production.
File Transfer	All output designated for FTF to CSA locations	Daily	N/A	File(s) to be made available for transfer to destination to allow delivery by 07:00 hours the next working day.

POL00028135

6. DISABILITY LIVING ALLOWANCE COMPUTER SYSTEM

This application deals primarily with the payment of Disability Living Allowance, which may be made via order book, girocheque, automated credit transfer or payable order. Payments generated by this application are currently produced at all four ACCs.

Table 6.1

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Printed	"A" Type Girocheques linked (input by 12:00 hrs)	Daily	Royal Mail	To be ready for the last scheduled 1st class collection on the same working day as the batch run; to be delivered by 1st class post.
Printed	All "Jumbo" Type Girocheques linked and "A" Type linked (input after 12:00 hrs)	Daily	Royal Mail	To be mailsorted and made ready for the last 1st class collection on the working day after commencement of the batch run; to be delivered by 1st class post.
Printed	Order Book Renewals	Daily	Royal Mail	To be mailsorted and made ready for the last 2nd class collection three working days immediately following the most recent batch run; to be delivered by 2nd class post.
Printed	Miscellaneous Order Books	Daily	Royal Mail	To be mailsorted and made ready for the last 2nd class collection on the working day immediately following the most recent batch run; to be delivered by 2nd class post.
Printed	Notifications (Claimant)	Daily	Royal Mail and Courier	To be mailsorted and made ready for the last scheduled collection on the working day immediately following the most recent batch run.
Printed	Notifications (Third Party Non-Sensitive)	Daily	Royal Mail Courier	To be mailsorted and made ready for the last 1st class collection on the working day immediately following the most recent batch run; to be delivered by 1st class post. To be ready for the last scheduled collection on the working day immediately following the batch run.
Printed	Notifications (Third Party Sensitive)	Daily	Courier	To be ready for the last scheduled collection on the working day immediately following the batch run.
Printed	Reports (Various)	Various	Various	As required.
Printed	Prints (Various)	Daily	Courier	As required.

POL00028135

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Magnetic	Compensation Recovery Unit	Monthly	Courier	To be ready for collection on the working day immediately following the batch run.
	ASD	Quarterly	Courier	To be ready for collection on the working day immediately following the batch run.
Magnetic	GIREC Tape and MFL Tape	Weekly	Courier	To be ready for scheduled collection on the day immediately following the batch run.
Magnetic	ACT (BACS Tape)	Daily	Midland Bank	To be ready for scheduled collection on the working day immediately following the batch run.
File Transfer	All output designated for file transfer by PMS	Daily	N/A	File(s) to be made available for transfer to destination to allow delivery by 10:00 hours on the day following the batch run.

POL00028135

7. AA65+ COMPUTER SYSTEM

This system deals primarily with the payment of Attendance Allowance, which may be made via: order book, girocheque, automated credit transfer or payable order. Payments generated by this application are currently produced at all 4 ACCs.

Table 7.1

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Printed	"A" Type Girocheques linked (input by 12:00 hrs)	Daily	Royal Mail	To be ready for the last scheduled 1st class collection on the same working day as the batch run; to be delivered by 1st class post.
Printed	All "Jumbo" Type Girocheques linked and "A" Type linked (input after 12:00 hrs)	Daily	Royal Mail	To be mailsorted and made ready for the last 1st class collection on the working day after commencement of the batch run; to be delivered by 1st class post.
Printed	Order Book Renewals	Daily	Royal Mail	To be mailsorted and made ready for the last 2nd class collection three working days immediately following the most recent batch run; to be delivered by 2nd class post.
Printed	Miscellaneous Order Books	Daily	Royal Mail	To be mailsorted and made ready for the last 2nd class collection on the working day immediately following the most recent batch run; to be delivered by 2nd class post.
Printed	Notifications (Claimant)	Daily	Royal Mail and Courier	To be mailsorted and made ready for the last scheduled collection on the working day immediately following the most recent batch run.
Printed	Notifications (Third Party Non-Sensitive)	Daily	Royal Mail Courier	To be mailsorted and made ready for the last 1st class collection on the working day immediately following the most recent batch run; to be delivered by 1st class post. To be ready for the last scheduled collection on the working day immediately following the batch run.
Printed	Notifications (Third Party Sensitive)	Daily	Courier	To be ready for the last scheduled collection on the working day immediately following the batch run.
Printed	Reports (Various)	Various	Various	As required.
Printed	Prints (Various)	Daily	Courier	As required.

POL00028135

Existing Output Handling Deadlines

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Magnetic	Compensation Recovery Unit	Monthly	Courier	To be ready for collection on the working day immediately following the batch run.
	ASD	Quarterly	Courier	To be ready for collection on the working day immediately following the batch run.
Magnetic	GIREC Tape	Weekly	Courier	To be ready for scheduled collection on the day immediately following the batch run.
Magnetic	ACT (BACS Tape)	Daily	Midland Bank	To be ready for scheduled collection on the working day immediately following the batch run.
File Transfer	All output designated for file transfer by PMS	Daily	N/A	File(s) to be made available for transfer to destination to allow delivery by 10:00 hours on the day following the batch run.

POL00028135

8. FAMILY CREDIT/DISABILITY WORKING ALLOWANCE COMPUTER SYSTEM

This application deals primarily with the payment of Family Credit and Disability Working Allowance which may be made via: order book, girocheque or automated credit transfer. Payments generated by this application are currently produced at all 4 ACCs.

Table 8.1

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Printed	Order Books, Girocheques and Associated Notifications	Daily	Royal Mail	To be made ready for the last scheduled 1st class collection one working day after input to the system; to be delivered by 1st class post.
Printed	Urgent Enquiries/Letters and Notifications	Daily	Royal Mail	To be made ready for the last scheduled 1st class collection one working day after input to the system; to be delivered by 1st class post.
Printed	Renewal Reminders	Weekly	Royal Mail	To be made ready for the last 2nd class collection two working days after the daily batch run from which they are produced; to be delivered by 2nd class post.
Printed	Non-Urgent Post (Various)	Daily	Royal Mail	As required.
Magnetic	National Girobank (BACS)	Weekly	Courier	To be ready for collection by 16:00 hours on the working day immediately following production.
	Others (Various)	Various	Courier	To be ready for collection by 07:30 hours on the third working day following production.
File Transfer	BAS	Daily	N/A	File(s) to be made available for transfer to destination to allow delivery by 07:00 hours the next working day after entry.
File Transfer	ASD - DWA Statistics	Daily	N/A	File(s) to be made available for transfer to destination to allow delivery by 07:00 hours the next working day after production.
File Transfer	All Reports designated for mainframe printing at offices	Daily	N/A	File(s) to be made available for transfer to destination to allow delivery by 07:30 hours the next working day after entry.

POL00028135

9. SOCIAL FUND COMPUTER SYSTEM

This application deals solely with social fund payments which are made via girocheque. Payments generated by this application are currently produced at all four ACCs.

Table 9.1

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Printed	Girocheques including Payment Letters (input before 15:00 hours)	Daily	Royal Mail	To be ready for the last scheduled 1st class collection on the same day as input to the system; to be delivered by 1st class post.
Printed	Girocheques including Payment Letters (input after 15:00 hours)	Daily	Royal Mail	To be ready for the last scheduled 1st collection one working day after input to the system; to be delivered by 1st class post.
Printed	Letters (Various)	Daily	Royal Mail	As required.
Printed	Reports (Various)	Various	Courier	As required.
Magnetic	PBMIS Statistics Tapes	Monthly	Courier	To be despatched to the appropriate IBM Mainframe site by the 1st working day following the completion of the SFCS month-end statistics run.
	National Girobank GIREC Tapes	Weekly	Courier	To be made ready for collection by 16:00 hours on the Monday following production.
File Transfer	All outputs designated for FTF to Offices	Daily	N/A	File(s) to be made available for transfer to destination to allow delivery by 07:00 hours the next working day.

POL00028135

10. NUBS2 COMPUTER SYSTEM

This application deals solely with the payment of Unemployment Benefit which may be made via : girocheque or automated credit transfer. Payments generated by this application are currently produced at all 4 ACCs.

Table 10.1

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Printed	Girocheques	Daily	Royal Mail	To be mailsorted and made ready for 11:00 hours the day following input to the system; to be delivered by 1st class post.
Printed	Local Office Forms and Schedules	Daily	Courier	To be ready for collection one working day after input to the system.
Magnetic	ACT Tapes	Daily	Courier	To be ready for collection by 12:00 hours on the working day immediately following production.
File Transfer	DCI NIRS	Daily	N/A	As required.

POL00028135

11. CHILD BENEFIT COMPUTER SYSTEM

This application deals solely with the payment of Child Benefit, which may be made via: order book, girocheque or automated credit transfer. Payments generated by this application are currently produced at one ACC.

Table 11.1

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Printed	Girocheques	Daily	Royal Mail	To be ready for the last scheduled first class collection on the working day immediately following commencement of the batch run; to be delivered by first class post.
Printed	Order Books (First Class)	Daily	Royal Mail	To be ready for the last scheduled first class collection on the working day immediately following commencement of the batch run; to be delivered by first class post.
Printed	Order Books (First Class)	Daily	Various	To be ready for the last scheduled second class collection four working days immediately following commencement of the batch run; to be delivered by second class post.
Printed	Urgent Notifications	Daily	Various	To be ready for the last scheduled first class collection on the working day immediately following commencement of the batch run; to be delivered by first class post.
Printed	Other Printed Output	Daily	Various	To be ready as required; to be delivered by second class post as appropriate.
Magnetic	ACT Tapes	Daily	Courier	As required.

POL00028135

12. WAR PENSIONS COMPUTER SYSTEM

This application deals solely with payments of war pensions which may be made via: order books, girocheques, automated credit transfer and payable orders. Payments generated by this application are currently produced at all 4 ACCs.

Table 12.1

OUTPUT TYPE	SERVICE CATEGORY	FREQUENCY	COLLECTION METHOD	DEADLINE FOR COLLECTION
Printed	Overseas Payable Orders	Twice Weekly	Messenger	To be ready for despatch in time for the 08:00 hours transport to Norcross within two working days of the batch run being completed.
Printed	Emergency Order Books	Twice Weekly	Royal Mail	To be ready for the last scheduled first class collection on the working day following the run being completed.
Printed	UK Payable Orders and Renewal Order Books	Twice Weekly	Royal Mail	To be ready for the last scheduled second class collection two working days following the run being completed.
Printed	Notifications and Schedules	Various	Messenger	As required.
Magnetic	BACS Tapes TAPS Tapes MFL Tapes	Various	Various	As required.
File Transfer	Mednet Download	Following Batch Run	N/A	File(s) to be ready for transfer to destination to allow delivery by 05:30 hours following the batch run.

POL00028135

Appendix 3-8

Benefit Payment Services - Volumes

POL00028135

APPENDIX 3 - 8

BENEFIT PAYMENT SERVICES - VOLUMES

1. INTRODUCTION

This appendix provides information and relevant volumes relating to matters associated with the benefit payment service currently offered by the Contracting Authorities. The intention is to provide prospective Service Providers with:

(a) background information, allowing the Service Providers to obtain a view as the scale of the benefit payment service required in terms of customers and complexity (Section 3 Customers and Benefits);

(b) the volumes of Instruments of Payment and subsequent relevant benefit payment transactions generated by the existing benefit payment service (Section 4 Benefit Payments);

(c) indicative forecasts relating to the anticipated scale of the benefit payment service in the future (Section 5 Future Volumes);

(d) existing enquiry dialogue accesses generated by customer or staff action within the existing benefit payment system (Section 6 Enquiry dialogue Volumes).

2. BUSINESS VOLUMES

The Business volumes outlined in the following sections are intended to give an overall context for the Benefit Payment Service. They are by definition, subject to significant change over time due to a wide range of factors such as legislative imperatives (e.g. the introduction of new benefits) and operational changes (e.g. the introduction of new methods of payment). The Service Provider should therefore, in no way, take the following volumes to be definitive or guaranteed levels of business.

3. CUSTOMERS AND BENEFITS

The DSS currently administer the payment of more than 30 individual benefit types which are grouped under some 19 generic benefit groups. The exact number and types of benefits payable, together with the numbers of customers to whom they are payable, are subject to frequent change as new benefits are introduced or old benefits withdrawn. The introduction or withdrawal of benefit types may be further complicated by the fact that not all customers may be simultaneously affected by a change. As an example Disability Living Allowance (introduced in April 1992) took over all previous Mobility Allowance customers but only some Attendance Allowance customers (those aged under 65). The picture is further complicated by the fact that many customers are in simultaneous receipt of more than one benefit. The present benefit system does not generate individual customer accounts, relevant management information is therefore difficult to obtain.

3.1 Benefit Types

The table below (*Figure 1*) lists the generic benefit groupings and provides indicative numbers of customers per benefit group. This information is illustrative only, having been obtained as a 'snapshot' of the customer base in August 1994. The table also provides an indication of the numbers of customers per benefit group who receive their benefit payments by either order book or girocheque. It must be stressed that customers may be in receipt of more than one benefit simultaneously and that no account of this overlapping has been taken when compiling these figures.

POL00028135

Figure 1

Benefit Type	Benefit Group No.	Number of Beneficiaries (1000s)	Number paid by order book or girocheque (1000s)
Attendance Allowance	13	948	41
Child Benefit	05	6868	5266
Disability Working Allowance	14	4	2
Disability Living Allowance	07	1131	903
Family Credit	08	503	422
Guardian's Allowance	05	2	0
Industrial Injuries Disablement Benefit	12	300	0
Invalid Care Allowance	13	237	246
Invalidity Benefit	14	2092	2081
Sickness Benefit	14		
Severe Disablement Allowance	14		
Social Fund	N/A	N/A	N/A
Income Support	11	5670	3503
Maternity Allowance	13	19	15
Retirement Pension	13	10151	6726
Widows Pension	13		
Unemployment Benefit 2	N/A	701	2620
War Pensions	06	386	168
Pneumoconiosis, Byssinosis and Miscellaneous Diseases Benefit Scheme	12	N/A	N/A
Totals		29,012	21,993

1 Numbers of beneficiaries do not match with those paid by order book or girocheque as:
- a number are paid by ACT and ;
- where multiple benefits are awarded to customers, the benefits can be combined to make a single payment

2 to be replaced by Jobseekers Allowance from mid-1996.

3.2 Customers

The estimated customer base for calendar year 1993 is shown below in ***Figure 2*** to provide indicative figures in relation to the possible numbers of card-carrying customers. The numbers will change over time due primarily to economic factors. In addition the relative use of automated credit transfer can be expected to increase.

Figure 2 **Current Customer Base**	
Customers receiving benefit at post offices	21,200,000
Customers receiving benefit via ACT	5,400,000
Customers who are alternate payees	3,900,000
Total number of customers	30,500,000

The numbers above represent the estimated caseload at any one time. Due to the fact that some customers will claim intermittently, numbers of card holders may be somewhat higher than those eligible to collect benefit at post offices (25,100,000 in the above table).

POL00028135

The number of new customers notified to CMS / PAS will clearly be at its highest during the initial roll-out period and will, to a large extent, be dependent on the Service Provider's proposals.

3.2.1 Changes to Customer's Personal Details

During the life of their claims to benefit customer's personal details may change. Some of these changes may be relevant to their payment of benefit, others may not. The Service Provider should note that not all change information will be passed on to them. For example in the case of changes relating to customers who are not paid by the card-based method of payment.

The current levels of changes to relevant personal details are as shown below in ***Figure 3***. through to ***Figure 8.*** The numbers given represent changes per year.

Changes of Name

Figure 3 **Change of Name**	
Notification of change of name	875,000
Notification of alias Correction of alias or real name Removal of alias	550,000
Total name changes	1,425,000

POL00028135

Changes of Address

Figure 4 Change of Address	
Change of address	11,400,000
Change of Dead Letter Office (DLO) address	530,000
Total address changes	11,900,000

The Service Provider should note that 3,300,000 of these change of address notifications originate from the National Insurance Recording System (NIRS) and are not, in general, limited specifically to benefit recipients. A Dead Letter Office (DLO) address is one which the DSS held as the customer's address following a claim to benefit, however there is information available (e.g. an unsuccessful attempt to make a home visit) which indicates that the customer is no longer resident.

Death of a Customer

Figure 5 Death of a customer	
Notification of Date of Death (from benefit systems)	705,000
Notification of Date of Death (from registrar)	15,000
Correction to Date of Death	5,000
Removal of Date of Death	20,000
Total date of death notifications	745,000

Other Personal Details

The volume of revisions to other personal details (such as Date of Birth, Sex, National Sensitivity) are much lower than any of the changes listed above and do not significantly affect overall volumes. However, they are listed below for completeness.

Figure 6 Birth	
Verification of Date of Birth (almost all on reaching pension age)	540,000
Correction to Date of Birth	65,000
Total	605,000

Figure 7 Sex	
Correction to Sex	10,000

Figure 8 Sensitivity	
Change to National Sensitivity	1,000

4. BENEFIT PAYMENTS

This section deals with volumes relating to Instruments of Payment issued to customers and benefit payment transactions relevant to this procurement.

POL00028135

4.1 Instruments of Payment and Transactions - Existing Levels

The table below, ***Figure 9***, provides an indicative overview of the numbers of Instruments of Payment issued and subsequent benefit payment transactions over a five year period from 1989 to 1994. Certain figures are not available, where figures are not known the relevant box is shaded.

Figure 9 IOP issues and Transactions 1989 - 94	1989/90 (M)	1990/91 (M)	1991/92 (M)	1992/93 (M)	1993/94 (M)
No of Order Books Issued - System Produced				50.90	52.55
No of Order Books Issued - Clerically Produced				3.86	5.2
Total No of Order Books Issued	48.83	47.23	49.93	54.76	57.75
No of Order Book payment transactions at Post Offices	817.21	819.67	832.55	851.29	866.52
No of Girocheque payment transactions at post offices.	68.23	70.07	87.55	94.73	94.64
Total transactions made at Post Offices	885.44	889.74	920.10	946.02	961.16

4.2 Benefit Payment Transactions - Order Books

This section deals with current volumes of benefit payment transactions relevant to this procurement i.e. those conducted at post offices where the method of payment is by order book or girocheque. In 1993/94 over 90% of all such benefit payment transactions conducted at post office counters was order book based (this calculation excludes associated payment transactions such as Welfare Food tokens, Christmas bonus payments etc.).

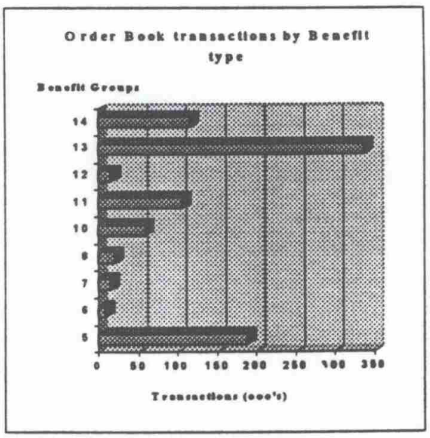
4.2.1 Transactions by Benefit Type

The table at ***Figure 1*** shows the relationship between benefit types and benefit group numbers. ***Figures 10*** and ***11*** below illustrate the number of benefit payment transactions which occurred in 1993/94 in respect of each type of benefit.

Figure 10

Benefit Group	Transactions (M)
14	117.19
13	337.22
12	15.79
11	105.44
10	58.70
8	20.97
7	14.35
6	8.16
5	188.70
Total	866.52

Figure 11



POL00028135

4.2.2 Periodicity and Pay-Days

The table below illustrates the daily transaction profile in respect of order book based benefit payment transactions by benefit type.

Figure 12 Daily transaction profile

Benefit Group No.	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
05	48.9	23.9	8.8	8.2	6.4	3.8
06	25.4	7.8	35.3	20.1	8.4	3.0
07	9.0	4.0	58.0	18.3	7.9	2.8
08	3.1	68.5	12.1	8.0	5.4	2.9
10	15.2	20.0	5.1	46.4	10.5	2.8
11	38.8	18.4	13.9	19.5	7.1	2.3
12	3.9	2.5	54.8	24.8	9.8	4.2
13	26.6	17.1	5.5	38.5	9.7	2.6
14	19.5	20.2	23.0	28.0	7.3	2.0
Total	26.4	19.5	12.9	30.0	8.5	2.7

The following table indicates the daily transaction profile averaged across all benefit types :

Figure 13

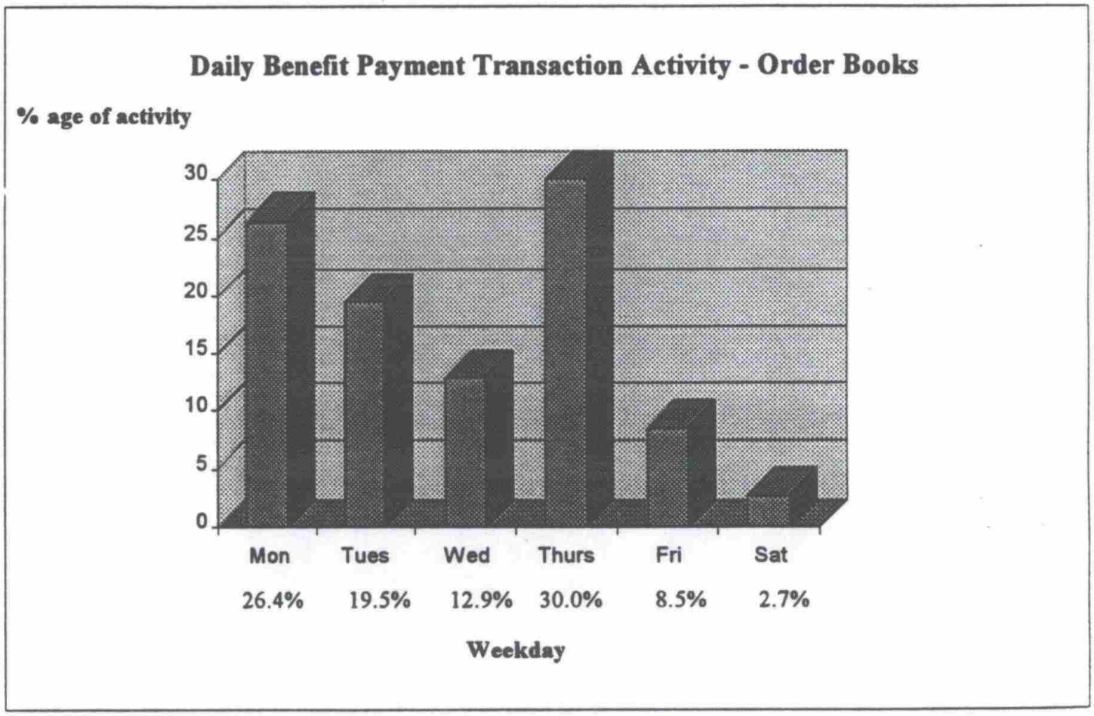


Figure 13 represents the average daily profile of order book benefit payment transactions. In the order of between 16M and 18M payment foils are encashed per week. The overall profile reflects the transaction peaks on Mondays and Thursdays which are due to the existing allocation of pay-days (due dates of encashment) by benefit type. This profile may change significantly as a result of operational and statutory revisions, such as an alignment of pay-days across benefits. In addition, short term variations

POL00028135

will occur due to the nature of the benefit process. For example, Cold Weather Payments are issued in a locality if the temperature, as measured at the local weather station, falls below certain levels for a specified period of time. There are a total of 3.3M customers who are deemed to be eligible for Cold Weather Payments. The maximum number of additional payments (throughout the UK) in one week is therefor 3.3M. The worst case on record is one occasion when 50% of those deemed eligible qualified for payment.

Figure 14 Cold Weather Payments	
Number of eligible customers	3,300,000
Number of weather stations	67

Associated Transactions

The Service Provider should note that transactions associated with payment by order book, such as payment of Christmas Bonus, do not currently affect overall numbers of transactions since they are combined with other benefit payments. For completeness, information relating to such transactions is provided below:

Figure 15 Christmas Bonus	
Christmas Bonus Payments made during 1993/94	10,151,000

Figure 16 Welfare Food Tokens	
Welfare Food Token transactions during 1993/94	65,318,000

There are transactions associated with benefit payments which do add to the number of total post office based transactions e.g. :

Figure 17 Prescription refunds	
Number of prescription refunds during 1993/94	113,000

4.2.3 Transactions by Region

POCL is organised on a regional basis comprising seven geographically based regions. Benefit payment transactions are not equally dispersed throughout these regions. The table below indicates the percentage share of benefit payment and associated transactions by region. The figures are based on a average 12 month period during 1993/94.

Figure 18 **Benefit Payment and associated transactions by POCL region**

POCL Region	% age of Order Book Transactions	%age of Girocheque Transactions	%age of Milk Token Transactions
Scotland and Northern Ireland	9.99	14.6	11.05
North East	16.42	15.9	15.30
North Wales and North West	16.11	14.1	14.65
Midlands	13.51	12.7	13.80
South Wales and South West	14.18	11.8	12.15
North Thames and East Anglia	16.69	17.6	19.15
South East	13.10	13.3	13.90

POL00028135

4.2.4 Foreign and Casual Agency Encashments

The existing benefit payment service does not provide a detailed breakdown of 'foreign' (those made away from the nominated post office) or 'casual agency' (those where payment is received by an ad hoc proxy) encashments. However BA has carried out various selective studies in these areas. These have shown some variation, but provide some indication of the scale of these types of benefit payment transaction:

Figure 19 Foreign Encashments (%age of all foils encashed)	
Average figure from National studies	4.45%
Average figure from studies restricted to London	10.55%

Figure 20 Agency Encashment (%age of all foils encashed)	
Average figure from National studies	12.77%

4.3 Benefit Payment Transactions - Girocheques

Girocheques comprise between 9% and 10% of all benefit payment transactions at post offices made during the year 1993/94.

4.3.1 Urgent Payments

Clerically issued girocheques are often (though not always) used as the medium to provide for urgent and/or one-off payments to be made to customers. Service Providers should be aware that an indicative worst case scenario for the number of urgent payments per year can be assessed from the level of clerically issued girocheques per year. The figures below are per annum:

Figure 21 Clerically Issued Girocheques 1993/94	
Employment Service Issues	3,000,000
Income Support	4,500,000
Social Fund Crisis Loans	700,000
Total	8,200,000

4.4 Order Book and Girocheque Post Office Notifications

Within the existing benefit payment service processes a post office notification procedure (designed to prevent the encashment of an IOP and called a 'Stop' notice) may be used both to:

- revise entitlement to or re-rate payments due to changes in customer circumstance; and
- stop lost and stolen order books and Girocheques.

In the former process a notification is also sent to the customer requesting that they return their order book, and stating the reason. The overall use of this mechanism is highly dependent on the characteristics of each benefit. Income Support, which is a volatile benefit, has a high percentage of stop notices issued in respect of all IOPs that it issues whilst Retirement Pension, a relatively stable benefit, has far lower levels. The table below gives indicative percentages of Stop notice issues against IOP issues:

POL00028135

Figure 22 Percentage of all IOPs that are stopped/cancelled			
Benefit Type	Total IOP Issues	Total Stops	%age Against Issues
Income Support	12,000,000	1,620,000	13.5%
Disability Living Allowance	1,500,000	72,000	4.8%
Child Benefit	16,000,000	160,000	1.0%
Retirement Pensions	17,400,000	87,000	0.5%
Average			4.3%

The percentages imply that, of approximately 50 million order books and 20 million girocheques within the above survey (it excludes 70 million Unemployment Benefit girocheques), around 3 million are stopped. Of that 3 million, reported order book loss is approximately 300,000 per annum. Various internal DSS reports indicate that the actual level of loss may be higher than this The Service Provider should also note that, of the 50 million order books issued, at least 10.2 million are recalled for various reasons. If there is no response to the recall notice within six days, a stop notice is issued to the post office.

A new card-based MOP should enable benefit staff to make revisions to future payments without necessarily recalling an issued Instrument of Payment. Therefore the volumes of stops received by PAS should be considerably lower than current levels.

Some of the current losses of order books and girocheques are due to the fact that they have value in themselves and are therefore attractive items to potential fraudsters. It is anticipated that any future card or token would have no inherent value, as a result overall losses should correspondingly be somewhat lower.

5. BENEFIT PAYMENT TRANSACTIONS - FUTURE VOLUMES

This section indicates anticipated future volumes in respect of order book and girocheque payment transactions.

Category of Transaction	95/96	96/97	97/98	98/99
Order book benefit payment transactions at post offices:	861M	861M	867M	867M
Girocheques - total benefit payment transactions at post offices :	88M	88M	88M	88M
Total benefit payment transactions at post offices :	949M	949M	955M	955M

6. ENQUIRY DIALOGUE ACCESSES MADE OF THE EXISTING SYSTEMS

6.1 Introduction

Individual DSS Benefit computer systems incorporate a number of dialogues through which all work, leading to the payment of benefits, is processed. It is likely that the volume of enquiries made through these dialogues may be of particular relevance to this service requirement. These enquiries are made by authorised members of staff with access to relevant dialogues, which are normally accessible from computer terminals situated in DSS offices throughout the UK.

POL00028135

The table below (*Figure 24*) provides indicative volumes for the numbers of available dialogues and relevant accesses for each of the main benefit systems (for which information is available).

Figure 24 Indicative volumes of available dialogues and accesses in a typical year

Benefit Computer System	Number of available dialogues	Total number of dialogue accesses in a typical year
Income Support Computer System	41	506,250,000
Social Fund Computer System	150	96,169,711
Disability Working Allowance	24	300,802
Disability Living Allowance	47	150,028,780
Child Benefit Computer System	4	5,590,552
Incapacity Benefit Computer System	21	77,567,537[1]
Pensions Strategy Computer System	28	87,887,423
Family Credit Computer System	24	N/A
Totals:	339	923,794,805

1 This figure is estimated.

6.2 Enquiry dialogues

The information provided below shows indicative volumes relating to the number of occasions on which enquiry dialogues were accessed during the year 1993/94 and an indication of the numbers and types of the most common form of accesses via these dialogues.

In a future automated benefits payment system some of these enquiries, subject to negotiation, may require access to data held on the Service Provider's computer systems. The number and nature of such enquiries will depend on the nature and scope of the service provided. Potential Service Providers should assess for themselves the likely number and nature of enquiries they may expect to have to deal with. The following information is provided only for guidance.

Information related to enquiry dialogue accesses is collated based on the 14 most used dialogues within a year. The tables below therefore refer only to relevant (i.e. enquiry) dialogues which amongst the 14 most used dialogues logged, per benefit system, during the year 1993/94.

6.2.1 Income Support Computer System

Dialogue Reference Number	Number of accesses via DSS offices (1993/94)	Dialogue Function
IS502	100,000,000	Used to obtain an historic view of a customer's payment record.
IS500	90,000,000	Used to view customer and or claim details, this facility applies primarily to 'live' or recently dormant claims
IS530	45,000,000	Used to view and enter case control codes, which may be either user or system set
IS510	37,000,000	Enquiry/Notepad - provides a view only facility in relation to dialogue IS110 entries and order book recall notice issues
IS503	27,000,000	View only facility showing a summary of payment award and overall entitlement information
IS220	8,000,000	Used for management checks relating to the accuracy or

POL00028135

Dialogue Reference Number	Number of accesses via DSS offices (1993/94)	Dialogue Function
		quality of payment awards
IS430	<100,000	Used to record reported lost, stolen or destroyed IOPs

6.2.2 DWA Computer System

Dialogue Reference Number	Number of accesses via DSS offices (1993/94)	Dialogue Function
DW141	106,854	Used to make general enquiries concerning the status of the claim or customer
DW109	1740	Used for case control procedures

6.2.3 DLA Computer System

Dialogue Reference Number	Number of accesses via DSS offices (1993/94)	Dialogue Function
DA500	4,900,000	Used to make enquiries relating to a customer's personal circumstances
DA510	3,200,000	Enquiry facility relating to Motability
DA501	3,200,000	View only facility to provide a case summary
DA502	3,080,000	Used to support historic payment enquiries

6.2.4 Child Benefit Computer System

Dialogue Reference Number	Number of accesses via DSS offices (1994/95)[1]	Dialogue Function
CBC001	3,209,804	Used to obtain a full print-out of the customer's account record

1 Estimated.

6.2.5 Incapacity Benefit Computer System

Dialogue Reference Number	Number of accesses via DSS offices (1993/94)	Dialogue Function
RP001	10,999,863	Enquiry facility - used to view customer's personal details
RP002	9,939,592	Enquiry facility as above
RP008	5,029,502	Enquiry facility used to show the breakdown of benefit entitlement
RP702	1,131,466	Used to maintain IOP details (e.g. record the loss or theft of an IOP)

6.2.6 Pensions Strategy Computer System

POL00028135

Dialogue Reference Number	Number of accesses via DSS offices 1993/94)	Dialogue Function
RP001	20,768,188	Enquiry facility providing summary details of customer accounts
RP002	11,750,622	Case control enquiry facility
RP004	8,748,427	Enquiry dialogue for breakdown of payment calculation
RP704	1,466,461	Used to record returned IOPs
RP702	1,026,522	Used to record lost IOPs

6.2.7 Family Credit Computer System

Dialogue Reference Number	Number of accesses via DSS offices (1993/94)	Dialogue Function
FK041	3,811,106	Enquiry facility used to view customer account details
FK007	16,889	Used by supervisors to investigate the workload and identify problem areas

POL00028135

Appendix 4-1

POCL Information Systems Security Policy

POL00028135

POST OFFICE COUNTERS INFORMATION SYSTEMS SECURITY POLICY

FOREWORD

POCL's systems for processing information are becoming more complex and are subject to new and changing risks with the introduction of new technology and new business services to clients and customers. The value of information is growing rapidly as businesses depend increasingly on up-to-date facts about the environment in which they are operating, within POCL and outside. The need for adequate security protection of our assets is more important than ever. However, we must ensure our security is efficient and reliable while being provided at acceptable cost.

As new services are introduced, clients are increasingly asking for evidence of security assurance on information systems and services. To support the Customer First principle, POCL needs to demonstrate to staff, agents, clients and customers its commitment to information systems (IS) security.

This document sets out POCL's policy for the protection of its information assets, including hardware, applications, networks and databases against loss of any of the following:

- confidentiality
- availability or access to the information
- integrity of the information's content.

Its primary aim is to achieve a comprehensive and consistent approach to IS security in POCL's operations and business services.

POCL is committed to preserving its reputation for high standards and quality of service, and preventing the loss of assets.

The Policy therefore requires each business unit and their sub-contractors and agents to adopt the *Post Office Information Systems Security Code of Practice* to implement appropriate measures to protect IS assets commensurate with relevant business and technology risks.

POL00028135

CONTENTS

POL00028135

1. INTRODUCTION

The purpose of security is to ensure **business continuity** and minimise **business damage** by preventing and minimising the impact of security incidents.

This Information Systems (IS) Security Policy forms part of the overall Post Office Counters Ltd (POCL) approach to security and falls within the umbrella framework of the Post Office Security Policy.

1.1 What is Information Systems Security?

Managed effectively, Information Systems (IS) security provides an essential component of an **enabling mechanism for information sharing,** which ensures the protection of *information and computing* assets.

Business is becoming more competitive and customers and clients are making more demands in levels of service. Good security will help to underpin the availability of information systems to meet the service level expectations of customers and clients.

Increasingly the market trend is towards closer vertical integration of POCL's and client systems to meet client needs and win new business. To maintain a consistent level of protection for information and computing assets from end to end, there needs to be a common understanding that the responsibilities for implementing and managing security controls must be shared by all parties concerned.

The information systems security policies of clients, agents and sub-contractors must be compatible with those of POCL to protect the sharing of information. The same applies to other POCL security policies and standards in force.

Information Systems security management has three basic components:

Confidentiality: *protecting sensitive information from unauthorised disclosure*

Integrity: *safeguarding the accuracy and completeness of information and computer software*

Availability: *ensuring that information and vital services are available to users when required.*

POL00028135

The enforcement of an IS security policy should improve customer and client perception of the quality of our services, as well as staff and agents attitudes towards our services.

1.2 Policy and Legal Requirements

All POCL business units, subcontractors, agents and business associates must conform to the POCL Information Systems Security Policy. In addition, it is a mandatory requirement that POCL complies with IS security related legislation. This includes:

* *The Data Protection Act 1984:* Protection of personal data in computer systems against unauthorised access or modification, denial or access or destruction

* *The Official Secrets Act 1989:* Protection of unauthorised disclosure of all information gained while in POCL's employment, including material with privacy and related marking

* *The Computer Misuse Act 1990:* Protection against hacking, unauthorised modification and misuse of computer systems, networks and data

* *The Copyright, Designs and Patents Act 1988:* Protection against software piracy and infringement of intellectual property rights

* *EC Directive on Legal Protection of Databases 1993:* Protection against unauthorised use or access of proprietary databases

* *The Companies Act 1985:* Protection against falsification of Post Office and POCL owned records and procedures

* *The Post Office and Telegraph Acts:* Protection against the communication of information to unauthorised persons. Use of information classification to help identify the need for restricted handling of certain types of data or information.

1.3 Authority and Control

This Policy has been prepared by Information Systems Strategy Unit (ISSU) on behalf of the Counters Executive Committee. Changes and updates will be the responsibility of ISSU.

POL00028135

2. POLICY STATEMENT

POCL will actively maintain a security infrastructure to direct and manage information security.

All POCL business units must:

* ensure all POCL employees, business associates, clients and sub-contractors are aware of information systems security and related policies and practices to the extent that their duties require, and fully understand their responsibilities (including their legal obligations) for protecting information and computing assets from end to end

* limit access to information and other IS assets to those whose duties require it and who have the necessary authority

* ensure that risks are reduced to an acceptable level by applying protective measures, based on risk assessment and criticality of the information, and which conform to minimum standards recommended in the *Post Office Information Systems Security Code of Practice* modified for POCL's business and computing environment. The Code of Practice may be superseded by a specific POCL Information Systems Security Code of Practice in future

* implement and enforce the POCL information systems security policy

* monitor and review their security arrangements to ensure that policy, standards and procedures remain relevant and effective

* investigate breaches or attempted security breaches in information processing systems.

3. ACCOUNTABILITY

All POCL employees, agents and sub-contractors are accountable for safeguarding the business assets of POCL and its customers and clients, and maintaining the integrity and confidentiality of their information obtained in the course of POCL business.

The Counters Executive Committee is accountable for ensuring that adequate protection, in the form of security policy, standards and procedures, are in place.

POL00028135

The Policy is to maintain suitable records of all actions on POCL's information processing systems to ensure they can be attributed to individuals.

4. SECURITY ORGANISATION

4.1 Information Systems Security Infrastructure

Control and implementation of information systems security will be governed by a security management structure to approve policy, assign security roles, and coordinate the implementation of security measures in client services, internal systems and computing facilities across business units.

4.1.1 Management Direction

Management direction will be provided through a high level steering group, headed by the Director of , and representing all businesses and departments. The steering group will be accountable to the Counters Executive Committee for the *POCL Information Systems Security Policy*.

The steering group is responsible for:

1. Reviewing and approving the *POCL Information Systems Security Policy* and responsibilities

2. Recommending to the Counters Executive Committee major initiatives to enhance information systems security

3. Reviewing the effectiveness of information systems security policy, standards and procedures

4. Monitoring exposure to major threats to POCL's information systems assets

5. Approving specific methodologies and processes for information systems security (eg risk assessment, user authentication)

6. Liaising with the ISSU to ensure concurrence with ISSU policies.

4.1.2 Information Security Coordination

The initiation, control and implementation of information systems security will be the responsibility of system owners. The manager with responsibility for Information Systems Security (to be referred to as the

POL00028135

IS Security Manager) will play a supporting role to ensure the security practice is in accordance with the *Post Office Information Systems Security Code of Practice*.

The IS Security Manager will be accountable to the Steering Group and will be responsible for:

1. Implementing and supporting POCL-wide information systems security policy and initiatives

2. Implementing and maintaining security awareness programmes

3. Reviewing and monitoring security incidents in POCL's operations and business services

4. Agreeing and implementing security policy, standards and procedures

5. Monitoring and reviewing security arrangements to ensure that policy, standards and procedures remain relevant, effective and efficient

6. Agreeing and implementing specific roles and responsibilities for the protection of individual assets (both physical and information) and for carrying out specific security tasks across business units.

In particular, the IS Security Manager will ensure:

- the various assets and security processes associated with each individual system are identified and explicitly defined

- the managers responsible for each asset or security process are agreed and the responsibility documented

- authorisation levels are clearly defined and documented.

4.1.3 Security Incidents

All incidents affecting the security of information systems must be reported to line management and investigated by the appropriate authority. Managers will report security incidents to the IS Security Manager who will maintain records for periodic analysis. Where necessary, the IS Security Manager will inform the Post Office Investigation Department (POID).

Material breaches will be subject to disciplinary action.

POL00028135

4.1.4 Accountability for Assets

All major *information assets* must be accounted for and have nominated *owners* to maintain appropriate levels of protection.

Owners will be assigned for all *information* which is available for *shared* use. Rules for information ownership will be defined in the future *POCL IS Security Code of Practice.*

The owner will define who is authorised to access the information. Access shall be denied unless express authority has been granted. It will be the owner's responsibility to ensure appropriate controls are applied to the information which they own.

The information system owner is responsible for ensuring appropriate controls are applied in their systems to process information to prevent unauthorised access, modification or destruction of information assets.

Responsibility for implementing security measures may be delegated but the accountability must remain with the nominated owner of the asset.

4.1.5 Independent Audit of Information Security

Implementation of information security must be independently audited by security specialists with the appropriate skills and experience.

These security audits are to be carried out on a regular basis to provide assurance that POCL's practices properly reflect the policy, and the latter is feasible and effective.

The audit findings of security implementations in POCL's client services may be made available to specific clients if appropriate.

5. MANDATORY REQUIREMENTS

5.1 Key Controls

The following controls are **mandatory requirements** for information systems security.

These requirements apply to both POCL employees, agents and third parties with access to POCL's internal systems or business services.

POL00028135

5.1.1 Information Security Document

Each business and group in POCL is to implement and enforce the POCL Information Systems Security Policy by producing a security statement which addresses the following controls:

- security responsibilities
- security education and training
- reporting security incidents
- physical security
- virus control
- business continuity
- information classification
- information exchange.

5.1.2 Allocation of Security Responsibilities

Responsibilities for the protection of individual assets and for carrying out specific security processes must be explicitly defined.

5.1.3 Security Education and Training

Users should receive appropriate training in POCL's policies and procedures - including security and legislative requirements, and other business controls - as well as appropriate training in the correct use of IS facilities before access to IS services is granted.

5.1.4 Reporting Security Incidents

Incidents affecting security must be reported to the IS Security Manager for investigation and, if necessary, escalated to the Counters Executive Committee.

5.1.5 Physical Security Control

Resources used in information processing, such as buildings, offices, PCs and host computers, file servers, electronic storage media, electrical services, communications media and paper records, must be protected from unauthorised access, misuse, damage or theft.

5.1.6 Virus Control

Virus detection and prevention measures and appropriate user awareness procedures must be implemented in accordance with the *Post Office IS Security Code of Practice* on virus control.

POL00028135

5.1.7 Business Continuity

Each business unit must ensure that a managed process is in place for developing and maintaining a business continuity plan, to reduce the risks from deliberate or accidental threats to deny users access to vital services or information.

Plans are to be developed to enable internal operations and business services to be maintained following failure or damage of vital services, facilities or information.

5.1.8 Control of Proprietary Software

Proprietary software must only be used within the terms of the licence. Software must never be copied without the owner's consent.

Each business unit should keep an inventory of all proprietary software in use.

5.1.9 Safeguarding POCL Records

It is a legal requirement that important manual and electronic records must be retained for fixed periods. They must also be safeguarded from loss, destruction and falsification.

Guidelines for securing POCL records are given in appropriate *Post Office Procedures.*

It is a requirement that adequate precautions are to be taken against falsification of records and to discover any falsification that occurs.

5.1.10 Information Classification

Information owners will be responsible for classifying any information which they consider to be *sensitive*, ie which would expose POCL, clients or customers to serious consequences in the event of a security breach.

Guidelines for privacy and related marking, custody and reproduction of privacy material are given in the *Post Office Information Security Code.*

5.1.11 Compliance with Data Protection Legislation

Applications handling personal data on individuals must comply with data protection legislation and principles.

POL00028135

Compliance with data protection legislation is to be managed through the Group Data Protection Manager who provides guidance to managers, users and sub-contractors on individual responsibilities for protecting personal data and the procedures that should be followed.

It is the responsibility of the owner of the data to register the data with the Group Data Protection Manager and to ensure compliance with the data protection principles defined in the legislation.

5.1.12 Information Exchange Control

The exchange of information between POCL and its clients, between companies in the Group or with an external party, must take place in accordance with formal procedures which reflect legal requirements and the sensitivity of the information. This applies to both electronic and physical means of transferring information.

5.1.13 External Contractors and Suppliers

The use of external personnel must be subject to contractual obligations and to controls implemented by local management. Evidence may be required of the integrity of external contractors and of their internal security controls.

External personnel should not be allowed access to any classified information without prior written authority of the information owner and completion of a non-disclosure agreement.

Suppliers of goods and services for use in information processing must guarantee compliance with this Policy.

Where externally supplied goods or services are used to process critical information, evidence of the supplier's security procedures may be required.

5.1.14 Compliance with Security Policy

Systems must be independently reviewed to ensure compliance with POCL's security policies and standards. The reviews must be carried out on a regular basis.

Each business unit should conduct or sponsor regular reviews of the compliance of its systems with POCL's security policies, standards and other security requirements.

The Post Office Information Systems Security Code of Practice should be referred to for guidance when implementing the key controls.

POL00028135

Appendix 4-2

A Code of Practice for Post Office Systems Security

POL00028135

A Code of Practice For Post Office Information Systems Security

Status: Authorised
Version History: Version 1.5 (28/10/94)
Version 1.4 (20/9/94)
Version 1.3 (13/5/94)
Version 1.2 (21/2/94)
Authors: iT Risk Management Group

POL00028135

CONTENTS

POL00028135

POL00028135

INTRODUCTION

Purpose

The purpose of the Code of Practice is twofold:

- establishment of a baseline with which Post Office Businesses can implement, develop and monitor common and effective information security management practice and procedures.
- provision of a global reference standard for inter-business trading, sub-contracting and the procurement of all Information Systems (IS) services and products.

Focal Point

This Code of Practice is intended as a focal point for use throughout the Post Office by Managing Directors, Business Systems Directors and employees who are responsible for initiating, implementing and maintaining IS security within their respective organisation.

This publication has been produced by the iT Risk Management Group as the recommended Code of Practice for the management of Post Office Information Security.

The Code of Practice is based upon the Draft BSI Code of Practice for Information Security Management provisionally allocated BS7800.

POL00028135

INFORMATION SYSTEMS SECURITY MANAGEMENT

Introduction

Managing IS security requires the selection and implementation of appropriate security measures and a programme of continuous monitoring and control to ensure an acceptable level of security is maintained.

This section outlines the strategies each Business should aim to achieve.

Scope

The guidelines enable businesses to quickly assimilate the processes of IS security and ensures a baseline coverage across the Post Office. It provides an overview and model of the code of practice for IS directors, managers and users. The guide enables the reader to quickly appreciate the strategic role of IS security and its implementation.

Establishing a Baseline Level of Security

The majority of security controls documented are recommended as good standard practices for all situations and should provide an appropriate baseline level of security.

- Information Security Policy
- Allocation of Security Responsibilities
- Business Contingency Planning
- Virus Controls
- Personnel Information Security Awareness
- Security Incidents Reporting Procedures
- Data Protection Legislation
- Proprietary Software Control
- Computer Misuse
- Safeguarding Post Office Records

These controls are essential and provide the cornerstone for IS security. Their implementation is, therefore, primary in any security infrastructure.

POL00028135

INFORMATION SYSTEM SECURITY KEY CONTROLS

A number of controls in this Code of Practice are critical requirements for IS security. These controls, which are mandatory, apply equally across all Post Office Businesses and environments, forming the IS security policy for the Post Office:

Post Office IS Security Policy

Management should set a clear direction and demonstrate their support for IS security through the issue of a Post Office IS security policy, which must be made available to all Post Office employees responsible for IS security.

The Post Office Information Systems Security Policy provides general guidance on the allocation of security roles and responsibilities. However, these should be supplemented with a more detailed local interpretation for individual Businesses. Each Business should explicitly define responsibilities for individual assets and security processes (e.g. business continuity planning).

To avoid any misunderstanding about respective responsibilities, it is essential that the areas for which individual managers are responsible are clearly defined.

••••••

Management Direction

Management direction is provided by the Group Technical Policy Committee (GTPC) which ensures that there is clear management direction and visible senior management support for security initiatives.

The GTPC addresses the following items:

- Reviewing and approving Post Office IS security policy and responsibilities.
- Monitoring exposure to major threats to Post Office IS assets.
- Initiating work to enhance IS.
- Reviewing the effectiveness of IS security policy, standards and procedures.
- Approving specific methodologies and processes for IS security (e.g. risk assessment, classification system).

Information Security Co-ordination

A cross functional security group should be established within each Business to initiate and control the implementation of IS security.

The security group should address the following items:

- Implementing and supporting Post Office wide IS security policy and initiatives.
- Implementing and maintaining IS security awareness programmes.
- Reviewing and monitoring IS security incidents.
- Agreeing and implementing IS security policy, standards and procedures.
- Monitoring and reviewing IS security arrangements to ensure that policy, standards and procedures remain relevant.
- Agreeing and implementing specific roles and responsibilities for the protection of individual IS assets (both physical and information) and for carrying out specific security processes.

POL00028135

Independent review of IS security.

Implementation of IS security should be independently reviewed.

The Post Office Information Systems Security Policy sets out corporate responsibilities and policy for IS security. However, each Business should ensure that the practice of IS security is reviewed independently, through internal or external audit teams, to provide assurance that business practices properly reflect the policy and that the policy and controls are feasible and effective.

Risk Review

Business risks and IS security management controls should be regularly reviewed to address changing business requirements and priorities.

In overview, the assessment of risk takes into account the following factors:

- the nature of the business information and systems
- the business purpose for which the information is used
- the environment in which the system is used and operated
- the protection provided by the controls in place

A risk assessment should identify exceptional business security risks beyond those controlled through the measures prescribed by the baseline standard.

POL00028135

Security Responsibilities

Throughout the code of practice and other security guidelines, it is appropriate to suggest a model for the identification of generic responsibilities throughout the business. The model presented in Fig 1 provides a model specifically to indicate the depth and breadth of security administration and policy review at each elemental stage and to categorise four information system roles.

The following describe the key roles and responsibilities of employees with reference to the context of the ten key security controls applied to the PO business.
Every employee coming into contact with any information system whether automated or not, should adopt the minimum role identified as USER. All the essential key controls are allocated as a guideline through each identified role. Reference should be made to the key control chapters to the detail processes involved and required of the role.

As part of the educational and training requirement of the IS Security Policy, specific single sheet leaflets should be produced for each of the IS roles below and distributed to the relevant employees. The sections below only mention those added responsibilities considered the delegation of the overall Post Office IS security management policy.

Sponsor

A sponsor is any person who has the role to manager business resources, including information, strategically. Project sponsors should afford a policy based approach to prescribing IS security.

A sponsor should fundamentally act in the following manner with respect information security:

- Encourages
- Endorses
- Progresses

A sponsor should have the key business responsibility for the following key controls:

- Business Continuity Planning Process
- Compliance with Data Protection Legislation

POL00028135

Developer

A developer is any person who has the role to advise and construct the mechanisms for information access using appropriate information technologies. Developer should ensure a system wide approach to developing products which adhere to a secure and practical business practice.

A developer should fundamentally act in the following manner with respect information security:

- Builds
- Plans
- Resolves

A developer should have the key business responsibility for the following key controls:

- Information Security Education & Training
- Compliance with Data Protection Legislation

Manager

A manager is any person who the role to manager business resources, including information, tactically.
Their main task is to maintain and continue the secure environment

A manager should fundamentally act in the following manner with respect information security:

- Enforces
- Mediates
- Audits

A manager should have the key business responsibility for the following key controls:

- Virus Controls
- Control of Proprietary Copying
- Compliance with Data Protection Legislation

User

A user is any person who comes into contact with any form of business information, whether through the use of information technology, or not. End users must ensure any specific security practices are followed.

A user should fundamentally act in the following manner with respect information security:

- Assists
- Adheres
- Adopts

A user should have the key business responsibility for the following key controls:

- Reporting of Security Incidents
- Safeguarding of Company Records
- Compliance With Security Policy
- Control of Proprietary Copying

POL00028135

Business Contingency & Continuity Planning

Business contingency plans are required to plan for interruptions to business activities.

Business continuity plans are required to protect critical business processes from major failures or disasters.

There must be a business continuity planning process to develop and maintain appropriate recovery plans fro critical business processes and services. The objective of business continuity planning is to ensure that the Post Office's critical business activities are restored and maintained as quickly as possible following any major disaster or failure that affects essential services or facilities.

Business Contingency requirements should be predetermined, co-ordinated, fully up to date, test proven and regularly reviewed.

A contingency plan is an emergency fallback facility which provides an alternative, temporary means of continuing processing, in the event of any damage or failure of equipment.

Information resource and distribution managers should ensure that appropriate contingency arrangements are established for each IS service.

Contingency requirements for individual systems should be specified by the business application owner, based on a business continuity planning process. Service providers will need to co-ordinate contingency requirements for shared services, and draw up an appropriate contingency plan for each service.

Business continuity planning process

There must be a managed process in place for developing and maintaining business continuity plans within each Business and subsidiary of the Post Office.

Business continuity planning involves identifying and reducing the risks from deliberate or accidental threats to vital services. Plans are developed to enable business operations to be maintained following failure or damage of vital services or facilities.

The planning process should focus primarily on keeping critical business processes and services running (including staff and other non-computing requirements) rather than just focusing on the contingency arrangements for computer services.

Business continuity planning framework

A consistent framework of business continuity plans should be maintained.

A single framework of corporate plans should be maintained to ensure that all levels of plan are consistent, and to identify priorities for testing and maintenance.

Each business continuity plan should need to specify clearly the conditions for activating the plan. New plans need to be consistent with established emergency procedures (e.g. evacuation plans) and existing contingency arrangements for computer services, telecommunications and accommodation.

Different levels of plan are required, because each level should have a different focus and may involve different recovery teams.

The model business continuity plan has four main components:

POL00028135

- Emergency procedures - which describe the immediate action to be taken following a major incident which jeopardises business operations or human life.

- Contingency procedures - which describe the action to be taken to move essential business activities or support services to alternative temporary locations.

- Recovery procedures - which describe the action to be taken to return to normal full business operations, usually at the original site.

- Test schedule - which specifies how and when the plan should be tested.

Each level of plan, and each individual plan, should have a specific custodian. Emergency procedures, manual contingency plans, and recovery plans, are the responsibility of the appropriate business process owner. Contingency arrangements for alternative technical services, such as computers and communications, are the responsibility of the service provider.

Business Impact Assessments

Business Impact Assessments should be performed prior to the creation or development of any business continuity planning, but the information obtained from them should also be used to ensure that the degree of risk reduction, acceptance and transfer are appropriate for the system(s) under review.

Business Impact Assessments identify the individual components required for the performance of specific business operations and establish the value and criticality of assets and data used within each function and for the overall processes.

A Business Impact Assessment should be performed, with the aid of specialist advice, prior to and in conjunction with, or after Risk Assessment. However, a joint assessment should always be performed in cases of new installations.

Testing business continuity plans

Business continuity plans should be tested.

Many plans fail when tested - often because of incorrect assumptions, oversights or changes in equipment or personnel. The effectiveness of a business continuity plan cannot be determined without regular testing. Such test also ensure that the plan is fresh in the minds of all members of the recovery team, and other relevant staff.

A test schedule for the business continuity plan should be drawn up. The schedule should indicate how and when each element of the plan should be tested.

A phased approach to testing is recommended, based on frequent tests of individual components of the plan. This ensures that the plan is kept alive and up-to-date throughout the year. It also reduces the dependency on (less frequent) all-out tests of the full plan.

Updating business continuity plans

Business continuity plans should be updated regularly.

Business continuity plans quickly become out of date because of changes in business or organisation. Regular updating is essential to protect the investment in developing the initial plan, otherwise the effectiveness of the plan should be degraded.

POL00028135

Personnel Information Security Awareness

Awareness programmes should be developed to maintain a consistently high understanding of the need for security. A positive attitude should be engendered throughout the organisation. There must be an understanding of the need for the identification and acceptance of common purposes within each level.

Users must be given adequate IS security and technical training.

Users should receive appropriate training in IS security policies and procedures, including security requirements and other Business controls, as well as training in the correct use of IS facilities before access to IS services is granted.

The authority for and scope of their access rights, including any restrictions imposed, must be formally written.

These measures are necessary to ensure that security procedures are correctly followed, and to minimise possible security risks to the confidentiality, integrity and availability of data and services through user error.

This policy should be applied to both Post Office employees and third party users.

Recruitment Security

Security should be addressed at the recruitment stage and included in job descriptions and contracts.

Job descriptions should define security roles and responsibilities.

Applications for employment should be screened if the job involves access to Post Office IS facilities handling sensitive information.

Staff with access to classified or sensitive information should be required to sign a confidentiality undertaking.

POL00028135

Security Incidents Reporting Procedures

Security incidents must be reported using a defined procedure in a timely fashion.

Procedures should be established through which different types of security incident; breach, threat, malfunction and weakness - any of which may result in business impact - are reported to the correct focal point as soon as possible. All employees and other persons working in IS environments must be made aware of these procedures and be required to act upon all observed and suspected occurrences.

The occurrence, or suspected occurrence, of any event which has security implications must be brought to the attention of management at the earliest opportunity.

A security incident is any event that has, or could have, resulted in loss of or damage to Business assets, or an action that is in breach of Business security policy or procedures.

All such persons should be informed that they should not attempt to prove a suspected weakness under any circumstances as their actions could be interpreted as a potential misuse of the system.

POL00028135

Virus Detection and Control

Virus prevention, detection measures and appropriate user awareness procedures must be implemented.

The basis of protection against viruses should be based upon staff awareness, appropriate system access controls and the following specific guidelines:

- Users should be reminded that prevention is better than cure.
- Staff, subcontractors and agents of the Post Office must be required to comply with the Post Office Software Policy
- approved anti-virus software should be used
- software and data content of systems supporting critical business processes should be regularly reviewed. The presence of any spurious files or unauthorised amendments should be formally investigated
- personal software, free or unsolicited software (including games) must never be used
- all diskettes must be checked for viruses before use. Management procedures and responsibilities must be established for the reporting of and recovering from virus attacks
- procedures of actions to be taken in the event of a virus attack being discovered should be developed, documented, known by staff and available for use
- appropriate recovery arrangements should be established for virus attacks, including all necessary data and software back-up facilities.

These measures are especially important for network file servers supporting a number of workstations.

Protection from Malicious Software

Precautions are required to prevent and detect the introduction of malicious software.

Information resource software is vulnerable to unauthorised modification. A range of malicious techniques have been developed to exploit this vulnerability, including 'computer viruses', 'network worms', 'Trojan horses' and 'logic bombs'.

Managers of IS facilities should be alert to the dangers of malicious software and should consider the need for special measures to prevent and detect the introduction of malicious software. In particular, it is essential that precautions are taken to prevent and detect computer viruses on personal computers.

POL00028135

Proprietary Software Control

Software Copyright

By virtue of the Copyright, Designs and Patents Act 1988 a computer program is classed as a 'literary work' and is thus afforded the protection of the law of Copyright.

Copyright prohibits the unauthorised copying of copyright work, irrespective of the medium on which it is held. Therefore, if the same software is, (contrary to the terms of licence), installed onto more than one processor, there will be an infringement of copyright.

It is the responsibility of each Post Office Business to ensure that its employees do not infringe the rights of the owner of the copyright software.

Each Business should:

- comply with the Post Office Computer Software Policy
- conduct software audits on a regular basis
- establish and maintain a software purchasing and distribution procedure
- register all software as an asset
- implement and maintain a software policy
- implement and maintain a staff training programme on the legal use of software

Resilience

The increasing dependency on computer systems for business and operational solutions makes it essential that the software deployed on systems can be restored if circumstances demand it.

All system and application software should be backed up in compliance with the system recovery guidelines.

All Systems and application software should have a nominated "owner" which shall be a named person or group.

POL00028135

Data Protection Legislation

The handling of personal data must comply with the data protection legislation and principles.

Unless the owners consent is given, copyright material must not be copied.

Post Office IS facilities must only be used for authorised business purposes.

Post Office Records must be safeguarded from falsification, loss and destruction.

There are a number of UK legislation's and Post Office regulations which affect the way we must handle and secure the Business data and information.

This section contains the relevant legislation's and regulations which must be adhered to when handling and processing business data and information.

Legal Compliance

Each Business should take the necessary precautions to avoid risking a breach of the Copyright, Designs and Patents Act 1988.

The application of approved "off the shelf" software MUST comply with the conditions of the Licence from the issuing authority. Adequate notice should be posted to warn personnel against the contravention of the conditions.

Penalties for breach of the Copyright, Designs and Patents Act 1988 are particularly severe for offences concerning software.

Each Business of the Post Office should establish and maintain procedures to ensure compliance with the relevant UK Legislation and Post Office regulations.

All line managers should ensure that employees are aware of relevant UK legislation and Post Office regulations and their responsibility to comply. Additionally, line managers should ensure that staff are aware of the disciplinary consequences if legislation or Post Office regulations are breached.

Breaches of Legislation

Any breach of legislation could result in a criminal prosecution being brought against Post Office employees. Employees who infringe legislation may be guilty of a serious offence under the Discipline Code and may be dismissed as a result.

POL00028135

Computer Misuse

Under the Computer Misuse Act (1990) it is an offence to:

- access computer material without proper authority
- access computer material with intent to commit further offences
- modify computer materials without proper authority

whereby it is a criminal offence to access computerised data knowingly and without lawful authority. As a result it is a Post Office requirement that each Business identifies data and information which require particular protection, and that they effectively manage authorisation of access.

Failure to do so, or by using ineffective or non-existent security controls, may compromise Post Office Businesses in the ability to prosecute under this Act.

POL00028135

Safeguarding Post Office Records

Copyright, Designs and Patents Act 1988

This Act includes restrictions on the copying of documentation and software without the authorisation of the originator or copyright holder. Copying of copyright/classified material is restricted in the same way as any other copyrighted items.

whereby the copying of a software product without the authority of the copyright owner is an offence under this Act which can result in civil and criminal action against the Business and the individual involved. The individual is liable to a fine or a term of imprisonment or both. The Business may face a civil action resulting in an unlimited amount of damages awarded.

As a result, it is a Post Office requirement that each Business applies effective measures to ensure compliance with this Act.

More information can be sought from the Secretary's office, the Legislation section. Postline 5400-8049

Data Protection Act 1984

All individuals under the terms of the Data Protection Act, are personally liable for automatically processed personal data that they hold, use and/or disclose. This encompasses the need to protect sensitive and confidential data and information by adherence to IS security guidelines and the Post Office Information Security Code of Practice.

To comply with this Act all Post Office applications which involve the automatic processing of personal data must be registered with The Office Data Protection Manager ensuring that the registrations are put forward to the Registrar.

Data Subject Access Rights must be granted in accordance with the Act.

Additionally, each Business must apply appropriate controls and procedures to ensure employees comply with the eight principles of the Act.

The DPM can provide advice and guidance on all aspects of the implementation of the Act. He may be contacted at Concept 2000, Farnborough, on Postline 5401-8034.

Official Secrets Act

All employees are bound by The Official Secrets Acts of 1911 and 1920 and on recruitment (including contractors) they must sign a Declaration of their obligations under relevant Acts. A further declaration (Form P301) must be signed when an individual ceases employment with The Post Office to indicate his/her acceptance of continuing obligations. Employees are entitled to copies of Forms P13 and P301.

The Act prohibits unauthorised disclosure of all information gained while in Post Office employment, which includes material with classification marking.

Copies of the relevant forms can be obtained from local Personnel sections.

Post Office and Telegraph Acts

POL00028135

Under the provisions of various Post Office and Telegraph Acts an employee must not allow, or cause information (in any form) to reach someone not authorised to receive it. Classification assists in identifying the need for restricted handling of certain types of data and information.

••••••••

The Companies Act 1985

Adequate precautions should be taken within each Business to ensure against the falsification of Post Office owned records and procedures put into place to enable discovery of any falsification that takes place.

The Post Office Information Security Code

This Code replaces Postal Instructions in the series L1F0011 - L1F0025 which are now obsolete. The Code is designed to inform employees of the minimum guidelines of security to be achieved relating to the safeguarding of Post Office business information as well as providing advice and guidance on the subject.

POL00028135

IS SECURITY INFRASTRUCTURE

This code of practice recognises that some controls are not applicable to every IT environment. In the following chapters physical and environmental aspects of control are detailed, so that the key security roles and responsibilities can identify the areas of business upon which Information Security can be applied.

A common model of the IT architecture to which information security should be applied is described.

The Security Process Model

The following are identified as the basic four elements in the security infrastructure. Each of these elements will be addressed separately. Refer to Fig. 2.

Information Resources

Information Resources are defined as those elements of the corporate infrastructure that offer shared processing resources as well as shared information repositories containing certain levels of corporate information.

Information Distribution

Information Distribution is defined as that part of the infrastructure that handles the intercommunication between applications as well the transmission of information from and to the information resources. The administration of access to all parts of the system is controlled through this system.

Work Groups

Work groups are defined as local resources enabling users to utilise local processing resources through workstations or personal and single user applications.

Users

There are specific security processes relevant to users identified in this category relevant to the temporary assimilation of data.

The IS Distributed Data/Processing Model

The above elements are combined to institute the distributed data/processing model as represented in Fig.3.

The model can furnish various configurations i.e. client/server, host based, distributed processing as well as provide a baseline for all security issues across the businesses no matter what level of application access, process or data usage is made.

The model describes and represents the naturally distributed architectures in use by the Post Office businesses: information resources and work groups can be placed anywhere around the information distribution system.

POL00028135

The IS Network & System Models

Information Systems can be represented by the combination of the system model (as the basis of a typical application) and the ISO OSI network model. By representing each element of an information system in this way, all the security aspects of the delivery and provision of information processing and storage can be addressed.

Systems consist of primarily hardware, operating systems, databases (as RDBMS's) and front end applications and tools. This representation is a generically manageable one because no regard to the specific problems of interconnectivity and portability need be addressed.

POL00028135

GENERAL IS SECURITY GUIDELINES

Security should be built into all IS systems

Security countermeasures are generally more effective and substantially cheaper when incorporated in the specification and design of application systems. All security requirements (including the need for contingency arrangements) should be identified, justified, agreed and documented at the requirements phase of the project as part of the overall business case.

This should also be applied to the processing of business critical and sensitive information through the use of word processors, databases and spreadsheets.

Security Requirements Analysis and Specification

An analysis of security requirements should be carried out at the requirements analysis stage of each development project and before the use of any new software products.

Business requirements statements, compiled through consideration of the infrastructure, for both new systems and enhancements to existing systems should include requirements for security controls.

Although such specifications are usually directed at the automated controls to be included in the system, the possible need for supporting manual controls should not be overlooked.

These considerations should also be applied when evaluating software packages for business applications.

Security requirements and controls should be based on both the business value of the IS assets involved, and the potential business impact which could be expected through the absence of security mechanisms or through failure of countermeasures.

Two aspects which should be borne in mind when analysing the requirements for security are:

- consideration of the need to safeguard the confidentiality, integrity and availability of IS assets
- identification of opportunities to use different types of controls to prevent, detect and recover from major failures or incidents.

In particular, the analysis should consider any need to:

- control access to IS and services, including any requirements to segregate facilities and duties
- produce audit trails of important events for both routine controls and special investigation purposes, including evidence in contractual or other negotiations
- verify and protect the integrity of vital data at all or selected stages of processing
- protect confidential data from unauthorised disclosure, including the possible requirement for the use of data encryption in special circumstances
- comply with regulatory, legislative and contractual requirements
- take back-up copies of essential business data

POL00028135

- recover from failures, especially for systems with high availability requirements
- protect the system against unauthorised amendment or modification
- enable the system to be operated and used securely by suitably trained non-specialist employees
- where appropriate, enable the system to satisfy the requirements of the external auditors, such as through the use of embedded software routines for sampling, and independent software to repeat critical calculations.

Security controls should be explicitly defined in all relevant documentation to safeguard against inadvertent compromise by IS support staff and users who are not aware of them

Security in Application Systems

Loss, modification and misuse of user data in application systems must be prevented.

The design and operation of IS systems should attune to generally accepted industry guidelines of good security practice which meet all relevant contractual and legislative requirements. However, additional countermeasures may be required for valuable or critical business assets and systems which process (or interface with others which process) sensitive data. Such measures should be determined on the basis of specialist advice, taking account of identified security threats and their possible business impact.

Security of Application System Files

IS projects and support activities must be carried out in a secure manner.

Access to system files should be controlled.

Maintaining the integrity of applications systems is the responsibility of the user function or development group to whom the application system or software belongs.

Systems Development

All Post Office IS systems should be developed in accordance with formal guidelines and procedures. The approval of the user and IS manager must be obtained before new systems are accepted. The respective internal and external audit organisation should be informed of all new systems as part of the IS planning and concurrence process.

Data Exchange

The exchange of data and software within the Post Office should be controlled so that loss, modification and misuse of data is avoided.

Exchanges of business data and software within the Post Office, and between the Post Office and other organisations, should be carried out on the basis of formal agreements and in accordance with legislative restrictions. Procedures and guidelines to protect media in transit should be formally established through the performance of risk assessment and the requirement for controls should not be overlooked when considering the security and business implications associated with EDI and electronic mail exchanges.

POL00028135

Security of Work Group Systems

Work Group systems are information resource based systems designed for office tasks. It may involve the use of electronic filing systems, WP systems, databases, computer graphic systems, Email and teleconferencing systems.

Electronic office systems provide the means for efficient, faster and more widespread dissemination of business information. However, security and business implications must be considered at system development stage to ensure control of associated business and security risks, and to enable appropriate policies, procedures and guidelines to be made available to users.

POL00028135

Information Resource & Distribution Management

Responsibilities and procedures for the management and operation of all information resources and distribution through networks must be established.

Management and operational responsibilities for information resource and network facilities must be clearly defined and supported by appropriate operating instructions and incident response procedures. The principle of segregation of duties should be applied, where appropriate, to reduce the risk of negligence and deliberate system misuse.

Procedures for the operation of all information resource systems should be fully documented and made available to staff.

Operational Processes

The following operational processes should be considered:

Operating Procedures Documentation
Clear operating procedures should be prepared for all operational information resource systems to ensure their correct and secure operation. Documented procedures should also be required for system development, maintenance and test work, especially if this requires the support or attention of other organisational functions such as information resource operations.

Documented procedures should also be prepared for system housekeeping activities associated with information resource and distribution management, such as computer start-up and close-down procedures, data backup, equipment maintenance, computer room management and safety.

Operating procedures should be treated as formal documents and kept secure. Any changes to the document must be controlled and approved by authorised management.

Incident Management Procedures

Responsibilities and procedures for incident management should be established.

Segregation of Duties

For sensitive data or activities the risk of negligence or deliberate system misuse is reduced through the segregation of duties.

Consideration should be given to separating the management and execution of certain duties (or areas of responsibility) in order to reduce opportunities for unauthorised modification or misuse of data and services. This control is particularly important for information resources supporting financial applications.

Small divisions may find this control difficult to achieve, but the principle should be applied as far as it is possible and practicable.

Separation of Development and Operational Facilities

Development and testing facilities should be isolated from operational systems.

POL00028135

Development and testing activities may cause unintended changes to software and data which is sharing the same computing environment. Segregation of development and operational facilities is desirable to reduce the risk of accidental changes or unauthorised access to operational software and business data.

Operational Change Control

Changes to IS facilities and systems should be controlled.

Common causes of system and security failures can be attributed to inadequate control of changes to IS facilities and systems. Formal management responsibilities and procedures are necessary to ensure satisfactory control of all changes to equipment, software or procedures.

Planning Processes

The following planning processes should be considered:

System Planning and Acceptance

Advance planning and preparation is required to ensure the availability of adequate capacity and resources.

Future capacity projection requirements should be made to reduce the risk of system overload. The operational requirements of new systems should be established, documented and tested prior to their acceptance. Fallback requirements for services supporting multiple applications should be co-ordinated and regularly reviewed.

Capacity Planning and System Acceptance

The criteria for new systems should be established and suitable tests conducted prior to them being commissioned.

Information resource managers should ensure that the requirements and criteria for acceptance of new information resource systems are clearly defined and agreed, documented and tested.

The operations function should be consulted throughout all stages in the development process for major new developments, so as to ensure proper operational efficiency of the proposed system design.

Appropriate tests should be carried out to confirm that all aspects of the acceptance criteria are fully satisfied.

POL00028135

Information distribution management

Special attention should be given to the security management of networks, particularly if they span organisational or corporate boundaries. A risk assessment should be carried out to determine the level of security required to protect the confidentiality integrity and availability of data passing over networks.

The managers of Information Distribution are responsible for the documentation of the network. This includes a full asset register of all equipment, fully documented connection diagrams and, where possible, cabling diagrams. Two up-to-date copies are to be kept, one within the information distribution management group and another at a secure off-site location.

Where transmission equipment relies upon data programmed into a piece of hardware, information distribution management should ensure that backup copies of the configuration data within these items are taken and are kept at a secure off-site location.

Information Resource Management

The following guidelines should be considered with respect to information resource management:

- administrators must keep a diary of changes made to the system. If this is kept as a file on the system hard copies should be printed and stored each time the file is updated.
- access to resources MUST be authorised by the appropriate manager using access request forms.
- access privileges must be cancelled, changed or reviewed upon user job change, transfer or termination of employment

Information Distribution Management

The following guidelines should be considered with respect to information distribution management:

- a process should exist for security issues to be escalated. The issues to be escalated should be locally defined.
- the system should be monitored for violations, attempts at unauthorised access and to ensure optimum utilisation.
- a process should exist for the escalation of operational incidents, misuse-use or other breaches of security guidelines.
- access privileges must be cancelled, changed or reviewed upon user job change, transfer or termination of employment

Work Group Management

The following guidelines should be considered with respect to work group management:

- a process should exist for security issues to be escalated. The issues to be escalated should be locally defined.
- network users should be provided with instructions regarding security guidelines.

POL00028135

- all network hardware should be afforded physical security in line with the applications security guidelines.

- an up-to-date user profile record should be maintained.

- access privileges must be cancelled, changed or reviewed upon user job change, transfer or termination of employment

Network Security Controls

The security of computer networks requires a range of controls. This covers all types of networks i.e. communication networks, Local and Wide area networks and distributed computing systems.

Information distribution managers must ensure that appropriate controls are established to protect data in networks and connected services from unauthorised access. In particular, the following items should be addressed:

- where possible, operational responsibility for networks should be separated from information resource operations

With respect work group management:

- responsibilities and procedures should be established for the management of remote equipment, including that in user areas

With respect to information distribution management:

- special controls, such as data encryption, message authentication or remote access controls should be considered to safeguard the confidentiality, integrity and availability of data passing over the networks and the connected systems

- communications network equipment of critical IS are to be kept in a secure environment.

overall close co-ordination should be applied to information resource and distribution management activities so as to ensure that security measures are consistently applied across the IS infrastructure and service to the business is optimised

Communications Information distribution management

The level of detail and formality of procedures required to manage and operate information resource and network facilities should vary considerably according to the circumstances and the nature and sensitivity of the business applications. For example mainframe computers and specialist operations functions require a more extensive set of procedures and controls than a department using office technology. But in principle the same security processes should be applied with appropriate interpretation.

POL00028135

Media Security and Handling

Computer media should be physically protected and appropriately controlled.

Operating procedures should be established to protect computer media and system documentation from damage, theft and unauthorised access.

Management of Removable Computer Media

Control over the movement of removable computer media should be established and maintained.

All procedures and authorisation levels should be clearly documented.

Data Handling

Procedures for handling confidential and sensitive data should be established in accordance with the Post Office Information Security Code.

Confidential and sensitive data must be protected from unauthorised disclosure and misuse.

Procedures should be drawn up for the secure handling of all sensitive input/output media, including; documents, fax, telexes, tapes, disks, reports and other sensitive items such as blank cheques, invoices etc.

Disposal of Media

Computer media which is no longer required should be disposed of under appropriate secure conditions.

Confidential and sensitive Post Office information may be disclosed to unauthorised persons through the careless disposal of computer media. In order to minimise the risk of this, clear procedures for the secure disposal of media should be established at each site.

Security of Media in Transit

Whilst in transit computer media can be vulnerable to loss, damage, compromise, corruption and misuse.

System Access Management

Unauthorised access to Post Office information resource systems must be prevented.

Access to Post Office information resource systems, services and data must be controlled on a need to know basis whilst satisfying Business requirements in accordance with corporate and business policies for information dissemination and entitlement. In addition, all contractual and legal requirements to protect such access must be adhered to.

POL00028135

Information Access Policy

Business requirements for access control must be defined and documented.

In order to implement and maintain an effective level of control of access to IS services and data service providers must be given a clear statement of the business requirements for system access.

Each business 'application owner' should establish a clearly defined access policy statement, which specifies the access rights of each user, or user group. Such policy should take account of the following:

- the security requirements of individual applications
- business and departmental directives for information dissemination and entitlement
- contractual and legal requirements to protect access to data, information and services.

It is recommended that the minimal requirement for control of access to computer services (including standalone PCs and file servers is an effective computer generated password system which can not be bypassed. Where possible the system should automatically require the user to change the password on a regular basis.

A defined access policy should govern users access to data and application system functions. This policy should be based on individual business application requirements, and be consistent with corporate and/or business information access policy.

Application of the following controls should assist in supporting access policy requirements:

- where access controls are installed which allow user access to be restricted to particular data and applications they should be activated and used

- user documentation should be tailored to assist in restricting user knowledge of data and application system functions to areas to which they are authorised access. However, this may not always be practical where staff are trained in several functions of a system to allow for coverage of leave and vacancies

- the access rights of authorised staff should be controlled in terms of their read, write, delete etc. command capabilities

- where the operation of a system provides outputs, such as printing, this output should contain only data relevant to the use of that output. Such outputs should be periodically reviewed to ensure that redundant data is removed.

POL00028135

Monitoring System Access and Use

Unauthorised computer access and activities must have monitoring and detection mechanisms.

Service providers and system 'owners' should establish a process for monitoring system access and use to establish the effectiveness of mechanisms which are designed to ensure compliance with the information resource access policy.

Security of Network Services

Prior to using a network service the associated risks should be established.

Businesses using network services should ensure that their network provider gives a clear description of the security attributes of all services used, and should establish the security implications for the confidentiality, integrity and availability of business applications.

- It may be necessary to divide large networks into separate domains.
- Computer networks within the Post Office are increasingly being extended beyond traditional organisational and corporate boundaries, with Business partnerships requiring the interconnection and sharing of computer and network facilities.
- Such extensions increase the risk of unauthorised access to existing computer systems that use the network, particularly where protection from other network users is required because of their sensitivity or criticality.
- In such circumstances, controls should be introduced within the network to segregate groups of users and computers.
- Security control of large networks should be established by dividing them into separate logical domains, each protected by a defined security perimeter and a network gateway. Access between domains can then be controlled by the secure gateways, incorporating appropriate routing and connection-capability controls.
- The criteria network domain segregation should be based on business access control policy and requirements, whilst taking account of the relative cost and performance impact of incorporating suitable network routing or gateway technology.
- An assessment of risk and business impact may be required to determine the correct criteria.

POL00028135

Project Development Security Requirements

Introduction.

Drawing up a Security Requirement at the development stage of any IS project is an essential part of the Risk Management process by ensuring that it is implemented as a planning activity and a prerequisite to establishing the true cost of developing and producing a system. In the long run it is likely to lead to cost savings.

Each Post Office Business must ensure that procedures are in place to enable security requirements to be addressed at the development stage of all IS projects.

Physical & Environmental Security

Physical security is an essential ingredient for the protection of assets and information in all areas of computerisation. The application of appropriate physical security facilities provides the means by which identified levels of risk exposure are reduced to an acceptable level and creates the mechanism to enable management to maintain control of the environments once secured.

The primary objectives of applied physical security measures are to:

- reduce the likelihood of a threat impacting the computer systems or business operations
- detect and indicate immediately in the event of a threat penetrating the applied protection
- directly counter some types of threat in the event of the protection being penetrated.

Physical security requirements should vary throughout the Post Office depending on the local circumstances, the scale and organisation of IS services provided as well as the sensitivity and criticality of the data and business activities. A data-centre should require a much higher degree of security protection for its IS facilities than office accommodation. However, the concepts of secure access controlled areas, controlled perimeters, and general security mechanisms are universally applicable when applied with appropriate interpretation.

Businesses with expanding IS operations should ensure that physical security measures can be expanded to serve the needs of likely future requirements, especially as such measures may be costly and difficult to apply retrospectively.

Secure Areas

Unauthorised access to data, or damage to and adverse interference with IS assets and services must be prevented.

IS facilities supporting classified, or critical or sensitive business activities should be housed in secure areas.

IS facilities should be protected by a defined security perimeter, incorporating a balance of protection barriers, access control facilities and detection mechanisms. A clear desk policy should be put into place to reduce the risk of unauthorised access to or damage to paper and media.

POL00028135

Asset Registration & Control

All IS assets should be accounted for and have a nominated 'owner'.

'Owners' should be identified and assigned responsibility for the maintenance of appropriate security measures. Responsibility for implementing security measures may be delegated - though accountability should remain with the nominated owner of the asset.

Inventory of Assets

Registries should be maintained of all major information and IS assets.

A registry should be maintained of the major assets associated with each IS. Each asset should be clearly identified and its "ownership" and security classification agreed and documented.

Assets associated with IS include the following:

- Information assets - databases and data files, system documentation, user manuals, training materials, operational or support procedures, contingency and disaster recovery plans, backup and recovery arrangements.
- Software assets - system software, application software, development tools and utilities.
- Physical assets - computer and communications equipment, magnetic media (tapes and disks), specialist technical equipment (power supplies, air conditioning units), furniture, accommodation.
- Staff Assets - skilled personnel required to operate, develop, maintain and use the IS.

Information Privacy Markings

Security and/or privacy markings can be used to indicate the need and priorities for security protection.

Security and privacy markings are used by the Post Office to identify information which requires more than normal protection from unauthorised access. The markings to be used depend on the estimated degree of damage that disclosure to unauthorised sources may cause to Her Majesty's Government, or the Post Office in terms of its commercial dealings, standing in the community or in its relationships generally. Although the application of security and privacy markings generally rests with the originator of the information Risk Assessments can be carried out to determine the required marking.

Security and Privacy Marking Guidelines

The protection applied to classified, sensitive and personal information should be consistent with business and legislative requirements.

Security and privacy measures for business information should take account of the needs for sharing or restricting information, complying with legislation (e.g. The Data Protection Act), and take account of the business impacts associated with unauthorised access or damage to the information. In particular, consideration should be given to the following requirements:

POL00028135

- Confidentiality - business need to share and/or legislative requirements to restrict access to information with regard to confidentiality, and the controls required to restrict access to the information.
- Integrity - the business need to control modifications to information, and the controls required to protect the accuracy and completeness of the information.
- Availability - the need to have information available when required by the business and the controls required to achieve this.

Security of Third Party Access.

Secure access to the Post Office IS facilities by third parties must be maintained.

The risks associated with access to Post Office IS facilities by third parties should be assessed and appropriate security controls implemented.

Contracts with third parties involving access to Post Office IS facilities should specify security conditions.

Access to Post Office IS facilities by third party users might present a security risk. Where there is a business need for such access, a risk analysis should be carried out to determine the security implications and control requirements. The controls should be agreed in a contract with the third party.

Identification of risks from third party connections

IS facilities may be put at risk by access from third party locations with inadequate security management. The risk analysis should take into account the type of access required, the value of information, the security measures employed by the third party and the implications of the access for the security of the IS infrastructure.

Access to IS facilities by third parties should not be provided until the appropriate countermeasures have been implemented and a contract has been signed defining terms of connection.

POL00028135

GLOSSARY OF TERMS

Network - Those elements which make up the information distribution infrastructure ie. network communication servers, concentrators, bridges, routers, LAN cabling, LAN interface and network operating systems.

Computer - Those elements which make up the information resource infrastructure ie. database servers, Email servers, peripherals, multiple-media environments and work-stations.

LAN - Local Area Network. A generic term for the transport mechanism for a local (e.g. site or building) network. The thing that makes current LANs special is their intimacy with the connected machines; effectively the LAN acts as an extension to the internal bus of the attached system, and allows a single system to be built from physical dispersed components.

POL00028135

Appendix 4-3

The "Distribution" interface

POL00028135

DISTRIBUTION

This appendix describes the requirements for the interface with the POCL distribution function. The systems required to support the distribution function are currently being reviewed and it is likely that a number of interfaces will be required.

1. OVERALL PRINCIPLES

Distribution systems will cover:

- cash
- value stock
- transaction stock.

Value stock is defined as all value and security items.

All cash remittances and orders are to be broken down by denomination and, if possible, series. OverNight Cash Holding (ONCH) data is to be split note and coin. Receipts and deposits are to be summarised to provide end-of-day totals for cash and cheques.

Value stock data is to be broken down by item code and sub-set (e.g. special issue stamps).

2. INFORMATION AREAS

2.1 Stock Holdings and Flows for Inventory Management Purposes:

ONCH - end-of-day cash holdings daily by note and coin.

Payments and receipts broken down by cash and cheques with min/max. holdings of cash during the day - daily.

Value stock holdings by item and sub-code daily.

Transaction stock - weekly summary of stock on hand (possibly just a sample of items).

Possible requirement: enquiry on cash holdings during the day.

POL00028135

2.2 Order Information - for Automated Order Processing

These need to be sent via an interface to the distribution centre system at the time of input for:

- cash orders
- value stock orders.

Transaction stock would probably be acceptable overnight, although 'as input' might be preferred. This interface is most likely to be to Swindon or another separate system.

2.3 Remittances and Returns.

This data is needed for accounting, reconciliation, monitoring, to avoid data re-input at cash centres, and for service monitoring.

This should cover contents by denomination (and series if possible) for cash; by item and sub-set for value stock. Exact times and dates should be recorded and there should be a quality check measure.

The information is required to be sent when the remittance is received or the return is passed to the carrier for both cash and value stock remittances. This will allow the distribution centre system to ensure the integrity of the end-to-end process and will avoid losses and the need for re-input of data, and provide a more secure audit trail. A facility could also be included to relate remittances to orders in the outlet and eventually to accept information from the distribution centre system on remittances to outlets for audit purposes and avoiding data re-input in the outlet.

[Transaction stock remittance requirements are not fully defined at this stage.]

2.4 Transfer of Data

A direct and immediate interface to the distribution system(s) will be required for InPay and OutPay transactions performed within cash centres. This interface will need to transfer transaction data by denomination, series and state/fitness status (e.g. ATM fit).

There may also be further specific requirements for data on other transactions performed within cash centres to be transferred to the distribution system(s) (e.g. Postal MVL applications).

2.5 Remittance Marking

There will be a requirement to consider the possibility of marking remittances in some machine readable form, possibly bar-coding, in order to make these interfaces easier to operate.

POL00028135

3. Timescales

Overnight Cash Holdings	Day 1 of roll-out (the system to which this interfaces will go live in 1995).
Remainder	From 1996/1997 depending on the outcome of the current review. (The main POCL system is going live in Q1/Q2 1996 and work on subsequent phase requirements will start in 1995 for delivery in 1996/7.)

POL00028135

Appendix 4-4

The Post Office (Group) Information Technology Architecture and Policy

POL00028135

THE POST OFFICE

INFORMATION TECHNOLOGY

ARCHITECTURE

AND POLICY

version 1.00 25/10/94

GROUP IT DIRECTORATE
Manor Offices
Old Road
CHESTERFIELD
Derbyshire
S40 3QT

POL00028135

POL00028135

1: INTRODUCTION

1. INTRODUCTION

IT in The Post Office

The Post Office increasingly relies on information technology (IT). As the cost effectiveness of IT improves, and as new means to capture data or present information becomes available, the technology becomes more pervasive. More and more computer systems are being deployed throughout the organisation.

As more application systems are deployed, they address a growing proportion of business activity. In so doing, these systems are important not only in their own right, but also in terms of their interfaces to one another. One provides data to another, two systems may share common data.

Moreover, more and more personal computers and local area networks are now being deployed as local initiatives, but will ultimately require access to systems at a regional and national level.

Unfortunately, getting computers to communicate with one another effectively is often far from straightforward. Managers often wonder

- why is it difficult to consolidate staff costs?
- why is it complex to connect our purchasing systems to our suppliers?
- why do people need to re-key data from one system into another?

The answer to these questions is usually that, in the past, systems have sometimes been developed on a project-specific basis without a common technical or application framework to support interaction between systems and departments.

Part of the resolution to the problem lies in the design of the individual computer applications and, particularly, the steps taken to ensure consistency of data. Equally important is the need to establish a planned set of computing and communication facilities that can provide the flexibility and connectivity required. This is known as the Technical Infrastructure.

How a Technical Infrastructure Works.

Instead of separate "islands of information", it is becoming important to have complete inter-operability of systems and staff. To address this need, the vast majority of PCs, minis and other equipment are being interconnected. Cabling is being used to link together all equipment within a building. Telecommunications links are being used to link buildings together. With appropriate software data can be quickly and accurately transferred from one system to another. The ultimate aim is to enable any PC or terminal to give access to applications and data on any computer, subject to appropriate security controls.

This assembly of computers, devices, cabling and link represents an infrastructure. This document is a framework that defines the components of this technical infrastructure and how they fit together. We refer to this framework as an architecture.

POL00028135

It is Post Office Policy that all IT investments should be made within such a framework. This framework is defined by the Group Technical Policy Unit (TPU), under the auspices of the Group Technical Policy Committee. All Post Office Businesses are represented on this committee, which sponsors a research programme to keep this architecture and associated standards and policies up to date.

This Policy Document is published annually. It is supplemented by a list of approved hardware and software products, which is updated regularly in line with decisions made by the Group Technical Policy Committee (GTPC) and its subcommittees. More detailed reports are produced on individual research projects and are available from the TPU.

The format of the document has evolved over the years in line with changes in technology. Whereas at one time architectural definitions revolved around host computers, the arrival of client server computing, along with the widespread proliferation of interconnected PCs and LANs has made life a lot more complicated. New layers of software are having to be introduced, spread across all the components of the infrastructure to enable them to communicate with one another effectively. This includes the provision of tools to enable technical problems to be isolated and to deal with information security.

This issue of the Infrastructure Policy has been structured to recognise this trend, although the relevant software products and related standards are, in many cases, only just starting to appear in the market place.

Structure

Section 2 provides an overview of major developments and trends in the IT industry which will have an impact upon the Post Office.

Section 3 outlines the architectural framework within which the standards and policies for the various hardware, software and telecommunications will be defined.

Section 4 provides guidance on how to select the appropriate platforms for client server systems, and also provides an overview of the 5 major client server models.

Sections 5-12 define the standards for the various components, including the cross platform software elements, as outlined above.

For more detail on current standards the reader is recommended to refer to the Post Office Strategic Products Catalogue, soft copies of which may be obtained from iT/Technical Assessment Services. The catalogue has the added value of being maintained as current, in line with changes in Technical Architecture, whereas this document will be revised once, or at most twice, each year.

Section 5, apart from defining current standards, also identifies strategic directions, where they have been defined. These are contained within 'Directional statements'.

POL00028135

Authority

The Technical Infrastructure Policy is formally authorised by the Post Office Executive Committee (POEC) on the advice of the Group Technical Policy Committee (GTPC). It is the responsibility of the Group Director, Information Technology in the role of strategic adviser to the Post Office Board, to maintain it and be responsible for the authorisation of any deviations from it through the process of Technical Concurrence. This responsibility may be devolved to individual units for sub MaPEC projects in accordance with agreed procedures GTPC(..)...((Ref). (See GTPC file))

Benefits

The Technical Infrastructure Policy identifies specific hardware, software and communications systems which will deliver accurate, secure, cost-effective and appropriate functionality and inter-operability, at minimal risk.

The main benefits to be gained from a defined Technical Architecture include:

- lower technology evaluation and procurement costs, because hardware and software evaluation is carried out against generic requirements, instead of being repeated for every project;
- lower prices, because the strategic products can be procured in larger quantities;
- more flexible in staffing and lower retraining costs, because fewer technical environments have to be supported;
- greater levels of in-house expertise, through concentration on fewer targets;
- less need to develop or purchase special conversion and communications software to bridge between incompatible environments;
- faster and cheaper application development, because a mature high function environment can be selected and staff made familiar with it;
- greater opportunity for standardisation of the user interface;
- matching infrastructure components to business demand;
- reduction of training and support costs through standardisation;
- cheaper connectivity;
- the opportunity to develop close relationships with manufacturers and suppliers.

Further Reading

A more detailed understanding of the Technical Architecture is available from the following papers which have been influential in determining changes in the Technical Architecture.

Prefix	Title	Issue Date
iT/TPU/276	Enterprise Client Server Computing/The Hype	07/22/94
iT/TPU/275	ATM: Management Positioning Paper	07/07/94
iT/TIU/250	Introduction to EDI	04/26/94
iT/TIU/239	Testing of Printers for Parcelforce Intertrak	04/12/94
iT/TIU/230	NT Status Report	03/28/94
iT/TIU/229	MS Daytona Brief	03/28/94
iT/TIU/212	Multimedia Position Paper (Second Edition)	02/01/94
iT/TIU/205	IP - New Generation	02/05/94

POL00028135

Prefix	Title	Issue Date
iT/TIU/202	LOS Executive Summary	12/07/93
iT/TIU/192	Large Open System - Main Report	11/04/93
iT/TIU/179	Personal Computer Evaluation - 1993	09/22/93
iT/TIU/165	NOS Positioning Paper	08/24/93

POL00028135

2. INDUSTRY TRENDS OVERVIEW

This section outlines some of the major trends within the IT industry, in order to set the context within which Post Office technical infrastructure policy and architecture has been defined.

2.1 CENTRAL COMPUTING

Pressure continues to mount on the mainframe and the traditional "Glasshouse" approach to computing. This pressure is largely due to organisational re-engineering, which has empowered the expectations of users who have been seduced by the attractions of Graphical Interfaces (GUI) to their PC systems; the industry shift to the new paradigm of Client Server, and the increasingly positive price/performance equation offered by mid-range computers.

The pressure has resulted in the major player in this market space, IBM, recording the largest losses in corporate history and laying-off huge numbers of staff in a world-wide re-structuring program. The result will be a new IBM which will encourage internal competition and no longer protect its mainframe business from products such as the RS6000. IBM will increasingly enter the Consultancy, Systems Integration and Outsourcing markets in order to broaden and strengthen its portfolio.

During this period, the OEMS such as HDS and Amdahl have been hit equally hard. In essence their market space has become untenable and they are seeking to position themselves as Value Added Compatibles (VACs) and move into other ranges by means of alliances and partnerships. It remains to be seen how, and if, they will achieve this shift.

In parallel with this activity, manufacturers considered traditionally to be in the Unix midrange, market are extending upwards with ever more powerful RISC-based processors such as the HP T500 range. These processors are becoming credible from a price/performance viewpoint but are still immature from a systems management angle. They are not yet a true alternative mainframe for organisations such as the Post Office which balances massive daytime OLTP Workload with complex schedules of overnight batch processing.

The next five years will witness the death of traditional ECL based mainframe technology. As early as 1996, all mainframe manufacturers can be expected to have low-cost CMOS versions of their products. These will begin to approach the price levels of 'Unix' processors but enjoy the management structures normally associated with mainframes.

POL00028135

In a similar timescale, all mainframe manufacturers can be expected to include parallel processing technology in their ranges. Some, like IBM, have already announced steps along this route with attached processors to handle large volume OLTP and decision support. These processors will be faster, smaller and cheaper than traditional equivalents.

Massively Parallel Processing architectures (MPP) will begin to move out from the scientific market where, already, too many vendors are chasing too few opportunities, and address the commercial computing world. New vendors, such as KSR, Meiko and NCube will appear in this market alongside established vendors such as IBM, Tandem and NCR. There will be significant challenges, however, to the success of MPP in the commercial arena. There are very few skilled people available to develop the applications which exploit this technology. There are very few tools available to assist with processes like database design and no real production management systems. At the same time the reliability and security demands of the commercial market are very different to those of the scientific. MPP will have a niche-role, commercially, until those questions of management and development technology have been addressed.

There is a new role emerging for large central computers. As well as being effective servers for high volume transaction processing and the management of large 'enterprise' databases, they are ideally placed and suited to provide back-up and archive management services for distributed enterprise data.

In order to survive, it can be expected that selling prices for mainframes will plummet and previously proprietary manufacturers will embrace open systems technology. In the latter half of the decade, alternative mainframes such as MPP will take a significant share of the large systems market particularly in the decision support and OLTP areas. It can also be expected that the power of Unix processors, such as the HP9000 range, will increase to the extent that they will be fighting head-to-head with IBM mainframes. The differentiators will be price and system management ability.

2.2 DISTRIBUTED COMPUTING

The very issues which are accelerating the shift from traditional mainframes to open, client-server architectures are highlighting the immaturity of the management environments for client server and the rapidly increasing complexity of the task. In addition, the selection of strategic vendors and products is made all the more complex because of the price pressures and technology changes which will drive all but the best, and the most astute, from the market.

POL00028135

This is the arena where bottom-up and top-down will collide, both in the sense of strategies and hardware. The increasing power of multi-Pentium processor PCs (and, indeed later X86 processors) will overlay the mid-range, whilst small CMOS-based mainframes will encroach from above. At the same time, mid-range vendors themselves will expand to scale the complete spectrum from desktop to data centre. At the low-end they will compete head-to-head with Intel-based PCs whilst at the high-end they will be price and performance competitive with mainframes, at least on paper.

On the operating system front, the launch in 1993 of Windows NT Advanced Server gave notice of Microsoft's intention to offer a credible opponent for Unix. Current versions of 'NT-AS' are not yet sufficiently well supported with management tools or robust enough for mission critical applications, but experience suggests that it will not be too long before they are. Although NT will run on either Intel or RISC architectures, it will provide a powerful boost for the PC-based server platforms which have suffered in the past from the limitations of generic UNIX (such as SCO) compared to the servers available from the mainstream suppliers.

2.3 DESKTOP AND LANs

In 1993 we have seen the death of the 386 processor. Of the 40m or so Intel processors shipped in 1993, 32m are 486 technology. No one is shipping 386 devices for 1994. 486-based PCs are now considered the base product with 586 (Pentium) based systems being aimed initially at the power-user, and at server applications.

In 1994, Pentium-based processors will ship in volume and soon become the norm, even on the desktop. Intel are well ahead with planning for 686 and 786 technologies. The increasing power will be needed to exploit new graphical and video software, and, increasingly, hardware architecture and software will exploit and complement each other. This will be achieved by closer co-operation and partnership between vendors such as Microsoft and Compaq.

Whereas processor power has enabled even more complex software to be developed and, conversely, the demands of software increasingly influence processor and PC design, the real issues of 1993 have been in the Operating Systems arena. Windows is becoming the dominant desktop OS and will certainly be so for the foreseeable future In the LAN environment, the decision by Microsoft to discontinue development of LAN Manager, in favour of Windows NT-AS, has presented a major issue to the Post Office in that it will need to decide its migration path and timing. The extent to which LM/X (LAN Manager for Unix) will continue to be developed in line with NT-AS is currently an area of uncertainty. Within the Post Office this product has served as a link between the PC world and distributed UNIX servers. For a transitional period it will be necessary to support LAN Manager, LM/X, NT-AS as well as Netware, but some rationalisation needs to be sought in 1995.

There has been little innovation in desktop hardware in 1993/94. Vendors have been concentrating upon bringing the new higher performance CPUs on board, and improving quality and price performance in a more and more competitive market place. Vendor stability and strategic alliances are becoming the major differentiating factor in an increasingly commodity orientated market place. Second and third tier vendors are under great pressure, and may well disappear.

POL00028135

In 1994/95, innovation at the desktop will be driven by multi-media developments, many of which will become an integral part of the standard multi-media PC by the end of 1995.

- CD-ROM prices have fallen dramatically and increasing amounts of reference data are distributed using this medium. For the Post Office, these cost reductions make the economies of 'information kiosks', previously ruled out on the grounds of communication costs, much more attractive.

- Multi-media and the new 'document centric' software from Microsoft will integrate voice, video, text, image and graphics in everyday applications. Multi-media has hitherto been seen as technology for specific applications such as training but that will all change in the next few years. This type of integration will even be available to mobile users as their PCs attain the power of desktop equivalents.

- Also on the multi-media theme, there will be a trend towards convergence of domestic TV and Office/PC technology. Microsoft are extending into the domestic arena with 'Microsoft in the Home', and cable TV companies are beginning to build multi-media capabilities into terminating units. The danger for the IS industry is that these products may have no affinity whatsoever with the established standards of the DP industry.

In the office, the need for Business Process Re-engineering combined with an expanding reliance on team-oriented organisation structures, will drive office systems to deliver workflow applications and multi-media to the desktop. Office systems will increasingly need to support every aspect of our business, and the move towards these workgroup applications and technology enabled employees could well bring a shift back towards centrally planned and implemented office systems. This is particularly true of electronic mail, which is graduating from a local workgroup to an enterprise-wide and intra-enterprise technology. Within the next few years, electronic mail will become as fundamental to business operating as the telephone, and this technology will be backed up with integrated image and workflow capabilities.

Portable computing matured rapidly in 1993. Three categories of portable emerged in what will become an increasingly important market segment. Desktop equivalents, mobile companions and consumer devices are the established categories with desktop equivalents rapidly approaching the capabilities of fixed desktop machines.

The proliferation of mobile computing devices can be expected to continue during 1994/95, although most of the devices available are still of an experimental nature. The real benefits will come when they are used in a controlled manner as a key component of client-server architectures. More effective and generally available 'dial in' solutions will be an important factor, along with greater maturity in the wireless arena.

POL00028135

2.4 SERVICE MANAGEMENT

Traditionally, hardware vendors operated in vertically segmented markets where they provided not only the box, but also the systems management software to make it all work in a secure environment. This is the traditional 'Glasshouse' scenario. Industry moves towards open systems, client server and networked PCs have created the demand to provide service management across a heterogeneous array of hardware, software and communications. The demand is for a new, virtual Glasshouse. Further than that, the days when the IS department ruled over the Glasshouse without question have passed and the challenge has become one of being able to provide:

- a management environment which will encompass this diversity;
- tools which will automate and integrate the management processes;
- tools which may be operated at a variety of levels and regimes from centralised to distributed control.

The potential to deliver end-to-end service management across a variety of distributed platforms is gradually becoming reality. Products such as HP Openview, which has effectively become a de facto standard, are beginning to provide a sound basis for the required environment and tool kit.

Emerging standards such as Open System Foundations Distributed Computing Environment (DCE) have given credible vision to the industry and the suppliers to the Post Office are actively working within its framework. The same is true for the Distributed Management Environment (DME), although this initiative is now considerably less ambitious than was originally intended .

Communications and systems management will become a continuum in the coming year. 1994 is the year in which the Post Office must choose its platform and environment for providing seamless system management across the variety of techniques and organisations involved in delivering today's options to the end user. The solutions shortfall apparent now in the area of integrating new management solutions with those necessary for the management of legacy systems will gradually be eroded by the evolution of new products such as HP Openview.

The industry is also just starting to realise the potential security exposures inherent in the distribution of systems and interconnection of LANs. Business is now clamouring for cohesive security architectures across diverse central and distributed platforms. Regrettably, this issue has been neglected for a number of years and no standard solution exists. This will be the subject of much activity within the industry during 94/95.

2.5 APPLICATION DEVELOPMENT TECHNOLOGY

Three major areas of market activity can be identified - CASE, Client Server 4GLs and Object Orientation.

CASE tools were originally built on the structured methodologies of the late 1970's and the hardware and software environments of the early 1980's. In recent years they

POL00028135

have had difficulties in keeping up with technological change, and particularly with the moves to graphical user interfaces and client server architectures. Two approaches are in evidence: LBMS with System Engineer have been constructing bi-directional interfaces to popular client server 4GLs such as Powerbuilder and Visual Basic. TI with IEF have been extending their code generation concept to encompass a total closed client server environment with its own communications and system management software ported across a range of hardware, operating systems and DBMS platforms. This approach is likely to be modified in the light of the recently announced relationship with Microsoft.

In 1993, the industry seized on the concepts of **object orientation** as the basis for application technology in the 1990's. Three major drives may be identified, with some degree of overlap.

- As a basis for linking the components of compound documents, particularly in desktop applications. This is dominated by Microsoft's OLE2, but subject to challenge from the OpenDoc consortium.

- As a basis for defining a more stable interface between client and server in the client/server environment. Here IBM's DSOM will be aiming to pre-empt Microsoft's CAIRO; the next version of NT due probably in 1996.

- As the basis for a new approach to application development based upon re-useable components. Here Microsoft's CAIRO will be challenged by the forthcoming Taligent framework supplied by IBM and HP, and by Novell's Appware. The CASE tool vendors will also be aiming to evolve their tool sets and methodologies to include some elements of object orientated technology.

It is generally recognised that the market is wide open, with most vendors hedging their bets rather than committing themselves irrevocably to any individual protagonist.

There is likely to be an initial market for Microsoft OLE2 "Componentware" developing in 1995 providing comparatively low level functions such as spell checkers as 'add-ons' to the office application suite. More ambitious use of object orientation is likely to remain in the experimental domain for some years, until the tools are more mature, and the industry has learned how to use them.

2.6 COMMUNICATIONS

1993 has been the year in which network operators have been faced for the first time with the dilemma inherent in striking a balance between old and new technologies. Whilst technologies such as X25 and SNA have reached a degree of maturity, and can be managed to give a highly reliable service, the demands of inter-LAN communication are giving rise to new challenges which these technologies are proving unable to meet. This is not surprising given that WAN bandwidths are typically one hundredth that of LANs, and the unpredictable nature of end user driven demands.

POL00028135

New technologies such as asynchronous transfer mode (ATM) offer a long term solution, with the potential for virtually unlimited bandwidth 'on demand'. Unfortunately it is going to be some years before these are widely deployed, and available at acceptable prices. In the meantime, Megastream-rate cell switching technologies, in conjunction with frame relay protocols offer an interim solution, and are being evaluated for inclusion in the Post Office network in 1995.

One consequence of the extension of LAN communications across the WAN has been the need to standardise on the use of routable protocols. TCP/IP has become a worldwide de facto standard for corporate networks, but is creaking beneath the inadequacies of it own structure, and particularly the inability of its addressing structure to support the number of workstations now being installed. A Mark 2 version which will overcome these problems is expected to be agreed in 1995, although it will take some years to roll out. In the meantime interim solutions are needed.

On large campus sites, even LAN bandwidths will be under pressure once use of multimedia becomes widespread. Distributed backbones will give way to single box "collapsed backbones" which provide a ready transition to ATM switches, which will become available at more affordable prices by the end of 1995.

Local Area Networks have become an indispensable component of Post Office Information Systems. Interconnected LANs are now key to business strategies, and the management and security issues surrounding them are becoming critical. LANs, in effect, have spelt the death knell of 'personal' computing and the PC has become the universal, networked workstation or client.

New network operating systems from Novell, and subsequently Microsoft will gradually attempt to introduce the enterprise directory and management capabilities that are needed.

Two major issues facing the Post Office will be provision of enterprise-wide inter-LAN networking to provide full functionality office systems, and the need to generate and maintain enterprise-wide directories of addresses and users. Products based on X400 standards for the former and X500 for the latter are slow to emerge and it will be necessary to put in place key transition strategies and sound across-business tactical solutions to achieve effective solutions.

One of the fastest growing trends in 1993 has been the demand for remote access to LANs and host services from mobile users and small remote units. Remote access is usually provided by dial-up networking, as opposed to leased lines.

The importance of adopting a credible electronic commerce strategy has been a feature of 1993. In addition to the need to trade electronically as part of our routine business operations, the Post Office has significant ability as a retail and distribution network to provide a unique range of products to its customers. The first steps towards this goal were taken in 1993.

POL00028135

2.7 CLIENT-SERVER ARCHITECTURES

Client-Server has been widely hyped as the answer to every IT problem, and the only way to develop systems in the 1990's. After some expensive mistakes, the IT industry is starting to come to terms with the reality. It is now widely recognised that client server systems are more expensive to develop and to deploy than conventional systems. Moreover, when implemented on a large scale they pose new management challenges for which technology has yet to provide a truly general solution.

However, client server systems can provide unique business benefits, and it is on this basis that they must be justified.

A widely quoted model, originating from the Gartner Group, identified five types of client server system. The vast majority of those implemented to day are either:

- server centric - where the majority of the application resides on the server, and the client handles the user interface
- client centric - where the majority of the application resides on the client, and the server handles the database management system.

The former has been used primarily as a means of providing a common new look interface across a range of legacy systems. It poses problems of change management particularly, and is not recommended for new developments.

The latter has been used very successfully in a LAN environment, but can cause performance problems when implemented on enterprise-scale wide area networks. It is not recommended for environments where client software is developed by end users.

Over time it is to be expected that the industry will move towards a distributed logic architecture, where application function is distributed between client and server to minimise data transfer requirements and, as far as is practicable, to de-couple the client and server development processes. The full realisation of this concept is dependent upon the availability of object orientated middleware frameworks, which today are in their infancy.

Much activity can be expected in the industry over the next few years, as vendors, consortium and standards bodies jockey for position as suppliers of major components for these future enterprise-wide system software architectures. In the meantime, the Post Office Technical Architecture is designed to incorporate client solutions where required, based upon interim best of breed technology and standards, and consistent with longer term industry directions.

POL00028135

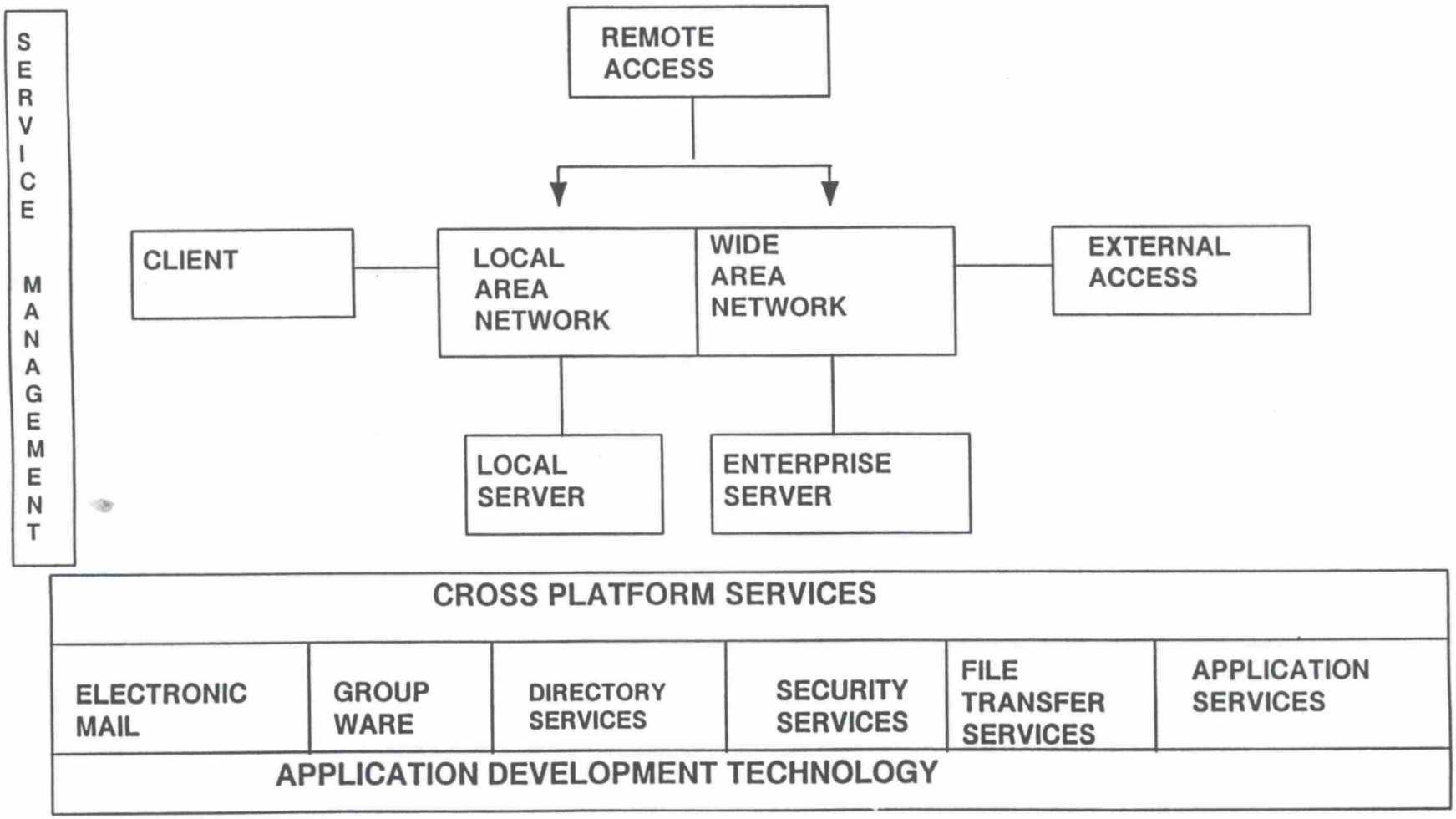


FIGURE 1: TECHNOLOGY ARCHITECTURE MODEL

POL00028135

3: TECHNOLOGY ARCHITECTURE OVERVIEW

3.1 INTRODUCTION

The purpose of this section is to outline the architecture model within which the standards and policies defined in this document are described. Its physical implementation will vary from one part of the business to another, but it is sufficiently general to cover most of the variations likely to be required.

Individual businesses will produce more detailed documents which will describe how the architecture will physically be implemented within their respective organisations. They may well decide to be more restrictive in the range of architectural options and products which they wish to approve.

3.2 ARCHITECTURE OUTLINE

The model recognises three major elements of processing

Clients
Local Servers
Enterprise Servers

It contains four elements of communications

Local Area Networks (LAN)
Wide Area Networks (WAN)
Remote Access
External Access

Next there are a number of cross platform services which may have a physical presence on any or all of the above components, but are required to provide particular services on an enterprise wide basis (e.g. security) or which are common to many different environments.

Also specifically identified in this context is the need for service management technology which can span all components of the architecture.

Finally there is a section on application development technology, as this too, is closely related to the environments in which the applications are required to operate.

POL00028135

3.3 **Clients** in this context are the physical workstations through which end users gain access to information systems. They may be physically connected via a LAN (4.6) or via a remote access service (4.8). The standard client is a personal computer (PC) but more specialised clients may be used when the occasion demands (e.g. counter terminals, bar code readers).

3.4 **Local servers** are attached to a LAN, and are used to meet the needs of clients attached to the same LAN or via a remote access service. A Local server may also be a client of an enterprise server or another local server. Local servers are used to provide network operating system services (NOS), and to host local applications. They may also serve as protocol translation gateways for access to conventional host applications, in which case they will emulate a terminal control unit, and the security gateway. In this context their functions may also be extended to allow the direct connection of dumb terminals.

3.5 **Enterprise servers** are used to host applications and databases that need to be accessed from many different locations. They may also be used to host enterprise wide services such as those outlined in 4.10 and 4.11. They are normally housed in purpose built, professionally staffed data centres.

3.6 **Local Area Networks (LAN)** are used to interconnect clients and servers in a single geographical location.

3.7 **The Wide Area Network (WAN)** interconnects major Post Office locations. It handles voice and data traffic. With today's technology, WANs transmit data very much more slowly than LANs, and this is a major constraint on the overall performance of the architecture.

3.8 **Remote access services** are used to allow clients operated by Post Office staff to access the Post Office infrastructure from locations which, for reasons of cost or volatility (e.g. hotel rooms), are not connected to the WAN. Depending upon the type of application, they may provide access to a LAN or to a central server. For security, cost and performance reasons there are constraints on the facilities that they provide.

3.9 **External Access Services** are used to interconnect the Post Office IT infrastructure with the outside world. This may be used to access external information databases, for electronic data interchange with customers and suppliers, or to provide specialised electronic services to our customers. Special security provisions are required to ensure that the integrity of the internal Post Office infrastructure is not compromised.

POL00028135

3.10 The term **Cross Platform Services** is used to describe software products that are common to several components of the infrastructure, or need to work together in a co-operative way in order to provide a facility across the entire enterprise. These are as follows. Today most exist only in embryonic form, if at all.

3.10.1 **Electronic Mail.** This is the set of services required to provide for enterprise wide mail exchange. It includes:

- mail access facilities at the client level, including the mail enabling of applications.
- mailbox facilities at the local server level
- mail exchange backbone capabilities at the Enterprise level
- mail directory synchronisation and maintenance facilities

3.10.2 **Groupware.** This includes all types of software, beyond basic mail and calendar facilities, designed to aid collaborative working across the organisation.

3.10.3 **Directory Services.** This covers all requirements for directory services that extend beyond the bounds of an individual application.

3.10.4 **Security Services.** This covers the hardware and software required to control access to applications with the infrastructure.

3.10.5 **File Transfer Services.** These are general purpose file transfer facilities that can be used to move data between components of the infrastructure.

3.10.6 **Application Services.** These are general purpose software facilities provided to enable the implementation of cross platform applications (notably client-server).

3.11 **Service Management** facilities are those that are provided to enable operational management of the enterprise. They are a special example of cross platform service, in that they need to be provided in some form on every component of the infrastructure, and increasingly will need to co-operate. Their major purpose is:

- To enable changes to be introduced to the infrastructure in a non descriptive fashion.
- To enable faults to be diagnosed and repaired when they arise.
- To enable the information processing and storage capacity of the components of the infrastructure to be adjusted in line with changes in demand.
- To allow usage of the infrastructure to be recorded for billing purposes.

POL00028135

3.12 **Application Development Technology** covers the methodologies and tools used for the development, testing and implementation of applications that will run within the technical environment. In addition to CASE tools, computers, 4GLs and the like, there is now a strong linkage to specific run time environments and cross platform middleware services (4.10). This is particularly so for client server applications, and for those which need to be integrated with office automation services.

POL00028135

4: TECHNICAL ARCHITECTURE FOR APPLICATIONS

4.1 Introduction

The purpose of this section is to provide some guidelines for the positioning of individual applications within the overall technical architecture. It is based upon research carried out under the auspices of the Technical Policy Unit, covering experience both within the Post Office and in other large organisations. Inevitably it is of a very general nature, given the complexity of this subject and the limited space available.

4.2 Client Server Architecture

In spite of the current enthusiasm for client server architecture, it must be recognised that conventional host-terminal systems will generally be less expensive and more reliable, particularly where they involve large numbers of users in multiple locations. Client-server should be used for such applications only where there are specific business benefits to be gained. Generally this will be where one or more of the following apply:

- A highly interactive GUI user interface is needed with fast response times, combined with the sharing of data across multiple locations.
- Access is required to a number of existing host systems, but the current user interface is unacceptable, either because it is too complex or inconsistent with other applications.
- A high degree of integration is required with existing or planned local desktop applications.

Even in these circumstances there can sometimes be a less complex or more economic alternative to a full client server solution. This may be achieved by taking periodic extracts from a central database, which are then transferred to the desired location using a software distribution or file transfer utility, or even on diskette or CD ROM. Where this is not acceptable, use of a data replication utility may be considered to enable multiple copies of a central database to be resynchronised at pre-set intervals.

4.3 Choice and Location of Servers

Central servers should generally be used where data needs to be shared across multiple locations, or where data is mission critical or sufficiently large in volume to require professional management. If local data is likely to exceed a few gigabytes then local staffing implications need to be considered.

Local servers should be used for data which is only required at the location concerned (or at directly dependent locations with remote access). They may also hold extract or replicated copies of central data (see above).

In choosing appropriate server technology, the ratio of data storage volume to processing power is a useful indication.

- Mainframes should generally be used where this ratio exceeds 400 Megabytes per MIP and for databases in excess of 20GB. They should also be used for

POL00028135

applications requiring very high transaction processing volumes, although the capability of the HP9000 and Tandem computers are now such this will rarely be a constraint in itself.

- HP9000 Unix processors are appropriate for applications with requirements that do not exceed the above thresholds. Unlike mainframes, they will generally need to be dedicated to a single application.
- PC based servers running Windows NT or Novell Netware should not be used for databases in excess of 1-2 GB. The limiting factors primarily relate to system management software and i/o processing capability.

These figures are, of course, only a very general indication. The capabilities of PC and midrange devices are continuing to improve, and other factors need to be taken into account. These include backup and recovery requirements, batch processing, and staffing considerations at the location concerned. At present PC based servers are not approved for local applications requiring complex processing, primarily owing to software limitations.

4.4 Functional Distribution

In client-server systems processing is split between a client, which handles the user interface, and a server which handles the database. Application logic may be on either processor, or on both. In more complex situations there may be more than one server. These might be arranged in a peer configuration, where the client has simultaneous sessions with several servers, or hierarchical, as when a local server requests data from one or more remote servers.

A number of models have been proposed within the IT industry to classify alternative client server configurations. As noted in section 2.7, the vast majority of applications today are either client centric or server centric.

- In a server centric system, the application logic all resides on the server - often a conventional host system - and the client is used only to provide the user interface. This is often used as a means of updating existing applications without charging the host resident code. Existing dumb terminals can continue to be used.
- In a client centric systems, all the application logic runs in the client, and the server runs a conventional database management system. The client issues remote SQL calls to the client, using communications "middleware" provided by the DBMS supplier or a third party. The advantage of this "remote data access" technique is that no special application coding is required.

This approach is appropriate where locally based applications on multiple sites need to share access to a common database.

Client centric systems can involve very large amounts of WAN traffic when client and server are in different locations. This problem may often be avoided by using some application logic on the server to optimise communication between the two. This is known as the "distributed logic" model.

Within the Post Office Technical Architecture only the simpler forms of client server application are currently supported. Excluding products which are confined to use within a single local area network, these are follows:

POL00028135

- Ingres Net allows a single Windows client or a local Unix server to access a remote Ingres database. The Ingres embedded logic facility allows a limited amount of application specific data selection logic to be installed on the central server.
- Visual Basic in conjunction with the approved SNA gateway product allows graphical front ends, running on Windows 3.11 clients, to be built for existing mainframe applications. It should be noted that the client software has to be updated whenever changes are made to the host system, and that the operational implications require careful consideration.
- In house developed LU 6.2 code allows local UNIX servers to have real only access to central mainframe DB 2 databases.

The middleware services required to support client server working are included within the "cross platform services" layer of the architecture at section 10.6. Those currently approved do not have the sophistication to cope reliably with simultaneous access from a client to multiple servers, or more sophisticated forms of distributed logic. New products will be evaluated within the TSMC work programme in accordance with business priorities as and when they become established in the market place.

4.5 Decision Support

In principle the remote data access technique may be used to allow locally developed decision support applications to gain access to centrally managed data. However, the extract and replication techniques outlined in 4.2 may often be more appropriate, as they represent less of a risk to the performance and integrity of operational systems using the same data.

TYPE OF AD HOC ACCESS TO CENTRAL DATA			
	USE LIVE DATA	REPLICATE DATA LOCALLY	COPY DATABASE
FEATURES	Production data in place	Data replicated to local (LAN) server	Data replicated to central copy database
UPDATE	(Yes) Potentially	No	No
PRODUCT EXAMPLES	CMS Gateway, Ingres/DB2 Gateway	Infopump	Intellect
DATA CURRENCY	Real Time	Periodic replication	Periodic replication
WAN IMPLICATIONS	Depends on method but requirement is single key access	Periodic (probably) overnight downloads bandwidth, time and cost	Enquiry traffic only - query processing is centralised

The choice of technique will depend upon operational considerations such as transaction rates and data volumes and the level of data currency required.

POL00028135

4.6 Distributed Database

Distributed database techniques, in which a single database management system controls databases in multiple locations, are not approved for use within the Post Office on account of the technical limitations of relevant software and the operational difficulties associated with its use. Where data needs to be shared across multiple sites, it should either be centralised or replicated, as outlined in section 4.2.

POL00028135

5. PLATFORMS

This section covers the three major types of processing platforms outlined in the architecture model:

- **Clients** - PC Workstations are recommended as the universal client.
- **Local Servers** - associated with a specific LAN or Workgroup community.
- **Enterprise Servers** - centralised data centre processors serving a wider community.

The relevant subsections outline the hardware and software environments currently approved for use within the Post Office. They also contain an indication of the type of application for which each should be used.

More specific information on technical architectures for different types of application is contained in section 4.

5.1: Clients

Hardware:

The standard desktop access device is an IBM compatible PC

The current entry level configuration is:

486SX/33 12mb RAM 200mb disk SVGA monitor
16-bit Ethernet Card with 10BaseT Connector or 16-bit Token Ring Card

1 year directional statement: 486DX2/66 16 mb RAM 340mb hard disk SVGA local bus 1mb VRAM with PCMIA

2 year directional statement: upgrade 486DX2/66 to Pentium using P24T chip with CD-ROM

Compaq and Toshiba docking stations are not compatible

Note: Apple Macintosh is specifically excluded

Operating System:

Current desktop operating system is Windows for Workgroups (current release) when networked, and Windows 3.1 when free-standing.

Portables use DOS6.2 and Windows (current release), but will soon also be Windows for Workgroups

Directional statement: Windows 95 (Chicago) both for desktop and portables

Note: specifically excluded are:- NT (at the desktop), UNIX (all flavours), and OS/2

POL00028135

Communications:	Directionally, it is recommended that all workstations are LAN connected to facilitate software update and remote system management, as well as providing access to Electronic Mail and enterprise systems. For details of Communication Hardware and Software, see Section 6
Middleware:	See Sections 10, 11 and 12
DBMS:	Microsoft Access Lotus Approach (under review)
Star.dard Applications:	Microsoft Office for Word Processor, Spreadsheet, Presentation Graphics Standard Virus Toolkit For other software refer to the Strategic Products Catalogue. PC users should be aware of PO policies on viruses, software and security
Multimedia:	We expect that in 1 to 2 years PCs will be supplied as standard with multimedia capability. This means they will have in-built CD-ROM, sound and moving image capability. The Compaq range of internal CD-ROM drives is the current standard. Other standards are currently under review.

Note: The Microcomputer Users Policy Committee (MUPC), as a sub-committee of GTPC, is responsible for developing, publishing and disseminating the Corporate policy on desktops and Local Area Networks (LANs). This section covers an overview of the strategy. A more detailed subsidiary document, the Strategic Products Catalogue, identifies the approved hardware and software for this platform.

5.2 Local Servers

5.2.1 INTEL - based servers

Recommended where

- Databases up to a size of approximately 10 MB are being shared.
- PC-like applications and/or utilities such as Lotus Notes are being shared by a local user community.
- Utilities such as FAX are being provided.

Hardware:

File Server:	Single or multi processor (486DX/66, Pentium - 60) 24mb RAM, disk capacity dependent on application. 16-bit Ethernet Card with 10baseT or 16-bit Token Ring Card.
Application Servers:	Intel-based application servers are not currently approved for general use. The role of Windows NT as an application server is still under review.

Print, Fax and Gateway Servers: as per desk top but 386 and older machines can be redeployed as print servers and gateway servers

POL00028135

Operating System:	**Either: a) Microsoft Windows NT/AS (replacing LAN manager/OS/2)** **Directional statement: Daytona (NT AS v3.5) in late 1994 and Cairo in 2 years** **Or b) Novell Netware 3.12 (for stand-alone LAN's) & 4.01 (for enterprise services)** **Directional statement: Novell Netware 4.X. Novell Netware 3.X to be phased out.**
Note: SCO/UNIX and UNIXWARE are specifically excluded	
Comms Software:	**see sections 6 & 8**
Comms protocol:	**Netbios and IPX should be phased out. The migration should be to TCP/IP.**
Middleware:	**See Sections 10, 11 and 12**
DBMS:	**This area is under review pending the approval of Microsoft NT as an Application Server. In the absence of proven support for Ingres as an NLM, once-off approval for use of Sybase NLM for MIS applications has been granted to POCL only, subject to review by GTPC.**
Standard Applications:	**Network versions of Office core products as per Client; it is recommended that they are run from the server. For other applications refer to the Strategic Products Catalogue.**

Note: All Servers should be located in appropriately secure environments and subject to a rigorous set of backup procedures. Details of backup devices may be found in the Strategic Products Catalogue.

POL00028135

5.2.2 RISC-based servers

Recommended for use where:

- greater than 10MB databases are being shared
- applications are distributed enterprise systems
- DP services are being provided on a free-standing basis for small business units.

Hardware:	HP 9000-series model E-range, G-range, H-range & I-range. HP 9000 model T500 is not suitable for use as a local server due to specialist environment and power needs.
Operating system:	HP/UX (current release)
Comms software:	see sections 6 & 8
Comms protocol:	TCP/IP SNA LU6.2 for IBM Mainframe access
Middleware:	see Sections 10, 11 and 12
DBMS:	CA-Open Ingres

Note: Use of alternative DBMS where mandated by specific Application Packages is subject to one-off approval by the TPU.

Standard Applications: Management agent for HP OpenView - see Section 11

5.2.3 AS/400 Servers

Recommended and approved only as the platform for existing Post Office standard packages such as JBA financial systems, Software 2000 Human Resources. AS/400 may also be considered as a general purpose free-standing DP environment in small independent business units.

POL00028135

5.3 ENTERPRISE SERVERS

Definition: Processors providing services to multiple locations and/or requiring controlled environments.

Centrally sited computers are used in the Post Office to fulfil two main functions:

- the traditional role of supporting large scale applications on a single centralised data model providing interactive access to a large community of geographically dispersed users and complex batch workloads;
- an emerging role as server in major Client/Server applications where high volumes of data are required to be held in secure, central locations and complex batch and/or decision support processing needs to take place.

In particular, existing central mainframe infrastructure is currently the most effective vehicle for high volume TP and large on-line databases where there is a high data:MIPS ratio. Centrally sited data and processors are particularly suitable when any part of the stored data may be accessed by any user, from any location and where that data must be up to date and consistent.

5.3.1 IBM-compatible

Hardware:	IBM 3090-compatible
Operating software:	MVS/ESA
Comms software:	VTAM NCP
Comms protocol:	SNA (LU2 and LU6.2) TCP/IP (under review)
Middleware:	TP Monitor (CICS) File transfer (XCOM 6.2) Access security (TOP SECRET) TSO
DBMS:	DB2

Standard Applications: Refer to the Strategic Products Catalogue

5.3.2 RISC-based

An HP9000 range server may be sited centrally to provide volume data access to remote users or as an integration link between distributed systems. Care must be exercised when considering this option as, although the raw power of the larger HP9000 machines is approaching that of the more traditional enterprise servers, such as the IBM System/370, they do not yet have the I/O capacity or the management tools and techniques necessary to make them complete 'Mainframe Alternatives'.

Hardware:	HP 9000 models T500/1-12

POL00028135

Operating system:	HP/UX (current version)
Comms software:	See sections 6 & 8
Comms protocol:	TCP/IP
Middleware:	The role of TP Monitor is presently under review File transfer - UUCP, FTP Access security - native UNIX products
DBMS:	CA-Open Ingres (under review)

Standard Applications: N/A

5.3.3 Other Enterprise Servers

Tandem:

Tandem Fault Tolerant Systems may be considered as an alternative to IBM mainframes for applications with the following requirements:

- continuous on line operation;
- very high levels of availability;
- specialised security;
- short and consistent response times;
- external gateway functions.

Tandem also provides the platform for the strategic EDI Gateway supporting all international EDI standards and X.400/X.435.
A decision to use Tandem must take account of the operational implications of any interaction required with databases in other environments.
Tandem systems are not intended to support a mixed general purpose data processing workload for which purpose configurations, ranging in throughput capability from the top end of the IBM mainframe range to well down into the HP9000 range are available. Remote operation is possible with the smaller configurations and distributed relational databases are supported with full integrity control.
OSI, SNA and TCP/IP communications protocols (including PU5) are supported and a variety of products are available to allow co-existence with the IBM environment.

- Fault tolerant processing is based upon Tandem equipment using the Guardian Operating system. Generally the policy is to remain close to the current release, but any new release involving major application or hardware changes will be subject to strategic review.
- A common technical environment is preserved for all systems.
- For existing systems the ENSCRIBE data management system will continue to be used. New applications will use Non-Stop SQL, which will also be considered for major enhancements to existing systems.

Hardware:	Tandem Himalaya
Operating system:	Non-Stop Kernel with Guardian Personality
Comms software:	In-built in OS

POL00028135

Comms protocol:	TCP/IP
Middleware:	TP Monitor (Pathway) File transfer (XCOM) Access security (Safeguard)
DBMS:	Enscribe, Non-stop SQL
Standard Applications:	N/A

POL00028135

6: LOCAL AREA NETWORKS (LAN)

The role of Local Area Networks (LANs) within the architecture is to provide the medium through which workstations at a location gain access to shared computer systems/applications, peripheral devices and files at that location and to the Wide Area Network (WAN).
It is now established Post Office policy to use a PC as the standard desktop device providing access to all data and applications wherever they may reside. Hence LANs have assumed the role as the first link in the communications chain to providing the required service delivery. As such, LANs are also an established part of Post Office policy.

The three elements to the LAN infrastructure are the:

- physical cabling system used within the building;
- link level protocols used to attach devices to the network and send data from one to another;
- LAN Network Operating System (NOS).

Hardware and Cabling:

- The LAN adapter card fits in the PC and enables physical connection to the LAN media.
- The wiring centre, or hub, contains the necessary circuitry to provide the required LAN topology; e.g. token ring or Ethernet.
- The lengths of cable attaching the adapter card to the wiring centre.
- Local bridges enable two or more LANs of the same topology to be connected together.
- A router may be used to connect multiple LANs. A router must be used if the LANs are of different media types (i.e. Token Ring to Ethernet).
- Gateways are used to translate LAN protocols to protocols optimised for WAN transmission (e.g. across X.25 or SNA networks). These have the advantage of allowing the use of standard network management techniques, but their throughput is not as high as that of the simpler bridging and routing devices. Approved hubs and routers are shown in the Strategic Products Catalogue.

Software:

- The network operating system provides a set of standard network services, e.g. file and print and a set of programming interfaces to enable development of networked applications.
- Network management software gathers statistics and generates error messages relevant to the device in which it is installed. Network management information can be exchanged with an appropriately configured network management console (see Section 11).

Current Approved Components:

Cabling:	Structured cabling based upon UTP.RJ45 to be used throughout. Category 5 capable of supporting 100 mbps is recommended

Note: A structured cabling system is cheaper if correctly designed in the first instance rather than built piecemeal or to the demands of individual projects. Budgetary provision should be considered on an infrastructure basis rather than project by project.

POL00028135

Topology: Two are approved:-

Ethernet which is low-cost and has a UNIX affinity

Token Ring which is particularly suitable for quick response data entry type applications and has an IBM affinity

Token Ring networks can also support a larger terminal population than Ethernet. Ethernet switching hubs are available to assist in managing this problem but are not currently approved.

Operating System: See Section 5.2.1

Communications Protocols: TCP/IP at the hub level

Note: Netbeui is no longer recommended for LAN applications, and is not approved for WAN applications. Existing usage should be phased out as soon as possible.

Detailed addressing standards are under development

Novell IPX is allowed in Netware environments although migration to TCP/IP is recommended

Lan Gateways: The Gateway server should be a minimum 486 running IBM Os/2 2.1 for 120 sessions.

EICON HSI/PC 1MB card
EICON SNA LAN Gateway software

POL00028135

7: WIDE AREA NETWORK

The Post Office WAN is designed to carry both voice and data communications between Post Office sites and to provide gateways to external networks and services

7.1 The Core Network (DCN)

Comprises leased (from BT and Mercury) 2 mbps lines Terminated by GPT ISDX Nodes. The Network protocol is DPNS. The technology used in the Core Network is under review.

7.2 The Voice Network

Access is provided by local PBX (Private Branch Exchange) attached to an ISDX Node or Network Terminating Unit (NTU) where additional services, such as video conferencing, are required over analogue lines

7.3 The Data Network

The outer core of the data network is based upon Cray 8500/8400 range as the standard data network switch for the DCN, with Cray 8300 employed on the 'outer-core'. Directionally ATM is envisaged.

Access is available from LANS via CISCO (400, MGS or AGS) routers. These routes are directly attached to the X25 network or via serial line to the nearest core route

Packet Assemblers Disassemblers (PADS) are used to connect asynchronous and SDLC devices

Dedicated SNA links are being phased out with these services being increasingly provided by QLLC over the X25 network

7.4 Addressing

All addresses are issued and managed by the iT Network Design Group. A comprehensive policy on naming and addressing is currently being developed.

7.5 Protocols

TCP/IP is the preferred network protocol. SNA is still used for mainframe access but is under review.

7.6 System Management

Cray Switches are managed by 5800 Network Management System. CISCO Routers are managed by Domainview

Integral network and system management based upon HP Openview is under development.

POL00028135

8: REMOTE ACCESS

The growth in both distributed computing and in LAN technology has led to an increase in the number of distributed applications within the Post Office and consequently in the number of remote users requiring access into these central services. It is anticipated that by the end of 1996 around 4,500 sites will need access to serve around 12,700 users with around 300 MB of data being transferred in around 270,000 hours of terminal connect time.

These remote users will therefore, require visibility to LAN based services and/or mainframe hosts and it is expected that these users will fall into one of the following three main categories:

A) 'Nomadic' or mobile users who will expect access from home, hotel room, or other remote location via a modem into either the LAN or host based systems;

B) Single remote users at a fixed site, who are not part of a LAN, but need access to business specific or mail type applications for timely information flow; and

C) Multiple remote users at a fixed or permanent location who may or may not be permanently part of a LAN infrastructure and will require dial-up access.

Remote access is the subject of current TSMC activity.

POL00028135

9: EXTERNAL ACCESS

9.1 EDI

As part of the Post Office Value Added Network (VAN), an EDI service has been established, based on a Tandem machine at Farnborough. All connections to EDI VAN's should be via this Gateway. The EDI Fact standard has been adopted for EDI formatting. The service uses software called Messageway from Logica/Tandem and has links to two third-party VAN's - GEIS and POSTGEM. GEIS is an international network; POSTGEM is a joint venture between Infonet (a Belgium-based VAN) and the Irish Post Office.

The software provides translation services to format information into the chosen message standard as well as controlling the data links to the VAN's.

9.2 Internet and similar Access

Access to public information networks such as Internet from the Post Office data network are specifically prohibited for security reasons. The provision of a firewalled gateway service is under consideration. Interim access should be via dedicated PSTN connection.

9.3 TCP/IP

The Post Office has an allocation of 4 Class B IP addresses. These are allocated to Royal Mail, Parcelforce, POCL and Group/iT/SSL. This limited allocation imposes significant restrictions upon lower level address space which is managed by the iT Network Design Group. Direct TCP/IP Access externally is not allowed (internal TCP/IP addresses must not find their way on to the external network); external access must be by an address-translation gateway.

9.4 Break In/Break Out

The Break-out product/service allows long distance voice telephony calls to be routed across the Post Office communications network which are subsequently passed to the public telephone operator closest to the destination for final local delivery. The service is enabled by the high functionality GPT ISDX digital PABXs that make up the core of the Post Office network. These switches are currently linked to both of the main public telephone operators, BT and Mercury, via high bandwidth (2 Mb/s) digital links which carries the DPNSS (Digital Private Network Signalling System) data stream which allows routing information etc. to be carried with the call.

9.5 Network External Access Security

Currently under investigation. All external connections must be via a gateway that provides appropriate protection.

9.6 Customer Links

Currently under investigation on a project by project basis.

POL00028135

10: ENTERPRISE (CROSS PLATFORM) SERVICES

10.1 Electronic Mail

The approved and recommended mail product for Post Office use is cc:Mail at both Client and Server Post Office level. To enable the use of other Mail clients and messaging services, a backbone Mail exchange infrastructure would be required with a directory service. Options for this are under consideration.

10.2 Groupware

Lotus Notes is the interim standard product for Groupware and group oriented workflow applications.

Investigation is currently underway to provide inter-Business Groupware capability.

10.3 Directory Services

It is recognised that Group Directories and Directory structures must be available to provide effective cross-business mail and groupware services. The appropriate standard for such directories is X.500 and a structure based on this is being developed.

10.4 Security Services

Another area where further work is being undertaken to provide a platform independent security architecture. The Distributed Computing Environment (DCE) looks likely to provide assistance in this area. At present, platform specific security facilities are implemented as outlined in sections 5 and 6. Additional security for dial up connecting is provided.

10.5 File Transfer Services

Mainframe to other platform file transfer is undertaken using the XCOM6.2 product based on the SNA LU6.2 protocol. File transfer in a TCP/IP environment uses UUCP.

10.6 Application Services

Cross platform services based on APPC LU6.2 conversations are useful in circumstances where low volume DB2 access via CICS is required. A number of robust solutions exist and the technique is recommended.

This area is currently the subject of further investigation. Current facilities for supporting client/server applications are outlined in section 4.

POL00028135

11: SERVICE MANAGEMENT

Service levels provided by traditional mainframe services have set user expectations at a higher level than can be expected in a distributed environment with the current levels of software maturity. Additionally, increasing numbers of both Open System and PC Lan environments, with associated hidden support costs, will increase the cost of service management. The current aim of service management is thus to control costs whilst providing a stable service environment that meets customer expectations in an immature environment.

The Open Software Foundation (OSF) have developed a model to overcome inherent problems with proprietary solutions to service management, particularly in the distributed systems environment that is becoming increasingly popular within the Post Office. The OSF definition, known as the Distributed Management Environment (DME) provides a framework into which management for both applications systems and networks, developed by Independent Software Vendors (ISV's), and other vendors, can be brought together more easily.

The significance of DME to the Post Office is as the framework for HP's Openview product. Openview has been the strategic service management tool for Open Systems for some time; recently it has been ratified as the strategic framework for end to end service management by GTPC.

The adoption by DME of Simple Network Management Protocol (SNMP) as its operational protocol has lead to SNMP becoming far more widely implemented within service management applications. For this reason it is recommended that SNMP should be adopted as the protocol by which management can take place.

The recent creation of the DeskTop Management Task Force (DMTF) by a consortium of major IT vendors, has lead to the development of service management standards based at the PC hardware and microcode level. Currently these standards are not compatible with SNMP but it can be expected that products will emerge, during the next two years, that bridge the DME/DMTF gap.

Additionally, the MicroSoft Hermes product will be released in late 1994 specifically aimed at providing service management facilities for the desktop. Microsoft's position as the leading software vendor for PCs will ensure that Hermes is adopted as a major tool for service management.

Group TPU will monitor developments in this area.

11.1 Overall Policy

- Wherever possible equipment should be managed using SNMP based management applications.
- Management of TCP/IP Networks and equipment wherever possible by HP Openview or compliant applications.
- The purchasing of other management applications/element managers is discouraged.
- Desktop Management solutions should interface with the SNMP world. DMTF solutions will be adopted as Policy at the appropriate time.

POL00028135

11.2 Platform Specific Management Tools

11.2.1 MVS Platform

Operating System:	
Performance Monitoring:	Candle Omegamon and IBM RMF.
Job Scheduling:	Netmaster.
Automation Products:	Netmaster.
Security:	Top Secret.
Database Management System:	
Monitors:	DB2, QMF, Insight DB2.
Utilities:	Copy Plus, Reorg Plus, Recover Plus, DB2 Mastermind.
Communications:	
Monitor:	Netmaster.
Configuration Management:	Netmaster.
File Management:	IBM Core products for Libraries, VSAM, and Sequential Files . Endeavour.
Overall System:	Netmaster.

11.2.2 Unix Platforms

Operating System:	
Performance Monitoring:	HP Glance and HP Glance PCS.
Job Scheduling:	HP Maestro.
Database Management System:	BMC Patrol.
Communications:	HP Openview.
File Management:	HP Openview.
Overall System:	HP Openview.

POL00028135

11.2.3 Intel Platforms

Operating System:	
Performance Monitoring:	None Recommended.
Job Scheduling:	None Recommended.
Database Management System:	Native Access.
Communications:	Openview, Intel Landesk Manager (Novell Netware Only), Insight Manage (Compaq Only), Directionally MS Hermes. Novell Netware and Lan Manager provide some features.
File Management:	HP Openview, Directionally MS Hermes.
Overall System:	HP Openview, Directionally MS Hermes. Novell Netware and Lan Manager provide some features.

11.2.4 Tandem Platform

Operating System:	
Performance Monitoring:	Peek, Viewsys, Measure
Job Scheduling:	Netbatch
Automation Products:	Netbatch, TACL
Security:	Safeguard
TP Monitors:	Pathway
Database Management System:	
Monitors:	DSAP, TMF, ENSCRIBE
Utilities:	DCOM, TMF
Communications:	
Monitor:	CMI, SCF
Configuration Management:	CMI, SCF
File Management:	FUP
Overall System:	Viewpoint

11.2.5 AS/400 Platform

Refer to Group Technical Policy Unit for details.

POL00028135

12: APPLICATION DEVELOPMENT TECHNOLOGIES

In order to be competitive in Application Development, an adequate infrastructure to ensure the optimal productivity of technical staff needs to be maintained
In order to ensure these aims are met and that the Application Development process is supported to that end, there is a continual process of documenting and disseminating standards and procedures for new environments and techniques, pooling 'best practices' to modify existing standards and procedures and the evaluation and implementation, where beneficial, of tools aimed at increasing productivity.
A number of common standards, principles and methodologies are employed cross-platform. iT employs the Development Quality System (DQS); the DQS is specific to development activities and specifies standards and procedures (with supporting checklists and guidelines) relating to such matters as unit testing and other processes and techniques to support life cycle activity.
There are two formal application development methodologies in use, namely Information Engineering (IEM) and SSADM which effectively provide frameworks for the development of projects. Whether SSADM or IE is used on a specific project is customer driven but where there is no specific customer requirement as to methodology IE is used as the default. Use of these methodologies allows a standardised approach to systems development and the production of deliverables to the same format.
The IE and SSADM methodologies are increasingly being supported by the use of Computer Aided System Engineering (CASE) tools. Two CASE tools are currently in use, IEF from Texas Instruments and Systems Engineering (SE) from LBMS. CASE tools store systems data to aid the generation of Information Systems by ensuring the completeness and integrity of the information required. Both IEF and SE can be used from initial analysis through to executable code generation on a number of platforms.
In addition, Rapid Application Development (RAD) and Joint Application Development (JAD) can encompass rapid analysis techniques which are CASE driven.
IEF will normally be used for developing new, and enhancing existing, CICS/COBOL/DB2 applications where code generation is expected.
LBMS/SE will normally be used to develop Client/Server applications.
Code generated applications MAY produce less efficient run-time code.

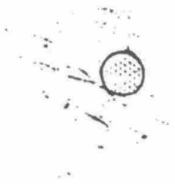
12.1 Intel Client

At the client workstation the GUI development is probably the most important feature.

12.2.1 Intel Server

Development tools used at PC server level include Visual Basic and C, C++ with Dbs such as Access/Foxpro/Clipper. Various tools can be deployed for testing - CANTATA testing envelope for C, and C++, as well as Evaluator for test script replay are recommended.

POL00028135



12.2.2 RISC Server

The approved development environment for this platform is CA-Open Ingres 4GL/DBMS

Other Tools are: Datagen test data generator
ABF Screen Design
CA-Open Ingres 4GL
VIFRED text editor

12.2.3 AS/400 Server

Applications in this environment are developed using RPG400 and Synon 2.

12.3.1 MVS Server

The development environment is based on the core IBM products CICS/COBOL II/DB2. TSO is used only for development purposes. Applications may be developed in a PC environment using Microfocus COBOL Workbench or generated from CASE tools eg IEF.

A number of development aids are used, for example: QMF and SAS which are used for query generation. SYNCSORT is the standard sorting package.

CICS Playback for test scripts/regression testing
Fileaid dataset manipulation
Intertest debugging aid for CICS transaction debugging

12.3.2 RISC Enterprise Server

This environment development is based on the CA-Open Ingres database and tool sets

12.3.3 Tandem Guardian Server

Environment: C, C++, TAL, TACL

Tools: DBaccess interrogation/modification tool
Control source code management
LOAD bulk testing facility
Testpro automated testing playback tool

POL00028135

Appendix 4-5

The ALPS Project

POL00028135

THE ALPS PROJECT

1. Overview

PC systems to support the ESNS application are being installed in approximately 1470 London Offices as part of the ALPS project. The ALPS project also provides for ECCO+ and APT functionality on the same equipment.

The ESNS system is designed to minimise the risk of fraud in benefits distribution. It does this by the validation of order books at the point of encashment using negative authorisation against an electronic stop notice

During the day Counter terminals capture details about each transaction that they perform. At the end of the day , the server gathers information from each counter terminal into one file ready to be uploaded to the Host polling system. During the night the host polling system dials up the post office and polls the server for the transaction file and status information. At a later point in time the host polling system downloads data files for the ESNS software including updates to the stoplist.

2 Hardware and Software

The table below summarises the minimum configuration of the equipment that is required to support the initial implementation.

	Server at Counter	Counter PC (non-server)	Accounting Device
Processor	486DX2-66MHz	486DX2-66MHz	486DX2-66MHz
Disks	420Mb	420Mb	420Mb
Spare bay for back-up system	Yes	No	No
Spare bay for CD ROM drive	Yes	No	No
3.5" Floppy Drive	Yes	Yes	Yes
RAM	16Mb expandable to 32Mb	8Mb expandable to 16Mb	8Mb expandable to 16Mb
Monitor	9" or 10" mono	9" or 10" mono	14" colour
Ethernet network interface card	Yes	Yes	Yes
Minimum No. Expansion Slots	4	3	2
Peripherals:			
Keyboard	Resembling ECCO+	Resembling ECCO+	Industry standard
Pointing Device	No	No	Yes
Bar-Code Reader	Yes	Yes	Yes
ISDN terminal adapter	Yes	No	No
Counter Top Printer	Yes	Yes	No
Back Office Printer	No	No	Yes

The Bar code reader is capable of reading Code39, UPC/EAN, and Code128 subset C

The Counter top tally slip printer EPSON TM- 270U compatible

Back office printers are compatible with the ECCO+ OKI ML385 in IBM Proprinter emulation mode.

Spare PC bays are combined - one spare for back up or CD ROM

The following software is also provided:

POL00028135

- virus checking software
- Microsoft DOS 6.22
- Microsoft Windows for Workgroups 3.11
- Microsoft 32bit TCP/IP
- FTP server.

POL00028135

Appendix 4-6

ECCO+ technical description

POL00028135

ECCO+ TECHNICAL DESCRIPTION

ECCO+ System

The ECCO+ system is based on personal computer technology. The system is installed in branch offices to support local accounting activities, and capture basic transaction details. A counter terminal is located at each counter position, and a back office processor is located in the back office. A simple local area network (LAN) has been installed in all offices, linking the counter terminals to the back office processor. The LAN is not currently used.

The requirement which ECCO+ was developed to meet is for a summarisation and balancing facility at point of sale. The objectives of the system are to :

a) Reduce the work in weekly balancing by :

- Totalling all transactions within groups
- Automatic arithmetic
- Identifying actual/potential mis-balances

b) Speed up the production of the office weekly cash account by eliminating the need to manually accumulate individual clerk balances.

c) Automate production of client summaries.

d) Improve efficiency at the counter by:

- Eliminating manual calculation
- Reducing the need to record transactions in writing
- Reducing errors

e) Improve the accuracy of client summaries.

f) Improve customer image of POCL.

g) Improve flexibility of staffing at the counter.

h) Provide the opportunity to more easily revise operational and accounting procedures.

i) Provide greater flexibility in meeting current and future accounting and information needs.

j) Provide the opportunity to reduce the frequency of stock checks.

k) Provide the opportunity to interface with other Post Office systems.

l) Allow 95% of transactions (by volume) to be accessed by dedicated keys.

Key Features

All transaction data is entered at the time of transaction.

A minimum number of keystrokes is required for clerks, using dedicated keys for most common transactions.

Where possible the system provides the price of an item.

Less common transactions use price look up code (PLU's exist for all items).

Running totals for each customer session.

POL00028135

Receipt option for customer.

Transaction data is written to hard disc/floppy disc at the end of each customer session.

Client Summaries

ECCO+ prints all Girobank summaries on client summary inserted in printer.

Other summaries are printed on tally roll (counter printer) or fanfold paper (back office printer) and sent to client in place of existing client summary (summaries currently provided are : Pension & Allowances, green Girobank cheques, postal orders paid, BT bill summary, redeemed savings stamps summary).

Other client summaries are currently completed manually (e.g. DNS, DVLA).

Balancing and Cash Account

When the stock unit balance is complete the data is transferred to the back office processor, currently by floppy disc.The system produces a trial balance (at any time during the week) and a final balance.

The balance takes only a few minutes to print on the tally roll.

When the stock unit balance is complete the data is transmitted to the back office processor.

When all stock unit balances are complete, the back office system automatically amalgamates them and produces the office Cash Account.

Each stock unit is held on one disc and one or more people have ownership of these, depending on whether the balancing is performed by each clerk or as part of a team.

Provides a comprehensive audit trail.

Each time a different person uses a stock unit, an individual password is required and therefore accountability is maintained on an audit trial that can be accessed by the manager at any time.

General

ECCO+ is linked to electronic postal scales in all offices comprising some 3000 scales in total which communicate via RS232 interface ports. There is generally one scale per two positions.

A facility to extract management information, on transaction data at the lowest level is also required. The data is required both for POCL internal use and for onward transmission to clients, in some cases.

The original ECCO+ specification identified a need to print on cut sheets, i.e. tax discs.

All databases must be parameter driven to enhance ease and speed of change.

Volumes

There are no available transaction volumes but the original sizing requirement during development was for up to 4,400 transactions per counter terminal per week with the back office processor required to hold two weeks data (i.e. 8,800 transactions) for each counter terminal (largest offices has 19 CTs).

POL00028135

NEW SOFTWARE DISTRIBUTION

Currently POCL prepares new versions of the software programs with an average 3-4 new versions each year. These are distributed on one or more discs to each site.

HELP DESK FACILITY

POCL operates a central help desk facility, located at Farnborough, which provides the first line of support to outlets for all education, hardware and software problems. There are around 1,800 calls per month with the majority split between education and hardware (roughly 45% and 40% respectively).

TRAINING

There is a one day training course in the use of the Counter Terminal and a two day course in the use of the back office system. These are both delivered off-site (in a POCL training office). These are only applicable when the clerks/manager are already conversant in working in a manual environment. For new clerks the use of ECCO+ is included in the standard five week counter training course.

INTELLECTUAL PROPERTY RIGHTS

All rights reside with the Post Office Group.

ECCO+ Hardware Specification

* 80386 SX micro processor in a ruggedised metal enclosure
* 2 Mb Ram
* 3.5 inch 1.44 - Mb floppy disc drive
* 101 key function - type keyboard with integrated magnetic card reader
*
* 9 inch hercules monitor
* Receipt/Journal printer
* 4 undedicated PS-232 serial interface ports
* PC-MoS/386 operating system
* 40 megabyte hard disc drive (back office processor only)

POL00028135

Appendix 4-7

APT technical description

POL00028135

APT TECHNICAL DESCRIPTION

APT SYSTEM

Automated Payments Terminal

The Automated Payments Terminal (APT) is essentially a personal computer packaged in a compact counter top unit. The unit has the following characteristics:

- A4 footprint.
- Full size numeric key pad.
- Calculator key-sized alphabetic key pad.
- Four function keys.
- Eight lines of 32 characters display (LCD) with adjustable contrast.
- Integral modem for communication (medium speed with error correction and data compression - V22 bis, V42, V42 bis standards).
- Track 2 magnetic stripe card reader (ISO 7811, 7812, 7813 standard).
- Smart card reader/writer (ISO 7816 pt 1, pt 2 standard).
- Schlumberger smart key reader/writer.
- Two PC-type serial ports for future use, for example, bar code reader.
- One PC-type parallel port for external printer if required, for example, slip printer.
- One port for an external smart token device, for example, contactless smart card reader.
- Internal battery to preserve memory during power failure.

More technically, the APT has the following characteristics:

- F8680 microprocessor (Intel 8086 - PCXT like) 7MHz speed.
- 1 Mbyte internal memory (RAM), split approximately half and half between working memory for running programs, and 'RAM-disk' for storing programs, transactions and reference data.
- MS-DOS 5.0 operating system.
- Standard PC-type BIOS for hardware control.
- 256 kbyte ROM.

  - 128 kbyte for operating system and BIOS.
  - 128 kbyte for basic communication/start-up program and diagnostics.

POL00028135

Current Constraints in APT System

The APT was designed to meet the requirements of the automated payments market, to support products with an identified client demand. In common with other transaction terminals, the APT has no disk, and its capacity is, therefore, limited to what can be held in its main memory. The main memory is used to hold programs, transactions, reference data and hot/stop lists.

The second area of limitation is the speed of the modem, used for despatch of transactions to the host, and receipt of programs, reference data and hot/stop lists. The APT modem is at least twice as fast as that in other standalone transaction terminals.

Main Memory

The APT will hold three average-sized hot lists and some 500-1300 automated payments transactions, depending on the type of transaction (magnetic stripe card transactions use less memory). The amount of space for transactions would reduce significantly if additional average-sized hot lists were to be held. The APT could not accommodate the size of hot list envisaged for systems such as ALPS.

Whilst transaction data and hot lists are only two of the types of information contending for memory space, they are the most dynamic: program and reference data requirements will increase but not with any significance when compared with hot lists.

The APT is, therefore, limited in its expandability for other schemes by its memory capacity, and this capacity would need to be addressed in order to use the APT for any schemes beyond automated payments.

Modem Speed

The modem is medium-speed, using data compression to increase capacity, and error correction to reduce failures resulting in retransmission. The length of a communication session is not an issue for the APT since it is dispatching transactions, and receiving new programs/hot lists overnight. The length of a communication session does have a cost implication though.

NON-APT EQUIPMENT

In addition to the APT described above, there are a number of local bill payment schemes using their own dedicated terminals. These are summarised in the following table:

Electricity Company	No of Terminals	Type of Equipment
Northern	100	Schlumberger
Eastern	50	Schlumberger
London	35	Schlumberger
South West	210	Schlumberger
East Midlands	32	Verifone

Water Company	No of Terminals	Type of Equipment
North West	11	Fortronic
Welsh	18	Fortronic
Mid Kent	1	Fortronic

POL00028135

Appendix 4-8

Polling and Terminal Control Service

POL00028135

POLLING AND TERMINAL CONTROL SERVICE

1. INTRODUCTION

1.1 This Appendix is adapted from APAY/PTC/001 (Operational Requirements for the Polling and Terminal Control Service). ***NOTE: references in this appendix to "mandatory requirements" and "desirable requirements" relate only to the APAY project and <u>not</u> to the present BA/POCL procurement.***

1.2 The document covers all processes required to be provided as a part of the polling and terminal control service.

1.3 The current operation is first described, with a summary of the various processes which comprise the operation. The mandatory requirements, followed by desirable requirements give the detail of the requirement for the polling and terminal control service..

1.4 Terms and Abbreviations

ALPS	Automation in London Post Offices
APT	Automated Payment Terminal
Branch office	A main post office wholly owned, controlled and staffed by POCL
DPC	Document processing centre - POCL's centre in central London
ECCO+	PC-based local accounting system in Branch offices
ESNS	Electronic Stop Notice System
ISDN	Integrated services digital network - a high speed digital dial up network
Kilostream	High speed fixed communication link
POCL	Post Office Counters Limited
PSTN	Public switched telephone network - analogue low to medium speed dial up network
SPSO	A sub-post office run on an agency basis for POCL
Utility	An electricity, gas or water company for which POCL provides a transaction collection service.

2. OVERVIEW OF THE REQUIREMENT

2.1 Requirement Summary

The requirement is for a transaction collection and terminal control service for the Automated Payments and benefits distribution system. The service will comprise the following processes:

Polling and terminal control

- transaction collection from POCL terminal network;
- transaction collection from document processing centre;
- new software distribution;
- reference data distribution;

POL00028135

- 'hot list' and tariff file distribution;
- APT and ALPS time regulation and clock change;
- ECCO+ system recovery;
- new terminal support;
- terminal replacement support.

Client transaction transmission
- collation of client transactions;
- onward transmission to clients according to service agreements;
- service agreement reporting;
- client transaction transmission to POCL accounting centre.

2.2 Current System Components

The automated payments system comprises the following components:

Automated Payment Terminal
- some 8000 terminals in 5000 offices throughout the UK;
- 8086 type processor;
- DOS 5.0 operating system;
- V.22 bis modem with error correction and data compression;
- up to 4 terminals sharing a single PSTN line;
- programmed start and stop time for polling;
- file-based information transfer.

ECCO+ System
- 680 offices throughout the UK;
- 80386 processor system;
- back office processor with diskette-based information transfer to counter terminals;
- PC-MOS operating system;
- V.32 modem with error correction and data compression;
- programmed start and stop time for polling;
- file-based information transfer to host.

ALPS System
- 1470 offices in the London area;
- terminals at all counter positions (some 4500);
- Intel 486 DX2 66 processor;
- 420 Mbyte disks;
- thin Ethernet LAN;
- Windows for Workgroups operating system;
- ISDN (basic rate service) communication using TCP/IP to create a LAN bridge;
- programmed start and stop time for polling;
- file based information transfer to host, using FTP.

Host system
- Tandem 3VLX and 4VLX systems;

POL00028135

- Guardian operating system;
- V.32 bis modems for utilities client transmission;
- Kilostream links for utilities client transmission;
- ISDN link for Benefits Agency (basic rate service);
- ISDN link for DPC transaction collection;
- Kilostream link for finance system transmission;
- V.22 bis modems for APT polling;
- V.32 modems for ECCO+ polling;
- ISDN primary rate service for ALPS PC polling, using an Ethernet connection to the Tandem.

Document Processing Centre

- Banctec 5500 ImageFirst systems.
  2 systems of:
  - 3 transports,
  - 2 controllers.

APACHI system

- Finance system front end;
- transaction level enquiry and reporting.

2.3 Current System Processing

The principal stages in the current system processing are:

- polling;
- transaction processing;
- client transmission;
- client file reception.

The automated payments processing cycle is shown in figure 2.1.

2.3.1 Polling

APT and ECCO+ polling takes place five nights a week, from Monday night through to Friday night. Polling may be extended to Saturday night in the near future. Polling is organised in two phases. The first phase - early polling - is to communicate with office terminals during specific agreed windows in the evening. The second phase - regular polling - covers the remainder of the terminal population.

The early polling phase commences at 17.30 and finishes at midnight. It is organised into half-hour windows. The terminal will be programmed to expect a poll during the window. Typically, the terminal is sharing a residential line, and so the polling window is agreed to minimise disruption to other uses of the line. Approximately 25% of terminals will be polled during the early polling phase.

POL00028135

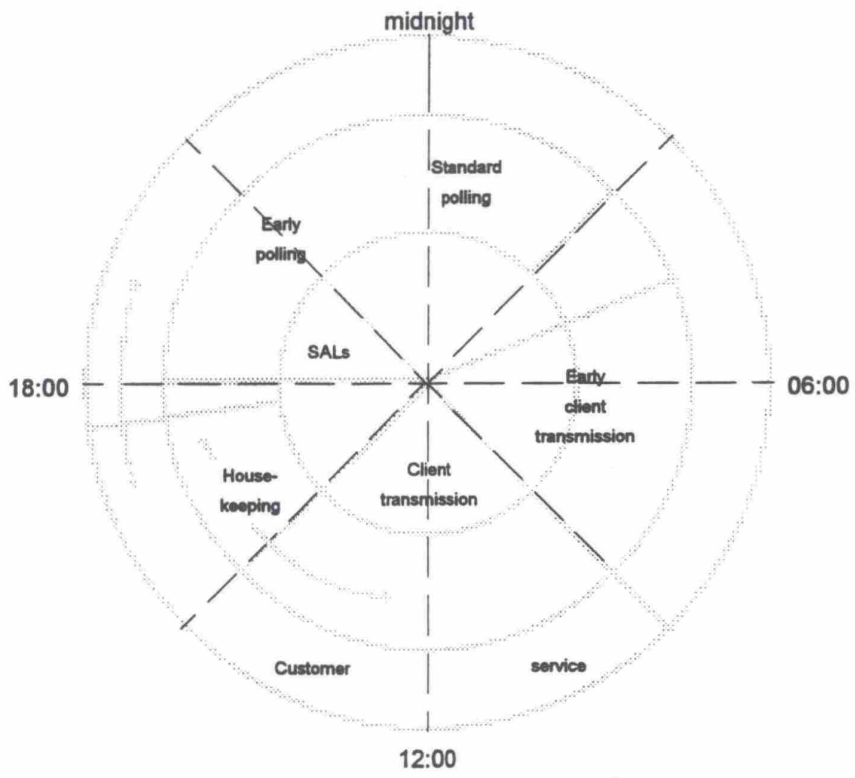


Figure 2.1 Daily processing cycle

The regular polling phase commences at midnight, to finish at 03.00. The terminals will be programmed to expect a poll during this window. Approximately 75% of terminals will be polled during the regular polling phase.

In many offices, more than one terminal will share the telephone line. Each terminal is programmed to answer the line after a set number of rings. By this means a strict order of answering is maintained, which corresponds to the terminal number sequence for the office.

Each terminal is polled only once during the night. During the communication session, transaction information is collected, new software and reference data is distributed, and new tariff files and 'hot list' information is distributed. Polling is attempted up to three times for each terminal.

Polling is dial up over the BT PSTN and the Post Office Postline private switched network.

ALPS PC polling will take place seven days a week. There will be two polling windows during each night. Each office will be polled in both of the windows.

The first window will be from 22.00 to 01.00. During this window, benefits and AP transactions will be collected, and AP hot lists and tariff files will be distributed. This is to allow the AP transactions to be processed.

POL00028135

The second window will be from 03.30 to 06.30. During this window, the Benefits Agency stop list update will be distributed. The time is set to be after the scheduled arrivla of the update from the Benefits Agency.

ALPS PC polling will be using BT ISDN services over the BT network.

The document processing centre is 'polled' by the collection of a file using ISDN during the early evening phase. This file accounts for some 30% of the transaction volume currently.

2.3.2 Transaction Processing

All transactions collected are streamed by client and service for transmission to client systems. Automated Payments transaction processing must complete by 03.30 for the first client transmissions.

2.3.3 Client Transmission

Client transmissions will take place from the early morning though to late afternoon. Generally, those clients with overnight batch processing can take a transmission into the late afternoon. Those clients with on-line customer service systems require transmissions to complete before the start of the day.

Client transmissions take place generally five days a week, from Monday morning through to Friday. Benefits Agency transmissions take place additionally on a Saturday. Transmissions may be excluded on bank holidays or local holidays for the client system centre. A transmission will include those transactions collected during the night. For Automated Payments clients, Monday's transmission includes transactions for Friday and Saturday. Specific service agreements for each client will state the transmission times and exceptions for that client.

For higher volume clients, transmissions use Kilostream. ISDN is being investigated for the near future, and will be used for the Benefits Agency. For other clients, transmissions use PSTN, with V.32 bis modems using data compression and error correction. Most transmissions are to a dedicated PC using XCOM. The Benefits Agency transmission will use FTP to a Unix buffer system. Others are direct to the client mainframe.

Automated Payment client interfaces conform generally to one of four standards. The magnetic stripe transaction interface is similar to the BACS standard. The smart key interface is to a Schlumberger client front end system. The WATERCARD interface is to a GEC Meters client front end system. The PISCES interface is to a standard agreed jointly with Landis and Gyr, Sligos and Yorkshire Electricity.

There is also a daily transmission of Automated Payments transactions to the POCL finance systems based in Chesterfield. This is a transaction level interface. This also uses XCOM over a Kilostream link.

2.3.4 Client File Reception

POL00028135

The smart card and smart key products have tariff and hot list information. A tariff file is received from the client to be distributed to a defined set of terminals. Similarly, a hot list type file is received from the client system to be distributed to a defined set of terminals.

For the Benefits Agency, a stop list update file is received from the client each night. This file consists of new and amended entries, and deletions from the master file.

The host contacts the client system daily to determine whether a file is available for collection. The specific client service agreement states the rules for collection and replacement of existing files. Generally, the files are collected during the early evening for distribution during that night's polling phases.

The distribution will be to a client agreed set of terminals only. The set will be defined for each client's distribution requirement.

2.4 Products Supported

The system supports the following products:

- magnetic stripe card;
- Schlumberger smart key for water and electricity;
- GEC Meters WATERCARD;
- Landis & Gyr PISCES electricity smart card;
- British Gas Quantum charging
- Electronic Stop Notice System for benfits payments,

2.4.1 Magnetic Stripe Card

Utilities issue magnetic stripe cards to their customers. The card identifies on track 2 and in the embossing the client, customer and service (e.g. token sale, prepayment). The customer presents the card at the counter with a payment. At an automated office (APT or ECCO+), the magnetic stripe is read and the transaction information is captured. This information is polled overnight by the host and then sent to the client.

At an office with an imprinter, the embossing is captured onto a sales voucher, which is electronically processed at the document processing centre. The transactions are polled by the host daily and merged with the transactions from the automated offices.

2.4.2 Schlumberger Smart Key for Water and Electricity

The utilities issue smart keys to their customers. The key carries value and tariff information to a meter or customer interface unit, and meter readings back to the transaction terminal. The transaction is very similar to the magnetic stripe card, except that the terminal updates the key with new tariff information and the money value of the transaction. The transaction information is passed to the client, and in a separate communication session, the new tariff file is received from the client.

POL00028135

Enhancements to the product include the use of special attention lists - a form of hot list. The special attention list is received from the client in the same communication session, and is distributed as a replacement file to all terminals agreed between POCL and the client.

The host translates some of the tariff and special attention list file information to the terminal format before distribution. It also translates some of the transaction information.

POL00028135

2.4.3 GEC Meters WATERCARD

This is similar in operation to the Schlumberger product. A smart card is used by the customer instead of a smart key. The hot list is known as an update list.

The host translates some of the tariff and update list file information to the terminal format before distribution. It also translates some of the transaction information.

2.4.4 Landis & Gyr PISCES Electricity Smart Card.

This is similar in operation to the Schlumberger product. A smart card is used by the customer instead of a smart key. The hot list is known as a command message file, and each message is distributed to a target set of up to three terminals. The host assembles command messages for each terminal before distribution.

The host translates some of the tariff and update list file information to the terminal format before distribution. It also translates some of the transaction information.

2.4.5 British Gas Quantum

British Gas issues smart cards to its customers. The card carries value and tariff information to a meter, and meter readings back to the transaction terminal. The transaction is very similar to the magnetic stripe card, except that the terminal updates the card with new tariff information and the money value of the transaction. The transaction information is passed to the client, and new tariff information is received from the client.

The product also includes hot lists. The hot list is received from British Gas and is distributed to terminals. The hot list comprises messages and actions targetted at specific customers. When a smart card is inserted in a terminal, the terminal will apply the action or message to the card if the card is identifed as relating to the customer. The card in turn will apply the action or message to the meter when the card is inserted in the meter.

2.4.6 Electronic Stop Notice System

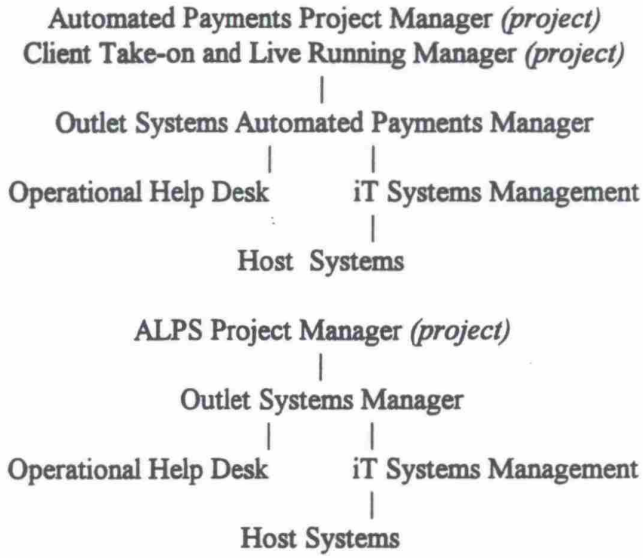
This is a benefits payment product, rather than an inpayment product. Each customer has a benefit book with a bar code on the front cover. The bar code is read at the terminal to identify the customer. The bar code information is checked against a stop list to see whether the payment can be made, or the book retained for dispatch to the Benefits Agency. A transaction record is created, but no financial information is captured.

Each night the host polls the transaction information for onward dispatch to the Benefits Agency computer. The stop list is updated each night from a file received from the host.

2.5 Current Management Organisation

Currently, the POCL systems are managed from within the Automated Payments and ALPS projects. The reporting structure is as follows:

POL00028135



2.6 Automated Payments Volumes and Profiles

2.6.1 Transaction Volumes (based on 1995 projections)

Total annual volume	125 million growing to 200 million
percentage through APT terminals	75%
percentage through ECCO+ offices	8%
percentage through ALPS	?%
percentage through DPC	17%
percentage magnetic stripe product	85%
percentage smart key	5%
percentage WATERCARD	5%
percentage PISCES smart card	5%

annual peak week	3% of annual volume
weekly peak day	32% of week

2.6.2 Average sizes

File sizes (kbytes)

APT program file	115
Smart key attention list	max 60
Smart key tariff file	max 5
WATERCARD update list	45
WATERCARD tariff file	0.4
PISCES command message file	50
PISCES tariff file	0.2
Reference data files (total)	1

POL00028135

Transaction record sizes (bytes)

	From poll	To client
Magnetic stripe card	59	107
Smart key	206	201
WATERCARD	338	285
PISCES	115	147

2.6.3 Terminal network

8000 APTs in 5000 offices, each APT polled
680 ECCO+ offices, each office polled
25% of terminals polled in early phase
1 DPC polled in early phase

2.6.4 Clients

10 clients growing to 20
4 clients using Kilostream/ISDN links
largest client transmission 200,000 transactions a day average
5 transmissions before 08.00 growing to 10
1 transmission completed by 07.30 to finance system

effective transfer rate for PSTN	920 txns/minute
effective transfer rate for Kilostream/ISDN	3500 txns/minute

2.7 Benefits Agency Volumes and Sizes

2.7.1 Transaction Volumes (average daily)

To Benefits Agency

Encashments	2,000,000
Stop transactions	4,000
Receipts	200,000
Issues	200,000

From Benefits Agency

Stops, recalls, expiries	18,000
Weeds	18,000

2.7.2 Transaction record sizes (bytes)

To Benefits Agency	52
From Benefits Agency	20

2.7.3 Terminal network

POL00028135

1500 offices in London area, both Branch office and SPSO. Two polls daily:

- BA upload and all AP 22.00-01.00
- BA download 03.30-06.30.

2.7.4 Client transmission

Stop list file received at 3am
Transaction file transmitted after 10am.

3. REQUIREMENTS

The requirements identified below must be satisfied in order that a service acceptable to POCL is provided. The requirements are grouped in the headings of the processes identified in section 2.1. Text in italics is for information to support the requirement.

3.1 Transaction Collection from POCL Terminal Network

Transactions are stored in files on the office terminals. Currently, there is one transaction file for each type of transaction (magnetic stripe card, WATERCARD, PISCES, smart key and ESNS).

For each terminal, a polling window will be established by POCL. The polling window may be a half hour window in the early phase, or it may be the regular phase window. To the terminal, the polling window will be identified in the terminal control reference data.

For the ALPS PC offices, there will be two polling windows each night.

Should it not be possible to collect transactions during the normal polling window, ad-hoc polling during the working day may be required. This may also be necessary if the office reports that the terminal has reached its capacity for transactions.

3.1.1 Transaction files must be collected from the APTs and ECCO+ systems according to the defined protocols.

3.1.2 Transaction files must be collected from the ALPS systems according to the defined protocols.

3.1.3 Each terminal must be polled in its defined polling windows. Up to three attempts must be made to achieve a successful poll. Only one successful poll must be established with any terminal in each of its windows. *An alternative strategy may be to propose the installation of dedicated lines in all offices, in which case polling may take place in a wider window. This strategy must take account of the need to distribute files received from clients (see 3.5.3).*

3.1.4 Terminals must be polled on Monday night through to Saturday night, except as indicated in 3.1.5.

POL00028135

3.1.5 Terminals will not be ready for polling on a Bank or other local holiday for the office in which the terminal is located. Polling need not be attempted to terminals on defined local holidays. In any case these attempts should not be counted as failures. APT and ECCO+ systems will not be polled on Saturday night.

3.1.6 In many offices, more than one terminal will share a telephone line. Terminals will answer poll calls in the order of their terminal numbers. Any retry strategy for failed polling must take into account the need to maintain this order.

3.1.7 A poll success rate of 97% must be achieved for 99% of normal polls.

3.1.8 Polling of individual terminals during the working day must be possible. This must be initiated by the polling service if a terminal has not been polled successfully on two successive nights. The time of poll will be agreed with the outlet.

3.1.9 Should an office report that a terminal has reached its capacity to the POCL operational help desk, the help desk will request that the service initiate a poll of the terminal. This poll must be initiated within 1 hour, following agreement with the outlet.

3.2 Transaction Collection from Document Processing Centre

3.2.1 Transaction files must be collected from the DPC according to the protocols defined in ref. 1.5.2.

3.2.2 The DPC must be polled on Monday night through to Friday night, excepting Christmas Day, Boxing Day and New Year's Day only.

3.2.3 A poll success rate of 99% must be achieved.

3.3 New Software Distribution

POCL will prepare a new version of the software programs in the APT. Typically 4-6 new versions may be expected in a year. Currently, this service is required for APTs only. It may be extended to other platforms at a later stage however. For any platform, the software programs may be presented as one or more files.

3.3.1 An electronic communication or magnetic medium link must be established for the receipt of new versions of software from POCL.

3.3.2 Following receipt of a new version of software programs for distribution, the software must be distributed successfully to all APTs in the managed network within 5 working days.

3.3.3 The previous version of software must be held ready for distribution as a contingency, should operational problems be experienced with the new version. If requested, the previous version of the software must be distributed successfully to all APTs in the managed network within 5 working days of the request.

3.3.4 Software must be distributed according to the identified protocols.

POL00028135

3.4 Reference Data Distribution

Reference data is used to determine the terminal's control characteristics, and to identify the clients for which POCL is providing a service at any terminal. New reference data is prepared for issue whenever a new client service is provided. Reference data may be supplied as one or more files.

3.4.1 Following receipt of a new version of a reference data file for distribution, the file must be distributed successfully to all APTs and ECCO+ offices in the managed network within 5 working days.

3.4.2 The previous version of the file must be held ready for distribution as a contingency, should operational problems be experienced with the new version. If requested, the previous version of the file must be distributed successfully to all APTs and ECCO+ offices in the managed network within 5 working days of the request.

3.4.3 Reference data files must be distributed according to the identified protocols.

3.5 'Hot list' and Tariff File Distribution

Hot list, update and tariff files are received from the client for distribution to a defined target set of terminals. Typically, new tariff files are available twice a year for each client. The tariff file is specific to a client. A new hot list file may be prepared each day for those clients using hot lists.

3.5.1 For each client providing hot list and tariff files, the files must be requested and received according to the protocols defined in the respective client interface specification. This specification also defines cut-off times for file reception.

3.5.2 For each Automated Payments hot list file and tariff file, the file must be processed and translated prior to distribution into the defined format for distribution.

3.5.3 For each new hot list or tariff file received, the file must be distributed to a target list of terminals during that night's polling phases. POCL will define the target terminal population for each client file to be distributed. POCL will also define the earliest window in which terminals are polled to which distribution must be achieved for any particular file. This will be related to the cut-off time in 3.5.1 above, and will be no less than half an hour after the cut-off time.

3.5.4 Hot list and tariff files must be distributed according to the defined protocols.

3.5.5 For any client, the file reception must be successful on 97% of valid days.

3.5.6 The distribution success rate to be achieved is as for polling (see 3.1.6).

3.6 APT and ALPS Time Regulation and Clock Change

POL00028135

The APT and ALPS system times are controlled by the host system. There are no facilities on the APT for time change in the office.

3.6.1 The polling system must maintain an internal clock which is accurate to within one minute of local time (BST or GMT according to time of year.)

3.6.2 The polling system must ensure that all APTs and ALPS offices are synchronised with its time, according to the defined protocols.

3.6.3 The polling system must maintain a clock change file for APT standard time changes in the defined format.

3.6.4 The polling system must distribute the clock change file to all APTs no later than four weeks in advance of any clock change to which the file relates.

3.7 ECCO+ System Recovery

The ECCO+ system uses a recovery file to facilitate recovery following a system failure.

3.7.1 The ECCO+ recovery file must be collected from all ECCO+ offices, and ALPS offices providing AP within ECCO+ functions, in the polling network during every polling session, according to the defined protocols.

3.7.2 On request from POCL, a recovery file for a specific office must be downloaded at an agreed time during the day. The service commitment must be to guarantee that this may be within 1 working hour after the request.

3.8 New Terminal Support

From time to time POCL will introduce automation to new offices, or add terminals to existing offices. An installation and training coordinator will commission the terminal in the office and coordinate the loading of new software and reference data. The details of the office and terminal, including services to be offered, will be made available normally at least two weeks prior to the commissioning.

3.8.1 Following a request from POCL, software and reference data for the new terminal must be prepared.

3.8.2 On request from the installation coordinator on the agreed installation date, the prepared software and reference data (see 3.8.1) must be downloaded to the new terminal within 30 minutes of the request.

3.8.3 On request from the installation coordinator, a poll of test transactions will be initiated, within 30 minutes of the request. These test transactions will be distinguishable from client transactions, and must be discarded.

POL00028135

3.8.4 The new terminal must be added to the nightly polling schedule in the window previously agreed with POCL, and be polled from the night of the installation date onwards.

3.8.5 During the initial contact with the installation coordinator at the office, a terminal serial number will be provided for recording in the polling system for later use in terminal authentication. The terminal serial number must be recorded in the system prior to any poll of test or live transactions.

3.9 Terminal Replacement Support

From time to time, terminals may fail in offices. They will be replaced under a maintenance contract with a third party within 8 working hours.

3.9.1 Following a terminal failure requiring replacement, the details of the replaced terminal must be removed from the polling schedules, and the details of the new terminal added.

3.9.2 Support for the commissioning of the new terminal must be provided as in 3.8.1 to 3.8.5 above.

3.10 Collation of Client Transactions

Transactions collected from the various office platforms and the DPC will be for a number of different clients and services. In order to prepare for transmission of transactions to clients in batched files the transactions must be sorted by client.

3.10.1 All transactions collected from the APTs, ECCO+ and ALPS offices and DPC must be sorted by client into client files for later transmission (see 3.11), except where indicated in 3.10.2. Any transaction collected must appear only once in a client file.

3.10.2 For magnetic stripe card transactions, reversed and reversing pairs of transactions must not be placed in client files. Test transactions, identified as relating to test clients, must not be placed in client files.

3.10.3 The transactions must be arranged in the client files in the order specified in the relevant client interface specification. *Generally, no sorting is required.*

3.10.4 Where it is not possible to identify the client, the transaction will not be placed on a client file (but see 3.13).

3.10.5 Files must be assembled in order to satisfy any timing requirements for transmission. For some clients, more than one file may be prepared and dispatched each day. If only one file is required, it must contain all transactions for the client collected overnight. If more than one file is required, all transactions must be contained in the set of files for that night's processing. *Generally, only one file will be required. Where more than one file is required, it is to achieve an earlier delivery of some transactions to facilitate client processing. The target for any earlier delivery will be defined in the interface specification. It is anticipated that only two clients will require more than one daily transmission.*

POL00028135

3.11 Onward Transmission to Clients

Generally, client files are dispatched to clients using communication links (PSTN or Kilostream/ISDN). For every client, POCL will agree an interface specification which forms part of the contracted service that POCL provides to the client. Some transmissions are timed to reach clients before the start of their day for customer service reasons. Others may be timed to reach the client before overnight batch processing.

3.11.1 Client files must be delivered to clients according to the protocols defined in the relevant interface specification.

3.11.2 Client files must be delivered to clients to the timings defined in the relevant interface specification.

3.11.3 Retransmissions following failures must be effected according to the procedures stated in the relevant interface specification.

3.12 Service Agreement Reporting

Service agreement reporting is required to demonstrate to POCL that the service standards expected are being met. This applies not only to standards specified within this document, but also to standards required to meet client contractual commitments.

3.12.1 A daily reconciliation report must be produced to show transaction volumes for all collections and client transmissions since the last report. The report must include all transactions for which no client is identified, and show reversed and reversing pair volumes not delivered to magnetic stripe card product clients.

3.12.2 Daily reports must be produced to show that requirements for service specified in earlier sections are being met.

3.12.3 For each client, a report must be produced daily showing transaction volumes by source (APT, ECCO+, ALPS, DPC) and by age (day B, day C, etc.) based on transaction date related to transmission date to client.

3.12.4 For all client transmissions, a report must be produced to show the performance of client transmissions. This report will give date and time of all transmissions whether successful or not.

3.13 Client Transaction Transmission to POCL Accounting Centre

3.13.1 Details of all Automated Payments transactions must be transmitted to the POCL accounting centre mainframe, according to the defined. This includes all reversed and reversing transactions, and all transactions for which a client cannot be identified.

3.13.2 Transmissions must be achieved to the specified timings.

POL00028135

3.13.3 Retransmissions following failure must be effected according to the stated procedures.

POL00028135

Appendix 4-10

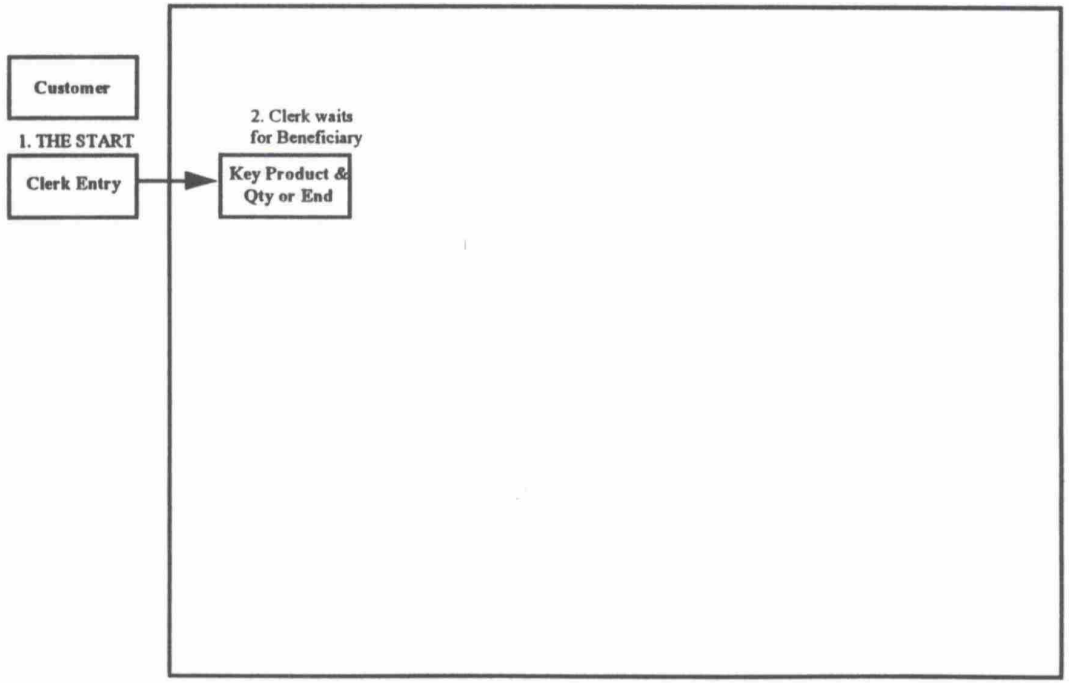
Exemplar Transaction Data Flows

POL00028135

The following 12 pages describe how the EPOS transaction will be used for Benefit Payment.

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

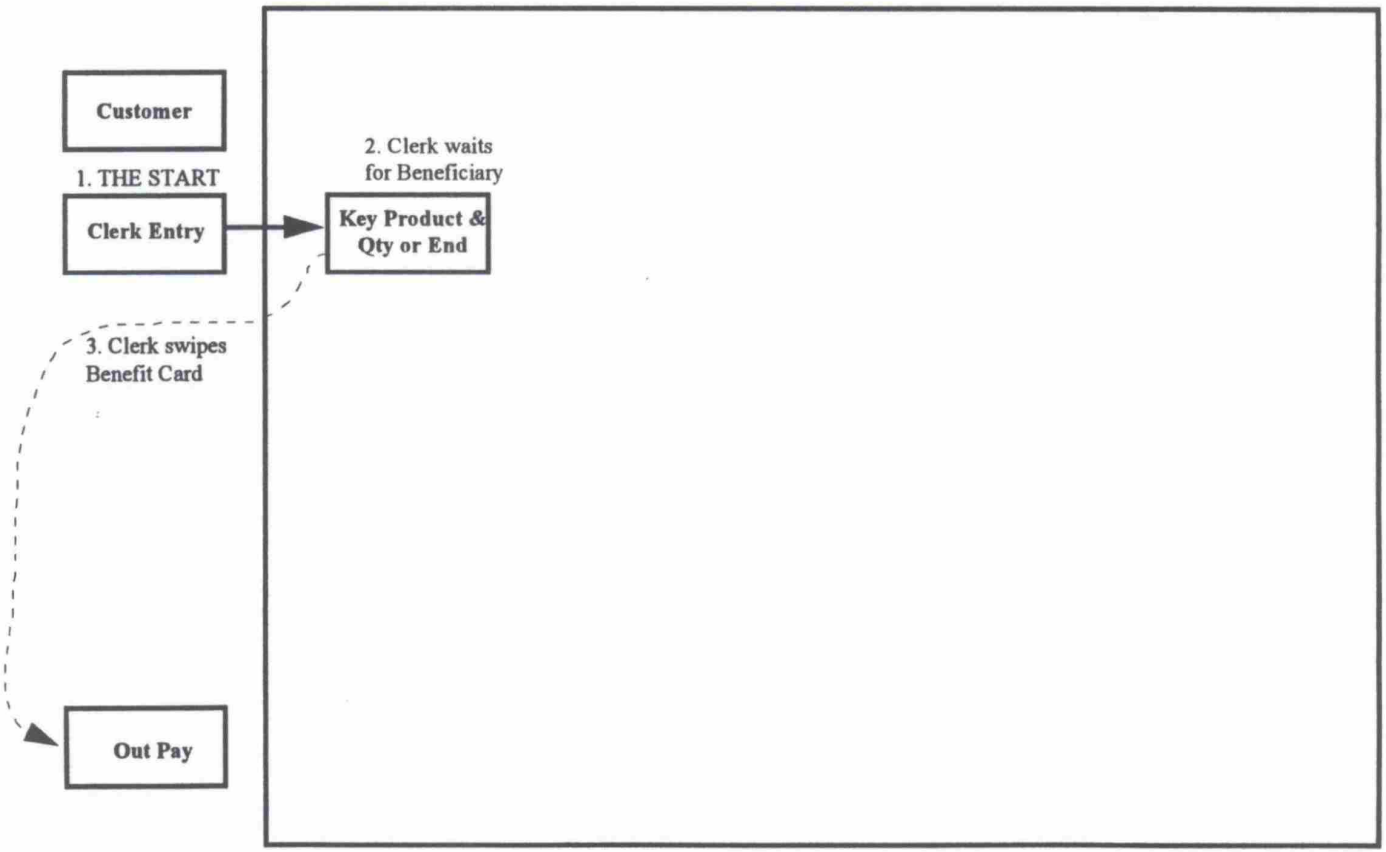
Basic EPOS Transaction



POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

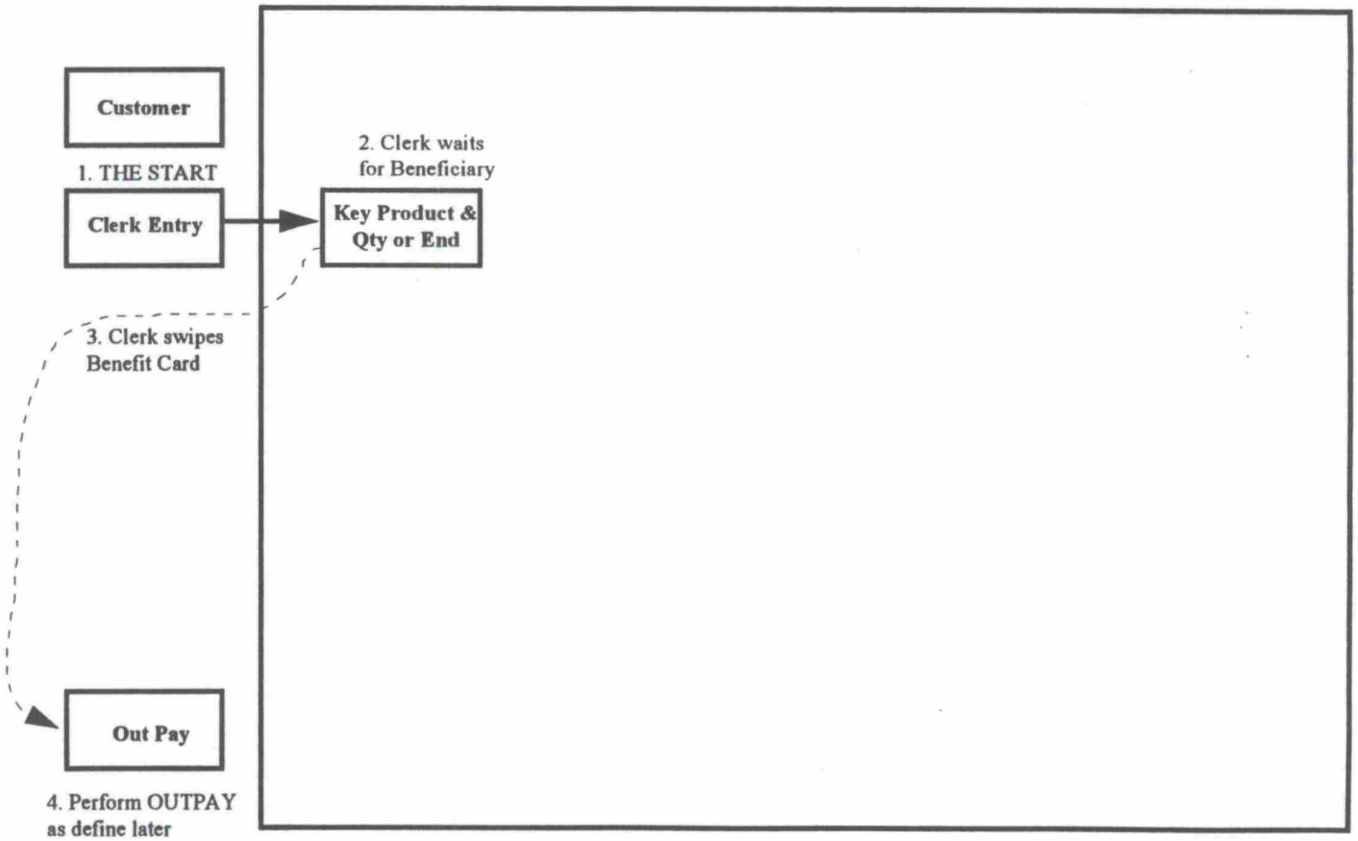
Basic EPOS Transaction



POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

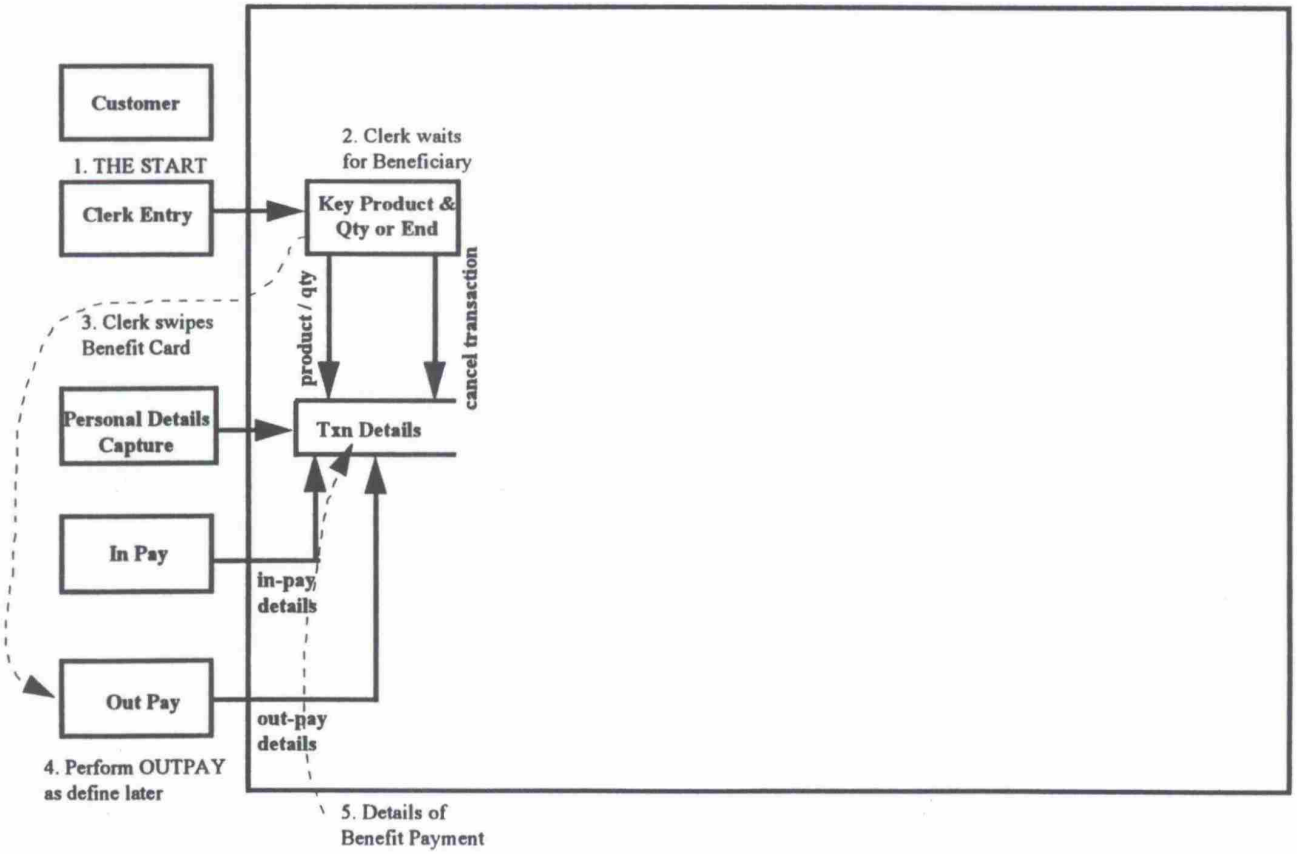
Basic EPOS Transaction



POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

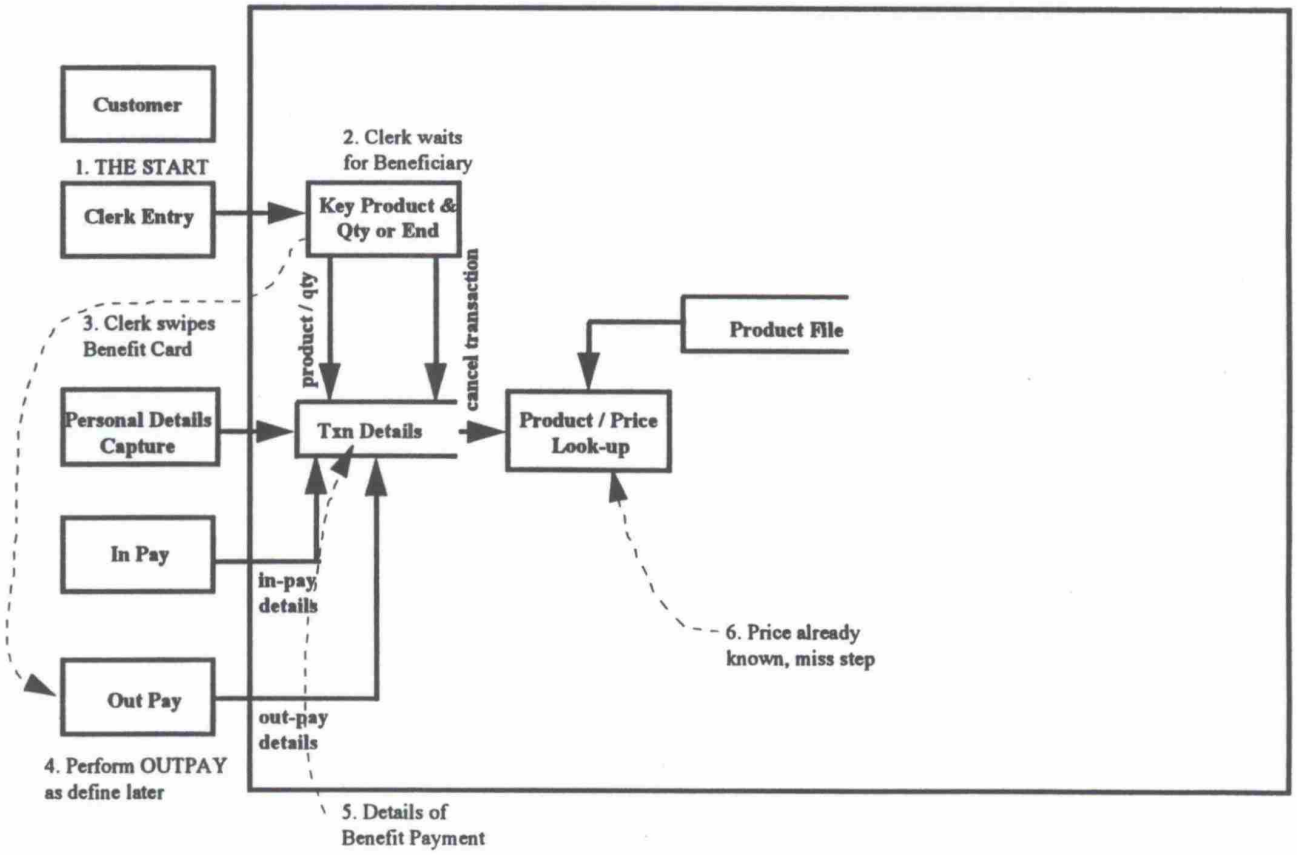
Basic EPOS Transaction



POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

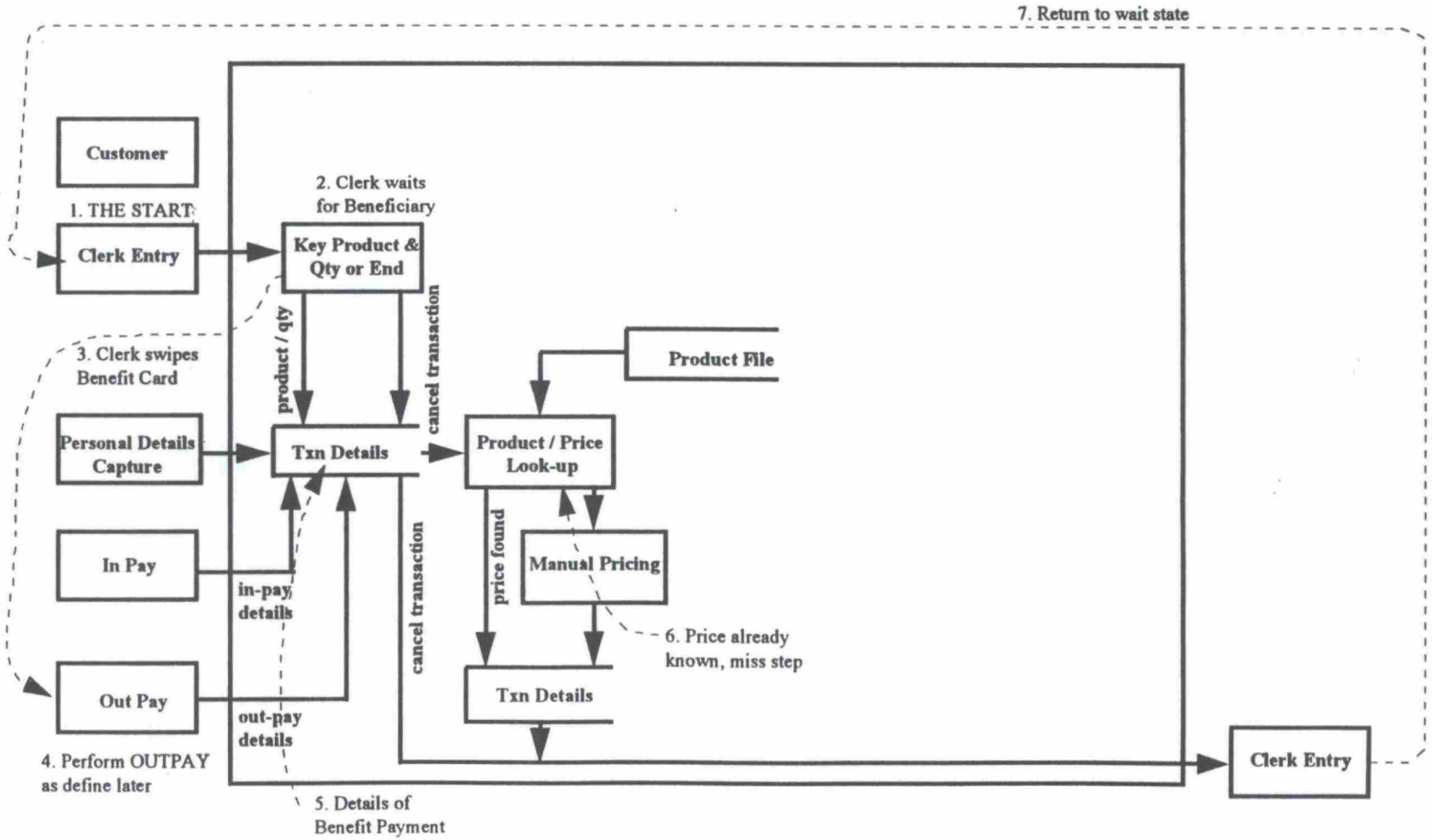
Basic EPOS Transaction



POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

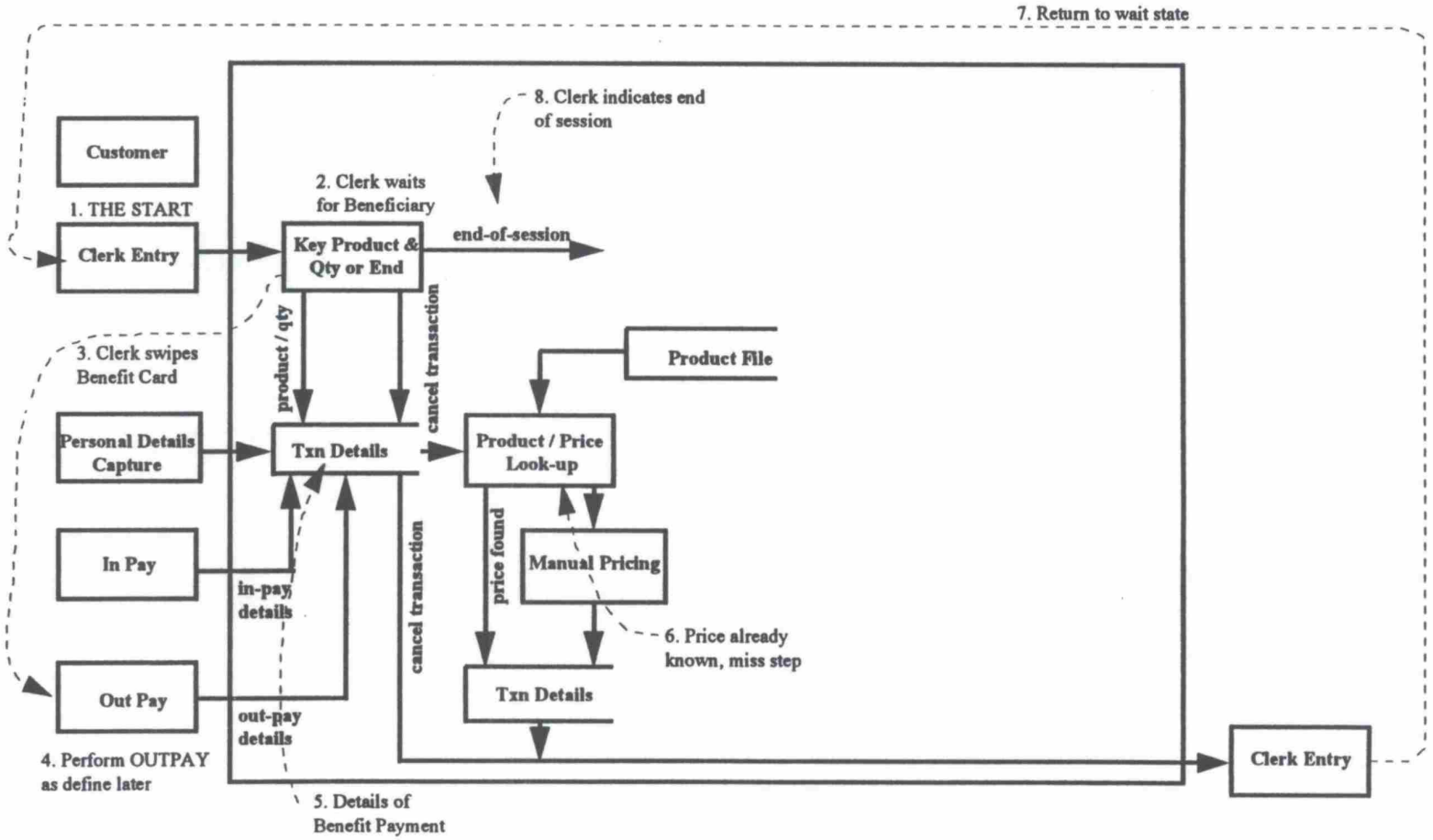
Basic EPOS Transaction



POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

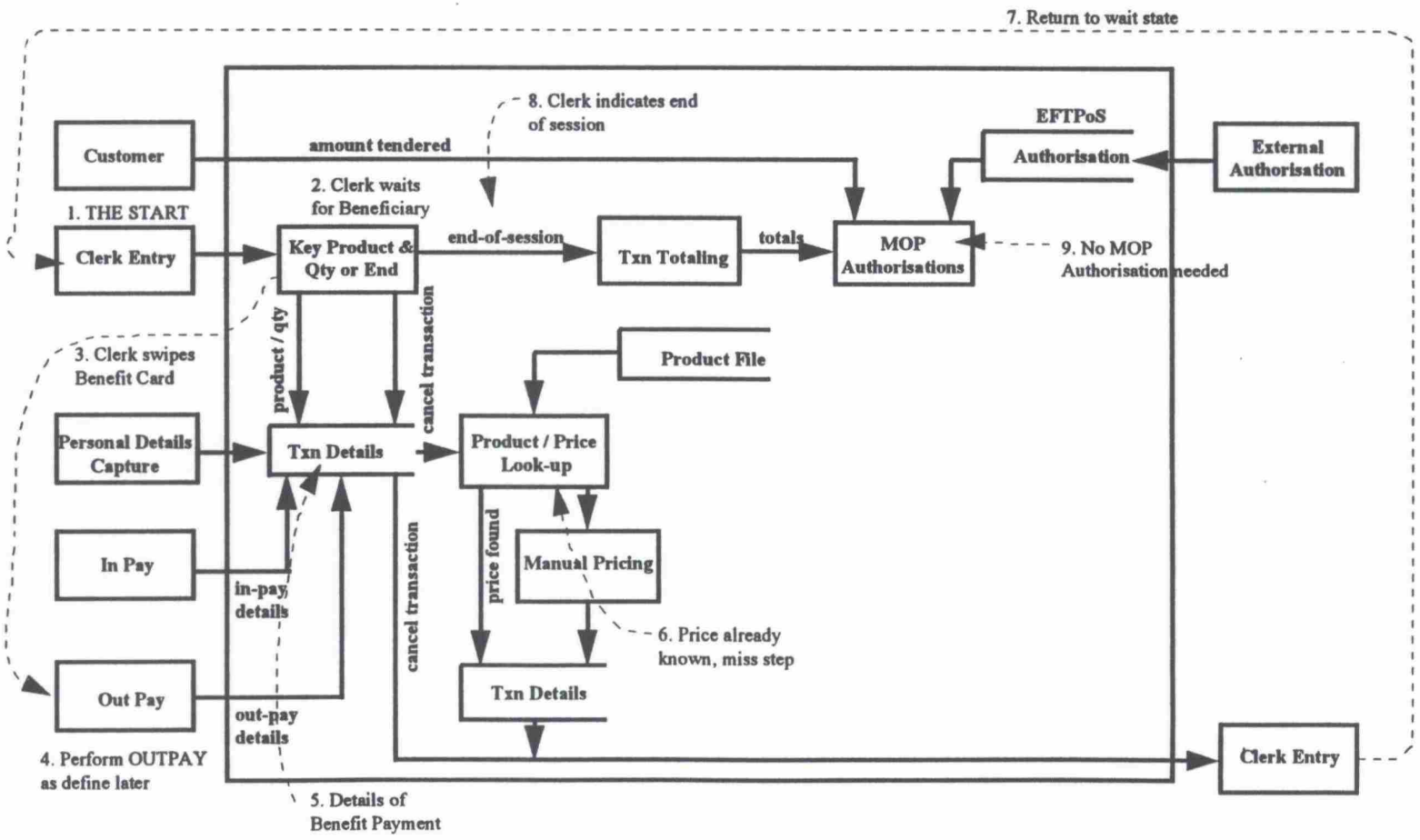
Basic EPOS Transaction



POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

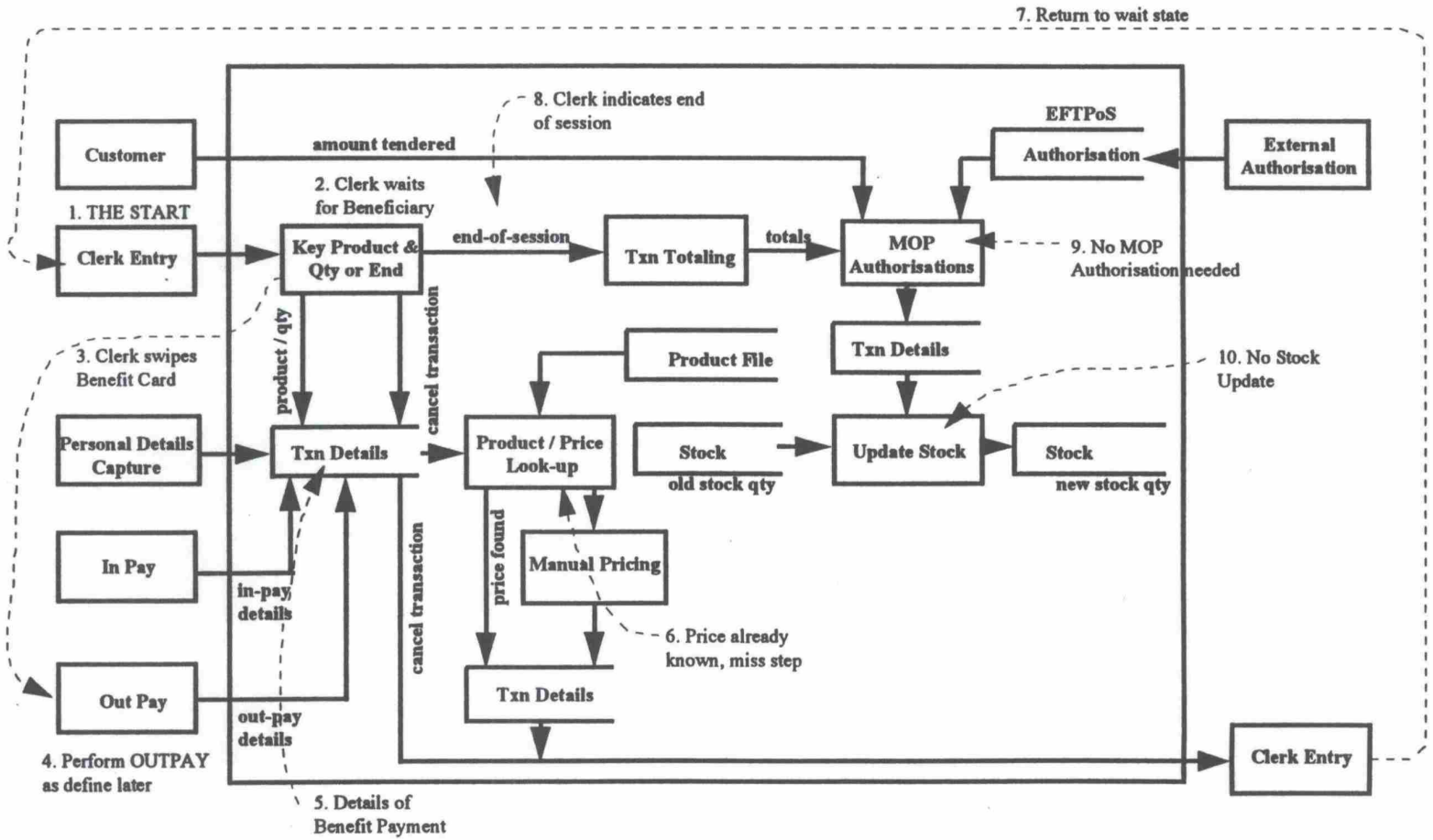
Basic EPOS Transaction



POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

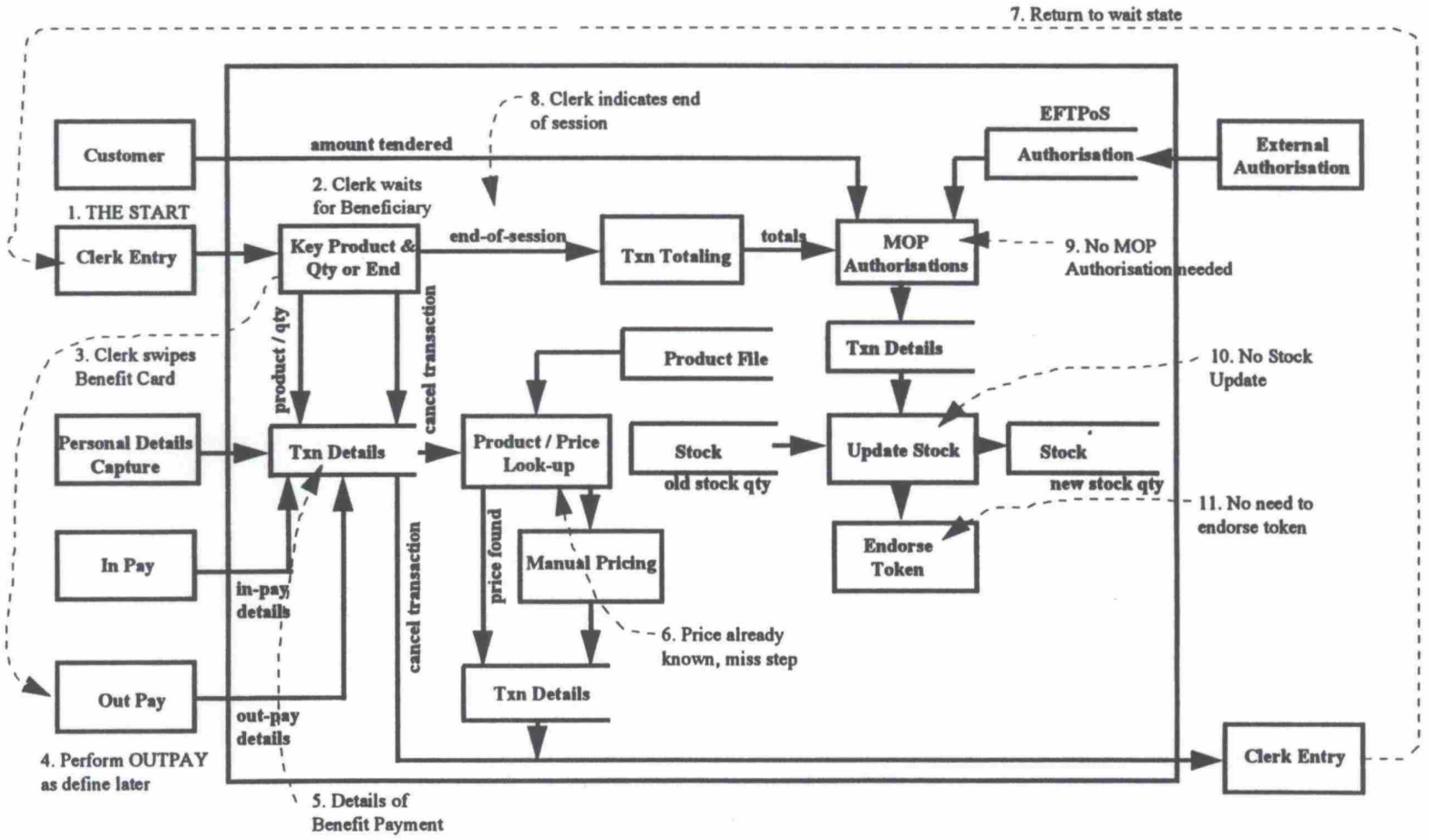
Basic EPOS Transaction



POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

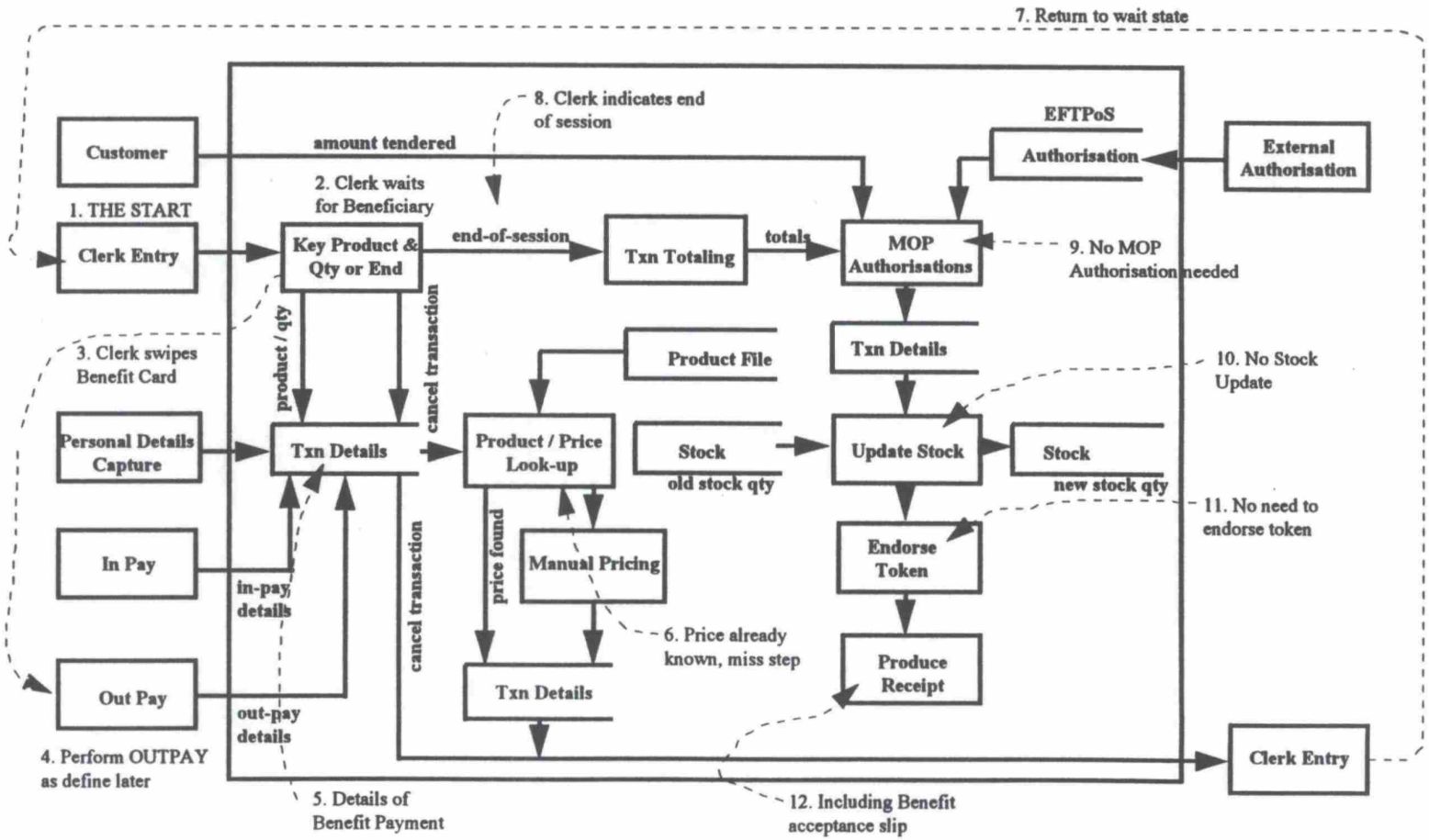
Basic EPOS Transaction



POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

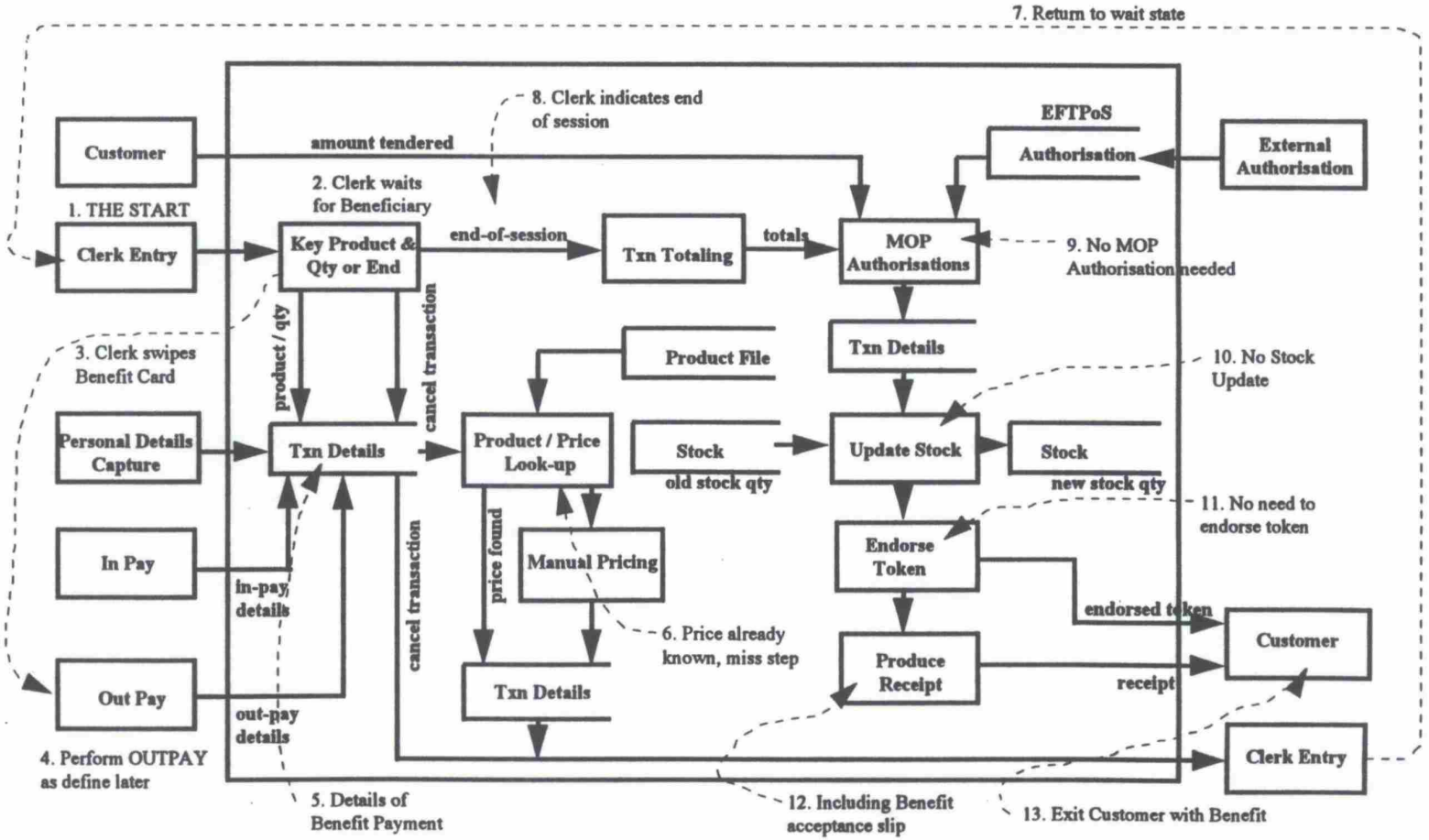
Basic EPOS Transaction



POL00028135

FOLLOW NUMBERED COMMENTS
TO UNDERSTAND BENEFIT PAYMENT COLLECTION

Basic EPOS Transaction

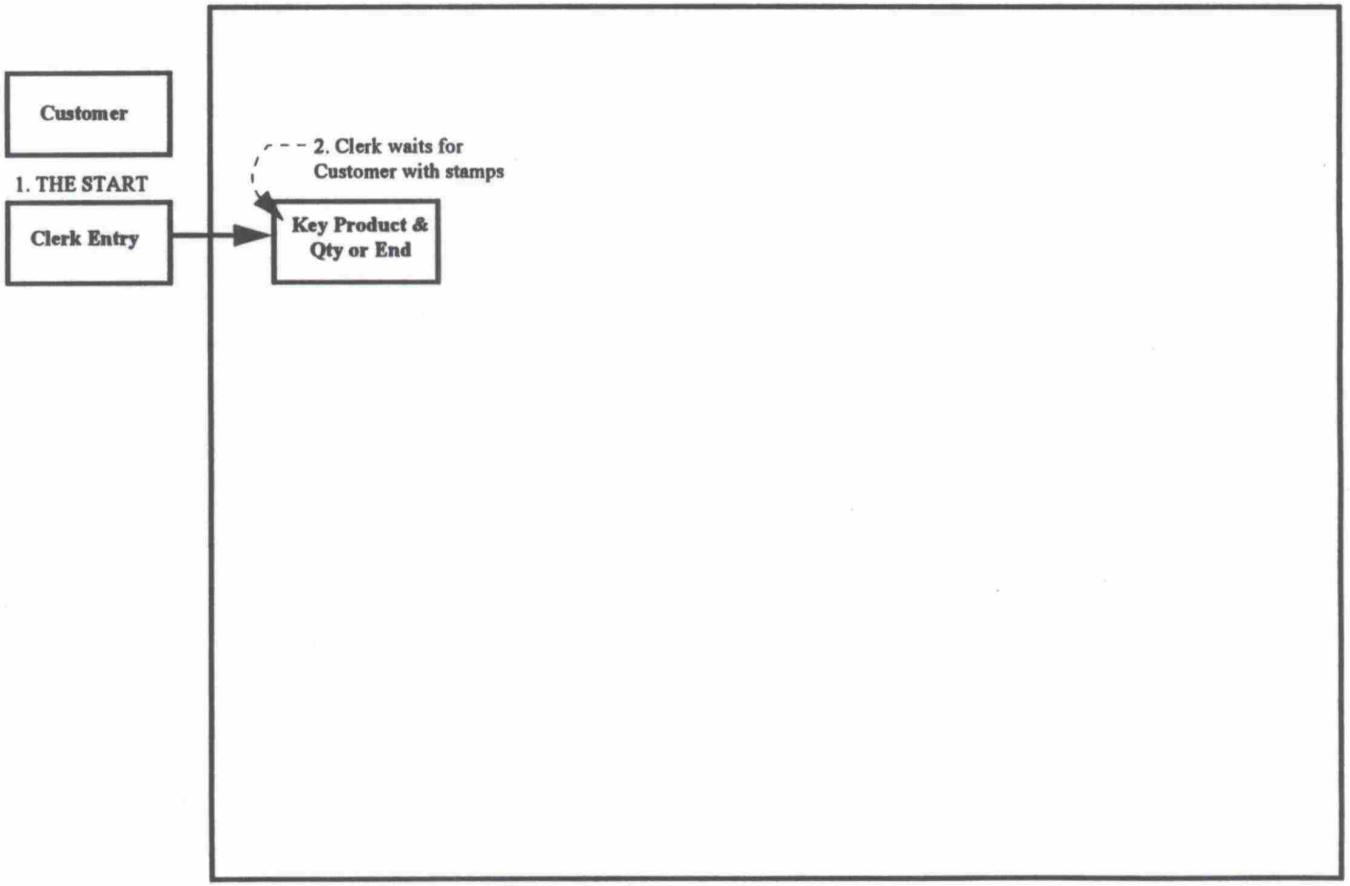


POL00028135

The following 13 pages describe how stamps, as an example, would be sold through the EPOS Generic Transaction.

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE

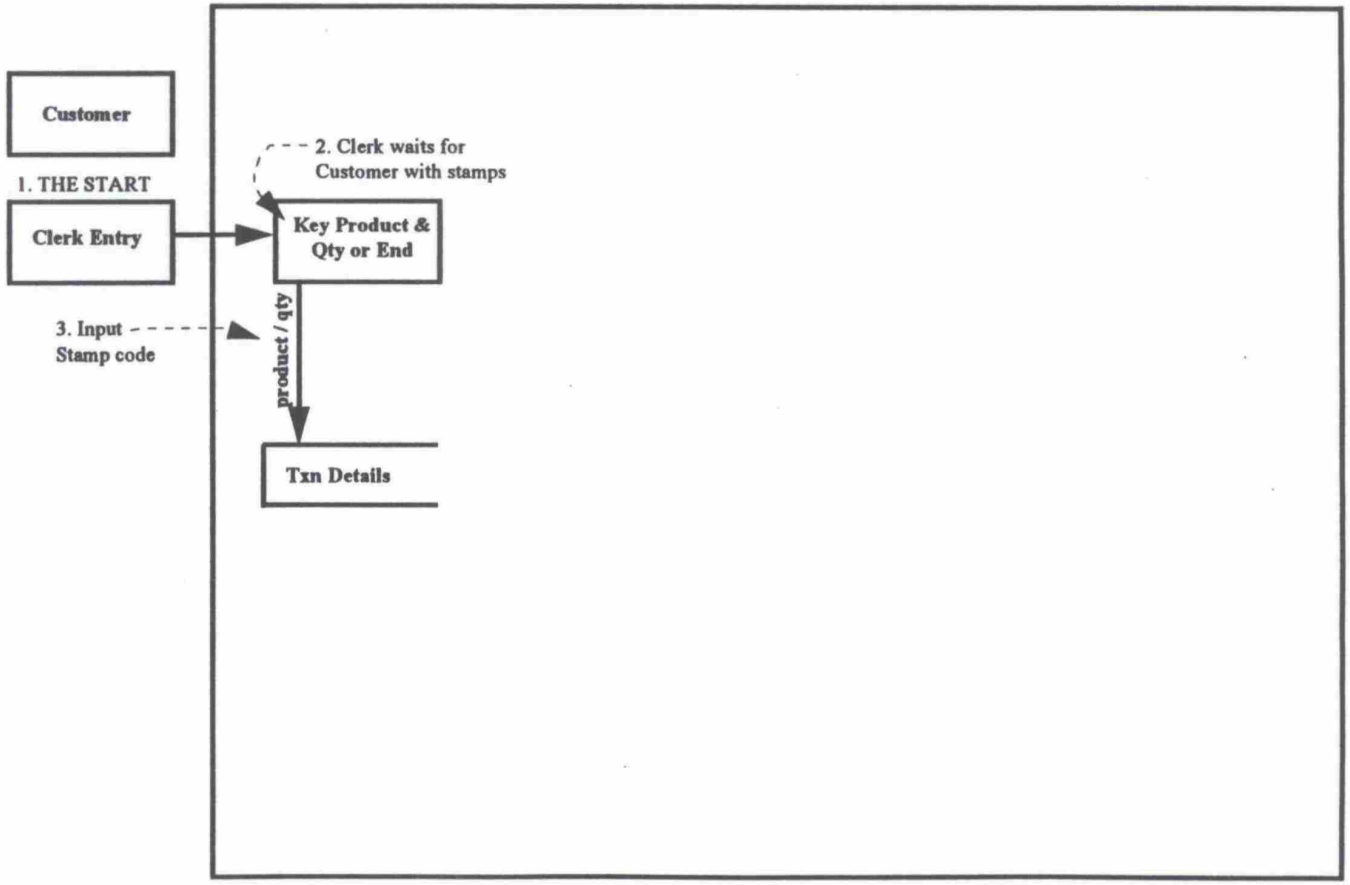
Basic EPOS Transaction



POL00028135

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE

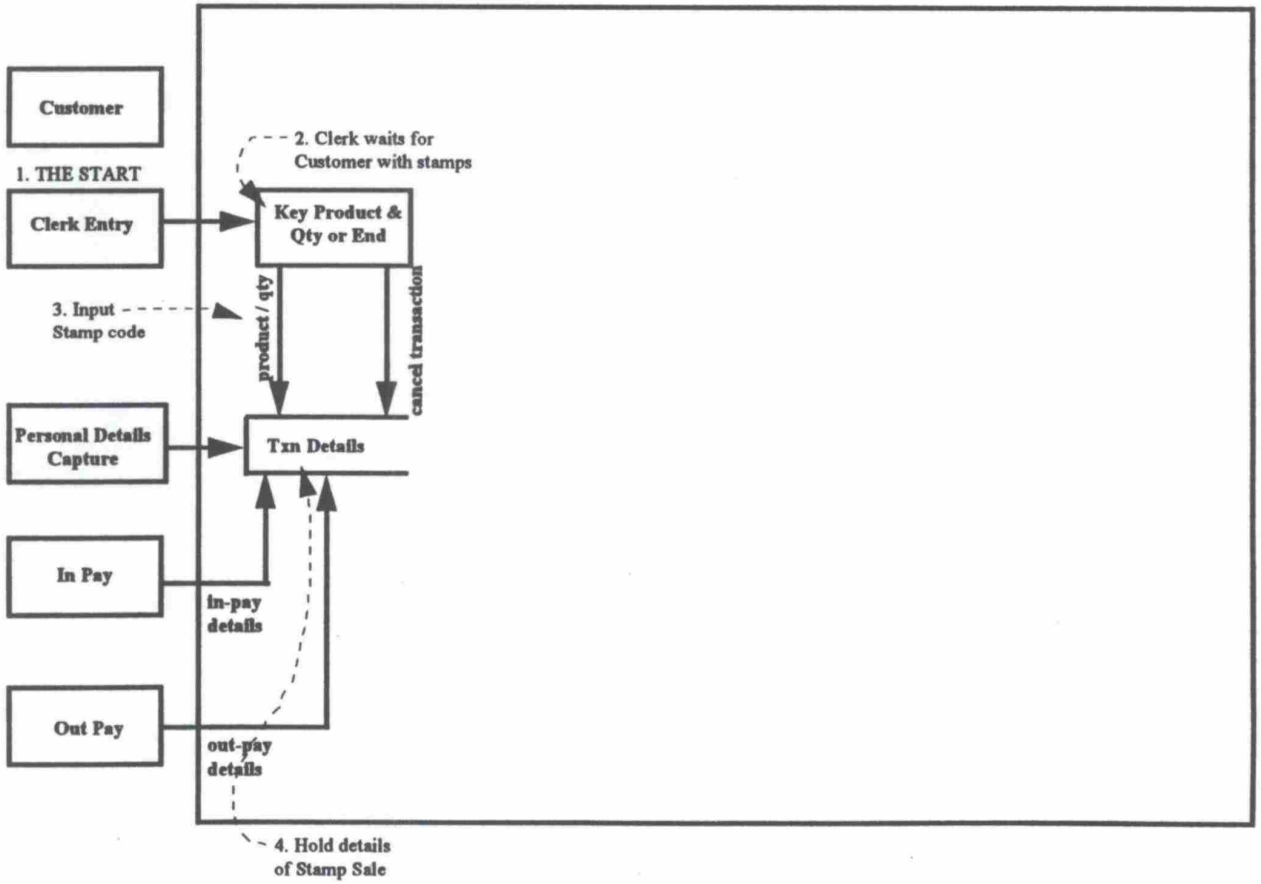
Basic EPOS Transaction



POL00028135

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE

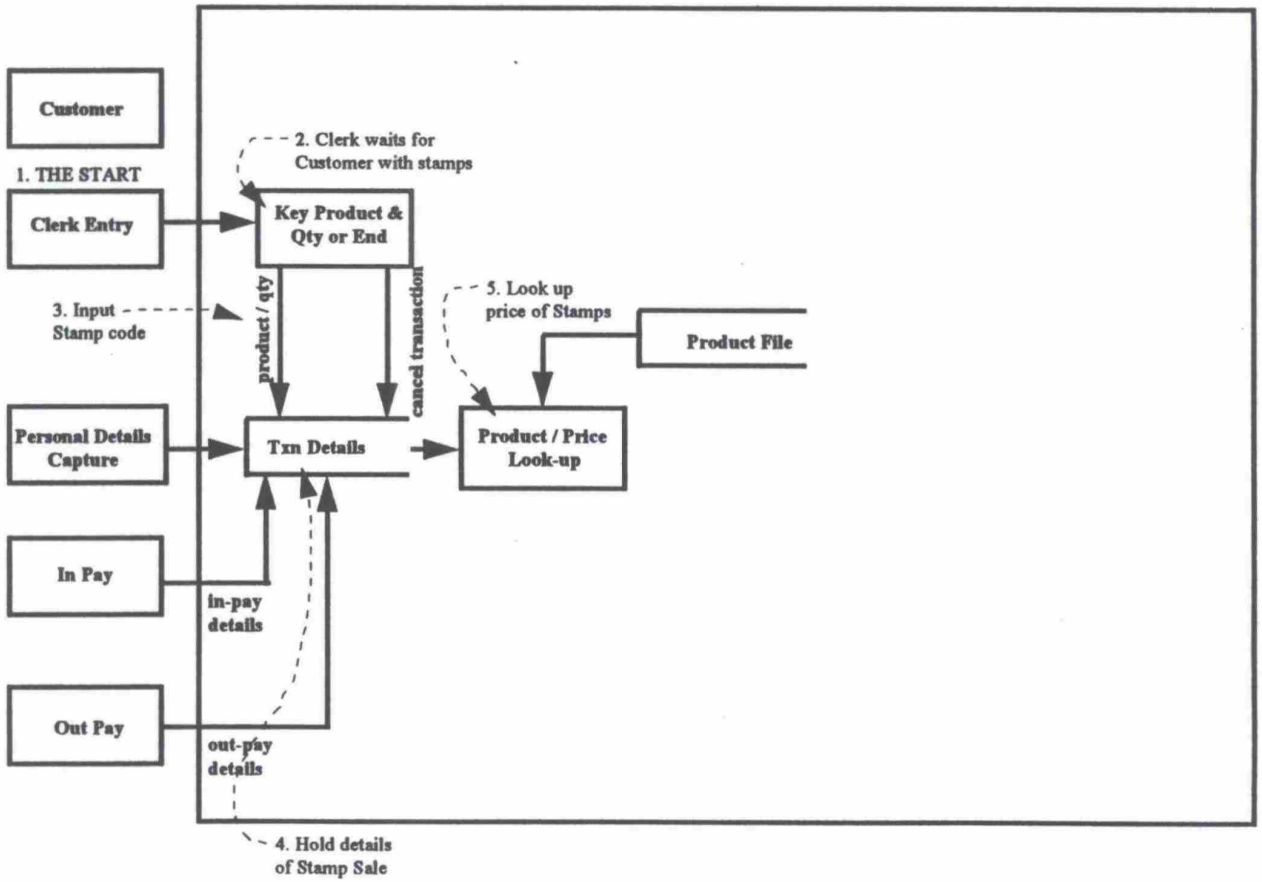
Basic EPOS Transaction



POL00028135

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE

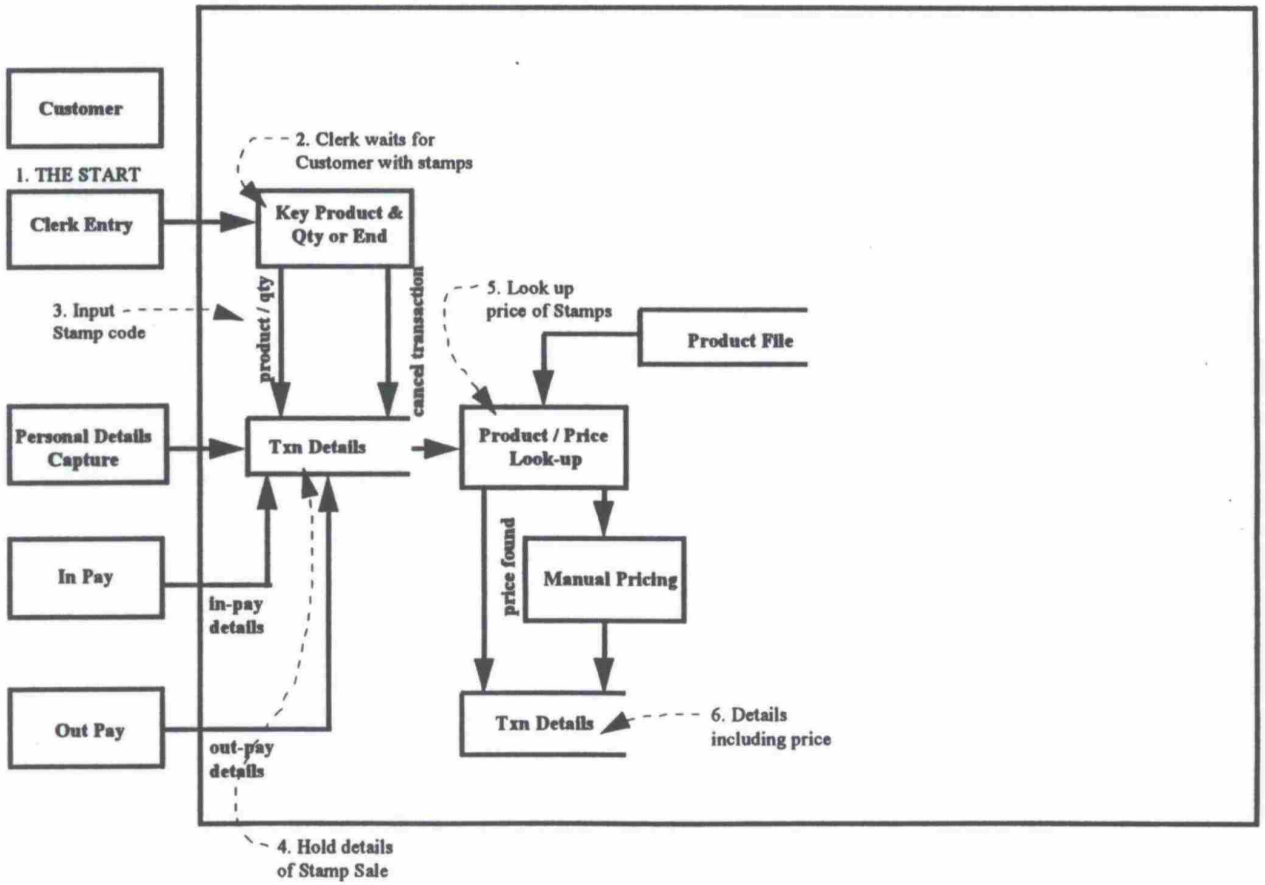
Basic EPOS Transaction



POL00028135

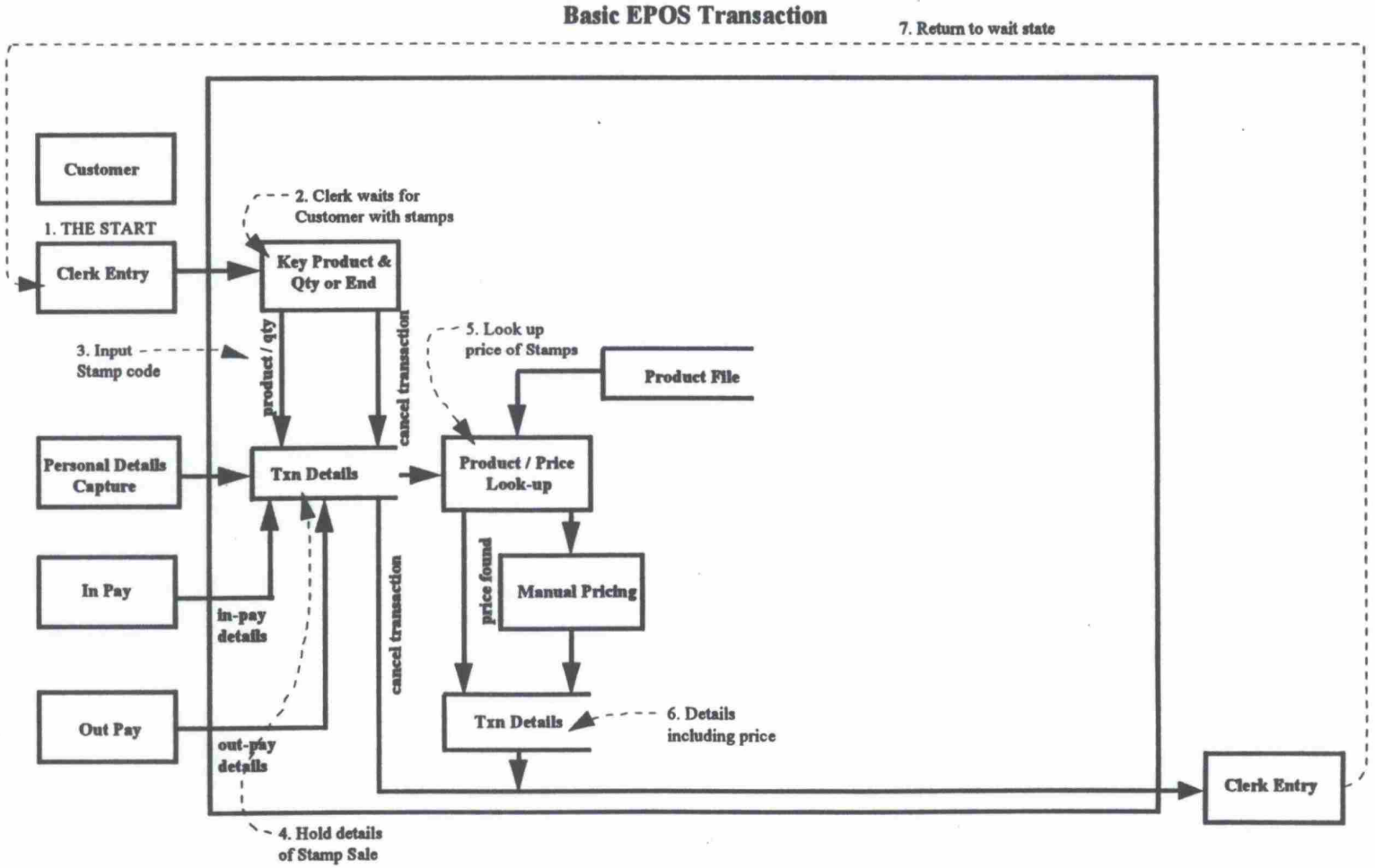
FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE

Basic EPOS Transaction



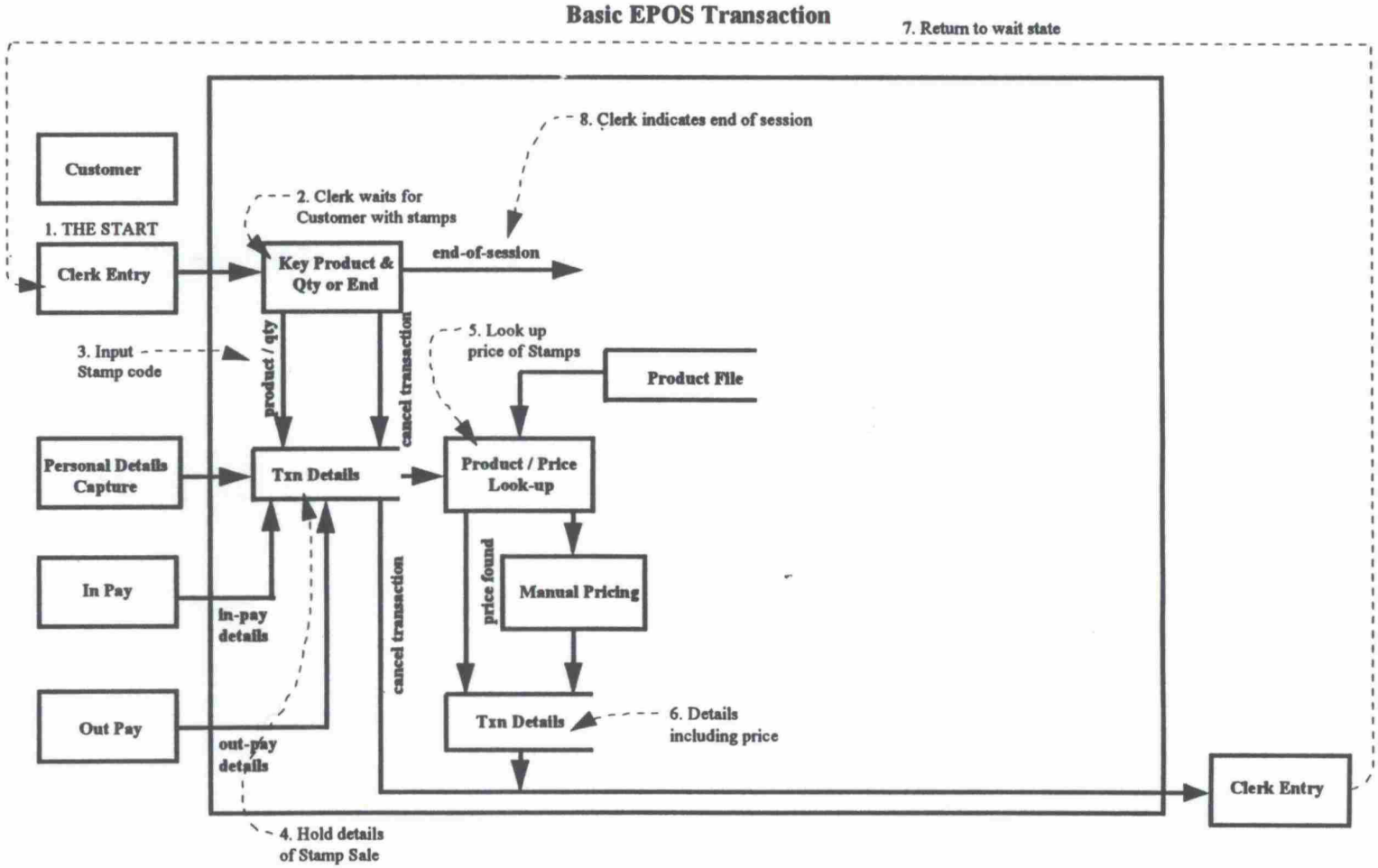
POL00028135

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE



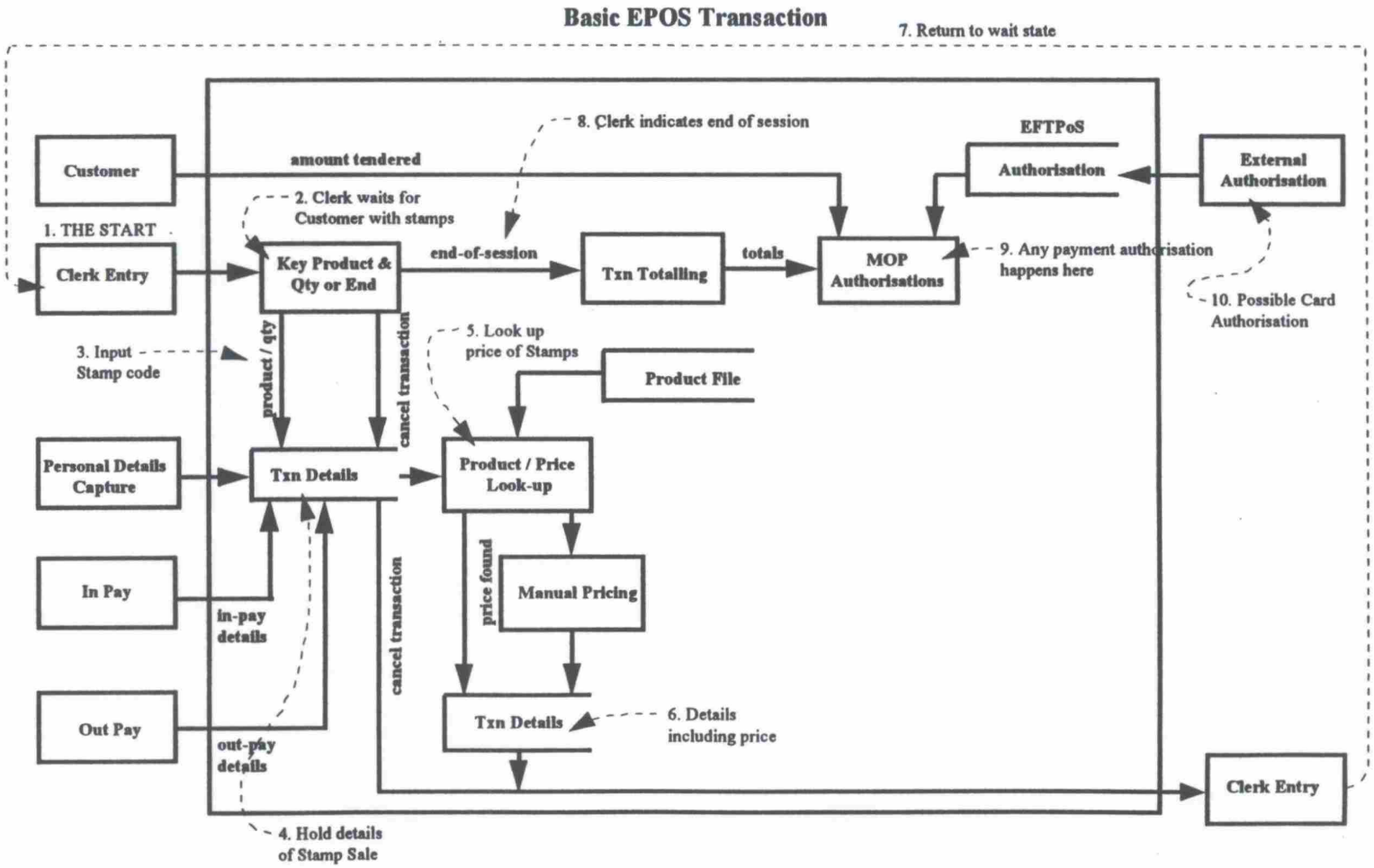
POL00028135

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE



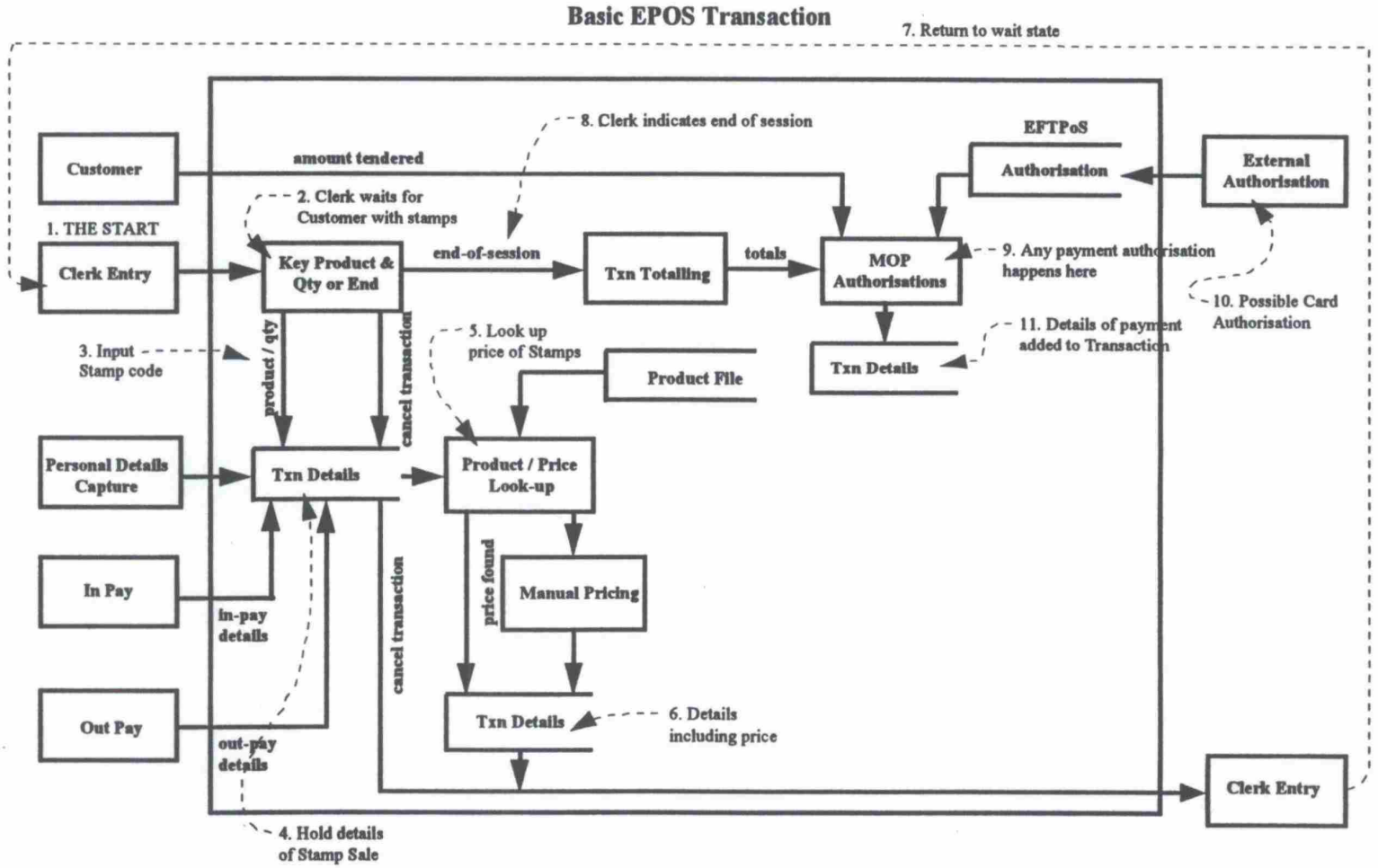
POL00028135

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE



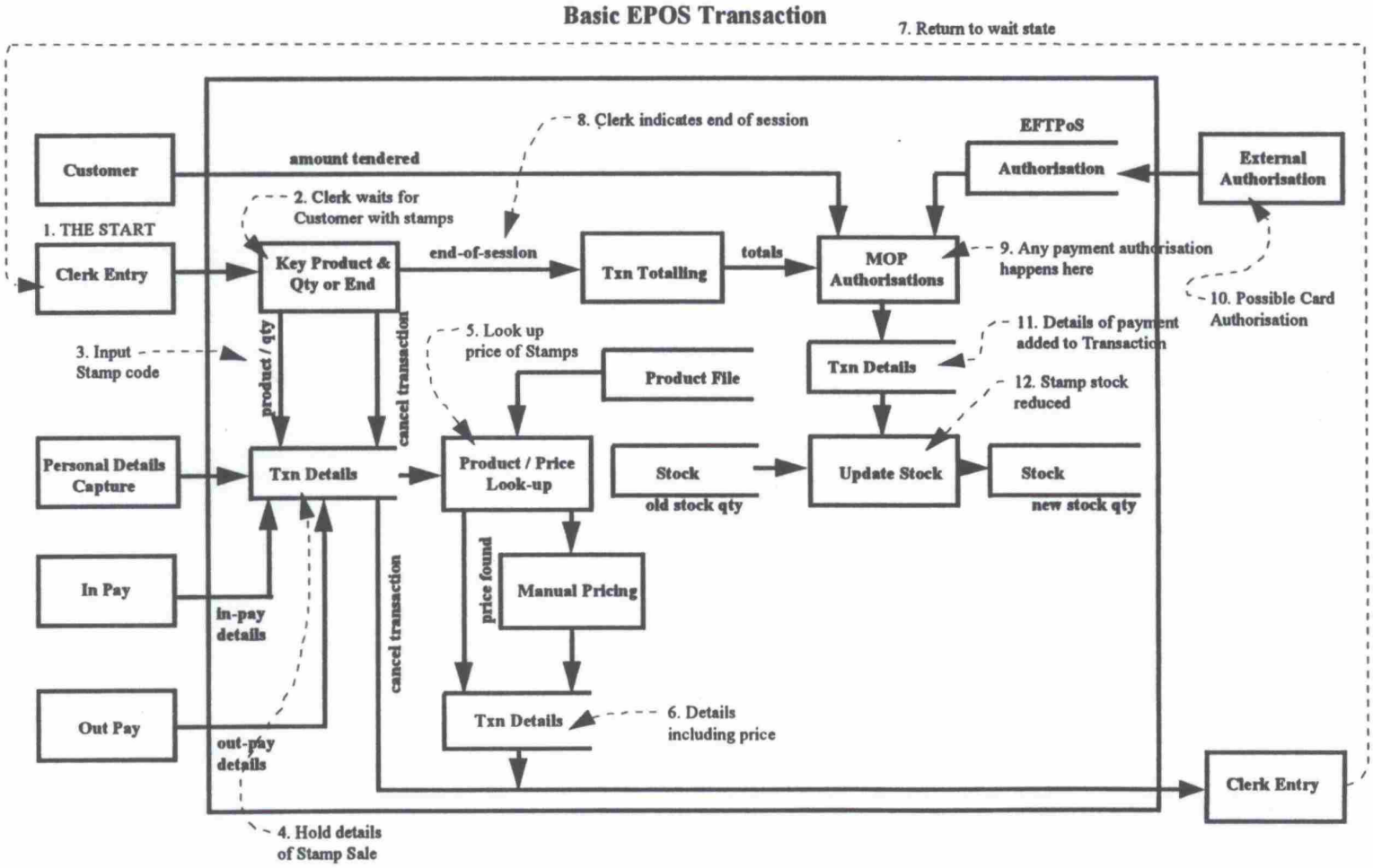
POL00028135

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE



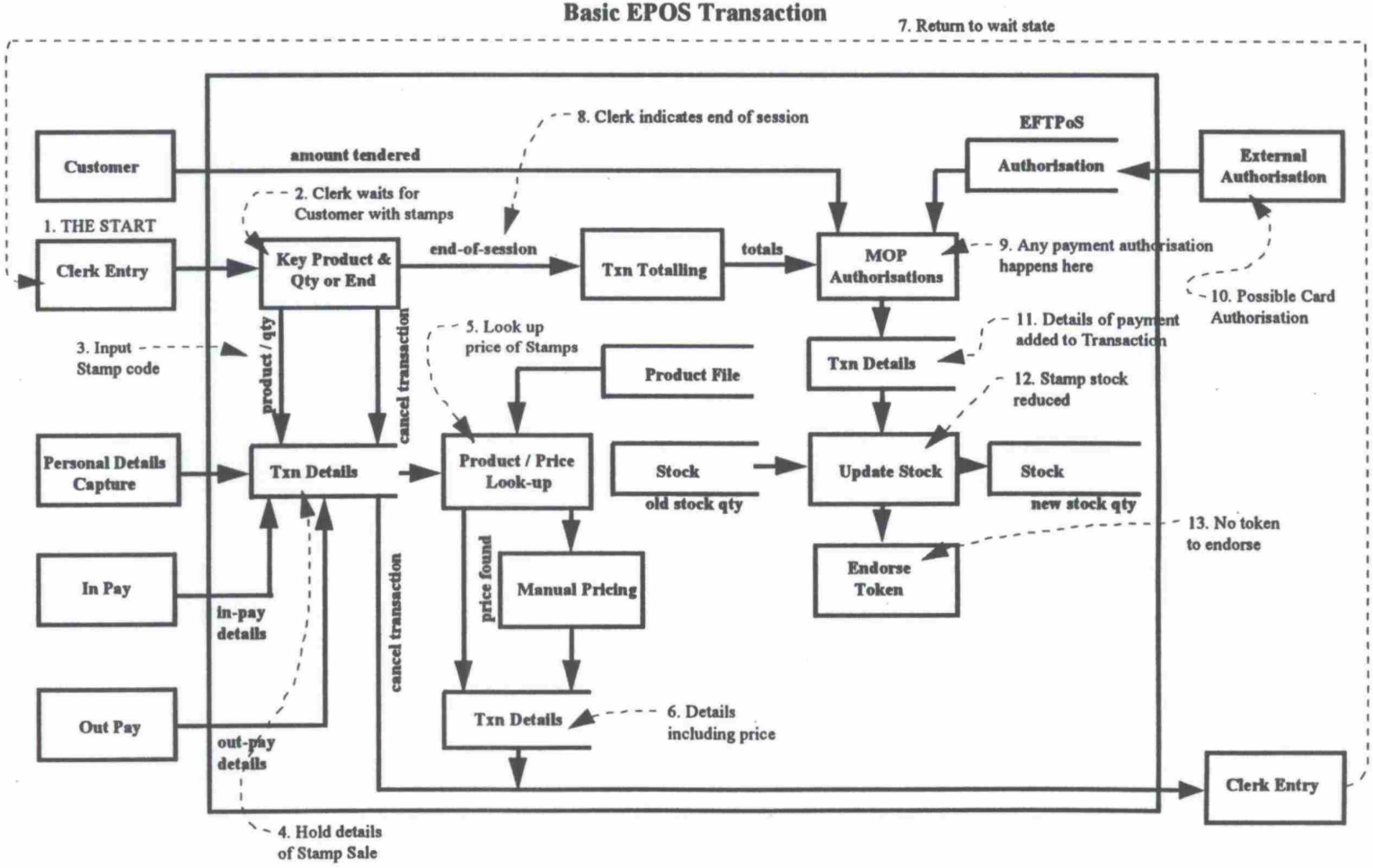
POL00028135

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE



POL00028135

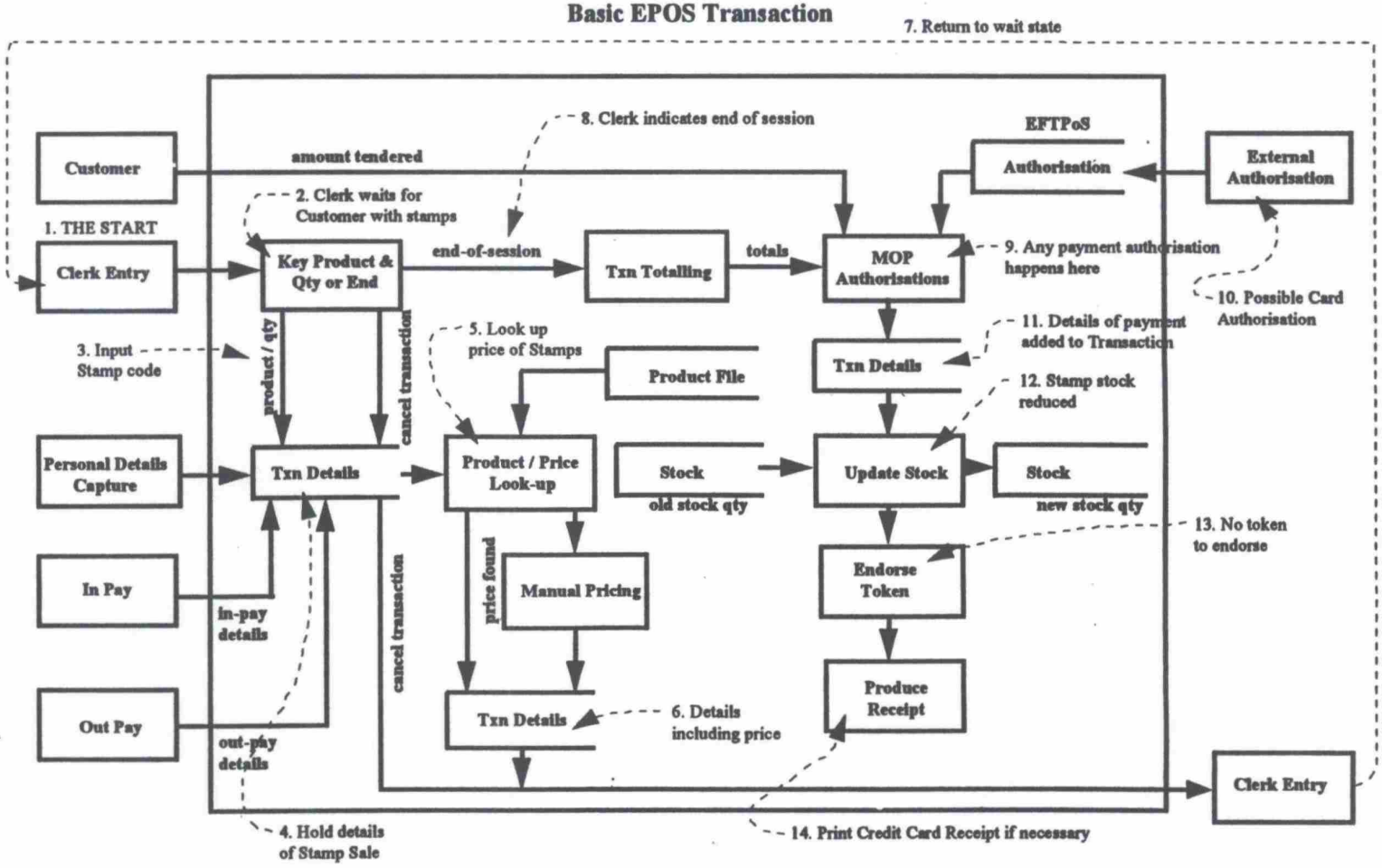
FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE



POL00028135

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE

Basic EPOS Transaction



POL00028135

FOLLOW THE NUMBERED COMMENTS TO UNDERSTAND A STAMP SALE