Document Title: Horizon Architecture Overview

Document Type: Architecture

Release: N/A

Abstract: This document provides an overview of the architecture for the Horizon solution.

Document Status: DRAFT

Originator & Dept:

Internal Distribution:

External Distribution: None

Approval Authorities: *(See PA/PRO/010 for Approval roles)*

Name	Role	Signature	Date
Giacomo Piccinelli	Chief Architect		

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PEAK/PPRR Reference
0.1	31/01/06	1st Version	
0.2	16/06/06	2nd Version	

0.2 Review Details

Review Comments by :	29/06/06
Review Comments to :	Originator & Document Management

Mandatory Review	
Role	*Name*
Agent Design Authority	Rex Dixon
Refdata Design Authority	Duncan MacDonald
Host Design Authority	Roger Barnes
Counter Design Authority	Chris Bailey
Crypto Design Authority	Alex Robinson
Networks Design Authority	Mark Jarosz
Systems Management Design Authority	Glenn Stephens
Estate Management Design Authority	Colin Mills
Platforms & Storage Design Authority	Mario Stelzner
Performance & Resilience Design Authority	David Chapman
Optional Review	
Role	*Name*
Application Design Team Manager	Tom Northcott
Agent Designer	Andy Williams
Host Designer	Rahul Shah Nasser Siddiqi
Counter Development Team Manager	Mark Scardifield
Host Development Team Manager	David Harrison
Agents Development Team Manager	Peter Ambrose

Infrastructure Design Team Manager	Nial Finnegan
Network Designer	Dave Tanner
SSC Manager	Mik Peach
Operations	Andrew Gibson Ed Ashford
Customer Services	Tony Wicks Brian Pinder
Chief Architect	Giacomo Piccinelli
Infrastructure Designer	Ian Bowen
Security Architect	Jim Sweeting
Service Architect	Robert Baulk
*Issued for Information – **Please restrict this distribution list to a minimum***	
Position	*Name*

(*) = Reviewers that returned comments

0.3 Associated Documents

Due to the number of references and to make it more readable, document References are embedded in the document, rather than being included in this table.

Reference	Version	Date	Title	Source
TD/ARC/040	0.1		Diagrams for Horizon Architecture Overview	

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

N.B. Printed versions of this document are not under change control.

0.4 Abbreviations/Definitions

[DN: need to review and add/remove as necessary]

Abbreviation	Definition
ACF	Autoconfig File – one file per outlet counter position.
ACP	Access Control Policy
EACRR	Enhanced Agent and correspondence server resilience and recovery
ADSL	Asynchronous Digital Subscriber Line. A new network method of connecting Post Office Ltd. Branches to the data centres.
AP-ADC	Automated Payment – Advanced Data Capture
APS	Automated Payments Service
Athene	Capacity Management Software
Aurora	System that allows remote console access for Unix systems.
BCV	Business Continuity Volume; part of an EMC Disk Array
Branch	Post Office outlet identified by a unique FAD. Within the HNG model, a Branch is a logical entity that can be composed of several physical locations at which business is transacted.
Bureau	Bureau de Change
Business Services	Those services in the Horizon system that are directly supporting the Post Office business. For example the application running on the counter.
CA	Computer Associates
Clerk	Staff working in a Post Office Branch
CLI	Service that allows a customer to see the number of the caller before answering the call.
C&W	Cable and Wireless.
DCS	Debit Card System (also supports Credit Cards)
DNS	Domain Name System
DRS	Data Reconciliation Service - A service introduced as part of network banking. Its main component is a database running on the host.
DVLA	Driver and Vehicle Licensing Agency
DWH	Data Warehouse
EDG	External Data Gateway
e-pay	Company that interfaces to the mobile phone companies for ETU.
ETU	E-Top-Ups. Ability to credit money to a mobile phone account.
EMV	Europay and Master Card Visa - enhanced method of verification of credit/debit cards using “Chip and PIN”

FAD code	Financial Accounting Division (a unique) identifier used to identify a Post Office branch
FS	Fujitsu Services
FTMS	File Transfer Managed Service
Generic Agent Server	The agent servers used to support the Existing services that transfer data between Riposte and the operational databases. Also known as "Bulk Agent Servers"
HSCSD	High-Speed Circuit-Switched Data (HSCSD) is circuit-switched wireless data transmission for mobile users at data rates up to 38.4 Kbps, four times faster than the standard data rates of the Global System for Mobile (GSM) communication standard in 1999.
HR SAP	Post Office Ltd Human Resources system based on SAP. Its function includes remuneration of branch franchisees for the business they have transacted in their Branch.
ITIL	IT Infrastructure Library. ITIL is an integrated set of best-practice recommendations with common definitions and terminology. ITIL covers areas such as Incident Management, Problem Management, Change Management, Release Management and the Service Desk
ISDN	ISDN, which stands for Integrated Services Digital Network, is a system of digital phone connections which has been available for over a decade
KMA	Key Management Application
LFS	Logistics Feeder Service
LUC	Look-Up Cluster
MID	Merchant Identifier issued by Streamline Merchant Services to identify the Branch from which a transaction originated
MIS	Management Information System
MOT	Ministry of Transportation (as in MOT Test).
NBS	Network Banking Service
NPS	Network Banking Persistence Service
OBC	Organisation Business Change
OMDB	Operational Management Database.
Operational Services	Those services that are needed to run the Horizon system that are not directly supporting the Post Office business. Examples include software distribution, audit, security management etc.
PAF	Postal Address File. A service to allow post codes and addresses to be looked up.
POL	Post Office Limited
POL FS	SAP based system providing financial accounting for the branch based business. This is the production system. There are other SAP systems in the data centre to support development and test.
PSTN	The public switched telephone network
RAS	A server that is dedicated to handling users that are not on a LAN but need remote

	access to it. The *remote access server* allows users to gain access to files and print services on the LAN from a remote location
RDDS	Reference Data Distribution System
RDMC	Reference Data Management Centre
RDS	Post Office Reference Data System
RMG	Royal Mail Group
SAP	Integrated suite of applications providing financial accounting and other business functions.
SAP ADS	POL' s Advanced Distribution System (based on the SAP package) that interfaces to LFS
SAS	Secure Access Server
SFS	Security Functional Specification
Shared Services	Those services that are used by both the Operational Services and Business Services. These are typically network components.
smart post	A service to allow mail rates to be looked up for parcels and letters.
SOAP	Simple Object Access Protocol
SRDF	Symmetrix Remote Data Facility; EMC technology used to replicate disk array data between two Campuses
SSC	Fujitsu's System Support Centre. 3rd Line support
Streamline	Merchant Acquirer for DCS.
SYSMAN2	The systems management environment on the Horizon environment.
TID	Terminal Identifier issued by Streamline Merchant Services to identify the terminal from which a transaction originated
TPS	Transaction Processing System

0.5 Changes in this Version

Version	Changes
0.1	1st Version
0.2	Updated sections not included in version 0.1. Updated following feedback

0.6 Changes Expected

Changes

Any changes following review

0.7 Table of Contents

1.0 Introduction

1.1 Purpose

This document provides an overview of the architecture for the Horizon solution. It assumes an S92 baseline. The document has 3 purposes:

- To provide an introduction to Horizon that is accessible to people with no experience of the system or Post Office.
- Provide sufficient detail to allow "architectural" impact analysis to take place for planned changes to the solution.
- To act as a "root" document to Horizon with cross references to the next level of design documents.

The document is not intended to provide a complete picture of every aspect of the solution, but is intended to cover the main areas to a reasonable degree.

The diagrams in this document have been included as "pictures" to keep the document size manageable. The original source material can be found in TD/ARC/040.

1.2 Business Context and Background

Post Office Ltd is a combination of a retail organisation and a financial services organization and offers a diverse range of services to its customers. Traditionally its main channel to customers is through its extensive branch network (approximately 14,000 sites as of November 2005 attracting some 28M customers per week). In recent years other channels have been developed (i.e. web sites, call centres etc) to support Post Office's entry into financial services products (e.g. insurance, credit cards loans etc). The vast majority of the branches operate on a franchisee basis with Post Office directly managing around 500 sites.

The Horizon solution has two main roles:

1. Provide the complete IT solution for the branch estate including applications, infrastructure, support and engineering.
2. Provide accounting functionality for the whole of the Post Office by hosting a SAP solution (called POL FS). The application development of this is handled by a third party directly contracted to Post Office.

The types of transaction that are supported in the branch include:

- Selling of fixed price goods and services
- Payment of Bills (utilities, local government etc) including where an online interaction is required (e.g. as in DVLA)

- Banking Services – deposits, withdraws, balance enquiries. There are two types supported – online requiring authorisation and offline which don't (e.g. Girobank). The majority of business is moving to the online model.
- Mobile phone electronic top-ups
- Bureau de Change
- Payment by Debit Card and Credit Card
- Electronic Data Capture (e.g. fishing license application)
- Parcels and Letters
- Charging of Smart Cards for Gas Prepayment (Quantum)
- Electronic Voucher Database Service to support the electronic voucher life cycle (known in Horizon as APOP Authorisation Service).

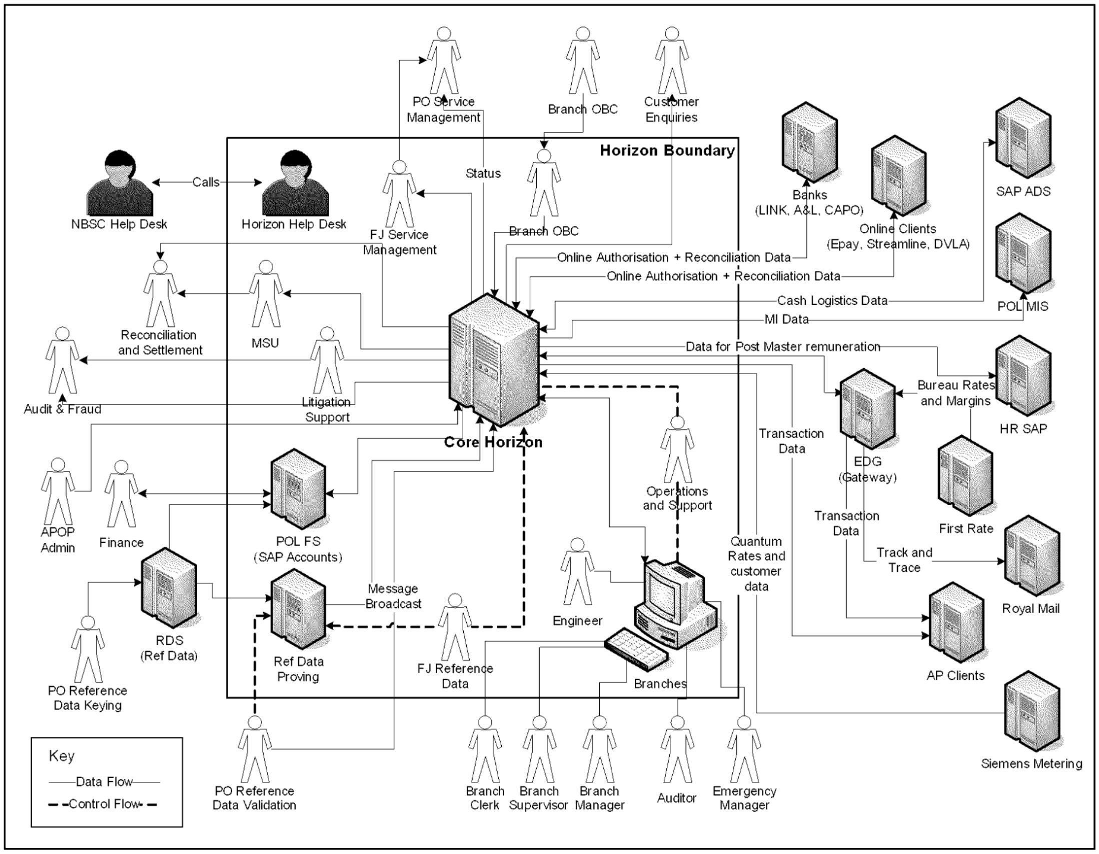
Within the branch estate, the majority of the products that are sold by Post Office are on behalf of a third party (a "Client" in Post Office language) – for example payment of a British Gas or BT Bill. The fees paid by the Client for this service are typically related to the amount of manual work that needs to be undertaken by branch staff rather than the value of the transaction – resulting in very low margins (Post Office's turnover is approximately 1% of the £110 billion worth of transactions it handles each year and its margin is a low percentage of this).

One consequence of the low margins is that Post Office has to be extremely careful to minimise the impact of any errors or faults in the solution. One example of this is that for online authorisations every individual transaction is reconciled with the third parties view and all errors are investigated (typical retail organisations would just check that the total for the day is accurate to within an agreed error margin with the third party).

The workload handled by the branch estate is large with peak transaction rates of around 800 transactions per second and a peak day of around 25M transactions. The peak is determined by the number of counters (approximately 35,000) and the rate at which customers can be served. The average basket size is very low (an average of 1.7 products).

1.3 IT Context and Users

The diagram below shows the wider context of the Horizon Architecture and the users:



There are four main areas within the Horizon Architecture:

1. POL-FS – financial accounting system based on SAP
2. Reference Data Proving – environment in which changes to reference data are proved before releasing into live (reference data controls things such as which products are sold, their price and where in the menu hierarchy they are displayed).
3. Branches – the branches themselves
4. Core Horizon – the central systems that support Horizon

Core Horizon communicates with the following systems:

- Banks (LINK, A&L, CAPO) for online authorisation of banking transactions and transaction data used for reconciliation.
- Online Clients (e-pay, Streamline, DVLA) for online authorisation of transactions and (for e-pay and Streamline) data used for reconciliation.

- SAP ADS – A Post Office system that handles cash and Foreign Currency logistics. Data includes cash on hand statements from each branch, planned orders, replenishment deliveries and delivery/collection data.
- HR SAP – A SAP system that handles remuneration to the branch franchisees and "multiples" such as Tesco.
- POL MIS – An Oracle based system to provide MI reporting to Post Office.
- First Rate – Provides bureau rate information. It is also passed all bureau transactions to allow First Rate to undertake MI.
- Siemens Metering – Provides Rates and Customer data for Quantum gas pre-payment card.
- AP Clients – Transaction information for Clients where payment information is collected by Post Office.
- Royal Mail and Parcel Force Worldwide – track and trace information for parcels and letters taken in a branch.
- RDS – Post Office system that provides reference data

Some communication is via the Royal Mail EDG system as shown. Others have direct connections from Horizon.

POL FS communicates with a number of external systems to transfer data. These are either directly or via EDG. These are not shown for clarity.

The users of the solution within Horizon (i.e. Fujitsu controlled staff) include:

- Operations and Support – 2nd and 3rd line support and network and data centre operations.
- Engineer – installation and swap faulty equipment in the branch. Has specific access to some functions in branch.
- FJ Reference Data – validates and releases reference data (with Post Office)
- Litigation Support – provides data from audit stream to Post Office. Data provided to Post Office out of band (e.g. email, CD).
- Management Support Unit (MSU) – investigates reconciliation errors caused within Horizon.
- FJ Service Management – service managers
- Branch OBC Team – manages physical changes to branch (open, shut, relocation etc).

The Post Office users of the solution include:

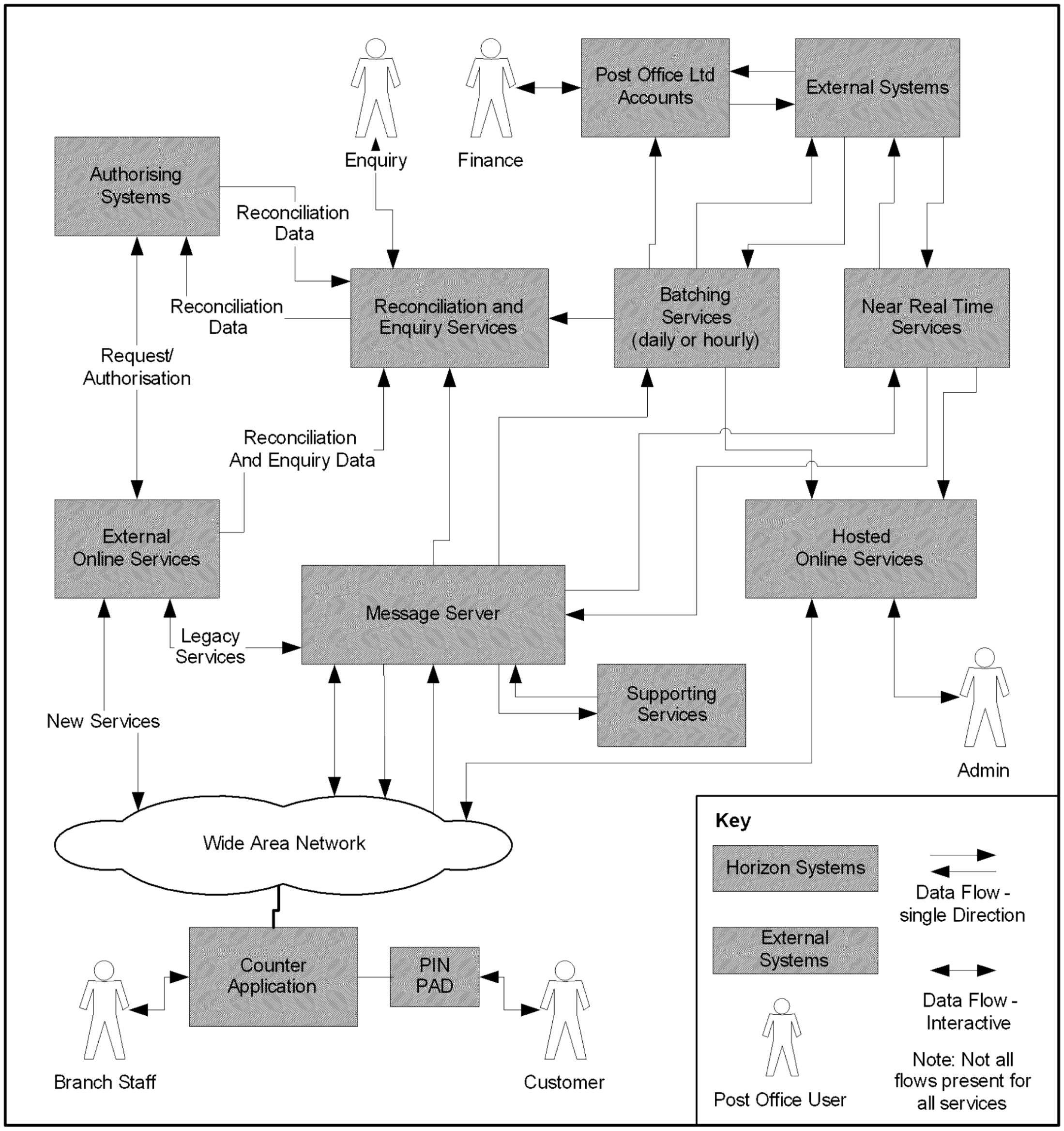
- Branch Clerk – normal user in branch, able to sell products etc
- Branch Supervisor – branch user able to the majority of activities of the Branch Manger. Main exceptions are create users and stock units.
- Branch Manager – branch super user able to create users, make account adjustments etc.
- Branch Auditor – auditor that visits a branch
- Branch Emergency Manager – manager that brought into a branch in emergency situations (e.g. normal manager is ill)
- PO Reference Data Validation Team – Post Office team that validates reference data changes. Works with FJ Reference data.
- Finance – finance functions on POL-FS
- APOP Admin – administration of data content of APOP database (electronic vouchers)
- Audit & Fraud – investigates audit information. Also has access to online transaction enquiry service (TES) for banking transactions.
- Reconciliation and Settlement – handles reconciliation and settlement with Clients.
- PO Service Management – Post Office service management. Is provided status of system via a Portal.
- Branch OBC – Post Office team responsible for branch physical changes
- Customer Enquiries – answers customer enquires for banking using online transaction enquiry service (TES)

2.0 Logical Architecture

This section describes the logical architecture to provide an introduction to the Horizon solution. It is split into two areas: Business Applications and physical structure

2.1 Business Applications

The diagram below shows a simplified view of the business applications for Horizon.



The key systems are described below:

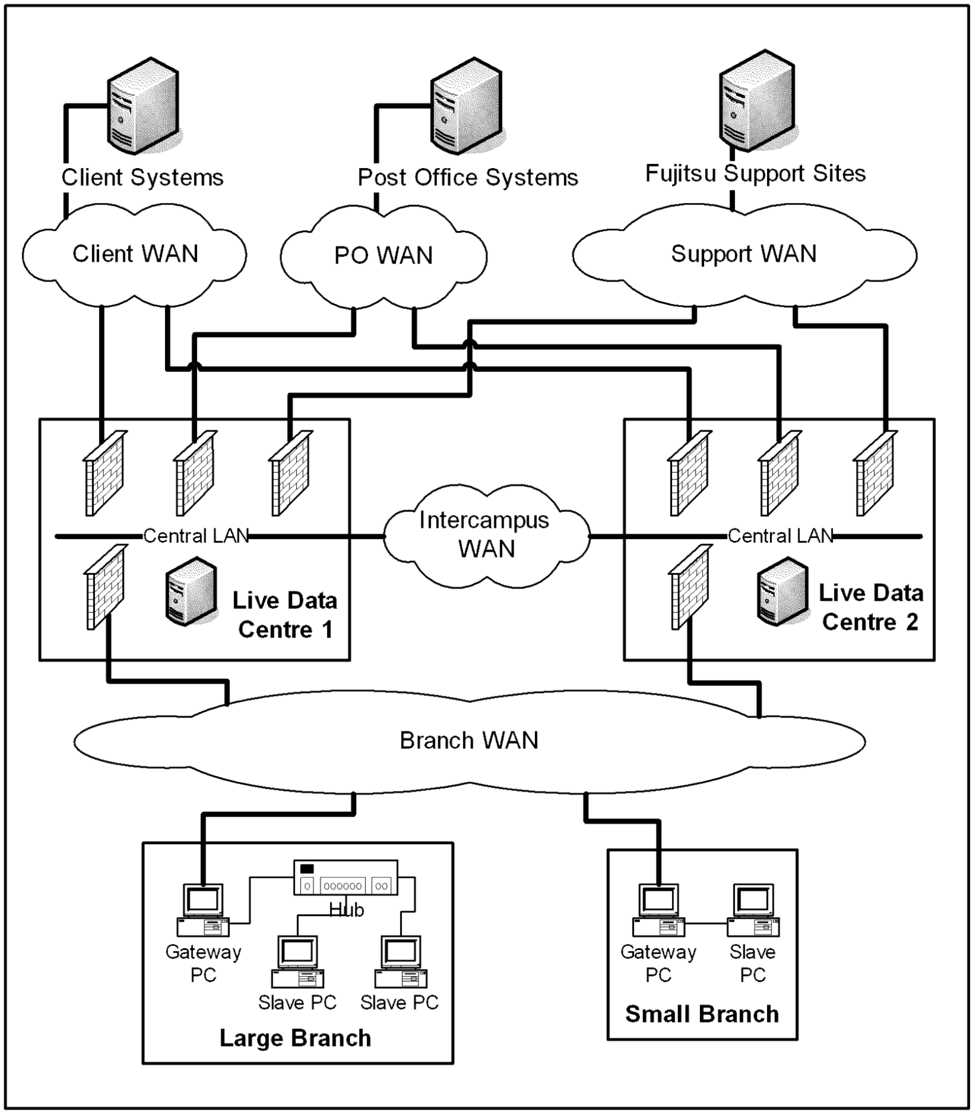
#	Name	Description
1	Counter Application	The counter application is used by branch staff to sell products and to perform back office functions. Business data held in the counter in a Riposte messaging system – all counters in a branch have a copy of the complete data.
2	PIN Pad	Allows customers to input smart card and PIN for banking and DCS transactions.

3	Message Server	Handles messaging to/from Branches for batch data transfers using Riposte (specialist messaging system from Escher Group). Also handles online authorisations for legacy services (Banking, DCS, ETU) – new services connect directly via SOAP.
4	External Online Services	Provides online authentication for counter transactions where a third party owns the system that authorises the transactions. Specific services supported are: • DCS for debit card and credit card authorisations • Banking for deposits, withdraws and balance enquiries • ETU to allow electronic top-ups for mobile phones • DVLA for authorising car tax
5	Hosted Online Services	Provides online authentication for counter transactions where the authorisation or information system is hosted by Horizon. Specific services supported are: • APOP databases - e.g. Postal orders • PAF to allow lookup of Postal Addresses •
6	Reconciliation and Enquiry Services	Provides Reconciliation and enquiry services for online authorisations. The specific systems are: • DRS (data reconciliation service) to reconcile individual transactions for the DCS, ETU and Banking services. • TES (transaction enquiry service) to allow Post Office to query transactions status for banking (only) • DWH (data warehouse) contains banking, ETU and DCS data for SLT calculations. • APS (automated payment system) which reconciles transactions between itself and TPS (transaction processing system).
7	Batching Services	Batches up data from branches to send to external systems – either all transactions or in summarised form. Also receives batch data from external systems for distribution to branches. The systems that pass data to external systems are: • TPS (transaction processing system) – provides daily data to other systems including POL-FS, POL-MIS and HR SAP. Also provides a feed to First rate for Bureau transactions. • APS (automated payment system) – provides daily data to AP clients (British Gas, BT etc). • LFS (logistic feeder service) – provides data on pouch collections and receipts at branches to SAP ADS on an hourly basis. Also nightly data on cash held in branches. The systems that receive data from external systems are: • APS – receives customer and tariff data for Quantum and Water Card service once per day. • LFS – receives planned order data (once per day) and pouch contents information (potentially hourly). • RDMC – receives Rates and Margins data for Bureau service
8	Near Real Time Services	Transfers data in near real time to or from external systems. The systems are: • APS – receives emergency customer data from Quantum for immediate distribution to the branches. • Track and Trace – provides data on parcels etc received by branches to Royal Mail and Parcel Force Worldwide

9	Support Services	Supports the business systems with reference data, security and SLT monitoring. The systems are: • RDMC and RDDS – reference data management and distribution systems. • KMA – key management system for branch security keys • OMDB – provides SLT monitoring for outbound data distribution. Also monitors branch connectivity. • DWH – SLT reporting for data file deliveries (inbound and outbound).
10	PO Ltd Accounts	An SAP system (called POL FS) that holds the accounts for Post Office Ltd.. This has lots of input and output feeds to external systems.

2.2 Physical Structure

The diagram below shows a view of the physical structure of the branches, network and data centres.



The key areas are described below:

#	Name	Description
1	Small Branch	The network in Small Branches (1 or 2 counters) consist of a gateway PC which connects the branch to the network and a simple cross over cable to the 2nd PC (if there is one)
2	Large Branch	In larger branches (3+ counters) one or more hubs are also used to provide the LAN connections.
3	Branch WAN	The gateway PC uses ADSL or ISDN as primary connections. ISDN and Dialled Mobile (using HSCSD) can be used in ADSL site for a backup connection. For a small number of branches that are out of distance from the nearest exchange, VSAT connections are used.

4	Data Centres	There are two data centres – in an active/active configuration with, under normal circumstances, both data centres supporting the branch workload. Within the data centre the LAN is split into a number of DMZ.
6	Intercampus WAN	To link the two data centres a high speed (gigabit) resilient network is used to provide a virtual LAN spanning both data centres and to carry storage data between two EMC arrays.
7	Client WAN	The Client WAN provides connections to a number of clients that the system uses. The following connections are provided by Fujitsu: • DVLA for online authentication of car tax. • Streamline for DCS transactions • EPAY for mobile phone top up (ETU) transactions • Alliance & Leicester for banking transactions The following connections are provided by third parties: • LINK for banking transactions • CAPO for banking transactions The connections are typically resilient fixed circuits of between 64kbits/s and 2Mbits/s, although Streamline uses X25 and ISDN. Most clients have a DR site that is also connected.
8	PO WAN	This provides connections to Post Office for both batch file transfer to other systems and also allows Post Office users access to the enquiry and POL-FS systems. The connection is a 2Mbit/s resilient circuit. There is also a connection to Post Office's DR site at Sunguard.
9	Support WAN	This provides access for the Fujitsu support communities to the data centre including: • Operations in Belfast • 1st and 2nd line support in Stevenage • 3rd line, Service Management, Litigation Support and MSU in Bracknell • OBC Team in Crewe

3.0 Application Architecture

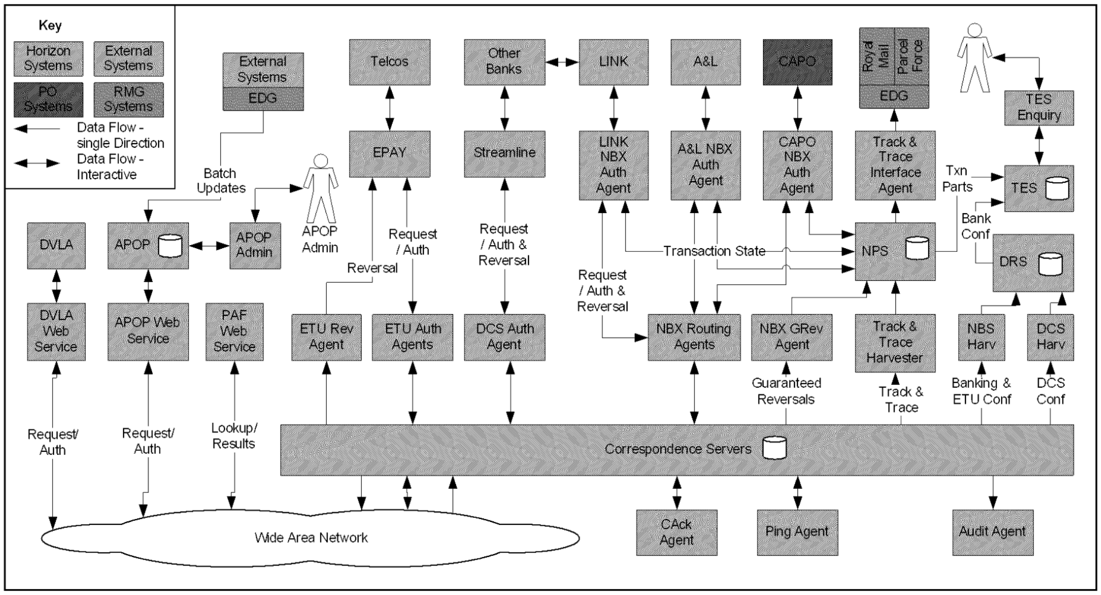
The application architecture has been split into a number of areas to allow the solution to be described as follows:

- Online and Near Real Time systems in the data centre. APOP Admin is included in this section for convenience.
- Batch systems in the data centre that handle the main business data and POL-FS.
- Supporting systems for reference data, SLT measurement Branch Monitoring and Key Management.
- Counter

This approach allows an understanding of all the elements that make up the different service. However some components do appear in multiple areas as a result.

3.1 Online and Near Real Time

The picture below shows the systems and flows within the data centre for online and near real time services. The batch aspects of the APOP service have also been included for convenience.



The components and their role are described in the table:

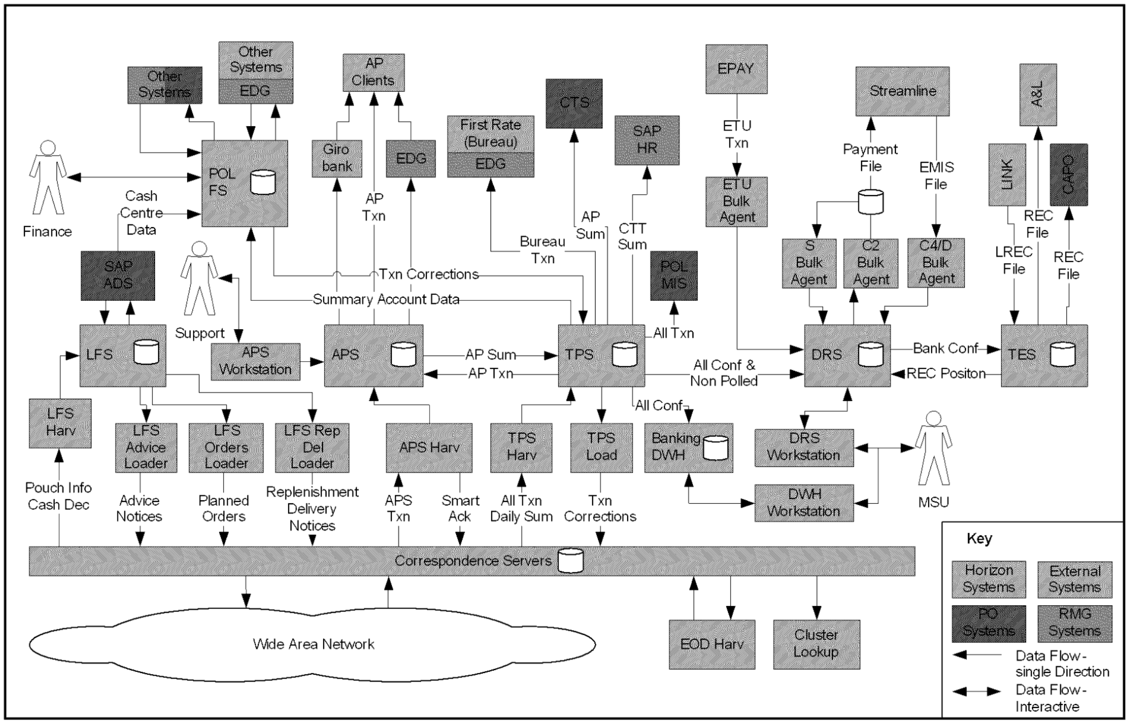
#	Name	Function	Documentation

1	Correspondence Servers	Messaging Servers that pass messages to/from the branches. Data is held either as messages with a given expiry period or as "persistent objects" which are retained until updated or deleted. For performance reasons, the branch estate is split into 4 "clusters" each handling round 3,500 branches.	None identified
2	Ping Agent Central Acknowledgement Agent (CAck)	The Ping Agent responds to application level pings from the counter via the correspondence servers. The CAck agent is used for recording receipt of messages at the data centre (mainly used for SLT monitoring). It is also used to acknowledges requests from the counter Smart Cache used to police use of Smart card charging (see security).	AD/DES/042 - CSR+ Common Agents High Level Design AD/DES/020 - Automated Payment System Agents for Release 2+ High Level Design
3	Audit Agent	Writes to text files all messages written or received by the correspondence servers for audit.	AD/DES/042 - CSR+ Common Agents
4	DVLA Web Service	Allows branches to authorise car tax in an online transaction to DVLA. Interface between the counter and data centre is SOAP.	DV/HLD/002 -DVLA Web Service
5	APOP Web Service APOP Database APOP Admin	A hosted online service that handles electronic vouchers. Requests/Authorisations from the counter are handled using SOAP to a Web Service. Batch updates to the database arrive via the EDG and are controlled by a Maestro schedule. A web based admin service allows Post Office staff to update individual records.	AP/HLD/008 -APOP Web Service AP/HLD/005 - APOP Voucher Host System High Level Design AP/HLD/009 - APOP Maestro Schedule AP/HLD/010 - APOP Administration Service Application High Level Design
6	PAF Web Service	Allows branches to look up postcodes and addresses. Interface between the counter and data centre is SOAP.	PF/HLD/002 - PAF Web Service
7	ETU Auth Agent ETU Rev Agent	Handles requests for authorisations to top up mobile phones. Requests are received from a counter via the correspondence servers and the authorisations written back the same way. A separate agent handles reversals to e-pay.	AD/DES/073 - High Level Design Specification for E-Top Ups Agents
8	DCS Auth Agent	Handles requests for authorisations for Debit and Credit Cards and also reversals. Requests are received from a counter via the correspondence servers and the authorisations written back the same way.	AD/DES/069 - High Level Design Specification for Debit Card Service Agents

9	NBX Routing Agent NBX GRev Agent LINK NBX Auth Agent A&L NBX Auth Agent CAPO NBX Auth Agent NPS Database	Handles online authorisation requests for banking transactions. Requests are received via the correspondence server in the routing agent which routes the request to the LINK, A&L or CAPO authorisation agent (as required). The authorisation agents hold state and audit data in the NPS database. Reversals are handled both via the routing/auth agents and also via a guaranteed route into the NPS. These reversals are then processed by the relevant auth agents.	NB/HLD/017 - High Level Design Specification for Agents for NBX, the NBE Replacement NB/HLD/013 - NBX Persistent Store High Level Design
10	Track & Trace Harvester Track & Trace Interface Agent NPS Database	Track and trace data from the branches are processed in near real time, with data passed to Royal Mail and Parcel Force via EDG. The NPS database is used as a staging post to screen duplicates.	DE/HLD/015 - High Level Design Specification for Track And Trace Agents NB/HLD/027 - NPS Track And Trace Changes HLD
11	NBS Harvester DCS Harvester DRS Database TES Database TES Enquiry	DRS handles reconciliation for banking, ETU and DCS. The confirmations generated by the counters are harvested in near real time to ensure the reconciliation position is up to date. There are two harvesters – one for NBS and ETU and one for DCS. The banking confirmations, together with transaction parts from NPS are passed to TES. An enquiry service is provided to allow Post Office staff to query the status of transactions. DRS and TES are also involved in the batch flows and there is a workstation to support reconciliation updates (see next section).	AD/DES/065 - High Level Design for Network Banking Agents NB/HLD/015 - S75 High Level Design for DRS NB/HLD/003 - Data Reconciliation Service Host High Level Design NB/HLD/016 - Transaction Enquiry Service High Level Design NB/HLD/022 - Transaction Enquiry Service (TES) Query Application HLD NB/HLD/023 - Transaction Enquiry Service (TES) Reporting High Level Design

3.2 Batch and POL FS

The picture below shows the systems and flows within the data centre for the main batch flows. The POL FS system is included for convenience.



The components and their role are described in the table:

#	Name	Function	Documentation
1	Correspondence Servers	Messaging Servers that pass messages to/from the branches. Data is held either as messages with a given expiry period or as "persistent objects" which are retained until updated or deleted. For performance reasons, the branch estate is split into 4 "clusters" each handling round 3,500 branches.	None identified
2	EOD Harvester	The End of Day Harvester ensures that there is a consistent set of data from the branch for the APS and TPS harvesters to use.	AD/DES/042 - CSR+ Common Agents High Level Design
3	Cluster Lookup	Cluster lookup is a generic service that tells other agents in which correspondence server cluster a particular branch resides and which branches are within a particular cluster.	AD/DES/036 - CSR+ Cluster Lookup Service Design

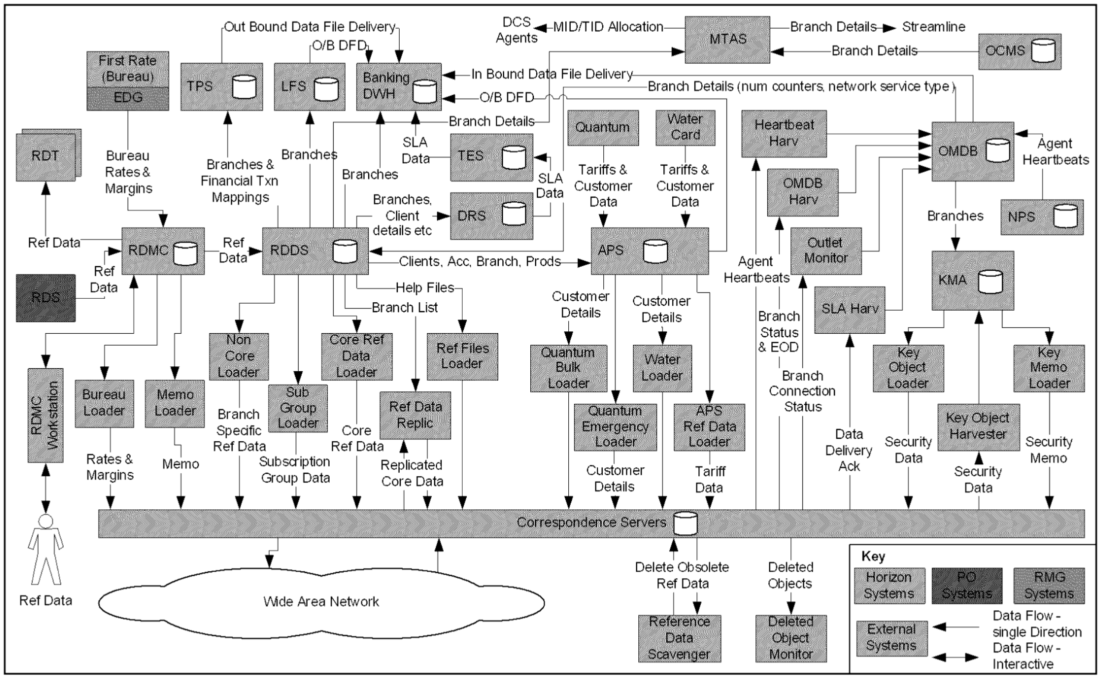
4	LFS Harvester LFS Advice Notice Loader LFS Planned Orders Loader LFS Replenishment Delivery Notice Loader LFS Database	LFS passes data between the counters and Post Office's SAP ADS system for cash and currency handling. The database is used as a staging post to screen duplicates. Pouch Information (both collections and delivers for all pouches – not just cash and Foreign Currency), and Cash Declarations are passed to SAP ADS. Advice notices, planned orders and replenishment delivery notices are received from SAP ADS. Note that advice notices have never been used.	AD/DES/015 - Logistics Feeder Service - Agents High Level Design for CSR+ LF/DES/003 - Logistics Feeder Service - High Level Design
5	APS Harvester APS Database APS Workstation	APS passes Automated Payment transactions to Clients – either directly, via Girobank or via the EDG. The harvester reads all APS transactions from the correspondence server to put into the database which then splits them by client. The database also provides a summary by client which is passed to Post Office Ltd's CTS process via the TPS database as well as checking that all AP transactions were also harvested into TPS. The harvesting agent also acknowledges smart transactions to allow the counter smart cache to operate (see security). The APS workstation is used to allow new clients to be added to the solution.	AD/DES/049 - APS High Level Design Addendum for Flexible Delivery Dates AP/DES/015 - APS Host High Level Physical Design AP/DES/004 – APS Design Specification (CSR+) AP/DES/010 - APS File Rejection Handling High Level Design SD/DES/073 - APS To TPS Reconciliation High Level Design Specification AD/DES/020 - Automated Payment System Agents for Release BI3 High Level Design

6	TPS Harvester TPS Loader	TPS takes all transactions from the counters and then passes them directly in either full or summary form to a number of other systems: • AP Transactions passed to APS to allow reconciliation between APS and TPS. • Bureau Transactions are passed to First rate via the EDG gateway. Horizon is responsible for delivery of files into Huthwaite, but not for putting data onto EDG itself. • AP Summaries are sent to CTS to allow Post Office to settle with their clients. Also Transaction Corrections and Error files. • Summaries are sent to HR SAP to allow remuneration to the branch franchisee for the transactions they have done. This data is provided monthly, with TPS keeping a running total. • Nearly all transactions are sent to POL MIS (some – e.g. balancing transactions) are suppressed. • All confirmations (Banking, ETU, DCS) are sent to DRS for reconciliation. • All confirmations are sent to the banking data warehouse for SLT calculations. • A summary position of the transactions traded that day is sent to POL FS. There are also transactions corrections received from POL-FS that are fed to the counters via TPS.	AD/DES/041 - TPS Agents for BI3 High Level Design DE/HLD/019 - TPS Host Changes At S90 HLD EA/HLD/003 - TPS Host Changes At S60 High Level Design EA/HLD/007 - Impact Release 3 - TPS Delta High Level Design EA/HLD/009 - TPS Hr SAP Summarisation & Transaction Corrections HLD NB/HLD/006 - TPS Host Changes To Store And Process Network Banking Transactions HLD NB/HLD/011 - TPS Host Changes At S50 TI/DES/002 - TPS Release 2 High Level Design
7	Banking DWH	Provides SLT calculations for banking. MSU are also able to query the history (91 days) for ad-hoc reports via a workstation.	DW/HLD/002 – BI3 Data Warehouse High Level Design Specification EF/HLD/007 - High Level Design - Debit Card MIS NB/HLD/001 - Network Banking MIS High Level Design ?? Workstation ??

8	DRS Database ETU Bulk Agent S Bulk Agent C2 Bulk Agent C4/D Bulk Agent DRS Workstation TES Database	DRS reconciles transactions for Banking, ETU and DCS with the clients. For ETU a payment file is received from e-pay and processed via the ETU bulk agent. For DCS a payment file is passed to Streamline via the C2 bulk agent. Once acknowledgement is received from Streamline that this has been received the S bulk agent puts the transactions back into DRS. Once Streamline have processed the payment file, they produce an EMIS file of the status for all transactions (i.e. whether settled or not) and this is loaded into DRS via the C4/D bulk agent. TES produces a banking reconciliation (REC) file for A&L and CAPO and receives one from LINK. All transactions are passed to DRS for reconciliation. For DRS there is also a workstation to allow MSU staff to update the reconciliation states of transactions.	NB/HLD/004 - Data Reconciliation Service Workstation High Level Design NB/HLD/026 - DRS Host Application And Workstation High Level Design Delta for Impact Release 3 DE/HLD/012 - TES Reports Data Extract HLD NB/HLD/019 - TES Maestro Schedule Design AD/DES/069 - High Level Design Specification for Debit Card Service Agents
9	POL FS	An SAP system that provides the accounts for the Post Office. As well as the data from the branches it has a number of feeds to/from other systems.	???
10	APS FTMS TIP FTMS GP FTMS NBX Connect:Direct Gateway DCSM	These components are responsible for file transfer to/from remote systems. For clarity they are not shown on the diagram. APS FTMS is responsible for file transfers to/from APS Clients. TIP FTMS is responsible for file transfers to/from Post Office systems EDG FTMS is responsible for file transfers to/from other systems via the EDG. GP FTMS is responsible for file transfers to other Fujitsu sites. NBX: Connect:Direct Gateway is responsible for file transfers to the banks. DCSM is responsible for file transfers to/from e-pay and Streamline.	NB/HLD/018 - Connectdirect Gateway HLD ??? for other elements

3.3 Supporting Systems

The picture below shows the supporting systems and flows within the data centre that cover reference data, security key management and SLT monitoring.



The components and their role are described in the table:

#	Name	Function	Documentation
1	Correspondence Servers	Messaging Servers that pass messages to/from the branches. Data is held either as messages with a given expiry period or as “persistent objects” which are retained until updated or deleted. for performance reasons, the branch estate is split into 4 “clusters” each handling round 3,500 branches.	None identified
2	RDMC Database RDDS Database Bureau Loader Subscription Group Loader Non Core Loader Core Ref Data Loader Ref Files Loader Ref Data Replicator Non DB Ref Loader Ref Data	The reference data system is responsible for ensuring that reference data is delivered to counters and is house kept appropriately. The RDMC database receives reference data changes from Post Office’s RDS system and then they are normally validated on the RDT rig (see infrastructure) by the Reference data team. Once the reference data is validated it is released via the RDMC workstation onto the RDDS database to allow it to be loaded into the correspondence servers. Loading takes place in several ways depending on its type: • Non Core (branch specific) is loaded directly into the branch. • Core (delivered to all branches) is loaded into a “dummy group” in the correspondence server. This is then copied to the branches through the reference data replicator agent. • Subscription Group data (which is written once each correspondence server cluster but can be read by all	AD/DES/020 - Automated Payment System Agents For Release 2+ High Level Design (for Memo loader) AD/DES/040 - Reference Data - Agents High Level Design for CSR+ AD/DES/070 - High Level Design for Agents for Escher Mails AD/DES/072 - High Level Design for Agents for Bureau de Change

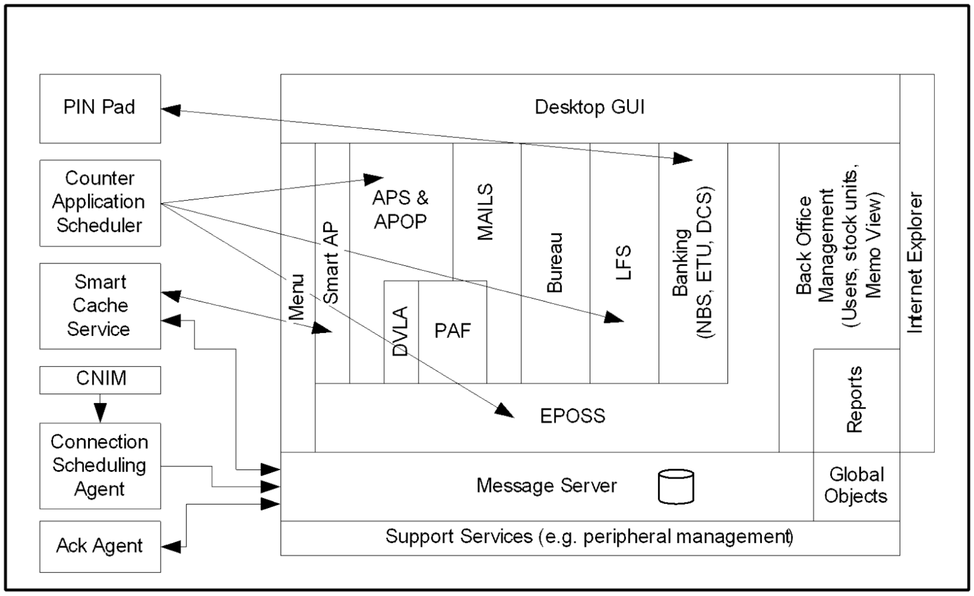
	Scavenger Deleted Object Monitor RDT Rig RDMC Workstation	• branches) is loaded through either the Subscription group loader or the Core Ref Data Loader depending on the data type. • Help text (which also uses subscription groups) is loaded via the RDMC workstation into RDMC. Once released into RDDS it is loaded via the file loader. • Other reference data that doesn't have an automated route is loaded via the RDMC workstation in a similar way to the help text. • Bureau rate and margins data are received from First Rate and loaded via RDMC via a subscription group. RDDS is not used to minimise delays in processing the data. There are also two agents that are responsible for housekeeping – Scavenger deletes superseded or obsolete reference data and deleted object monitor checks that this deletion has occurred correctly (since the correspondence servers are distributed then deletions can take place at different times on different nodes, potentially causing issues). Messages for counters (memos) are loaded via the RDMC workstation into the RDMC database. These are then loaded into the correspondence servers. Branch information also flows from RDDS to the other databases to ensure there is a consistent view of which branches are open and shut as well as required reference data.	AD/DES/074 - Design for 'D' Data Agents RD/HLD/001 – Design for WebRiposte Data Agents NB/HLD/030 - Issuer Referrals, Counter, High Level Design Specification RD/DES/051 - 'D' Data Distribution via RDMC/RDDS High Level Design RD/DES/054 - Reference Data High Level Design for S70 (EMV and NBE Replacement) RD/DES/056 - Reference Data End To End High Level Design for S80 RD/DES/062 - Reference Data High Level Design for S90 Bureau Debit / Credit Card Payment RD/DES/046 - RDMC High Level Design RD/DES/049 - Escher Mails for RDMC / RDDS High Level Design RD/DES/057 - RDMC / RDDS High Level Design for S80 RD/DES/058 - RDMC /RDDS High Level Design for S80 + 1 Sales RD/DES/047 - RDDS High Level Design AD/DES/072 - High Level Design Specification for Agents for Bureau De

			Change RD/DES/050 - RDMC/RDDS Host HLD for Bureau Phase 1 RD/DES/062 - Reference Data High Level Design for S90 Bureau Debit / Credit Card Payment
3	Banking DWH	Used for measurement of file delivery to clients and data delivery to branches. Also produces some banking reports	DW/HLD/007 - Datafile Delivery Performance Measurement High Level Design
4	APS Database Quantum Bulk Loader Quantum Emergency Loader Water Card Loader APS Ref Data Loader APS Ref Data Replicator	For pre-payment Gas (Quantum) and Water Card customer and tariff information is loaded into the correspondence servers as core reference data. For Quantum, customer information is targeted at a specific branch. This is either done overnight (bulk) or during the day (emergency). For Water Card customer information is sent to all branches and is only updated overnight.	AP/DES/015 - APS Host High Level Physical Design AP/DES/004 – APS Design Specification (CSR+) AD/DES/020 - Automated Payment System Agents for Release BI3 High Level Design
5	OMDB Database Heartbeat Harvester OMDB Harvester Outlet Monitor SLA Harvester SMDB Database (not shown)	The OMDB database collects status information for the branches and data centre agents. This is then used to trigger alerts etc (see systems management) The following information is collected about the branches: • Branch Status (WAN and LAN connection status generated by the gateway PC). • End of Day Markers (EOD) • Connection Status to the correspondence servers (when the branch last connected) • Acknowledgements of data delivery to the branch (for SLT measurement). OMDB also collects information on agent heartbeats to monitor the agents either directly from NPS (for the banking authorisation agents) or via the correspondence servers for the other agents.	AD/DES/062 - OMDB Agents High Level Design for CSR+

		The branch SLT information is sent to the DWH. Most of the data on the OMDB is replicated to a separate SMDB (Service Management Database) that is sited within a DMZ. This allows support and operations staff access to that data from the Fujitsu Services intranet.	
6	KMA Database Key Object Loader Key Object Harvester Key Memo Loader	KMA manages the cryptography keys needed in the solution (see security). For asynchronous functions data is transferred to/from the counters (and other servers) via the correspondence servers (loader and harvester). For some operations branch staff need to be involved and they are informed through memos (memo loader)	AD/DES/023 - Key Management Agent Design for CSR+ RS/DES/010 - Key Management High Level Design
7	MTAS OCMS Database	MTAS (MID/TID Allocation Service) is responsible for allocating MID (Merchant ID) to branches and TID (terminal ID) to counters. It takes feeds from RDDS and OCMS (database that handles opening of new branches) to determine branch status and then feeds data to Streamline on what has been allocated and to the DCS agents so that MID/TID can be added to each transaction sent to Streamline.	TD/HLD/003 - MID/TID Allocation Service High Level Design

3.4 Counter

The picture below shows the main components for the business application within the counter.



The components and their role are described in the table below. The framework for the counter application is based on the Riposte product from Escher.

#	Name	Function	Documentation
1	Desktop GUI Internet Explorer Menu	The presentation to the user is provided via a Desktop GUI within the Riposte product. Some reports and help text uses Internet Explorer to display the information. The menu hierarchy displayed by the GUI is defined in reference data.	SD/SPE/016 – Horizon OPS Menu Hierarchy
2	Message Server Global Objects	Messaging Servers that pass messages to/from the data centre. Data is held either as messages with a given expiry period or as "persistent objects" which are retained until updated or deleted. The message server is used to store reference data and also to record transactions generated from the counter. Global objects is a file on the counter that holds reference data for report definitions. It is not held in the message server due to its size. This approach also makes it easier to co-ordinate code change with report definition change.	???
3	Back Office Management	Back Office management is provided by the Riposte product to provide facilities such as log on, user management, stock management and memo view.	???

4	EPOSS Reports	EPOSS handles all the basic point of sale products (e.g. stamp sale). It also handles accounting functions such as stock unit declarations, rollovers and accounting summaries. Reports are handled through the reports module. Note that some of the documentation is out of date.	EP/DES/016 - EPOSS - End Of Day Service High Level Design EP/DES/019 - EPOSS High Level Design EP/DES/020 - EPOSS Reporting Service High Level Design EP/DES/021 - EPOSS Balancing Service High Level Design EP/DES/022 - EPOSS Transaction Service High Level Design EP/DES/025 - EPOSS End Of Day Service High Level Design
5	APS Smart AP Smart Cache Service DVLA APOP	APS handles all automated payment products. Within this there is a specialist module for Smart AP (with an associated Smart Card Cache Service to allow secure offline working – see security). DVLA also has a specialised service, including an online lookup via a SOAP request. APOP provides a generic online lookup of data via a SOAP request. It is used, for example, to handle allocation, printing and redeeming of Postal Orders.	AP/DES/012 - APS Counter High Level Design Specification AP/HLD/006 - APOP Counter High Level Design DV/HLD/001 - DVLA Counter High Level Design Specification AP/DES/017 - Protecting Smart Card Payment HLD Specification
6	PAF	PAF provides an address lookup service for use by APS and MAILS.	PF/HLD/001 - High Level Design - Counter PAF Module
7	MAILS	MAILS (known as "Smart Post" by users) provides postal services facilities such as pricing based on weight, destination, type and insurance needs. Help for MAILS is provided using local web content displayed via Internet Explorer.	DE/HLD/014 - High Level Design Specification for Track and Trace: Counter DE/HLD/020 - S90 Smartpost

8	Bureau	Bureau provides Bureau de Change services	DE/HLD/008 - Bureau de Change Counter High Level Design
9	LFS	LFS provides facilities for stock and cash management (e.g. pouch collection and delivery, including automated remittances for Cash and Foreign Currency, daily cash on hand details).	LF/DES/003 - Logistics Feeder Service - High Level Design EA/HLD/011 - LFS Counter Foreign Currency Auto Rems - Delta HLD
10	Banking PIN Pad	The banking module provides services for Banking, ETU (mobile phone top up) and Debit/Credit cards. For Banking and Debit/Credit cards the PIN Pad is used to allow customers to enter their PIN.	NB/HLD/002 - Network Banking Counter High Level Design ET/HLD/001 - Electronic Top-Up, Counter High Level Design Specification NB/HLD/008 - Debit Card System Counter High Level Design Specification NB/HLD/012 - EMV, Counter, High-Level Design Specification NB/HLD/029 - Bureau Plastic, Counter, High Level Design Specification NB/HLD/030 - Issuer Referrals, Counter, High Level Design Specification

11	Support Services Connection Scheduling Agent CNIM Ack Agent Counter Application Scheduler	The support services provide support for the business applications including peripheral management. The connection scheduling agent (aka Counter Call Scheduler) is responsible for scheduling connections between the local message store and the data centre messagestore. It is configured to optimise the need for timely delivery of data to the data centre and the need to minimise phone calls across the ISDN network. CNIM (counter network infrastructure manager), while not strictly a business application, is included for completeness. CNIM has two main roles – to control which phone numbers are used in ISDN sites (see Network) and to inform connection scheduling agent on the status of the network connection to the data centre. This status is then used by the counter applications to inform the user of network failures and prohibit some transaction types if the network isn't available. The Ack agent acknowledges delivery of data from the data centres to allow SLT to be measured. The Counter Application scheduler is responsible for scheduling batch operations within the counter applications (e.g. End of Day processing).	TD/DES/109 - Counter Application Scheduler High Level Design AD/DES/042 - CSR+ Common Agents High Level Design TD/SDS/002 - Counter Network Infrastructure Manager (CNIM) ??? EP/HLD/002 - High Level Design – Branch Network Resilience – Engineer's Counter Application

3.5 Interfaces

Each external interface to Horizon has an Application Interface Specification (AIS) and a Technical Interface Specification (TIS). The table below details these documents:

[DN: Sure some of these are no longer relevant; also I've probably missed some]

#	Area	AIS	TIS
1	APOP	AP/IFS/063 - POL EDG To Voucher Host System - Application Interface Specification AP/IFS/065 - APOP Host System Reporting To EDG Application Interface Specification	TI/IFS/008 - Horizon to Post Office Technical Interface Specification
2	APS	AP/IFS/003 - AP:Severn Trent Water Smart Key Interface Specification AP/IFS/004 - AP:Welsh Water Interface Specification AP/IFS/005 - AP:Girobank Interface Specification AP/IFS/006 - AP:Hampshire County Council Interface Specification AP/IFS/008 - AP:Eastern Electricity Smart Key Interface Specification	AP/IFS/030 - Pathway To Client Generic Technical Interface Specification AP/IFS/046 - Pathway To CQO Technical Interface Specification

		AP/IFS/009 - AP:Oxfordshire County Council Interface Specification AP/IFS/010 - AP:Anglian Water Interface Specification AP/IFS/011 - AP:Mid Kent Water Interface Specification AP/IFS/012 - AP:North West Water Interface Specification AP/IFS/013 - AP:Wessex Water Interface Specification AP/IFS/014 - AP:Yorkshire Water Interface Specification AP/IFS/015 - AP:Cambridge Water Interface Specification AP/IFS/016 - AP:United Kingdom Passport Authority Interface Specification AP/IFS/017 - AP:Three Valleys Water Interface Specification AP/IFS/018 - AP:Sun Alliance Interface Specification AP/IFS/019 - AP:Legal And Trade Interface Specification AP/IFS/020 - AP:South West Water Interface Specification AP/IFS/021 - AP:Yorkshire Electricity Giro Interface Specification AP/IFS/022 - AP:Vodafone Interface Specification AP/IFS/023 - AP:Yorkshire Electricity Interface Specification AP/IFS/024 - AP:Northern Ireland Electricity Host-Pc Interface Specification AP/IFS/028 - AP:British Telecom Interface Specification AP/IFS/032 - AP: Swalec Interface Specification AP/IFS/033 - AP:Scottishpower Interface Specification AP/IFS/036 - AP:Northumbrian Water Interface Specification AP/IFS/037 - AP:Knowsley Borough Council Interface Specification	

		AP/IFS/038 - Automated Payments Scottish Southern Energy Pocl Host/Client Interface Specification AP/IFS/040 - AP: North Surrey Water Interface Specification AP/IFS/042 - Pathway To Centeral Quantum Operations Application Interface Specification AP/IFS/043 - AP : Northern Ireland Electricity Interface Specification AP/IFS/044 - AP : British Gas Northern Interface Specification AP/IFS/045 - AP : Manweb Plc Interface Specification AP/IFS/047 - AP: Automated Payments Pocl Host/Client Systems Gec Watercard Interface Specification AP/IFS/053 - Pathway To Client Standard Watercard AIS AP/IFS/055 - APS DVL Northern Ireland Pocl Host/Client Interface Specification AP/IFS/056 - Pathway To Client Type 'G' Standard Magcard/Barcode Application Interface Specification AP/IFS/059 - Pathway To Client Type T Application Interface Spec AP/IFS/060 - Pathway To Client Bt Application Interface Specification AP/IFS/061 - Horizon To Client Type 'X' Magcard/Barcode Application Interface Specification AP/IFS/062 - Horizon To Client Type 'Xo' Application Interface Specification CR/IFS/002 - Automated Payments Interface Specification - EDG/Des	
4	Bureau (First Rate)	NB/IFS/012 - Bureau De Change - TPS To FRTS AIS RD/IFS/033 - Post Office to Fujitsu Services Application Interface Specification for Bureau de Change Rates	TI/IFS/008 - Horizon to Post Office Technical Interface Specification
5	CTS (AP Summaries)	EA/IFS/005 - Horizon To POL Client Transaction Summaries AIS	TI/IFS/008 - Horizon to Post Office Technical Interface Specification
6	DCS (Streamline)	EF/IFS/002 - Horizon - Streamline Application Interface Specification	EF/IFS/001 - Horizon - Streamline Technical Interface Specification

7	DVLA	DV/IFS/001 - Horizon To DVLA - Application Interface Specification	DV/IFS/002 - Horizon To DVLA - Technical Interface Specification
8	ETU (e-pay)	ET/IFS/001 - Application Interface Specification: Horizon To e-pay	ET/IFS/003 - Technical Interface Specification: Horizon To e-pay
9	LFS (SAP ADS)	BP/DES/023 - LFS to SAP ADS and SAP ADS to LFS Application Interface Specification BP/DES/022 – LFS Barcode Definitions	TI/IFS/008 - Horizon to Post Office Technical Interface Specification
10	NBS (Link, A&L, Card Account)	NB/IFS/024 - NBX - Link Application Interface Specification (AIS) NB/IFS/025 - NBX - Capo Application Interface Specification (AIS) NB/IFS/026 - NBX - A&L Application Interface Specification	NB/IFS/028 - NBX - Link Technical Interface Specification (TIS) NB/IFS/029 - NBX - A&L Technical Interface Specification (TIS) NB/IFS/027 – EMV – Banking NBX – POCA TIS
11	POL FS	EA/IFS/001 - Horizon To Post Office Ltd Financial Systems Application Interface Specification EA/IFS/002 - POL Finance Systems to TMS/Horizon Transaction Corrections Interface Specification EA/IFS/028 - Horizon To POL FS Interface Functional Specification The following are included for completeness, but are no longer relevant (either migration or Fujitsu is not responsible for the application) EA/IFS/007 - NRDS Vendor Master Data to POLFS Interface Specification EA/IFS/008 - POLFS General Ledger Master Data to NRDS Interface Specification EA/IFS/009 - NRDS Customer Master Data To POLFS Interface Specification EA/IFS/010 - NRDS Product Master Data To POL FS Interface Specification EA/IFS/014 - Error Notice (Tc) From CBDB To POLFS Interface Specification EA/IFS/016 - SAP ADS To POL FS Application Interface Specification EA/IFS/017 - Impact Programme Horizon To M1 (S70) Application Interface Specification EA/IFS/018 - Impact Programme Client Reported Errors Girobank To MI Application	AS/IFS/003 - Horizon To Post Office Limited Finance System Technical Interface Specification EA/IFS/029 - Impact Programme Management Information System S80 Technical Interface Specifications EA/IFS/030 - Impact Programme - POL Financial System S80 Technical Interface Specifications EA/IFS/032 - POL Finance Systems From Camelot Client Actuals Interface Specification EA/IFS/035 - Impact Programme Reference Data System S80 Technical Interface Specifications

		Interface Specification EA/IFS/023 - NRDS Client Master Data To POLFS Vendor Interface Specification EA/IFS/024 - Impact Programme POL FS To SAP ADS Application Interface Specification EA/IFS/025 - Impact Programme: POL FS to A&L - Application Interface Specification EA/IFS/026 - POL FS to NS & I Application Interface Specification BP/DES/030 – SAP ADS to POL FS Application Interface Specification	
12	POL MIS	EA/IFS/006 - Horizon To POL MIS AIS	TI/IFS/008 - Horizon to Post Office Technical Interface Specification
13	Reference Data	BP/IFS/008 - Application Interface Specification Reference Data To Pathway Non-Automated Type B Data BP/IFS/010 - Application Interface Specification Reference Data To Pathway BP/IFS/011 - Application Interface Specification Reference Data To Pathway Type B Data BP/IFS/012 - Application Interface Specification Reference Data To Pathway Type B Data	TI/IFS/008 - Horizon to Post Office Technical Interface Specification
14	HR SAP	EA/IFS/015 - Horizon To HR SAP System SPSO Counter Transaction Interface Specification	TI/IFS/008 - Horizon to Post Office Technical Interface Specification
15	TES Enquiry Service		NB/IFS/039 - Technical Interface Specification TES To POL
16	Track and Trace	AS/IFS/001 - Horizon To EDG AIS For Track And Trace	AS/IFS/002 - Horizon To EDG TIS For Track And Trace

3.6 Operational Schedule

The operational schedule is geared around the processing of data from the branches and delivery of that to the Post Office and Client systems. In addition there is data destined for the branches that needs to be delivered to the counter.

The actual schedule is quite complex due to the many different processes. The rough outline for the critical tasks is given below:

- 08:00 – Start of Branch Core Day (Monday to Saturday)
- 08:00 to 18:00 – Regular harvesting of LFS pouch delivery and collections for delivery to SAP ADS.
- 13:00 – End of Branch Core Day (Saturday)
- 18:00 – End of Branch Core Day (Monday to Friday)
- 19:00 – Branches declare "End of Day". Data is transferred from branches to the data centre over the next 30 minutes (randomised connections across the estate to avoid overloading the network).
- 19:00 to 20:30 – TPS and APS harvest data from the correspondence servers into their databases.
- 20:30 to 23:00 – TPS and APS host processing to produce files
- 22:00 to 23:00 – TES produces REC file for A&L and CAPO. REC Files delivered.
- 23:00 to 23:59 – Delivery of TPS and APS files to relevant systems
- 23:00 to 04:00 – TES Processing of LREC file from LINK. DWH and DRS processing.
- 23:00 to 08:00 – Backup of main databases once their overnight processing complete
- 20:30 to 21:30 – Backup of Correspondence Servers
- 20:30 to 02:00 – Processing and loading of reference data, APS tariff data and APS customer data into the correspondence servers (loading starts once correspondence server backup complete).
- 02:00 to 03:00 – Branches connect to the data centre to download any reference data required (randomised connections across the estate to avoid overloading the system).
- 03:00 to 03:15 – Branches reload the counter application through a process called "Clear Desk". This picks up any new reference data that is not dynamic.
- 06:00 – Processing of LFS Planned orders received from SAP ADS and loaded into correspondence server.
- 07:00 – Branches connect to the data centre to check for any LFS data or late reference data.

Full details of the operational schedule can be found in:

- AP/HLD/009 - APOP Maestro Schedule
- CS/HLD/003 - RDT Maestro Schedule High Level Design

- DW/LLD/027 - Data Warehouse Maestro Schedule - Solaris Systems
- LF/LLD/068 - LFS Host Maestro Schedule
- TD/DES/080 - Audit Server & Maestro Interface
- NB/HLD/019 - TES Maestro Schedule Design
- TD/DES/109 - Counter Application Scheduler High Level Design
- TD/HLD/001 - Pathway Maestro Schedule
- TD/HLD/002 - Horizon Maestro Schedule
- TD/HLD/002 - Horizon Maestro Schedule

4.0 Physical Architecture

This section describes the physical architecture of the solution excluding the network (which is covered under network services). It is split into data centres, other sites and branch infrastructure.

4.1 Data Centre

There are two data centres (Wigan and Bootle) to provide disaster tolerance with both sites handling business traffic. For some systems (typically those with databases) one site is used for normal operation with the 2nd site providing both resilience and DR.

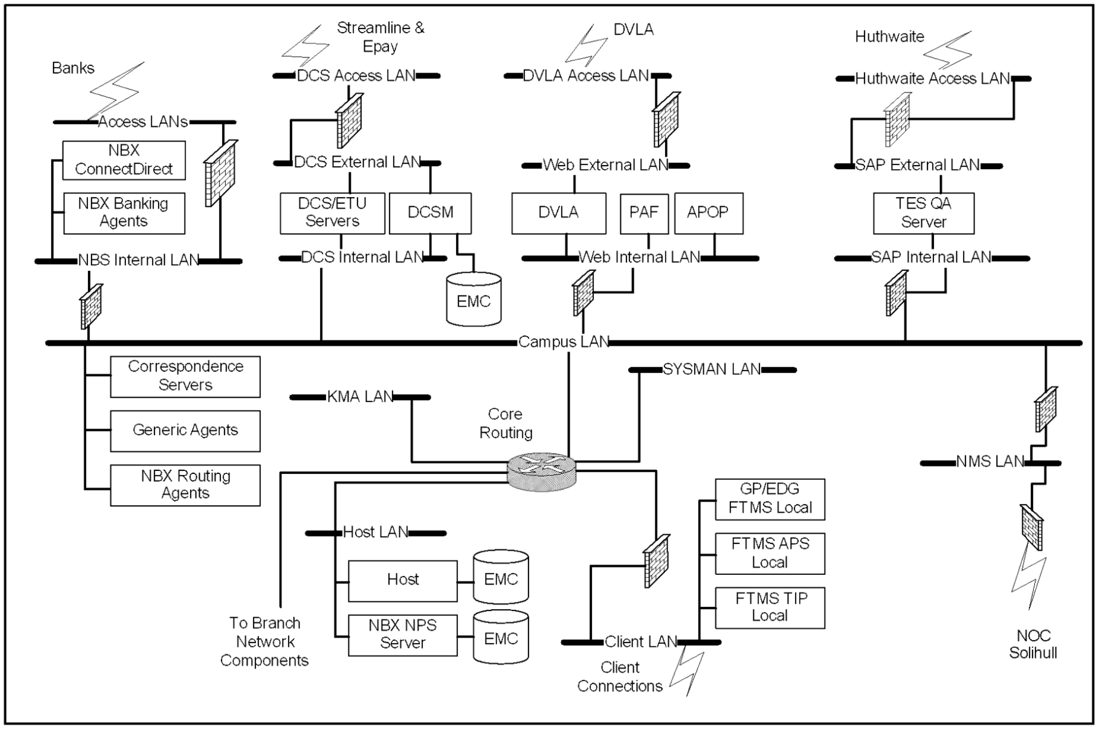
This section splits the data centre into a number of areas: business systems, POL-FS, SYSMAN, Storage and Audit and Support Systems. For each a brief description of the hardware, software and number of servers is provided.

All servers have the following software installed:

- Tivoli is included on all platforms for management. This is made up of the following products: IBM Tivoli Monitoring, IBM Tivoli Enterprise Console, IBM Tivoli Config Manager and IBM Remote Control [DN: Need to confirm this with Glenn].

4.1.1 Business Systems

The diagram shows the platforms for the business systems at one data centre (for location of VPN servers see LAN network diagram). The table gives details of these and the quantity at both sites (B=Bootle, W=Wigan).



#	Name	Function	Qty	Specification & S/W
1	APOP Application Web Server	Branch online APOP service	1 B 1 W	• Fujitsu Siemens RX200 S2, 2 cpu, 2G memory • Windows 2000 • Interstage App Server • Tivoli Client • APOP Web Service SD/DES/269 - APOP Web Service Platform Physical Design
2	Correspondence Servers	Messaging Server to pass messages to/from counters.	8 B 8 W	• Compaq DL360 (4 per site) and DL380 (4 per site), 2 cpu, 2G memory, Fibre channel connection on DL380 to EMC array • NT 4 • Riposte Message Server • Tivoli Client • Maestro Client • Brightstor Client (Windows) • Audit Agent • Deleted Object Monitor • Cluster Lookup Agent SD/DES/145 - Physical Design For Correspondence Server CSR+ (very out of date)

3	DCS Management Server	Runs DCS batch file jobs for payment files to/from Streamline and ETU and MTAS Disk is encrypted using Team crypto to protect payment files and EMIS	1 B 1 W	• Fujitsu Siemens F200, 2 cpu, 1G memory, Fibre Channel connection to EMC array • NT 4 • Team Crypto • Tivoli Client • Maestro Client • ETU Bulk Agent • S Bulk Agent • C2 Bulk Agent • C4 Bulk Agent • MTAS SD/DES/218 - Platform Physical Design for the DCS Management Server
4	DCS/ETU Servers	ETU and DCS Online Services	4 B 4 W	• Fujitsu Siemens F200, 2 cpu, 512M memory • NT 4 • Tivoli Client • DCS Auth Agent • ETU Auth Agent • ETU Rev Agent SD/DES/217 - Platform Physical Design for the DCS Agent Server
5	DVLA Application Server	Branch online service for DVLA	1 B 1 W	• Fujitsu Siemens, RX200, 2 cpu, 2G memory • Windows 2000 • Interstage App Server • Tivoli Client • DVLA Web Service SD/DES/239 - DVLA Web Service Platform Physical Design
6	FTMS APS Local	File transfer to AP Clients	1 B 1 W	• Compaq Proliant 5000, 4 cpu, ??? memory • NT 4 • Tivoli Client • FTMS SD/DES/163 - Physical Design for Pocl Aps Gateway Server - Local CSR+
7	FTMS GP/EDG Local	General purpose File Transfer and EDG connection for track and trace	1 B 1 W	• Fujitsu Siemens, RX200, 1 cpu, 1G memory • Windows 2000 • Tivoli Client • FTMS • Track and Trace Interface Agent SD/DES/262 - Edg (Gp) Ftms Local Gateway Physical Platform Design

8	FTMS TIP Local	File transfer to Post Office systems and BPOCL/WPOCL domain controller	1 B 1 W	• Compaq Proliant 5000 NT 4 cpu 512M memory • NT4 • Tivoli Client • FTMS SD/DES/165 - Physical Design for Pocl Tip Gateway Server - Local CSR+
9	Generic Agents	Runs agents that move data between databases and correspondence servers. Also some stand alone online services that use the correspondence servers.	4 B 4 W	• Compaq DL360 G2, 2 cpu, 2G memory • NT 4 • Tivoli Client • Maestro Schedule S/W • Riposte • Ping Agent • CAck Agent (including Smart Ping) • NBS Harvester • DCS Harvester • LFS Harvester • LFS Advice Loader • LFS Orders Loader • LFS Replenishment Delivery Notices Loader • APS Harvester • TPS Harvester • TPS Loader • EOD Harvester • Cluster Lookup Agent • Bureau Loader • Sub Group Loader • Non Core Loader • Memo Loader • Core Ref Data Loader • Ref Data Replicator • Ref Files Loader • Reference Data Scavenger • Quantum Bulk Loader • Quantum Emergency Loader • Water Loader • APS Ref Data Loader (same as Non Core Loader – configured to load from APS rather than RDDS) • Heartbeat Harvester • OMDB Harvester • Outlet Monitor • SLA Harvester • Key Object Loader • Key Object Harvester • Key Memo Loader SD/DES/138 - Physical Design for Agent Server CSR+

10	Host database server	Server that runs the Oracle databases for the business applications	1 B 1 W	• Fujitsu Siemens Prime Power 650, 8 cpu, 8G memory, Fibre channel connection to EMC array • Solaris • Oracle 8 and Oracle 9 • BMC Patrol (Oracle + Solaris KM) • Maestro Schedule S/W (Master) • Tivoli Client • Veritas Foundation Suite • Brightstor Client (UNIX) • APOP DB • DRS DB • TES DB • LFS DB • APS DB • TPS DB • RDMC DB • RDDS DB • Banking DWH DB SD/DES/234 - Solaris Host Infrastructure Design
11	NBX Banking Agents	Authorisation Agents for Banking	4 B 4 W	• Fujitsu Siemens R450, 2 cpu, 1G memory, Atalla Crypto Card • Windows 2000 • Atalla Load Balancing S/W • Riposte • Tivoli Client • Maestro Client • NBX Authorisation Agents (LINK, A&L, CAPO) NB/DES/007 - Platform Physical Design for the NBX Agent Server
12	NBX ConnectDirect Gateway	File transfer to/from banks	1 B 1 W	• Fujitsu Siemens RX100, 1 cpu, 1G memory • Windows 2000 • Tivoli Client • SQL*Server • Connect:Direct SD/DES/256 - Connect Direct Gateway Physical Platform Design Specification

13	NBX NPS RAC DB Server	Database server for NBX online application.	2 B 2 W	• Fujitsu Siemens Prime Power 650, 2 cpu 4G memory, Fibre channel connection to EMC array • Solaris • Oracle 9 RAC • BMC Patrol (Oracle + Solaris KM) • Maestro Schedule client) • Tivoli Client • Veritas Foundation Suite • Veritas Cluster S/W • Maestro Schedule S/W NB/DES/009 - Platform Physical Design Specification for Network Banking Oracle Real Application Cluster
14	NBX Routing Agents	Routes online traffic from correspondence servers to NBX authorisation agents	2 B 2 W	• Fujitsu Siemens RX200, 2 cpu, 1G memory • Windows 2000 • Tivoli Client • NBX Routing Agent • NBX GREV Agent • Track and Trace Harvester ??? NB/DES/008 - Platform Physical Design for the Nbx Routing Agent Server
15	PAF Application Server	Branch online PAF service	2 B 2 W	• Fujitsu Siemens RX200, 2 cpu, 2G memory • Windows 2000 • Tivoli Client • Interstage App Server • PAF Web Service • QAS Address Database SD/DES/238 - Paf Web Service Platform Physical Design
16	TES Query Application (QA) Server	Application layer for Post office to access TES and APOP databases	1 B 1 W	• Fujitsu Siemens Prime Power 250, 2 cpu, 2G memory • Solaris • Oracle App Server • Tivoli Client • TES Query Application • APOP Admin Application SD/DES/257 - Transaction Enquiry Service Query Application Platform Physical Design

17	VPN Loopback, Exception, Policy Management	Provides VPN management for VPN layer to branches	3 B 3 W	• Compaq Deskpro 6600, 1 cpu, 128 memory • NT 4 • Tivoli Client • Utimaco VPN SD/DES/125 - Physical Design for VPN Exception Server; SD/DES/126 - Physical Design for VPN Diagnostic Workstation CSR+; SD/DES/127 - Physical Design for VPN Policy File Manager Server CSR+
18	VPN Servers	Handles VPN connections from Branches	12 B 12 W	• Compaq DL360 NT 2 cpu , memory ???, • NT4 • Tivoli Client • Utimarco VPN Server SD/DES/124 - Physical Design for VPN Server CSR+ (note this is not up to date)

4.1.2 POL FS

The table below shows the platforms for POL-FS – the SAP system for the Post Office accounts. They are hosted in the Post Office DMZ except for the Centera array which is on the main LAN. The systems at Wigan are used for Testing. They also provide a half sized DR system in case of disaster at Bootle.

#	Name	Function	Qty	Specification
1	SAP Application Server	User access to SAP system	5 B 3 W	• Fujitsu Siemens Prime Power 450, 4 cpu, 8G memory • Solaris SD/DES/260 – Platform Physical Design Specification for POL FS Sap App Server
2	SAP Archive Centera Array	Archive of historical data	1 B 1 W	• EMC Centera EMC
3	SAP Archive Server	Archive of historical data	1 B 1 W	• Fujitsu Siemens Prime Power 450, 2 cpu, 8G memory • Solaris SD/DES/261 – Platform Physical Design Specification for POL FS Sap Archive Server
4	SAP Development Host Server	Host SAP database for development	1 B	• Fujitsu Siemens Prime Power 450, 2 cpu, 4G memory, fibre channel connection to EMC array • Solaris • Oracle SD/DES/254 – Platform Physical Design Specification for POL FS Sap Host

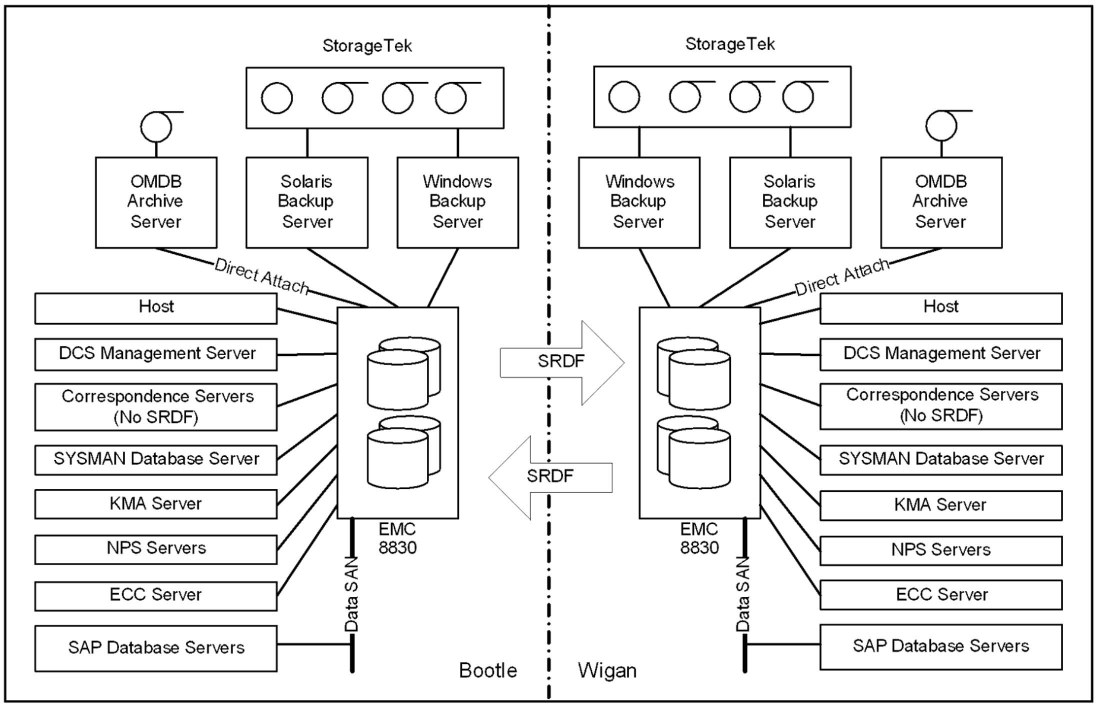
5	SAP Middleware Development	Development Support loading of batch data into SAP	2 B	• Fujitsu Siemens FSC Prime Power 450, 2 cpu, 16G memory • Solaris SD/DES/264 – Platform Physical Design Specification for the POL FS Sap Middleware Server
6	SAP Middleware Server	Support loading of batch data into SAP	2 B 2 W	• Fujitsu Siemens FSC Prime Power 450, 4 cpu 16G memory • Solaris SD/DES/264 – Platform Physical Design Specification for the POL FS Sap Middleware Server
7	SAP Production DR/QATest Server	Database server at DR site – used for QATest	1 W	• Fujitsu Siemens FSC Prime Power 1500, 8 cpu, 16G memory, fibre channel connection to EMC array • Solaris • Oracle SD/DES/254 – Platform Physical Design Specification for POL FS Sap Host
8	SAP Production Server	Database Server for main site	1 B	• Fujitsu Siemens FSC Prime Power 1500,16 cpu, 40G memory, fibre channel connection to EMC array • Solaris • Oracle SD/DES/254 – Platform Physical Design Specification for POL FS Sap Host
9	SAP Production Support Server	???	1 B	• Fujitsu Siemens FSC Prime Power 450, 4 cpu, 8G memory • Solaris SD/DES/254 – Platform Physical Design Specification for POL FS Sap Host
10	SAP SMC Console for PW1500	Support server for PW1500	2 B	• Sun UltraAX-e2, 1 cpu, memory ??? • Solaris ??? Documentation ???

Notes:

1. Need to check on #1 at DR site – EA/DPR/005 has 2 at DR site
2. What is #9 – can't find in EA/DPR/005
3. Need to add other s/w onto list

4.1.3 Storage and Audit

The diagram shows the SAN for storage and backup. In addition there are a number of platforms used for archiving which are attached to the central network which are not shown.

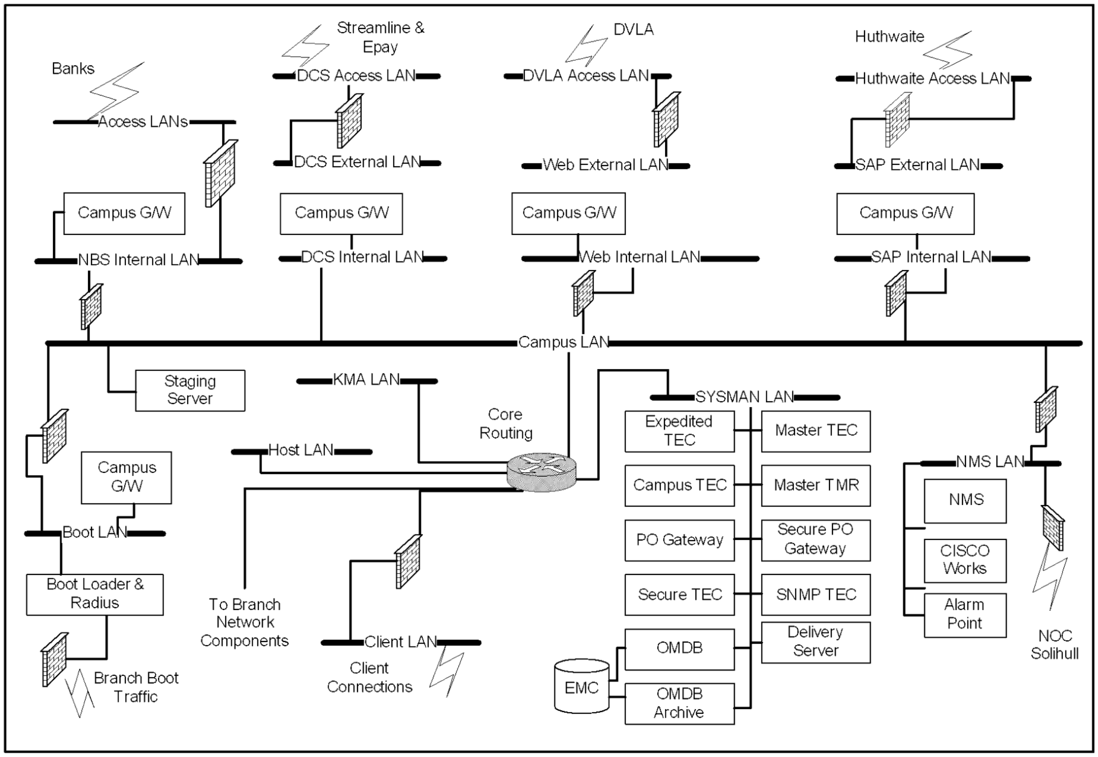


#	Name	Function	Qty	Specification
1	Audit Centera Array – Live (not in diagram)	7 year archive of data produced by Horizon	1 B 1 W	• EMC Centera array
2	Audit Server (not in diagram)	Server that archives the data into the Centera and supports retrieval.	1 B 1 W	• Compaq Proliant 7000, 4 cpu, 256M memory, local disk storage • NT 4 • Tivoli Client • SQL*server SD/DES/139 - Physical Design for Audit Server CSR+
3	Backup server - Solaris	Backs up Solaris platforms via EMC BCV for main systems and over the network for smaller systems.	1 B 1 W	• Fujitsu Siemens Prime Power 200, 2 cpu, 2G memory, fibre channel connection to EMC array • Solaris • Tivoli Client • Brightstor backup software SD/DES/259 - Platform Physical Design for Solaris Backup Server

4	Backup sever - Windows (aka Correspondence Server Backup)	Backs up Windows platforms via EMC BCV for main systems and over the network for smaller systems.	1 B 1 W	• Fujitsu Siemens RX300, 2 cpu, 2G memory, fibre channel connection to EMC array • Windows 2000 • Solaris • Tivoli Client • Brightstor backup software SD/DES/251 - Windows Backup Server Physical Platform Design
5	Backup StorageTek ACSLS Server	Controller for the tape library to allow multiple platforms to share	1 B 1 W	• Sun Sunfire v100, 1 cpu, memory ??? • Solaris
6	Backup Tape Library	Library shared by the backup servers	1 B 1 W	• StorageTek Tape Library
7	EMC Array	Main storage array	1 B 1 W	• EMC 8830 EMC
8	EMC ECC Server	Control software for the EMC array	1 B 1 W	• Fujitsu Siemens RX300 2 cpu 4G memory, fibre channel connection to EMC array • Windows 2000 SD/DES/271 - Ecc Server Platform Physical Design Specification

4.1.4 SYSMAN Platforms

The following platforms are used to support Systems management



#	Name	Function	Qty	Specification
1	Core Services Insight Manager Server	Provides hardware monitoring for servers	1 B 1 W	• ??? Specification ??? Documentation
2	Network Alarm Point Server	Raises Alerts on network failures	1 B 1 W	• Fujitsu Siemens RX100, 1 cpu, memory ?? • Windows 2000 ??? Documentation
3	Network CISCO Works Server	Network configuration	1 B 1 W	• Sun Sunfire 280R, 1 cpu, memory ??? • CISCO Works ??? Documentation
4	Network Management Server (NMS)	Staging platform for configurations to ISDN routers and Radius servers (Is this correct??)	1 B 1 W	• Fujitsu Siemens Scenic E600, 1 cpu, 1G memory • Windows 2000??? ??? Documentation

FUJ00098217

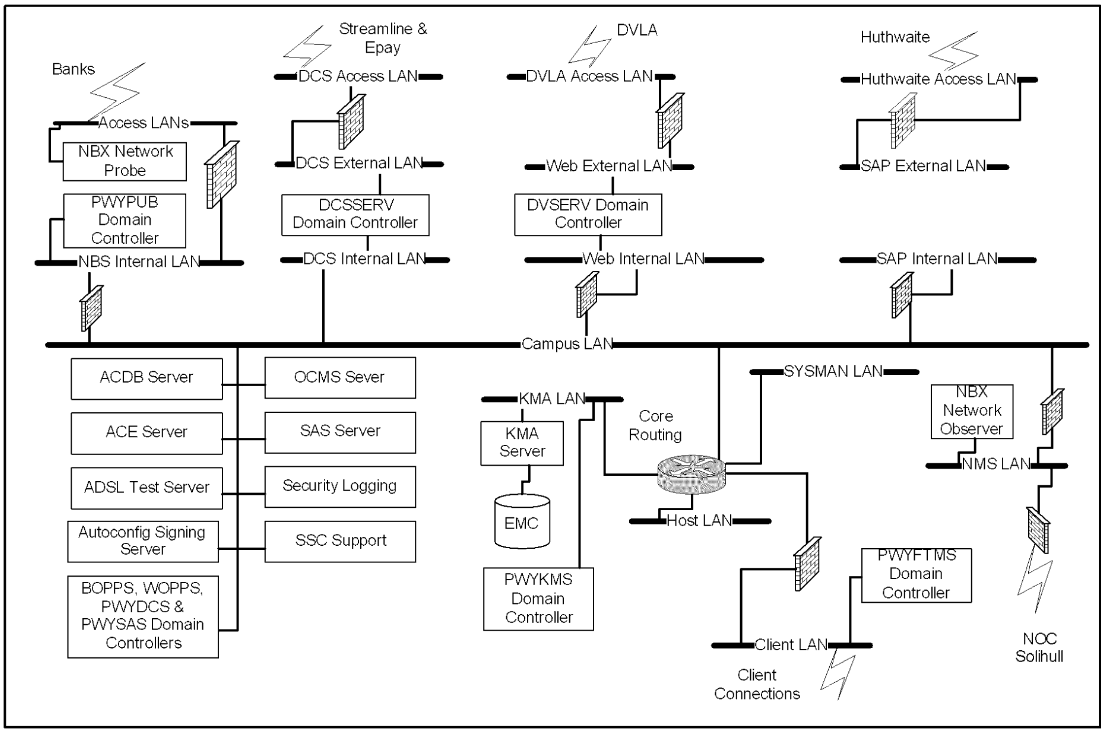
5	Network Management System (HP Openview)	Network Monitoring	1 B 1 W	• Sun Sunfire V890, 4 cpu, 16G memory • Solaris • HP Openview ??? Documentation
6	SYSMAN Delivery Server	Acts as gateway between PVCS and live system for code delivery. Also used for immediate fixes before counter is taken on by Tivoli framework	1 B 1 W	• Compaq Proliant 1600R, 1 cpu, 256M memory • NT 4 • Tivoli Client SY/DES/022 - Platform Physical Design Specification for the SYSMAN Delivery Server
7	SYSMAN Campus Gateway	Tivoli Gateways within DMZ Banking DMZ - 2 per site DCS DMZ - 2 per site PAF DMZ - 2 per site EDG DMZ - 2 per site Boot Loader DMZ - 1 per site	9 B 9 W	• Sun Sunfire v100, 1 cpu, 1G memory • Solaris ??? Documentation
8	SYSMAN Campus TEC	Tivoli TEC for campus events	3 B 3 W	• Sun Sunfire v100, 1 cpu, 512M memory • Solaris ??? Documentation
9	SYSMAN Expedited TEC	Tivoli TEC for expedited events	2 B 2 W	• Sun Sunfire v100, 1 cpu, 512M memory • Solaris SY/DES/023 - Platform Physical Design Specification for the SYSMAN Expedited TEC
10	SYSMAN Master TEC	Master TEC	1 B 1 W	• Sun SunFire 250, 1 cpu, 500M memory • Solaris SY/DES/026 - Platform Physical Design Specification for the SYSMAN Master TEC
11	SYSMAN Master TMR	Master TMR	1 B 1 W	• Sun SunFire 280R, 1 cpu, 1.5G memory • Solaris SY/DES/031 - Platform Physical Design Specification for the SYSMAN Master TMR

12	SYSMAN Operational Management Data Base (OMDB)	Main Database for Tivoli. Contains event archive, inventory and other data.	1 B 1 W	• Compaq DL580, 4 cpu, 2G memory, fibre channel connection to EMC array • NT 4 • Oracle SY/DES/027 - Platform Physical Design Specification for the Operational Management Data Base
13	SYSMAN Operational Management Database Archive Server	Backs up OMDB via EMC BCV (see storage)	1 B 1 W	• Compaq Proliant 5000, 4 cpu 1G memory, fibre channel connection to EMC array • NT 4 SY/DES/028 - Platform Physical Design Specification for the SYSMAN Operational Management Database Archive Server
14	SYSMAN Post Office Gateway	Gateway for counters on installation before they are fully taken on	1 B 1 W	• Sun Netra, 1 cpu, 256M memory • Solaris SY/DES/029 - Platform Physical Design Specification for the SYSMAN Post Office Gateway
15	SYSMAN Secure Post Office Gateway	Gateway for counters once they have been taken on. Estate split over 10 servers. 11th acts as a hot standby	11 B 11 W	• Sun Netra, 1 cpu, 256M memory • Solaris SY/DES/030 - Platform Physical Design Specification for the SYSMAN Secure Post Office Gateway
16	SYSMAN Secure TEC	Secure TEC	2 B 2 W	• Sun Sunfire v100, 1 cpu, 512M memory • Solaris SY/DES/025 - Platform Physical Design Specification for the SYSMAN TEC
17	SYSMAN SNMP TEC	SNMP gateway	1 B 1 W	• Sun Sunfire v100, 1 cpu, 512M memory • Solaris SY/DES/033 - Platform Physical Design Specification for the SYSMAN SNMP TEC
18	Core Services Staging Server	Staging of software for manual s/w distribution	1 B 1 W	• Compaq Proliant 1600 NT 1 cpu 128M memory SD/DES/185 - Physical Design for Staging Server CSR+

[DN: Not sure that the NMS (where radius configs/ISDN router configs) are delivered to is the platform above or whether a different one]

4.1.5 Supporting Systems

The diagram below how other supporting platforms fit into the solution (boot loader and boot server not shown – see LAN diagram).



#	Name	Function	Qty	Specification
1	ACDB Server	Autoconfiguration database server	1 B 1 W	• Fujitsu Siemens RX200, 2 cpu, 2G memory • Windows 2000 • Tivoli Client • SQL*Server SD/DES/142 - Physical Design for Auto Configuration Database Server CSR+

2	ACE Server	Provides SecureId access	1 B 1 W	• Sun Ultra5_10, 1 cpu, 128M memory • Solaris • Tivoli Client • ACE Software SD/DES/203 - Physical Design for SecureId Ace Server CSR+
3	ADSL Test Server	Allows a test to be conducted (movement of large file) on activation of ADSL in the branch to confirm working okay	1 B 1 W	• Fujitsu Siemens RX100, 1 cpu, 2G memory • Windows 2000 • Tivoli Client SD/DES/255 - Platform Physical Design Specification for the ADSL Test Server
4	Aurora Console Tower (Solaris Console Server)	Console access to Solaris servers	1 B 1 W	• Sun ???, 1 cpu, memory ??? ??? Documentation
5	Autoconfig Signing Server	Digitally signs autoconfig files to allow tamper check to be made on counter.	1 B 1 W	• Fujitsu Siemens RX200, 2 cpu, 2G memory • Windows 2000 • Tivoli Client SD/DES/180 - Physical Design for Auto Configuration Signing Server CSR+
6	Boot Loader	Provides Boot access for gateway PC for ISDN and ADSL network types.	1 B 1 W	• Fujitsu Siemens RX100, 1 cpu, 1G memory • Windows 2000 • Radius S/W • Tivoli Client SD/DES/232 - Bootloader Physical Platform Design
7	Boot Server	Provides boot access for VSAT network types. Also BBOOT/WBOOT domain controller	1 B 1 W	• Compaq ???, 1 cpu ??? memory ??? • Windows NT • Tivoli Client SD/DES/027 - Physical Design for Boot Server (note: out of date)
8	BTI Print Server	Raises paging alerts on Host errors	1 B 1 W	• Sun Ultra5, Solaris, 1 cpu memory ??? • Solaris ??? Documentation

9	Checkpoint Firewall-1 Firewall	Firewall (see network section for where used)	2 B 2 W	• Sun Ultra5_10, 1 cpu, memory ??? • Solaris • Checkpoint ??? Documentation
10	Domain Controllers - BOPSS/WOPSS	Domain controllers for main campus severs (e.g. correspondence servers). Separate domains for Wigan and Bootle	2 B 2 W	• Compaq Deskpro 6000, 1 cpu, 32M memory • NT 4 • Tivoli Client SD/DES/148 - Physical Design for Domain Controller CSR+
11	Domain Controllers - BVPN/WVPN	Domain Controllers for VPN domain. Separate domains for Wigan and Bootle	2 B 2 W	• Compaq Deskpro 6000, 1 cpu, 32M memory • NT 4 • Tivoli Client SD/DES/148 - Physical Design for Domain Controller CSR+
12	Domain Controllers – DCSSERV	Domain Controllers for DCS DMZ. Single domain across Wigan and Bootle	1 B 1 W	• Compaq Deskpro 6000, 1 cpu, 32M memory • NT 4 • Tivoli Client ??? Is the platform correct ??? SD/DES/148 - Physical Design for Domain Controller CSR+
13	Domain Controllers – DVSERV	Domain Controllers for DVLA DMZ (including APOP and PAF). Single domain across Wigan and Bootle	1 B 1 W	• Fujitsu Siemens RX100, 1 cpu, 512M memory ??? • NT 4 • Tivoli Client ??? Documentation
14	Domain Controllers – PWYDCS	Domain controllers for Master/Account domain (contains all users)	1 B 1 W	• Compaq Deskpro 6000, 1 cpu, 32M memory • NT 4 • Tivoli Client SD/DES/148 - Physical Design for Domain Controller CSR+
15	Domain Controllers – PWYFTMS	Domain controllers for APS and EDG/GP FTMS Servers	1 B 1 W	• Compaq Deskpro 6000, 1 cpu, 32M memory • NT 4 • Tivoli Client SD/DES/148 - Physical Design for Domain Controller CSR+

16	Domain Controllers – PWYKMS	Domain controllers for KMA	2 B 2 W	• Compaq Deskpro 6000, 1 cpu, 32M memory • NT 4 • Tivoli Client SD/DES/148 - Physical Design for Domain Controller CSR+
17	Domain Controllers – PWYPUB	Domain controllers for Banking DMZ. Single domain across Wigan and Bootle.	2 B 2 W	• Fujitsu Siemens FSC RX100 NT 1 cpu 512M memory • NT 4 • Tivoli Client ??? Is the platform correct ???
18	Domain Controllers – PWYRAD	Domain Controllers for Radius Servers. Single domain across Wigan and Bootle.	1 B 1 W	• Compaq Deskpro 6000, 1 cpu, 32M memory • NT 4 • Tivoli Client ??? Is the platform correct ??? SD/DES/148 - Physical Design for Domain Controller CSR+
19	Domain Controllers – PWYSAS	Domain controllers for SAS servers. Single Domain across Wigan and Bootle.	1 B 1 W	• Compaq Deskpro 6000, 1 cpu, 32M memory • NT 4 • Tivoli Client • ??? Is the platform correct ??? SD/DES/148 - Physical Design for Domain Controller CSR+
20	KMA Server	Database Server for KMA key management	1 B 1 W	• Compaq Proliant 5500, 2 cpu, 256M memory, fibre channel connection to EMC array. • NT 4 • SQL*Server • Tivoli Client SD/DES/133 - Physical Design for KMA Server CSR+
21	NBX Network Observer Server	Pulls network traces from Network Probe server to present to support user (in Network Management LAN)	1 B 1 W	• Fujitsu Siemens RX100, 1 cpu, 1G memory • Windows 2000 • Tivoli Client SD/DES/267 - Platform Physical Design Specification for the Network Observer

22	NBX Network Probe Server	Allows network traces to be taken between Horizon and banks	3 B 3 W	• Fujitsu Siemens RX100, 1 cpu, 2G memory • Windows 2000 • Tivoli Client SD/DES/266 - Platform Physical Design Specification for the Network Probes
23	OCMS Server	Operation Change Management System database server	1 B 1 W	• Compaq Proliant 1850R, 1 cpu, 256M memory • NT 4 • Tivoli Client • SQL*Server SD/DES/197 - Physical Design for OCMS Server CSR+
24	Radius Servers (Accounting, Management)	Accounting and Management records for radius connections	2 B 2 W	• Fujitsu Siemens RX100, 1 cpu, 1G memory • Windows 2000 • Tivoli Client • Radius S/W SD/DES/240 - Platform Physical Design Specification for the S60 Accounting Radius Server
25	Radius Servers (Dialledx3, ADSL)	Radius Servers to authenticate network access	4 B 4 W	• Compaq DL360 G2, 1 cpu, 256M memory • Windows 2000 • Tivoli Client • Radius S/W SD/DES/252 - Platform Physical Design Specification for the S60 Radius Dial (Authentication) Server; SD/DES/253 - Platform Physical Design Specification for the S60 Radius ADSL (Authentication) Server
26	SAS Server	Support access service. Terminal server to allow access to the data centre platforms for support.	3 B 3 W	• Fujitsu Siemens FSC R250 Windows 2000 1 cpu 2G memory SD/DES/224 - Platform Physical Design Specification for the Secure Access Server

27	Security Logging Analysis Server	Pulls security logs together for analysis	1 B 1 W	• Fujitsu Siemens FSC RX100 Windows 2000 1 cpu 2G memory SD/DES/272 - Platform Physical Design Specification for the Security Logging Server
28	Softek Servers	Provides analysis of network Radius records	2 B 2 W	• Fujitsu Siemens RX100, 1 cpu, 2G memory • Windows 2000 • Tivoli Client • Softek software SD/DES/250 - Platform Physical Design Specification for the Softek Reporter Software
29	SSC Support Server	Data storage and work area used by 3rd line support.	1 B 1 W	• Compaq Proliant 1850R, 1 cpu, 256M memory, local disk storage • NT 4 • Tivoli Client SD/DES/194 - Physical Design for SSC Support Server for CSR+

4.2 Other sites

There are a number of other sites that have servers and workstations. These are summarised by the table below:

#	Name	Function / Site	Specification
1	SSC Workstation	3rd Line Support Workstation. BRA01	SD/DES/172 - Physical Design For SSC Support Workstation Csr+
2	MIS Workstation	MSU Workstation BRA01	SD/DES/222 - Platform Physical Design Specification For The MIS Client Workstation SD/DES/223 - Platform Physical Design Specification For The MIS Support Workstation
3	RDT Rig RDMC Workstation	Validation of Reference Data changes before release into live BRA01	A number of systems including Solaris Host, Correspondence Servers, Agents and counters. SD/DES/167 - Physical Design For RDMC Administrator Workstation Csr+

4	Systems Management Workstations	2nd Line support (STE04) and Release Management (BRA01)	SD/DES/196 - Physical Design For Systems Management Access Workstation SY/DES/035 - Platform Physical Design Specification For Smc Workstation
5	PIN Pad generation Workstation	Management of PIN Pads Keys BRA01 secure room	SD/DES/211 - Platform Physical Design Specification For The Pin Pad Key Generation Workstation SD/DES/213 - Platform Physical Design Specification For The Pinpad Proving Workstation
6	Audit Workstations	Audit and litigation support access. BRA01	SD/DES/077 - Physical Design For Audit Workstation SD/DES/140 - Physical Design For Audit Workstation Csr+
7	KMA Workstation	Management of Keys BRA01 secure room	SD/DES/134 - Physical Design For KMA Workstation Csr+ SD/DES/135 - Physical Design For KMA Administration Workstation Csr+
8	Certificate Root Server	Production of root certificates. BRA01 secure room	SD/DES/136 - Physical Design For Ca Workstation Csr+
9	Atalla Card Loading Workstation	Loading of secure keys into Atalla cards. BRA01 secure room	SD/DES/214 - Platform Physical Design Specification For The Atalla Key Loading Workstation
10	Remote FTMS Servers	Remote server for handling file transfers. Huthwaite AP Clients	SD/DES/164 - Physical Design For POCL APS Gateway Server - Remote CSR+ SD/DES/166 - Physical Design For POCL Tip Gateway Server - Remote CSR+ SD/DES/263 - EDG (GP) FTMS Remote Gateway Physical Platform Design
11	One shot Password	Generation of one shot passwords for the branch by the help desk. STE04	SD/DES/162 - Physical Design For One Time Password Workstation Csr+
12	SecureID Workstation	Management of Secure ID for the data centres. BRA01	SD/DES/171 - Platform Physical Design Specification For Securid Workstation
13	Anti Virus Workstation	Management of Anti Virus. BRA01	SD/DES/212 - Platform Physical Design Specification For The Antivirus Workstation
14	KMS Help Desk Workstation	Access to key management system for some help desk functions. STE04	SD/DES/230 - Platform Physical Design Specification For KMS Help Desk Workstation
15	Network Management Workstation	Network Management. Wigan	SD/DES/274 - Platform Physical Design For Network Management Workstations

16	Security workstation	Analysis of security issues. BRA01	SD/DES/273 - Platform Physical Design Specification For The Security Workstation

4.3 Branch Infrastructure

A Post Office branch consists of 1 or more PCs with each PC having a number of peripheral devices attached. In branches with more than 2 positions un-managed 10Mbit/s hubs are used to connect the PC together.

The normal configuration for a Counter position is:

- PC Base Unit (400MHz Pentium II with 256Mbytes of memory and a PCI card providing multiple serial connections)
- Touch Screen (touch element connected via a serial connection to PC)
- LIFT Keyboard incorporating a Magnetic Swipe and Smart Card reader (serial connection for card reader)
- BAR Code Scanner (Serial Connection)
- Slip and Tally Roll Printer (Serial Connection)
- Weigh Scales (serial connection – normally shared between two counters with both counters having a separate serial connection).
- PIN Pad (Serial Connection)
- Optionally a Bureau de Change Rates Board (serial connection)

One PC in each branch acts as the "gateway PC" which provides network connectivity to the data centre and also acts as a server for a parallel port connected back office printer. There are two types of gateway PC:

- RAS which supports ISDN, ADSL and serial connected modems. This ISDN and ADSL connectivity is provided through internal PCI cards.
- VSAT which uses a LAN connection to plug into a PES (Personal Earth Station).

In single counter branches, the gateway PC has a second (removable) hard disk to protect data against hard disk failure. This is achieved through the use of a second Riposte instance which replicates data from the instance that is using the internal hard disk.

In addition, there is a mobile variant (nicknamed the "luggable") that is used in multiple locations.

These combinations lead to the following hardware types:

1. RAS Gateway – Single Counter
2. RAS Gateway – Multi Counter

3. VSAT Gateway – Single Counter
4. VSAT Gateway – Multi Counter
5. Mobile RAS
6. Mobile VSAT
7. Slave

Details of the Horizon configurations can be found in [BP/DES/003] and [CE/SPE/025].

5.0 Information Management

The table below summarises the data stored in each of the key systems in the solution:

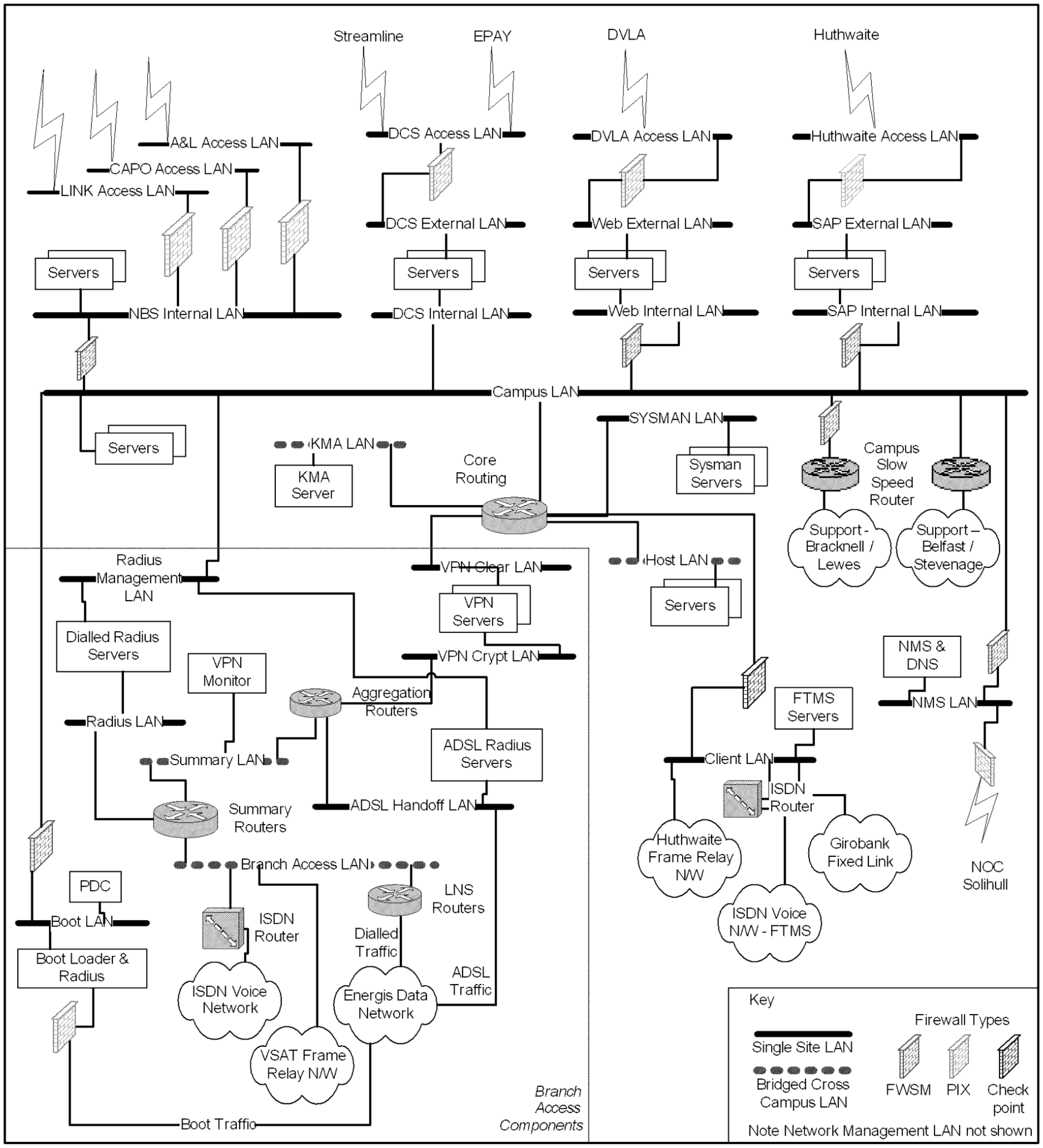
#	Database/System	Function/Data	Storage Period
1	TPS	Full transaction details sent nightly to other systems. Summary of some data once per month.	Up to 1 month for summary, full details 2 days
2	APS	APS Transactions sent nightly to AP Clients. Some data sent 5 days per week or once per week.	Up to 7 days, most 2 days
3	LFS	Transmission of data to/from SAP ADS	2 days
4	DRS	NBS, DCS and ETU reconciliation	3 months
5	TES	NBS Queries	6 months
6	DWH	NBS, DCS and ETU MIS Queries	3 months
7	RDMC & RDDS	Reference data	Permanent
8	Correspondence Servers and Counters	All transactions undertaken at counters.	42 days
9	OCMS & ACDB	Estate Management Data	Permanent
10	MTAS	MID/TID Allocation for branches	Permanent
11	KMS	Key management for branches	Permanent
12	OMDB & SMDB	Systems management for system	Permanent
13	NPS	Banking Persistent Data required to support online transactions	5 days
14	Audit (Centera)	Audit trail of solution	7 years

6.0 Network Services

This section covers the Network Services required for Horizon. It is split into Data Centre LAN, Main WAN circuits, Branch network and other circuits.

6.1 Data Centre LAN

The diagram below shows a logical view of the LAN within a single data centre.



[DN: Need to add the context switches to the picture]. The Context switches are to provide load balancing across the multiple servers for the applications (see Resilience section for more detail).

[DN: Need to add Boot Server to the picture – where does it go?]

6.2 WAN Circuits

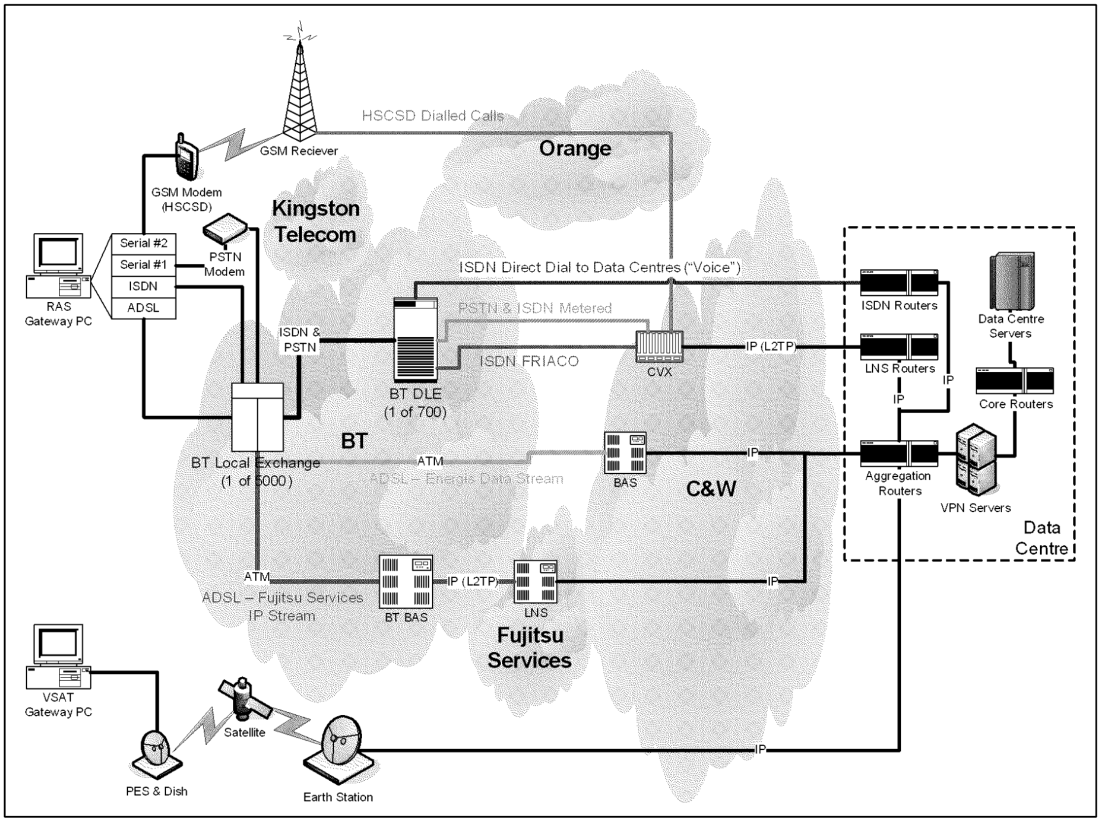
The data centres need to be connected to other sites to either carry business traffic or support traffic. The list below shows the connections and how they are provided. For most remote sites, Fujitsu has networking equipment required to provide the service (e.g. routers).

Type	Item	Data Centre Site Supplier	Other Site Supplier
Support Access	There are fixed circuits from the data centres to the following sites: 1. Bracknell 2. Stevenage 3. Belfast In addition there is an ISDN connection into Crewe for OBC team 4. Crewe	C&W – 1, 2, 4 BT - 3	C&W – 1, 2 BT – 3, 4
Streamline for debit card	1. Online Payment over X25 2. Batch Files, Bonded ISDN	1. TNS 2. C&W	1. TNS 2. Third Party
E-Pay for ETU	Twin 2 Mbits/s circuits with diverse routing into each site: 1. E-Pay Site 1 2. E-Pay Site 2 The E-Pay circuits are provided by C&W using IP Select.	C&W	C&W
DVLA for Car Tax	Twin 256 Kbit/s circuits with diverse routing into each site: 1. DVLA Site 1 2. DVLA Site 2 The DVLA circuits are provided by C&W using IP Select.	C&W	C&W
A&L for Banking	Twin 128 Kbit/s with diverse routing into each site: 1. A&L Main Site 2. A&L DR Site	C&W	C&W
EDS Card Account for Banking	Connections to the main and DR sites. These circuits are not part of the Fujitsu Service.	Third party	N/A
LINK for Banking	Connections to the main and DR sites. These circuits are not part of the Fujitsu Service	Third party	N/A
Post Office Ltd	Access from Huthwaite for Back Office access is via twin 2 Mbits/s with diverse routing. There are also connections into the DR site at Sunguard. These circuits are provided by C&W using IP Select. Also Frame relay connections for legacy connections. These are expected to be discontinued shortly.	C&W	C&W

Branch Main Access	All data from the branches for the main network is carried into the data centres through IP Select connections from the branch network provider. There will be twin (diversely routed) 155Mbit/s connections into each data centre to provide resilience.	C&W	C&W
Branch Direct Dial Access	To direct dial the branches from the data centres ISDN PRI are required.	C&W	N/A
Intercampus	The network between the data centres is use twin 1Gbit/s connections (diversely routed) to provide resilience.	C&W	C&W
VSAT Access	Frame Relay links from Hughes	C&W	C&W

6.3 Branch network

The diagram below shows a simplified version of the networks that make up the branch network:



There are two types of branches – the majority use a RAS Gateway PC, with a very small number (around 150) using a VSAT connection. VSAT is used where distance limits from the exchange prohibit the use of ADSL or ISDN.

RAS branches operate in one of two primary configurations: ISDN or ADSL. ADSL is the favoured configuration as it is lower costs and easier to manage, although there are some exchanges that BT has yet to enable.

Branches in Hull have a network service from Kingston telecom (rather than BT) and this uses ISDN connections. Investigations are underway by Core Services into how to provide ADSL for these sites.

All branches have VPN between the gateway PC and the data centre (see RS/DES/046 - VPN High Level Design]

6.3.1 ISDN Branches

For ISDN Branches, there are three possible routes to the data centre:

- Direct Dial (so called "Voice") in which one of the data centres is dialled directly by the branch. Resilience is achieved through having different numbers for each data centre. This route is bi-directional with the data centre also able to dial the branch. Call charges are billed by time.
- ISDN Metered in which a call is placed to the C&W CVX. The CVX answers the call and delivers IP (tunnelled as L2TP) to one of the data centres. Resilience is achieved through the tunnel connecting to an alternate data centre on failure. Call charges are billed by time.
- ISDN FRIACO which logically behaves the same way as ISDN metered, except for billing where a fixed cost per port is made irrespective of usage. Within C&W and BT the routing is also different with a fixed circuit between each DLE and C&W to handle these types of calls (for ISDN metered, normal call routing is applied between BT and C&W). Note that FRIACO is not available for Kingston Telecom branches. The FRIACO service purchased from C&W is only available during the day (01:00 to 17:30 Monday to Friday, 01:00 to 13:00 Saturday and 01:00 to 08:00 Sunday)

These routes are combined to provide different services as follows:

- Voice Dial On Demand – Branches always dial the data centre directly.
- Bronze Dial On Demand – Branches use a Metered connection if working with direct dial to the data centre as a second choice. This used to be much cheaper than the Voice Dial on Demand solution, but recent tariff changes mean that both services have similar running costs.

- Silver Daytime FRIACO – Branches hold open a FRIACO connection during the day, using a metered connection if this is not available. Out of hours they behave as bronze sites. This is used for larger sites.
- Silver Daytime Metered - Branches hold open a metered connection during the day. Out of hours they behave as bronze sites. This is very expensive and is therefore only used for a handful of large sites that cannot get FRIACO.

Details of how these behave can be found in TD/SDS/002 - Counter Network Infrastrucutre Manager (CNIM).

In addition, a "data recovery (Day J)" connection is possible using either PSTN or Mobile (HSCSD) that uses a metered connection. This is used when a phone line is broken for many days and data needs to be retrieved from the PC in the branch.

6.3.2 ADSL Branches

There are two types of ADSL in the solution - C&W Data Stream and Fujitsu Services IP Stream. Initially it was expected that all branches would use the Data Stream version, but this has proved to be expensive to rollout to the whole estate – particularly where only a few branches are connected to a BT local exchange. Therefore Fujitsu Services IPStream will be used for all low density exchanges (typically rural ones - estimated at 7,000 branches) with C&W data stream being used for the urban ones. [DN: rollout expected summer 06]

Two variants of IPStream are used depending on the size of the branch (larger branches need more guaranteed bandwidth to ensure good response times for online transactions):

- IP Stream Home for 1 to 3 counters – notionally a 50:1 connection ratio
- IP Stream Office for 4+ counters – notionally a 20:1 connection ratio.

ADSL branches can also use other connection types:

- Initial configuration is downloaded via PSTN (see estate management) via a metered called.
- Approximately 2000 branches are able to use ISDN as a backup (when in backup mode ISDN is held open permanently on a metered connection).
- Where an Orange signal is available an "on demand" backup service is available to allow the branch to operate using HSCSD via a modem carried by the engineer.

Further details can be found in:

- TD/SDS/004 - ADSL - High Level Design
- AS/DPR/025 – IPStream Design Proposal
- EP/HLD/002 - High Level Design - Branch Network Resilience

6.3.3 VSAT Branches

Where distance limits from the local exchange prohibit the use of ADSL or ISDN, then a VSAT connection is used.

For these a PES (personal earth station) is plugged into a VSAT gateway PC (which has a WAN network card as well as the LAN network card.

The use of VSAT is problematic in terms of reliability and planning permission for the dish. Once all branches than can be are moved to ADSL, it is planned to migrate the remaining VSAT branches to fixed circuits.

6.4 IP Addressing

This can be split into two areas, consisting of a Private Internet space termed the Horizon Private Internet Address space (PAS) and the Horizon Boundary Address space (BAS).

All PAS members are allocated from the IPv4 Address Space according to RFC 1918. PAS is a strict subset of RFC 1918 with well defined boundaries.

For each 3rd party with which Horizon exchanges IP data grams a Peering IP address island is defined. The collection of all such Peering IP address islands is orthogonal from each other and their union is the BAS.

It is intended that all members of the BAS are RFC1918 addresses however exceptions to fit in with 3rd party requirements will be considered.

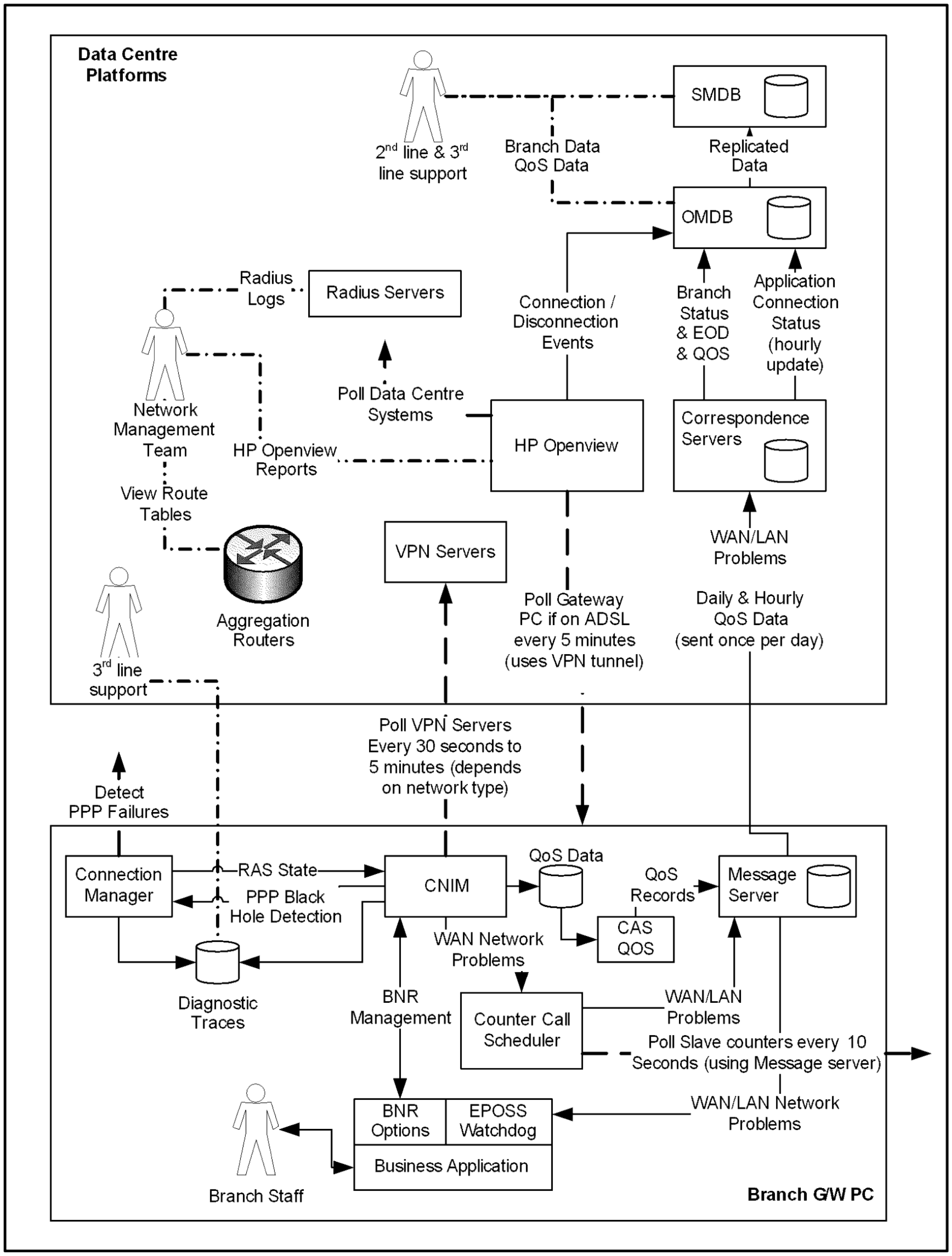
The table below shows how IP addressing is managed within the PAS:

Address Space	Assignment	Scope	Constant Next time is the same	Outgoing Connections to endpoint?	Routing
RAS Gateway PC WAN – ADSL, Dialled RAS	Dynamic by PPP from Horizon Radius Server	Unique within PAS	Yes	Yes	???
RAS Gateway PC WAN – ISDN	Static – allocated via autoconfig process	Unique within PAS	Yes since static	Yes	???
VSAT Gateway PC WAN	Static – allocated via autoconfig process	Unique within PAS	Yes since static	Yes	???

Branch LAN workstations	Static – allocated via autoconfig process	Unique within PAS since Subnet is unique per Branch.	Yes since static	Yes	???
Devices on Data Centre LANS	Static	Unique within PAS	Yes since static	Yes	
Loop back devices (i.e. addresses not associated with real interfaces bit associated with a device)	Static	Unique within PAS	Yes follows trivially since static	Yes	
Virtual Devices I.E. Load balancer and NAT projections	Static	Unique within PAS	Yes follows trivially since static	Yes	

6.5 Branch Network Monitoring

Monitoring of the branch network is complex due to the size and type of networks used. As a result there are a number of ways that the network is monitored as shown by the diagram below.



The key characteristics are:

#	Name	Function	Documentation

1	Connection Manager	Connection Manager is responsible for management of any RAS based connections (ADSL, BNR ISDN and BNR Mobile) including PPP failures. It writes diagnostics traces available for 3rd line support.	RS/DES/091 - Branch Connection Manager Detailed Design
2	CNIM CASQOS	CNIM Monitors the network at the IP level polling the data centres every 30 seconds to 5 minutes depending on the network type. If it detects a PPP black hole it tells Connection Manager so that the connection can be reset. CNIM writes Quality of Service (QoS) and diagnostic data on a regular basis to the local disk. Once per day CASQOS reads the QoS Data and writes it to the message server for transmission to the data centre. CNIM is also responsible for BNR management.	TD/SDS/002 - Counter Network Infrastructure Manager (CNIM) SY/SOD/007 - Network Banking - Outlet Network Quality Of Service Reporting System Outline Design
3	Counter Call Scheduler	The Counter Call Scheduler takes information from CNIM and the message server to detect WAN and LAN issues respectively. This information is written to the message server for transmission to the data centre and also for the counter business application.	See Application Section
4	Business Application BNR Options EPOSS Watchdog	The business application provides feedback to the Branch staff and also allows BNR options to be invoked.	See Application Section
5	HP Openview Radius Servers Aggregation Routers	HP Openview is used to Poll the branches that aren't dial on demand (i.e. ADSL and VSAT) to detect connection issues from the data centre. It is also used to poll the data centre platforms and network devices. Connection/Disconnection events are fed to the OMDB. The Network Management team have access to HP Openview reports together with Radius logs and the Aggregation routers to allow them to understand the status of the network.	???
6	Correspondence Servers OMDB SMDB	QoS and EOD data is Data is harvested from the Correspondence servers into the OMDB (and replicated to the SMDB) to provide information to 2nd and 3rd line support on the Branch status and QoS data. In addition, the connection status (checking when each gateway PC message server last connected to the correspondence servers) is checked once per hour.	See Application Section

7.0 Systems Management

The size and topology of the POL branch estate requires proactive and comprehensive system management such that every branch and individual counter position is under management and is being supported in successfully performing business transactions.

Similar considerations apply to the applications running in the data centres. Any anomaly can potentially have effects over large parts of the branch estate.

The system management solution can be decomposed into a group of component services which focus on individual functional areas. The component services inter work to deliver the required functionality and to achieve re-use of individual capabilities.

The following sections look at each of these individual components in turn.

7.1 Software Distribution and Management

Software distribution works in two modes of operation:

1. A software payload is pushed to the end system from the central management system.

2. A software payload is pulled by management agent software on the end system from a nominated depot. The depot may be co-located with the end system (such as another Counter in the Branch) or remote (i.e. within the data centre).

The software is installed and a permanent record is kept of its installation against the end system in the central system management inventory (the OMDB). All end systems in the data centre and the Branch estate can be updated through this service, however only some data centre platforms use this method due to cost of packaging – others are upgraded manually.

Peripheral devices that provide an API to update their firmware from the end system to which they are attached are also supported on this solution. Pin Pad's are example of this class of device

Both methods of distribution have an associated scheduling and targeting criteria. The targeting criteria is the statement of what end systems need to be updated and will allow such groups as single end systems, nominated sets of Branches (for pilot roll out of new facilities); and generic rules (such as all end systems who do not have the software already installed).

The scheduling criterion is the time at which the installation on the end system is actioned. Most software installations are invasive to the business and hence their schedules are chosen to be out of business hours. In the push mode the scheduling criteria is implemented by the central management systems. This scheduling takes account of the branch WAN network characteristics (e.g. maximum concurrency, maximum dial rate for ISDN etc).

The pull operation is driven by a local schedule on the end system which is only used for end system swap out. This is the automatic upgrade of a new end system from the software baseline present on that end system (i.e. at cold build) to the baseline of the live end system it replaces.

There are updates that require Branch wide installations (that is changes that need to be made to all Counters in a physical Branch at the same time) – for example updates to the Riposte desktop. The distribution facility includes the ability to co-ordinate updates across the whole branch with all counters having the software installed or (if there is an issue on one or more counters) for all counters to regress to the starting position.

To minimise the disruption to branch staff if a counter reboot is required during software a facility called "unattended reboot" is used. This allows the counter to be recovered to its post POLO (see security section) state in a secure way.

Further details can be found in:

- SY/SOD/005 - System Management - Software Distribution For FRIACO Networks
- SY/SOD/006 - Network Banking - Tivoli Based Supportability Tasks
- SY/SOD/007 - Network Banking - Outlet Network Quality of Service Reporting System Outline Design
- TD/SOD/002 - Unattended Reboot System Outline Design
- TD/SOD/007 - Outline Design For Remote Updating of PIN Pads

7.2 Distributed Monitoring

The Horizon solution relies on a number of platforms and applications working together to provide a business service. It is important that the operators can understand the state of the system from a service perspective so that issues can be prioritised and dealt with appropriately.

The central management system receives feeds (including application heartbeats) from the various platforms and applications and uses these to provide a summarised view of the following information:

1. Whether each business service is working fully, partially or not at all.

2. The state of resilience features that make up that service – for example resilience may be currently reduced due to an earlier failure.

3. Indicators that the service may have problems – for example higher business error rates than expected or volumes being processed are lower.

4. Indicators that the components that make up the service may have an issue – for example processor usage is much higher than expected.

Further details can be found in:

- SY/DAT/003 - SYSMAN Service Monitor Configuration
- SY/DES/018 - Online Transaction Monitoring System Outline Design

7.3 Event Management

Applications and operating systems within the solution can generate information that has operational significance and therefore needs to be dealt with either automatically or through operator intervention. The source of the events may be in the counter estate, data centre or network management component domains and these domains are linked to give an enterprise wide view for the operational support community. Individual domains may be solely managed through this enterprise view while other domains may have local management views. Any domain will always have a gateway though to the enterprise management domain.

Facilities exist to configure rules for the forwarding of events both at the originating end system, at a domain gateway or at reception in the central event management system. Certain domains will also provide tailoring at the user interface.

Details can be found in:

- SY/ION/006 - System Management - Counter Event Forwarding and Software Distribution
- SY/ION/007 - System Management - Advanced Event Archives Search Function
- SY/MAN/005 - Event Management Support Guide

7.4 Remote Operations and Secure Access

To support Horizon a number of support roles need access to the data centre systems.

For 2nd line support is via tasks that have predetermined functionality and whose access is role based.

For 3rd line support a support framework is provided that includes:-

1. Access to data centre resident Secure Access servers from Fujitsu Services locations during business hours or from support staff home locations out of business hours using secure workstation or lap top builds and encrypted communications

2. Two factor authentication at the Secure Access servers

3. Onward access from the Secure Access Servers to data centre platforms and counters using 3rd party COTS product management interfaces and audited client access to all Windows, Unix and Network platforms direct via IP or proxies.

5. Role based privileges for support access on platforms operating systems, hosted applications and database schemas.

Further details can be found in:

- SB/DES/008 – SecureId

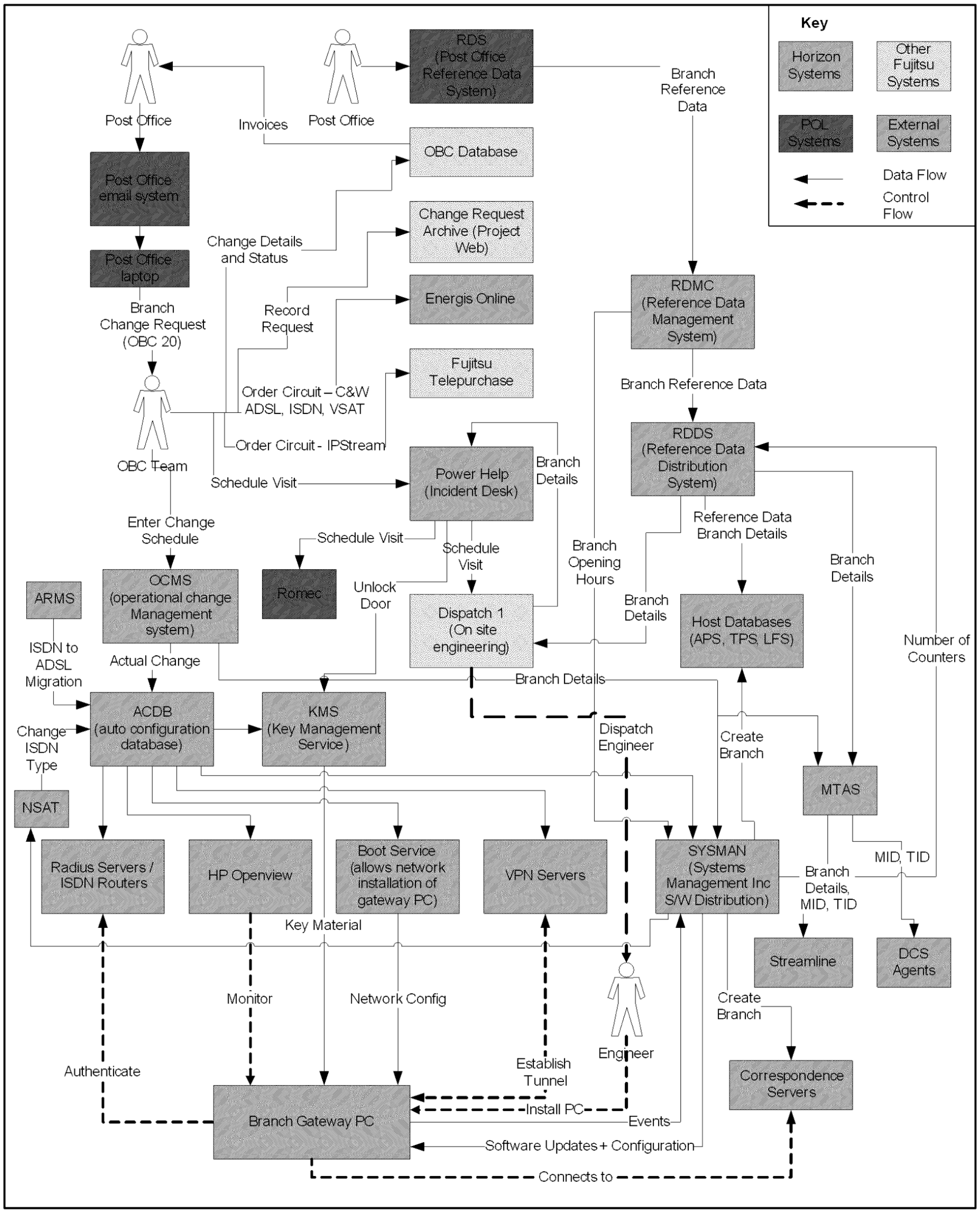
- SY/SOD/009 - Secure Support For Network Banking
- SY/DPR/001 - Out Of Hours Remote Support

7.5 Estate Management and Auto-Configuration

The policy for estate management is to de-skill as much as possible any engineering activities in the branch estate and to minimise the time taken for rollout of new branches and spares replacement. To this end, installation of new branches or replacement of failed equipment in existing branches is almost completely automatic – the engineers just have to plug in the equipment, scan a bar code and then wait for the system to be fully configured. This configuration includes the personalisation of network endpoints, branch router, counter positions, distribution of any sensitive key material (in a secure way) and any software fixes not included in the spare.

The diagram below shows the a simplified view of the systems and data flows involved in creating a new branch:

Data Flows In Horizon For Branch Physical Changes (OBC)
(Simplified – Ignores Systems that Transport Data)



FUJ00098217

The key characteristics are:

#	Name	Function	Documentation
1	Post Office RDS	Post Office make a request via email to open a new branch. The reference data for that branch is also entered into Post Office's RDS system.	n/a
2	OBC Team OBC Database Change Request Archive Energis Online Telepurchase OCMS	The Fujitsu OBC team have a Post Office laptop with access to the Post Office email system. They use this to retrieve the branch change request (OBC 20). This change is entered in the OBC database and the change request archive. The branch network service is ordered via either Energis online (for C&W services) or Fujitsu Telepurchase (for Fujitsu supplied services) The details are entered into OCMS (operational change management system) to schedule the changes in the solution.	TD/DES/106 - OCMS High Level Design
3	RDMC RDDS MTAS DCS Agents Host Databases	The reference data changes are received from RDS and passed to RDMC to process them. RDMS provides this to Sysman and RDDS. RDDS distributes the reference data to the host databases and MTAS (MID/TID Allocation Systsem). MTAS also receives a feed from OCMS. Between the two feeds there is sufficient data to allocate a MID and TID and send that information to Streamline.	See Application Section

4	ACDB KMS Radius Servers /ISDN Routers Boot Service VPN Servers SYSMAN Correspondence Servers	ACDB receives the change from OCMS and allocates network configuration to the branch and counter configuration for each counter position. The configuration data is feed to a number of systems including: • Radius Servers and ISDN Routers to allow network access • KMS to allocate key material for the branch • HP Openview to monitor the branch • Boot Service to allow network config to be distributed on installation • VPN Servers to enable a new VPN config • Sysman to allocate software baselines and configurations • Correspondence server and host databases (via SYSMAN) to open the branch. • RDDS (via SYSMAN) for the number of counter positions in the branch.	TD/SOD/006 – BI3 Estate Management System Outline Design TD/SOD/010 - ADSL - Estate Management System Outline Design DE/DES/015 - Pathway Autoconfig Bootserver Implementation CSR+ See also application section
5	Power Help Dispatch 1 Romec Engineer Gateway PC	The OBC Team also schedule engineer visits to install the branch via Power Help (the Incident desk). Romec (a Royal Mail group company) are requested to physically installed the new branch (wiring, physical machines etc). Dispatch 1 is requested to schedule a Fujitsu engineer visit to complete the installation (connection to the network, ensure it works etc). To enable this the door on KMS needs to be "unlocked" to allow the installation and this is triggered by Power Help.	n/a
6	NSAT ARMS	NSAT (Network Service type Allocation Tool) is used if the ISDN network type needs to be changed between Dial On Demand, Bronze Dial On Demand, Silver Daytime FRIACO and Silver Daytime Metered (see Network Section) ARMS (ADSL Rollout Management System) is used if the Branch needs to be migrated from ISDN to ADSL.	TD/DES/159 - Network Service Allocation Tool Design SY/SOD/020 - ADSL ARMS To Horizon Interface System Outline Design

7.6 Capacity Monitoring

In order to the system there is a comprehensive capacity monitoring system based on the Athene product from Metron. This consists of three elements:

- Immediate alerting on performance issues that could jeopardise the live service. These events are carried through the event framework to the monitoring system.

- On a daily basis performance data is collected from critical platforms an loaded into a "short term performance database" to allow problems to be investigated.
- On a monthly basis performance data is loaded into a "long term performance database" to support medium and long term trending.

More details can be found in

- TD/STR/002 - Athene Deployment Strategy

7.7 Scheduling

There are a number of scheduling methods used in Horizon. For the business applications in the data centre, Maestro is used. The master is run on the host systems, with clients running on each platform that requires scheduling services.

For the OMDB, the scheduling capabilities of the Oracle management suite are used [DN: need to check this].

For the counter business applications, a bespoke product called the "Counter Application Scheduler" is used (see the application scheduler). Other scheduling required is managed through the NT4 scheduler.

Details can be found in:

- TD/HLD/002 - Horizon Maestro Schedule

7.8 Time Synchronisation

Time synchronisation is achieved through the following components:

- GPS based Time synchronisation server(s) within the data centre as the master source. This avoids the need for an internet connection from the data centres.
- The data centre platforms (including the correspondence servers) use Network Time Protocol (NTP) to synchronise with the GPS receivers.
- The gateway PC in each branch synchronises with the correspondence servers. This is a feature of the Riposte messaging software.
- The slave PC in each branch synchronise with the gateway PC using Riposte.
- All platforms generate events that are collected by the event management system. This is a requirement of litigation support so that it can be demonstrated that the clocks have been kept in synch.

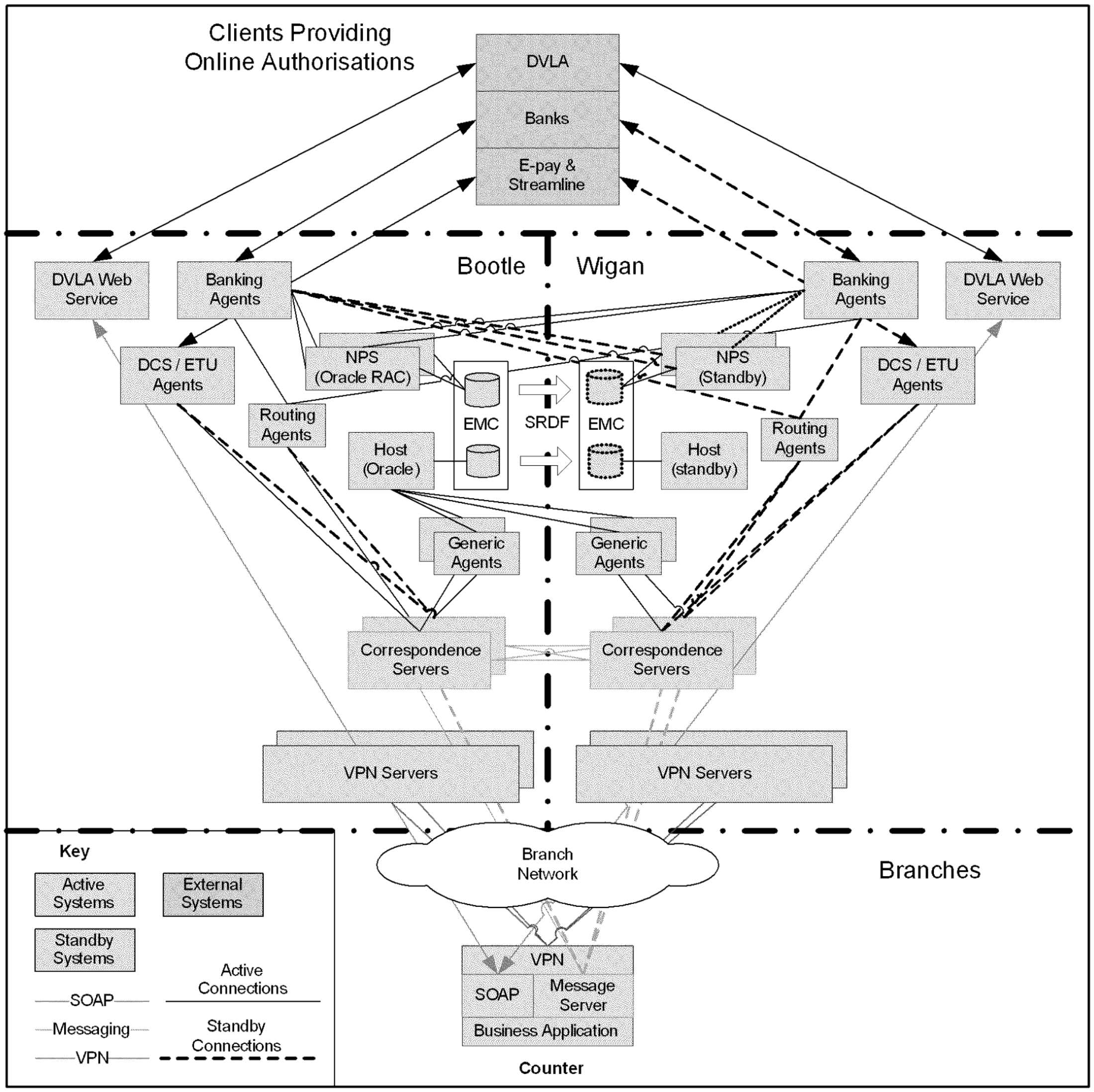
Further details can be found in:

- TD/ARC/005 - Time Service

8.0 Availability & DR

For the majority of the Horizon solution, resilience and DR are provided by the same mechanism, with a single data centre in its own right having very little resilience. This approach minimises the capital hardware costs in the solution. For a few components where rapid recovery is required, local resilience is provided (e.g. NPS database).

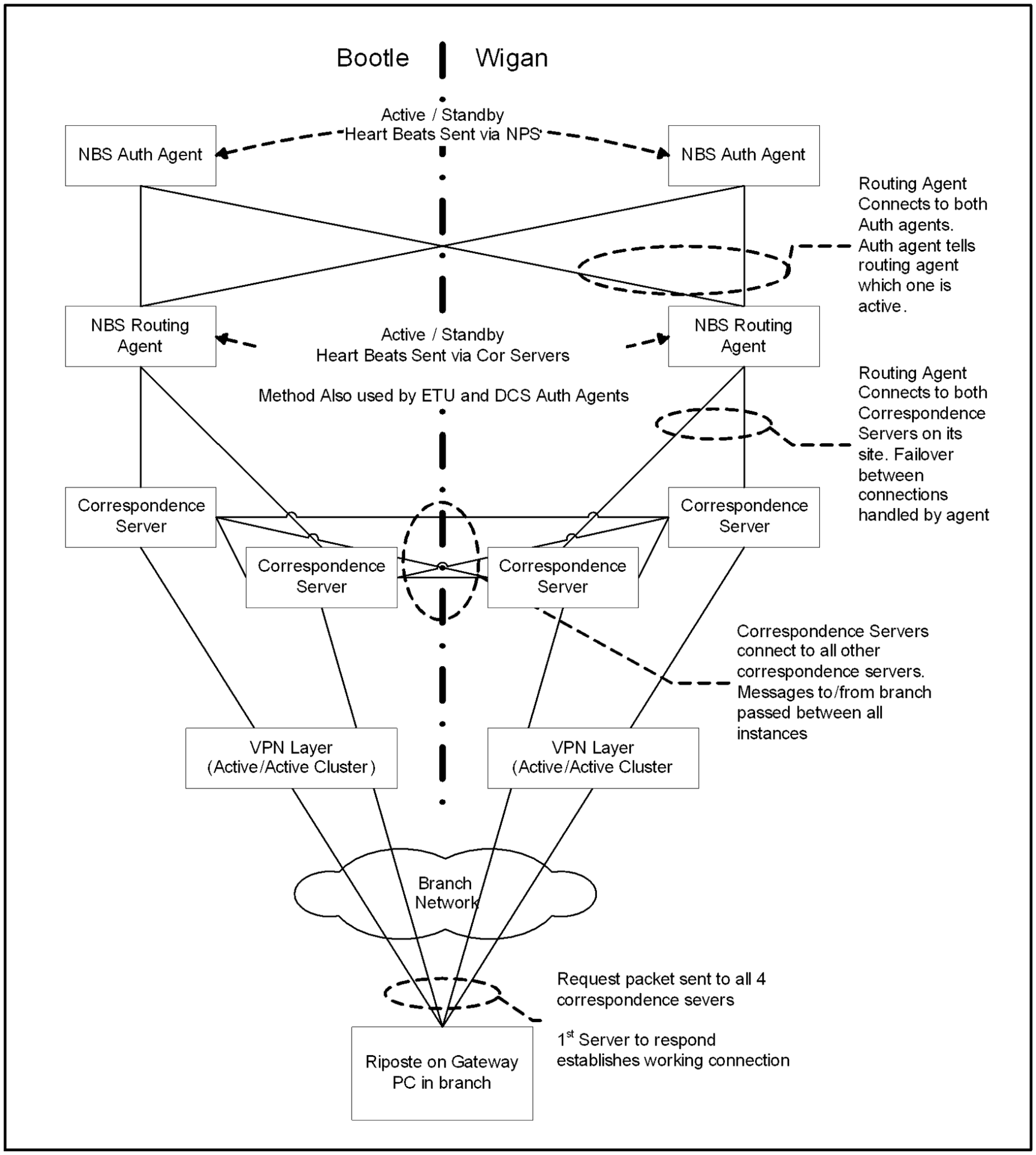
The diagram below shows a simplified view of the resilience and DR of the solution.



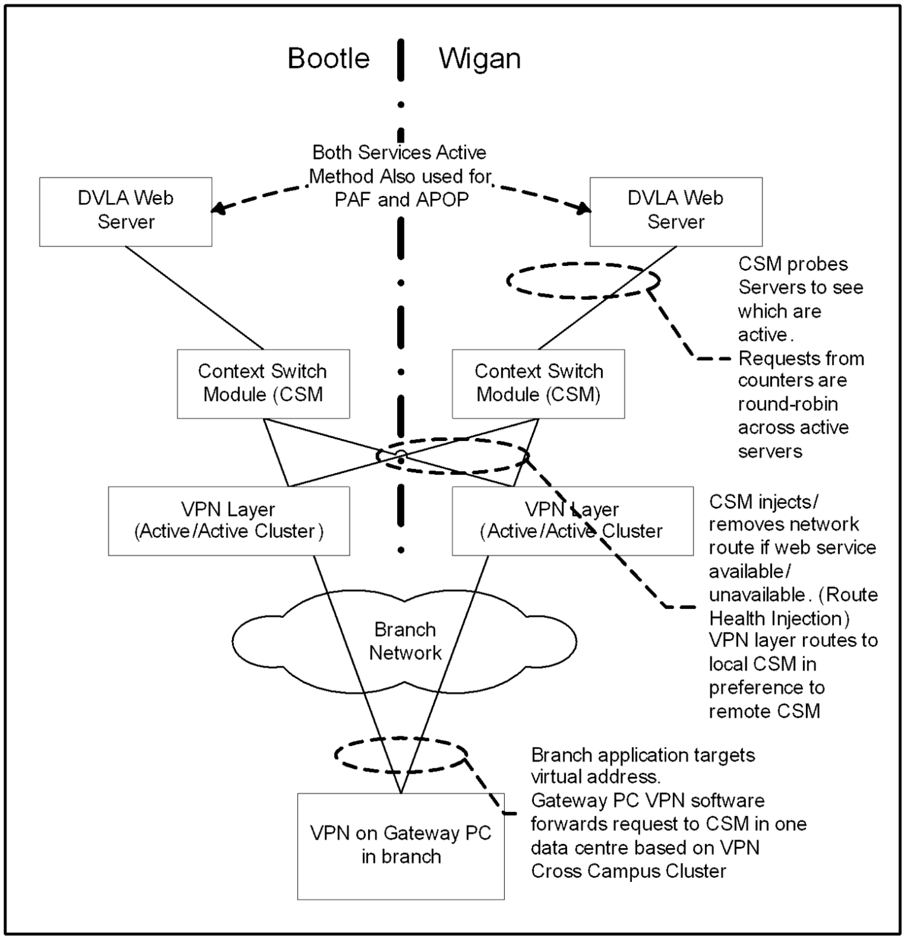
The main characteristics are that:

- The Branches have network connections that can use either data centre. The exact method used depends on the network type. Either both data centres are connected (as with ADSL or VSAT) or one data centre is connected normally with the branch able to use the other data centre if there is an issue (as with ISDN).
- The VPN software in the counter connects to multiple VPN servers at both sites to provide resilient encrypted tunnels.
- The Riposte message server at the counter is able to connect to 4 correspondence servers (2 at each site). At any one time only one connection will be used for normal traffic.
- Online Transactions Banking, ETU and Debit/Credit Card are picked up from the correspondence servers by the Routing Agents, ETU Agents and DCS Agents respectively. These are able to connect to both correspondence servers on the same site (one connection normally used). In the event of an issue at the main site, standby service will run at the other site.
- The Banking Authorisation agents receive transactions from the Routing Agents. These need the NPS database to hold state information for the online transactions. The NPS uses Oracle RAC to provide local resilience. In the event of site disaster, the NPS service is brought up at the other data centre. Data is replicated between the two sites using EMC SRDF technology.
- The DVLA service uses an active/active configuration where the service is live in both data centres.
- The Host service (used for batch processing) is live at one data centre. There is a standby server at the other data centre that is used for both DR and resilience. Data is replicated between the two sites using EMC SRDF technology.
- Data is transferred between the host at the data centre through generic agents. These run at both data centres.

The diagrams below show in more detail the two methods used between the branch and data centre to achieve resilience and DR for online services.


Bootle
Wigan
Active / Standby
Heart Beats Sent via NPS
NBS Auth Agent
NBS Auth Agent
Routing Agent Connects to both Auth agents. Auth agent tells routing agent which one is active.
NBS Routing Agent
Active / Standby
Heart Beats Sent via Cor Servers
NBS Routing Agent
Method Also used by ETU and DCS Auth Agents
Routing Agent Connects to both Correspondence Servers on its site. Failover between connections handled by agent
Correspondence Server
Correspondence Server
Correspondence Server
Correspondence Server
Correspondence Servers connect to all other correspondence servers. Messages to/from branch passed between all instances
VPN Layer (Active/Active Cluster)
VPN Layer (Active/Active Cluster
Branch Network
Request packet sent to all 4 correspondence severs
1st Server to respond establishes working connection
Riposte on Gateway PC in branch

Resilience for online transactions using Riposte


Bootle
Wigan
Both Services Active
Method Also used for
PAF and APOP
DVLA Web Server
DVLA Web Server
CSM probes Servers to see which are active. Requests from counters are round-robin across active servers
Context Switch Module (CSM
Context Switch Module (CSM)
VPN Layer (Active/Active Cluster)
VPN Layer (Active/Active Cluster
CSM injects/ removes network route if web service available/ unavailable. (Route Health Injection) VPN layer routes to local CSM in preference to remote CSM
Branch Network
Branch application targets virtual address.
Gateway PC VPN software forwards request to CSM in one data centre based on VPN Cross Campus Cluster
VPN on Gateway PC in branch

Resilience for online transactions using Web Services

Other areas of resilience are shown in the table below. In general there are resilient LAN in the data centre and the table highlights how this is used.

#	Area	Resilience Model	How Selection Made by User of Service
1	TES Application APOP Admin	Service: Active/Active Platform: Both Live LAN: Single IP Address – active/standby connections	User has different IP addresses for the different servers LAN failover automatic
2	Banking File Transfer APS File Transfer PO File Transfer	Service: Active/Standby Platform: Both live LAN:???	Manual failover
3	Correspondence Servers	Service: Active/Active Platform: All Live	As described above

		LAN: Single LAN used in each server for Branch traffic; other traffic spread over both LAN	
4	DVLA Sever PAF Server APOP Web Server	Service: Active/Active Platform: Both Live LAN: Single IP Address – active/standby connections	As described above
5	Host Server KMA Server OCMS Server DCSM Server	Service: Active/Standby Platform: Active/Standby Database: SRDF Replication LAN: Single IP Address – active/standby connections	Manual Failover for Service & Platform. LAN failover automatic
6	ACDB Server OCMS Server	Service: Active/Standby Platform: Active/Standby Database: Log shipping LAN: ???	Manual Failover
7	VPN Servers	Service: Active/Active Platform: All live LAN: ???	Counters automatically select working servers
8	Generic Agents	Service: Either Active/Active or Active/Standby (depends on agent type) Platform: All Live LAN: Single LAN used for connection to correspondence servers.	Automatic failover via Maestro schedules (for batch agents) and SYSMAN (for continuously running agents).
9	ETU/DCS Agents NBS Routing Agents NBS Authorisation Agents	Service: Active/Standby Platform: Both Live LAN: Single IP Address – active/standby connections	Automatic through agent code (see above)
10	NPS	Service: Active/Active within Data centre; Active/Standby across data centres Platform: All Live within data centre. LAN: Single IP Address – active/standby connections	Automatic failover for local resilience. Manual failover if other data centre used

9.0 Performance and Scalability

This section outlines the volumes that the solution needs to be support

9.1 Volumes

The table below summarises the product volumes that need to be supported by the solution

Volume	EPOSS	APS	NBS	DC	ETU	DVLA Online	PAF	Settlement	Total
Peak Month	105,205,376	40,641,694	41,847,560	4,210,000	1,422,417	3,603,876	11,969,806	119,631,436	328,532,165
Peak Week	35,319,442	11,511,888	10,960,032	1,264,768	462,075	2,080,110	4,002,430	36,112,618	101,713,363
Peak 2 Days	15,620,323	5,626,222	5,656,759	565,949	213,783	1,026,146	1,883,664	17,188,486	47,781,332
Peak Day	8,602,518	3,031,573	3,264,181	288,425	121,200	670,704	1,100,788	9,565,842	26,645,231
Peak Hour	1,230,160	560,841	694,976	79,368	17,254	92,724	162,246	1,730,259	4,567,828
Peak Sec By Service	344	179	222	22	5	27	46	532	1,377
Peak Sec Actual	42	179	222	22	5	27	0	293	790

The peak second numbers are the average rate over the peak 5 minutes. Two Peak second numbers are provided – one to give the peak for each service (although the peaks do not co-inside) and the actual number which is the highest workload possible given the throughput that can be achieved by the counters.

Full volumes can be found in PA/PER/033 - Horizon Capacity Management and Business Volumes.

9.2 Scalability

There are two broad approaches to scalability:

- Scale Wide – Where multiple instances of a particular component and be run in parallel and therefore additional resource can be added by increasing the number. An example would be adding more servers to the SM Application layer.
- Scale High – Where multiple instances cannot be run in parallel and therefore the capability of the component needs to be improved. An example would be a banking agent where the platform is upgraded to provide more processing agent.

There are two types of Scale Wide – those that require application or other change and those that can be achieved with no change.

The table below describes the possible scaling strategies for the key, performance critial components of the system:

#	Area	Scaling Approach
1	Banking Agents	Primary approach is to Scale High providing more processing power for the agent

	DCS Agents ETU Agents DVLA Agents	platforms or where a number of agents share a platform to split this across multiple platforms. It would be possible to Scale Wide if the number of instances is increased although this is likely to require other changes in the system (e.g. to increase number of PRI for banking).
2	PAF Agents APOP Agents Generic Agents Routing Agents	There are two options for this: 1) Make platform more powerful 2) Add additional platforms and instances It is likely to be most cost effective to make the platform more powerful.
4	Host	The host capacity is dominated by the need to support the overnight batch process. There are two ways to provide additional capacity: 1. Provide a more powerful host system (either faster processors or more processors) 2. Split the workload across multiple platforms (e.g. TPS database on one platform and DRS on a different platform. It is likely to be most cost effective to replace the host by a more powerful system with the same number of faster processors due to the way Oracle licensing works,
5	NPS	The NPS database is spread over two systems in normal operation. If one of these fails then the other takes over the whole workload. There are two ways to scale this platform: 1. Provide a more powerful host system (either faster processors or more processors). 2. Add an additional platform to provide resilience to the two other platforms – hence ensuring no one platform has to take the full workload. Given the type of hardware deployed (2 processors used in an 8 processor capable platform) the most cost effective approach is likely to be adding additional processors.
6	Correspondence Server	Given the structure of the correspondence sever clusters (i.e. a branch is a member of one of the 4 clusters) the only practical way to scale is to have faster processors. Given the way that Riposte works it is better to have a fast 2 processor system rather than a slower 4 processor system.
7	Data Centre LAN	The data centre LAN is composed of high speed switches (with 32Gbit/s backplanes) connected to servers via 100Mbit/s LAN. If this proves to the insufficient then there are three options for scaling: 1. Split the workload over more servers (each with 100Mbit/s LAN) 2. Upgrade the LAN to 1Gbit/s for selected servers 3. Reduce the bandwidth needed through application change (e.g. compression). Given the nature of the system, the most cost effective approach is likely to be reducing the bandwidth unless a small number of servers need to be changed.
8	Branch WAN	The Branch WAN has two bottlenecks – the individual bandwidth into each branch and the aggregate bandwidth across all branches. For individual branches it would be possible to add additional bandwidth through changing network technology (e.g. a high speed fixed circuit). However this is likely to be prohibitively expensive unless used in a very small number of branches. In

		practice it is preferable to keep the bandwidth usage to that that can be supported by the network technology. For the aggregate bandwidth, it is possible to purchase additional bandwidth from the network supplier. However this is likely to be relatively expensive. In practise therefore it is better to keep the bandwidth usage within the current design capability through application change.
9	Other WAN Connections	Other WAN connections (e.g. Banks, e-pay, Post Office etc) can be scaled through buying more capacity from the network supplier.

10.0 Security

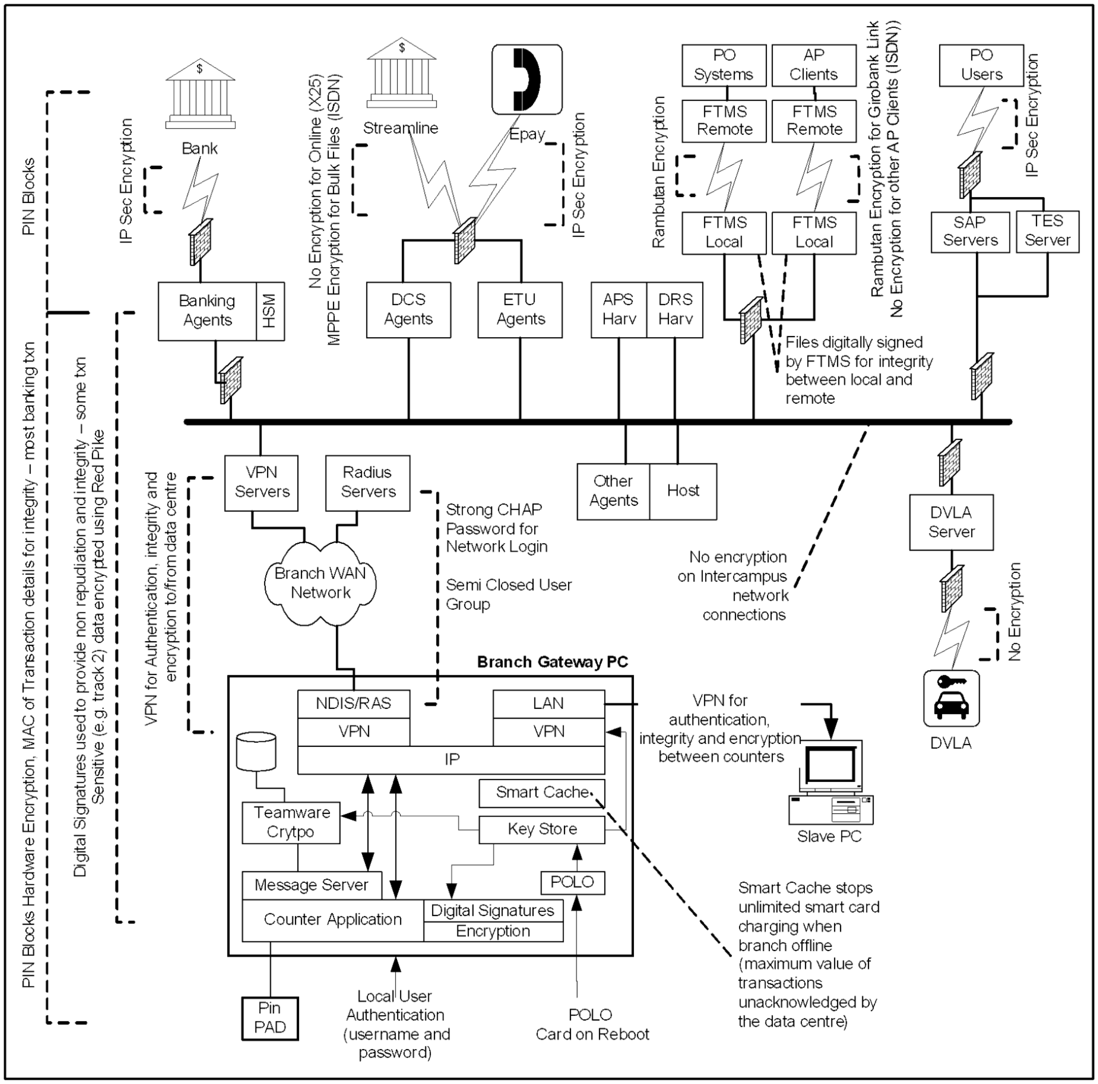
This section covers the key security features, key management and audit.

Other aspects of security can be found in:

- RS/POL/002 - Horizon Security Policy
- RS/POL/003 - Access Control Process
- RS/POL/004 - Computer Virus Policy
- RS/DES/080 - NT Domain Structure Design For Post Office Account
- RS/FSP/001 - Security Functional Specification

10.1 Security Features

The diagram below shows the main security features of the solution:


PIN Blocks
PIN Blocks Hardware Encryption, MAC of Transaction details for integrity – most banking txn
Digital Signatures used to provide non repudiation and integrity – some txn Sensitive (e.g. track 2) data encrypted using Red Pike
VPN for Authentication, integrity and encryption to/from data centre
Bank
IP Sec Encryption
Banking Agents
HSM
No Encryption for Online (X25)
MPPE Encryption for Bulk Files (ISDN)
Streamline
Epay
IP Sec Encryption
DCS Agents
ETU Agents
Rambutan Encryption
PO Systems
AP Clients
FTMS Remote
FTMS Remote
FTMS Local
FTMS Local
APS Harv
DRS Harv
Rambutan Encryption for Girobank Link
No Encryption for other AP Clients (ISDN))
PO Users
IP Sec Encryption
SAP Servers
TES Server
Files digitally signed by FTMS for integrity between local and remote
VPN Servers
Radius Servers
Strong CHAP Password for Network Login
Semi Closed User Group
Branch WAN Network
Other Agents
Host
No encryption on Intercampus network connections
DVLA Server
No Encryption
DVLA
Branch Gateway PC
NDIS/RAS
VPN
LAN
VPN
IP
Smart Cache
Key Store
Teamware Crytpo
Message Server
POLO
Counter Application
Digital Signatures
Encryption
VPN for authentication, integrity and encryption between counters
Slave PC
Smart Cache stops unlimited smart card charging when branch offline (maximum value of transactions unacknowledged by the data centre)
Pin PAD
Local User Authentication (username and password)
POLO Card on Reboot

Branch access to the data centre is controlled as follows:

- Closed user group in the network ensures only registered end points can get access to the data centre for ADSL and VSAT connections. For ISDN the closed user group is implemented on Voice access only.
- The gateway PC has to log into the network using CHAP authentication to the radius servers.
- VPN is used between the branches and the data centres and also between the branches. The key material for this on the branch PC is “unlocked” using a PMMC (Post Master Memory Card) and the POLO process. The PMMC is kept securely in the branch (e.g. kept in the safe).

- Where specific data needs to be protected from being read (confidentiality) or tampered with (integrity) then this is done by the application.

The POLO process is also used to unlock key material used to encrypt the hard drive and provide the keys used for digital signatures.

The closed user group in the network will be handled through:

1. ADSL– Implemented by network supplier
2. ISDN – Implemented by the network supplier for voice access. Not implemented on data access.
3. VSAT – Implemented by network suppler

The Radius Servers are split into two logical groups:

1. Dialled ISDN/PSTN
2. ADSL

Network links to third parties are encrypted where possible and this is shown in the diagram.

For banking, PIN Blocks are used to transport PINs from the PIN Pad to the Bank. The HSM (Hardware Security Modules) used by the banking agents decrypt the PIN Blocks from the PIN Pads and then encrypt them using a key shared with the bank. This is done as a single atomic operation to ensure that the PIN itself is never exposed.

To protect against re-play attacks on banking, all banking requests (with the exception of deposits) are protected by a MAC generated by the PIN Pad, using a key unique to the transaction.

Many transactions are digitally signed to check that they have not been tampered with during transmission as shown in the table below:

#	Data Type with Signature	Generated by	Checked By
1	AP Transactions	Counter	APS Harvester
2	Banking and ETU confirmation transactions	Counter	DRS Harvester
3	DCS Confirmation transactions	Counter	C2 Bulk Agent (produces payment file for Streamline)
4	Banking Requests and Reversals	Counter	NBS Authorisation Agent (except for Card Account withdrawal requests)

5	Banking Authorisations	NBS Authorisation Agent	Counter
6	ETU Requests and Reversals		ETU Authorisation Agent
7	ETU Authorisations	ETU Authorisation Agent	Counter
8	DCS Requests and Reversals	Counter	DCS Authorisation Agent
9	DCS Authorisations	DCS Authorisation Agent	Counter
10	APS Smart Transaction acknowledgements	APS Harvester	Counter

The APS Smart Transaction Acknowledgements are used by the Smart Cache to limit the maximum amount that can be charged by the counter without acknowledgement from the data centre. This is to limit the exposure if a PC is stolen.

The tables below list these and the other security controls in the solution. They are split into network, infrastructure and applications.

10.1.1 Network Security Controls

#	Control Name	Risk(s) Addressed
N1	DMZ Firewalls	Hacking attempts from client connections (banks, DVLA, streamline, e-pay)
N2	No direct internet access to/from data centres	Limit risk of hacking
N3	No wireless LAN access (Wi-Fi) allowed in solution	Limit risk of hacking
N4	Post Office DMZ Firewalls	Hacking attempts from Royal Mail intranet network.
N5	Closed user Group on most of branch network	Exposure to non-counter staff/kit. Limits number of end points that can attack the solution.
N6	Strong CHAP Password for branch network authentication	Exposure to non-counter staff/kit. Network end point requires valid username and password to attach to network
N7	VPN from branch to data centre	Confidentiality and integrity from branch to data centre. Also stops alien devices connecting to the data centre.
N8	VPN between counters in branch	Confidentiality and integrity from between counter positions. Also stops alien devices connecting to counter PC.
N9	Support DMZ Firewalls	Hacking attempts from Fujitsu support community. .
N10	Network encryption to banks and e-pay	Confidentiality and integrity of data while in transit.
N11	Network encryption to support sites	Confidentiality and integrity of data while in transit.

N12	Network encryption to Royal Mail sites	Confidentiality and integrity of data while in transit.
N13	MPPE (Microsoft Point to Point Encryption) protection of files to/from streamline	Confidentiality and integrity of bulk data while in transit to/from streamline.
N14	Radius servers segregated by logical network type	Security breach of one network type does not compromise other network types.
N15	Uses Private IP addresses which are not exposed across the system boundary	Limit risk of hacking

10.1.2 Infrastructure Security Controls

#	Control Name	Risk(s) Addressed
I1	No plug and play, floppy disk, CD etc in counter	Prevent alien code being loaded.
I2	Physical Controls on data centre access	Intrusion by non-authorised staff
I3	Access controls for support/operational staff – SAS, secure logon etc.	Exposure of system to non-authorised users
I4	Counter locked down (no access by branch staff to underlying OS)	Prevent staff hacking data centre
I5	Degauss disks /tapes before leave data centre	Stop sensitive data being exposed
I6	Anti Virus for at risk data centre platforms	Virus infection
I7	Secure Builds for servers	Reduce implications of hacking attacks – turn off unused features, make sure access controls correct etc.
I8	Physical Controls on access to key mgt functions and key handling	Access to keys by non-authorised staff
I9	Two-person controls on access to key material	Access to full keys by Fujitsu staff
I10	Patching of data centre platform operating systems	Address vulnerabilities in OS to stop hacking and viruses
I11	BIOS is locked down and only bootable from primary storage on counter	Prevent system being booted into a uncontrolled operating system
I12	Auditing of all support staff actions related to change of business data	Fraud by Fujitsu staff
I13	Pagefile & critical files (e.g. messagestore) encrypted on counters	Stop any data that is retained on the hard disk from being readable.
I14	Code signing	Prevent unauthorised code from being installed
I15	Signing of configuration files for counters	Prevent unauthorised configuration data from being installed.
I16	Patching of counter OS	Address vulnerabilities in OS to stop hacking and viruses

I17	Physical Controls on access to support workstations	Access by non-authorised staff to support functions
I18	Counter Application runs in non-privileged user	If application is bypassed in someway, user hasn't got sufficient privilege to hack machine.
I19	Counters have to be configured before can be used by the application	Stop unauthorised counters being added
I20	Counters are configured to only allow login to a given branch.	Stop users spoofing a branch to access its accounts from remote location.
I21	Counter Key material protected by PMMC and POLO Process – system will not work following reboot unless unlocked.	Stop system working unless have rebooted using the PMMC.

10.1.3 Application Security Controls

#	Control Name	Risk(s) Addressed
A1	PAN not printed in full on receipts	Prevent exposure of PAN
A2	Auditing of branch staff transactions and events	Fraud – used for litigation support, FSA requirement.
A3	Hardware encryption of PIN at counter and data centre, using Pinpads and Atalla HSMs	Exposure of customer's PINs – PINs are always held encrypted except when within tamper-resistant physical devices
A4	Logon/Logoff of branch staff to application	Exposure of system to non-authorised users
A5	Authentication of transactions to/from counter	Authentication of transactions to/from counter
A6	High Risk Transactions digitally signed	Transactions tampered with during transmission.
A7	Smart Cache in Counter stops unlimited charging of Smart cards without a connection to the data centre.	Stops unlimited charging of Smart Cards if a PC and the PMMC are stolen together.
A8	No email access for branch staff	Minimise risk of malware.
A9	No internet browsing capability for branch staff	Minimise risk of malware.
A10	CA for certifying counter/app server keys	Exposure of system to non-authorised users
A11	MAC of banking transactions	Replay of banking transactions
A12	Auditing of data passed across interfaces to external systems (e.g. banks)	Proof of data in case of dispute or fraud investigations.
A13	Users of Branch application are allocated role(s) to determine the functions to which they have access.	Higher privilege functions not provided to low privilege users.
A14	Branch Application provides facility to "lock screen"	Allows staff to lock screen while away from the counter to stop unauthorised users from using the application.

A15	Branch Application provides facility for user to quickly and simply logout in a clean manner.	Allows staff to logout quickly if threatened
A16	Track 2 data encrypted when stored	Exposure of Track 2 data to unauthorised individuals.

10.2 Key Management

There are a large number of keys used by Horizon to protect the system with each branch having their own set of keys. The keys managed in Horizon are:

- Audit Server (AUDS)
- Software Issue (SI)
- Client services Automated Payment service (AP)
- Post Office Filestore Encryption Key (FEK)
- Post Office Counters Ltd (POCL) Transaction Information Processing (TIP)
- POCL Reference Data (RD)
- Automated Payment service bulk Client transaction records (AP Client)
- Landis & Gyr 3rd party code and data protection (L&G Code)
- Landis & Gyr transaction-enabling functions (L&G Enabling)
- Smarts Acknowledgments (SA)
- Utimaco Virtual Private Network (VPN)
- Network banking PIN encryption by counter PCs(NBPO)
- Encryption of sensitive network banking transaction data within Horizon (NBTDO)
- Digital signing of network banking transaction data in the PO outlets (NBOC)
- Digital signing of network banking transaction data by Horizon agent servers (NBCO)
- Network banking PIN encryption by Horizon agent servers (NBPC)
- Encryption on the data links connecting the Horizon NBX systems to the FIs
- Rambutan encryption of data links (Rambutan)
- Network CHAP Secrets

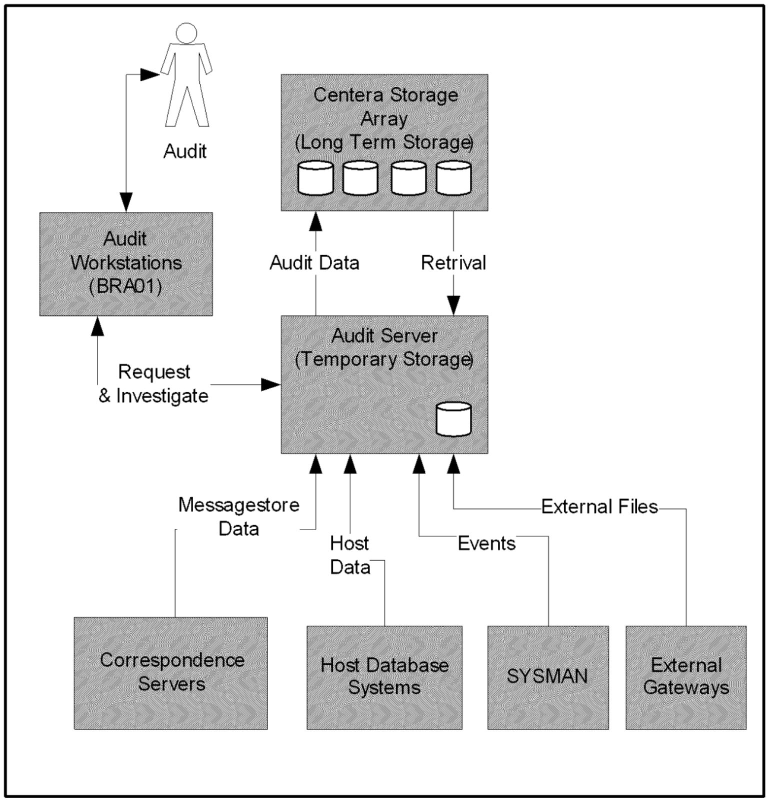
All high volume keys (including all Branch keys) are automated through the KMA Server. There are a small number of keys that require manual management.

Details can be found in:

- RS/DES/010 - Key Management High Level Design
- SD/DES/093 - High Level Design for CHAP Password Handling.

10.3 Audit & Litigation Support

The diagram below shows the key elements of the Audit and Litigation support system.



The Audit server is responsible for gathering Audit Tracks generated from a wide range of components of the Horizon system. The majority of data comes from the correspondence servers which includes all business data associated with the Branches.

As well as gathering and storing audit data on EMC Centera all of the Audit Tracks, the Audit Server provides facilities to retrieve data from the Audit Archive.

Tools to extract and prepare data for analysis are provided together with basic facilities to support internal Fujitsu Services data retrieval activities. Access, by Fujitsu Services staff, to the retrieval and extraction facilities is via the user interface provided on the Audit Workstation.

Details can be found in:

- SD/HLD/001 - Audit Data Collection & Storage High Level Design
- SD/HLD/002 - Audit Data Retrieval High Level Design