FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy	**Ref:**	RS/POL/003
	Version:	7.0
Commercial In Confidence	**Date:**	**14/04/2005**

Document Title:	Horizon Access Control Policy
Document Type:	Policy
Release:	BI3
Abstract:	This Access Control Policy (ACP) defines the policy for controlling access to resources in the operational Post Office Account solution.
Document Status:	APPROVED
Originator & Dept:	Bill Mitchell (CS Security and Risk)
Internal Distribution:	As Required
External Distribution:	Warren Welsh, Andrew Gibson, Colin Johnson

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

Name	Position	Signature	Date
Dave Baldwin	FS POA Director Customer Services		

0.0   Document Control

0.1   Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1, 0.2	28/10/96	Initial drafts for review by security team	
0.3	7/11/96	Initial Draft for internal ICL Pathway review	
0.5	6/12/96	Response to comments; Addition of new information including ICL Pathway Corporate Services domain, Network Management	
0.6	4/3/97	Further clarifications in many areas including network, Solaris access, Post Office outlets	
1.0	16/4/97	Terminology changes. Major updates to the Post Office section have been made. Numerous minor changes have been made.	
1.1/3		See separate note	
2	23/2/98	Draft version of 1.3.	
2.1, 2.2	Sep/Oct 98	See separate note Approval responsibility passed to John Dicks	
3.0	18/12/98	Minor updates	
3.1	May '99	Re-organisation and change to focus on policy, taking out most descriptive text; See separate note for changes and issues.	
3.3	Jan 2002	Removal of Benefit Encashment Service and so PAS/CMS, CAPS links, FRM, De La Rue etc and other changes	
3.4	May. 2002	Various updates/changes to reflect the S10 release state and thus serve as a baseline for NBS updates Further changes to incorporate new Fujitsu and Post Office references.	
3.5	July 2002	Incorporates comments from internal review	
4.0	July 2002	Minor updates	
4.1	August 2002	Various updates/changes to reflect the BI3 release state.	
4.2	August 2002	Incorporates comments from review primarily	

FUJ00088155
FUJ00088155

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

		relating to Section 3.5.2 concerning the management of NB related keys. Minor typographical changes.	
5.0	Sep 2002	For Approval	
5.1	Jul 03	Minor change to review list and table at section 6	
6.0	Aug 03	Incorporated changes to correct Role names. "PO key recoverer" changed. Minor typographical changes.	
6.1	10/1/05	To incorporate changes up to release S75	
7.0	14/04/05	For Approval	

0.2   Review Details

Review Comments by :	24th April 2005
Review Comments to :	Bill Mitchell

Mandatory Review	
FS CS Director	Dave Baldwin
Optional Review	
FS Crypto Dev TDA	Alex Robinson
FS Quality & Audit Manager	Jan Holmes
FS CS SSC Manager	Mik Peach
FS CS Business Services Manager	Richard Brunskill
FS Estate Management & Secure Builds Team	Mark Ascott
FS System Management Architect	Glenn Stephens
FS RASD - Infrastructure	Nial Finnegan
FS RASD Security TDA	Stephen Probert
FS CS OBC Service Manager	Denise Miller
*Issued for Information – **Please restrict this distribution list to a minimum***	
Post Office Ltd	Sue Lowther

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

0.3   Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001			Fujitsu Services Document Template	PVCS
CR/FSP/004			Service Architecture Design Document	PVCS
TD/ARC/001 [TED]			Technical Environment Description	PVCS
RS/POL/002 [SECPOL]			Post Office Account Security Policy	PVCS
RS/FSP/001 [SFS]			Security Functional Specification	PVCS
CS/FSP/003			PAS/CMS Help Desk Call Enquiry Matrix	PVCS
CR/FSP/006			Audit Trail Functional Specification	PVCS
ISO17799			A Code of Practice for Information Security Management	PVCS
DITSG/ITSS/0001.04			DSS IT Security Policy (Departmental IT Security Standards)	PVCS
SRR Appendix 4-1			Post Office Counters Information System Security Policy	PVCS
TD/DES/059			High Level Network Design for CSR & CSR+	PVCS
CS/PRO/090 [ACUA PPD]			CSR+ Access Control and User Administration Processes and Procedures	PVCS
NB/PRO/007			NB Manual Key and Password Management	PVCS
RS/REQ/022			Secure Role Definition for Secure NT Build	PVCS
RS/DES/080			NT Domain Structure Design	PVCS
RS/DES/081			Implementation Guide for NT Platform	PVCS
			SAP Security Operating Standard	PVCS

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

0.4   Abbreviations/Definitions

Abbreviation	Definition
ACP	Access Control Policy
ASD	Architecture and Strategy Development
CAW	Certification Authority Workstation
CESG	Communications-Electronic Security Group
CLI	Calling Line Identification
CS	Post Office Account Customer Services
DBA	Database Administrator
DC	Debit Card
DMZ	De-militarised Zone
DRS	Data Reconciliation Service
DSA	Digital Signature Algorithm
DWP	Department for Work and Pensions
ECCO	Electronic Cash Registers at Counters
EPOSS	Electronic Point Of Sale Service
ESNS	Electronic Stop Notice System
FTMS	File Transfer Management Service
Core Services	Fujitsu Services Core Services
HSH	Horizon Service Helpdesk
HFSO	Horizon Field Support Officer
IT	Information Technology
KEK	Key Encryption Key
KMA	Key Management Application
LAN	Local Area Network
MIS	Management Information Services
MI	Management Information (in Post Office Account CS).
NAO	National Audit Office
NBX	Network Banking Engine
NBS	Network Banking Service
NMS	Network Management Station
NT	New Technology (Microsoft's operating system)

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

OBC	Outlet Business Change
OBCS	Order Book Control Service
OCMS	Operational Change Management System
POA	Fujitsu Services, Post Office Account
POM	Post Office Manager
RDMC	Reference Data Management Centre
RDT	Reference Data Team
SMC	System Management Centre
SMDB	Service Management database
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSC	System Support Centre
TACACS+	Terminal Access Controller Access Control System +
TIP	Transaction Information Processing
TME	Tivoli Management Environment
VME	Virtual Machine Environment
VPN	Virtual Private Network

0.5   Changes in this Version

Version	Changes
7.0	For approval

0.6   Changes Expected

Changes
Comments from reviewers

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

0.7 Table of Contents

FUJ00088155
FUJ00088155

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: **14/04/2005**

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

1.0 Introduction

1.1 Purpose

This Access Control Policy (ACP) defines the policy for controlling access to resources in the Horizon system.

Effective control depends on:

* Understanding the information in the system and what access to it should be permitted, and where it is vulnerable;

* Having a clear definition of the roles and responsibilities of all personnel who need some form of access to the system;

* Setting access policies and controls to provide the required access while countering the threats and vulnerabilities.

1.2 Context

Information Security is based on a number of precepts, the most important of which are defined as being; confidentiality, integrity and availability,

These are broad categories of security controls which can be employed to provide various levels of security to guard against specific or perceived 'risks' which have been jointly identified by Post Office and Fujitsu. This document defines the policies for controlling access to the Post Office Account IT system in compliance with the Post Office Account Security Policy and fits into the structure of documents for Post Office Accounts security as illustrated in figure 1-1 below:
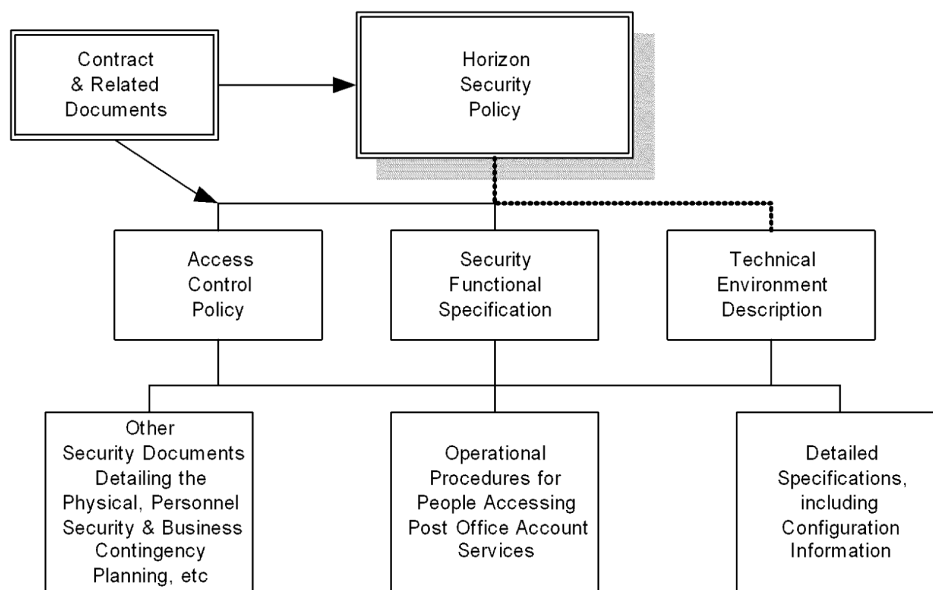

Figure 1 - 1 Post Office Account's Security Documents

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

BS/ISO IEC 17799, "A Code of Practice for Information Security Management", is primarily concerned with management and operational controls, but also sets out a number of technical security controls. BS/ISO IEC 17799 is used as the basis of Horizon's Security Policy and Procedures to define the controls used throughout Post Office Account.

Fujitsu Services shall operate a quality management system which complies with BS EN ISO 9001:2000 as defined within Schedule 2 of the Post Office ltd and Fujitsu Services Ltd Agreement.

- The Security Functional Specification (SFS) defines the security functionality that is incorporated into the Horizon system.

- The Technical Environment Description (TED) describes the architecture and technical environment for the Post Office Account solution.

Controlling access to IT resources requires a combination of both physical controls and manual procedures as well as technical controls on the IT system. Other documents define the related policies, procedures and processes, for example, for the physical security of information, including the procedures for entering a site and the safeguarding manual records, as well as procedures for using the system and the handling security incidents. Other documents define how the various Post Office Account components are configured and integrated into the system.

1.3   Effect on other Post Office Account Standards and Procedures

This Access Control Policy defines the policy for controlling both human and non human access to resources in the operational Horizon system. As explained in section 1.2 other documents give more details of the technical solution and the associated policies and procedures. The effect of the Access Control Policy on these other documents is:

1.3.1.1   Configuration documents should define in detail how systems are configured to conform to the ACP, for example, how the roles defined in the ACP are set up to restrict access as required.

1.3.1.2   The roles defined in the ACP should be used in other standards and procedures, not just information system controls. For example:

- where a role requires access to administrative privileges or sensitive data, this should be reflected in the level of vetting required for staff in that role;

- users in these roles must be formally registered and authorised to take that role by the appropriate authority before being added to the IT system. Records of all persons registered to use the system must be kept, though the way this is done may be role or service dependent.

1.3.1.3   Where physical security and/or procedures are required to complement the IT controls to achieve the required level of access controls, such procedures need to conform to the ACP.

1.3.1.4   The Post Office Account Security Manager will satisfy himself that the procedures at the various Outlets are in compliance with the Post Office Account security policies and specifications.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

1.4   Scope and Document Structure

This Access Control Policy defines how access to information system resources is controlled in the Post Office Account solution. It covers the Post Office Account Data Centre systems; Post Office Account managed systems such as interface systems at Post Office Ltd. Outlets and closely related Post Office Account systems. Access may be the result of direct user action, or automatically initiated activities. The ACP contains:

- An outline of the services, the roles of the people and the Outlets used in the Post Office Account solution (Section 2);

- The access control policies for the whole of Post Office Account, covering policies for authentication, information access within systems, system set-up and network access etc (Section 3);

- Specific access controls for human users - where the policies in Section 3 are specialised for particular user roles or there are exceptions to the general policies (Section 4);

- Specific access controls for particular systems - specialisation and exceptions to the policies in Section 3 and 5;

- A complete list of Post Office Account human roles and an overview of the IT access permitted to each of these (Section 6).

This document specifies access control policies, not the detailed procedures for configuring and operating these systems. Separate internal Post Office Account documents also cover system development and test systems and other activities prior to the handing over of the software for operational use.

1.5   Access Control Policy Review

This document will be formally reviewed at least annually. It will also be reviewed, where necessary, after a significant security incident, as part of an update following enhancements or new services being introduced, or a more general security policy review, and updated as and when necessary if there has been a significant security incident.

Responsibilities for the approval, review and issue of this document will conform to the review procedure for Post Office Account policy and standards defined in the Post Office Account Security Policy.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

2.0   Outline of Services, Roles and Outlets

The Horizon system can be described from different views as follows:

- The operational systems and their business users.

- The business management users of the system, including security and auditing.

- Outlet Business Change used during the introduction of new Post Office outlets.

- System & operational management and support.

This Section gives an outline of the people and systems involved as a context for the policies and roles described later. It is not intended as a complete description of the system - for that, see [TED].

2.1   Operational Services and their Main Users

The operational systems and their main business users and Outlets are shown in the following diagram.
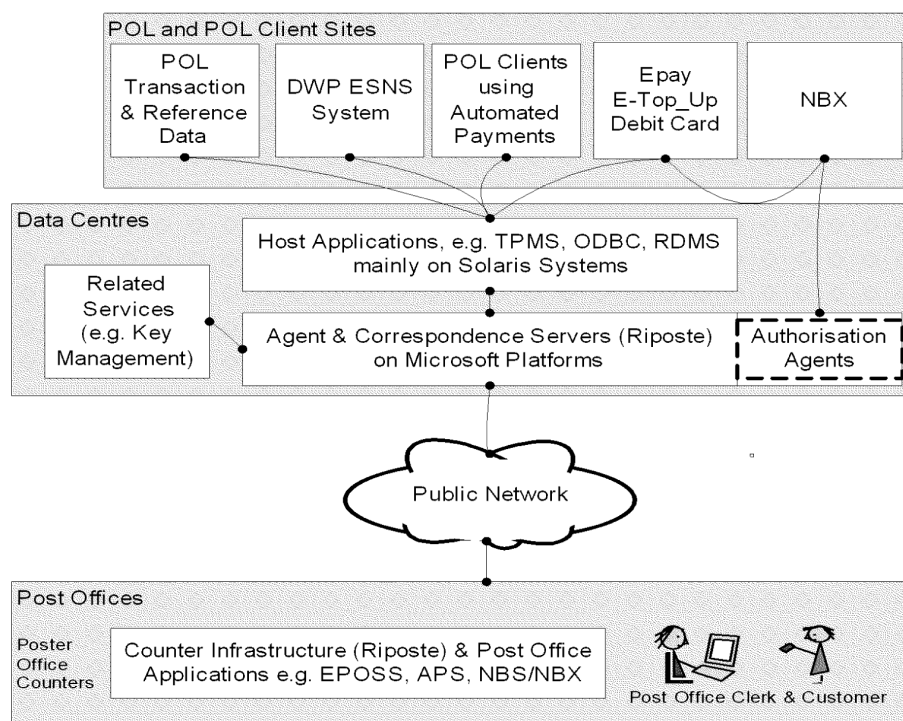
Figure 2 - 1   Main Operational Systems

2.1.1   Services, Systems and Interactions

Information is sent from Post Office Ltd. (reference data) and Post Office Ltd. clients (APS information from Post Office Ltd. clients) to the Post Office Account Data Centres. Most of this data is also forwarded to relevant Post Office outlets for use by applications there. Transactions at the Post Office outlets are recorded at the correspondence servers and forwarded to Post Office Ltd. and/or other Post Office Ltd. clients as relevant. NBS on-line transaction data is exchanged with the NBX via dedicated Authorisation Agents over an encrypted link.

At the Data Centres the main applications are on Solaris systems but the agents and correspondence servers which handle distribution of information to and from the Post Office outlets are on Microsoft servers, as are most of the supporting systems such as the key management systems. Post Office Systems are also Microsoft platforms

Apart from at the Post Office outlets, all activities are automated in normal circumstances, so there are no business users.

2.1.2   Roles

At the Post Office counters, operational roles are the Post Office Manager, Supervisor and Counter Clerk. There are equivalent roles in franchises and Sub Post Office outlets i.e. Sub Postmasters and their staff.

2.2   Business/Corporate Management

Post Office Account corporate management users and the systems they use are shown in the following diagram:

Figure 2.2 Corporate Management

2.2.1   Services and Systems

Corporate management services provide analysis and reporting of management information on Post Office Account's operation of the Horizon system. Systems include:

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

- MIS systems, including a financial system at a separate site.

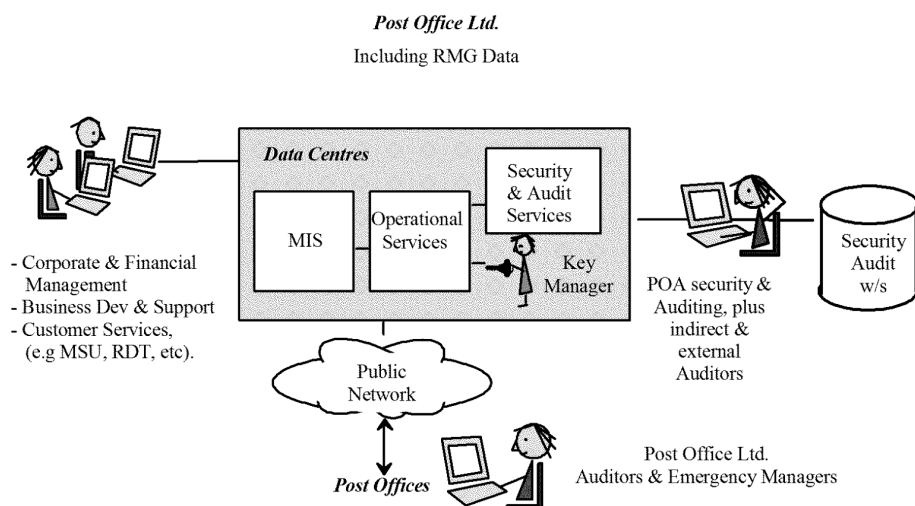The MIS systems at the Data Centre support a number of services including Contract Management, Reconciliation and Accounting and Asset Management.

CS Management Service user's access aggregated information via the SMDB, which is placed in a DMZ formed by the use of two separate firewalls. Authentication to the Webserver on the SMDB is by username and password.

There are also Security Specific Services including an Authentication Service for security token users and key management services. Keys are installed at the Data Centre and also at interface PC's at other sites.

2.2.2 Roles

The main roles are:

- A range of Post Office Account corporate management roles e.g. financial management, contract management and associated support roles.

- A number of Post Office Account customer service roles such as Management Support which assist business operations such as financial reconciliation of payments and Reference Data roles for maintaining reference data.

- Post Office Account Security Management, which manages security tokens for Post Office Account users. This includes the Post Office Account Cryptographic Key Manager who is responsible for generating and distributing all cryptographic keys used in Post Office Account to protect communications links, digitally sign information and encrypt filestores within Post Office account and at Post Office Outlets.
  The Key Manager will delegate some responsibility for installing and updating keys to Post Office Account Cryptographic Key Custodians and Cryptographic Key Handlers.

- Post Office Account Prosecution Support, which provides system data and associated information in support of investigations and litigation activities undertaken by or on behalf of Post Office Ltd.

- Post Office Account Auditors: both a Business Function Auditor responsible for general auditing of the Horizon system (focusing on business, rather than security, auditing) and a Security Event Auditor responsible for auditing all use of the Horizon systems. Both types of auditor access information on the Horizon system.

- Post Office Ltd. Auditors, Investigators and Emergency Managers who can access services at Post Office outlets.

  Post Office Ltd. and NAO Auditors also have indirect access to audit information at the Data Centres. This is via Post Office Account Auditors, rather than direct access to the Horizon system.

2.3 Outlet Business Change

The main people and systems involved in implementation of new Post Office outlets or their closure/suspension are shown in the following diagram:

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005
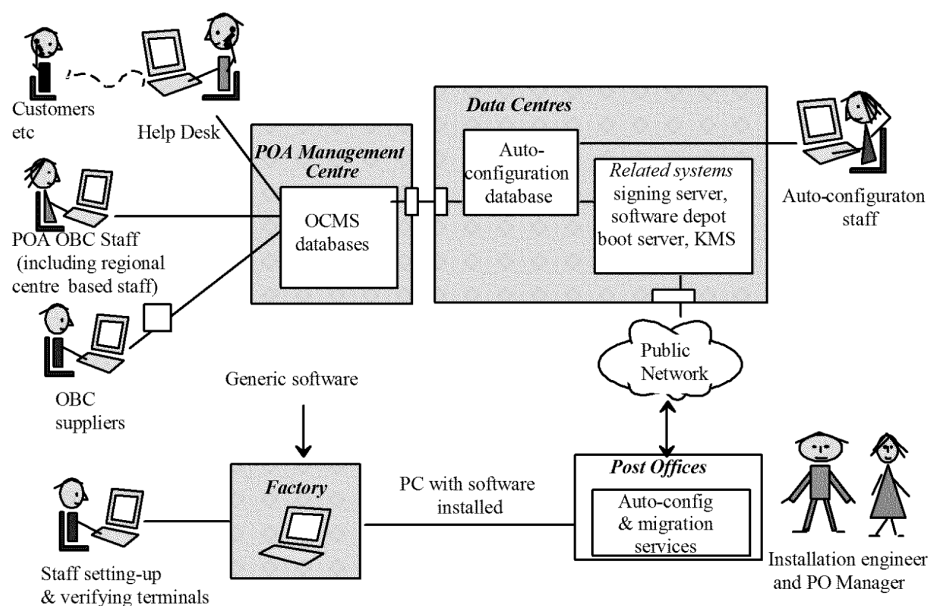
Figure 2.3 Outlet Business Change - Services and People.

2.3.1 Services and Systems

The OCMS database contains information about Post Office outlets where Horizon is to be implemented or withdrawn, for example, Post Office details, the state of the site etc.

Configuration information comes mainly from the auto-configuration system and is used in the initial set-up or in respect of decommissioning activities of Post Office outlets, updating the generic set-up of the counter systems as delivered. The auto-configuration process is very largely automated.

2.3.2 Roles

The main roles here are:

- The Help Desk;

- Outlet Business Change Team;

- The staff responsible for auto-configuration, who may need to amend information in certain circumstances.

In addition, there are Outlet Business Change suppliers who are responsible for site surveys, installation etc (who use bulk transfer, not interactive access to the OCMS database) and the people who set-up and verify the counter terminals in the factory.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: **RS/POL/003**
Version: **7.0**
Date: **14/04/2005**

2.4   System & Operational Management and Support

The main people and systems are shown in the following diagram:
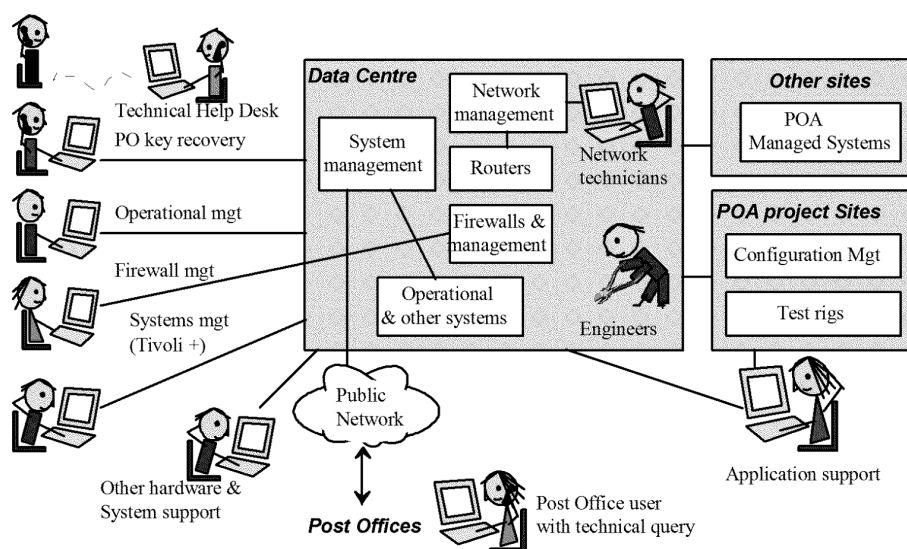
Figure 2.4 System Management & Support.

2.4.1   Services and Interactions

System and operational management and support users manage and support Post Office outlets, systems at the Data Centre (including routers and firewalls) and Post Office Account managed systems such as the interface PCs at Post Office Ltd.

The help desk handles all technical calls from Post Office Ltd. and other Post Office Account users including those from the Post Office requiring key and password recovery services.

Post Office Account project sites include a Configuration Management system that enables software to be distributed to the Horizon systems, including Post Office outlets. There are also test rigs used by application support staff for detecting and fixing bugs.

The technical help desk and system/operational management and support staff also use internal Post Office Account/Fujitsu Services support tools such as the Powerhelp and Problem Management systems for recording, progressing and monitoring calls to the help desk.

Note that many of the system and operational management and support staff are remote from the systems being managed.

2.4.2   Roles

The main roles are as follows:

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

- Operational Management (sometimes called System Administration): keeping the system running where this is not carried out by system management. Operational management is normally split into sub-roles, including:

  – System set-up and installation: setting up the base and application software on the system and configuring it for live running, including roles.

  – Software update, where this is not automated via system management.

  – Security/User administration: administering user security information such as their authentication information, the roles they can perform and the groups to which they belong.

  – Database (e.g. Oracle) or Package (e.g. Riposte) administration.

  – Computer operator: on most systems, this is a minimal role - switching on machines, loading media and similar operations.

  – Other system administration functions.

    Note that some package administration is done by people supporting the application users e.g. Discoverer and Business Objects are administered by corporate management support staff.

- System Management: monitoring events and resources in the operational system and taking appropriate action to rectify problems. Also, distributing software (complete new packages or patches), where this is automated, for example, at the Post Office outlets. Sub-roles for operational management separate specific roles and also separate administration of users and the Tivoli system itself.

- Network Management: managing the network, including routers and firewalls, which connect machines and Outlets.

- Application support; 2nd, 3rd and 4th line.

- Other hardware and system support.

- Horizon System and other technical help desks and supporting staff.

- Engineers.

2.5 Post Office Account Sites and Interactions

The main Horizon services run at the secure Post Office Account Data Centres. This includes primary operational systems, most corporate management systems, some Outlet Business Change and system & network management systems as outlined in previous sections.

The main operational and management services can be run at either site, if needed, though there is a prime site for each. Figure 2-5 shows the sites with electronic links to the Post Office Account Data Centres.

FUĴITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005
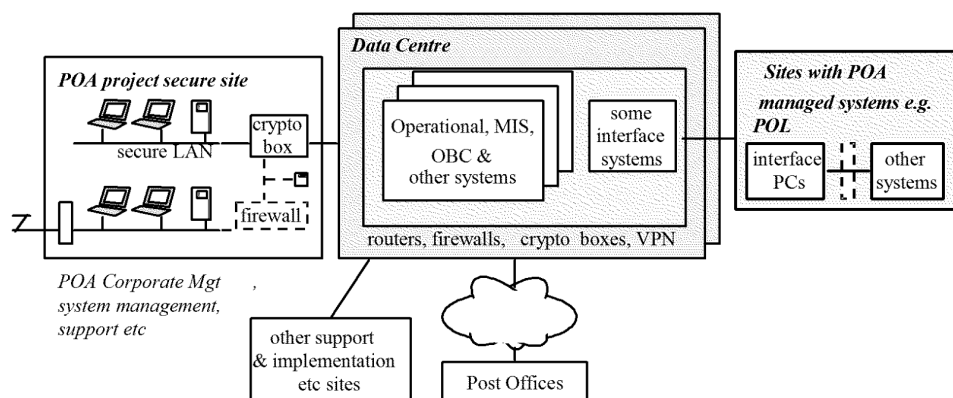
Figure 2.5 Post Office Account Data Centres and linked Outlets

All links to the Data Centres are protected by routers, firewalls and DMZs, cryptographic boxes or VPN (or a combination of these) depending on the requirements protecting each type of link and the data that travels over it. Routers and firewalls are also used to separate Data Centre systems in some cases.

Where Post Office Account communicates with other organisation's sites (such as Post Office Ltd.), Post Office Account will manage the interface PC/router at that site to provide a gateway between Post Office Account and that organisation's systems, however, this differs in a number of cases for services such as NBX for LiNK and CAPO, Streamline,and Epay

The main Post Office Account project sites that have access to the Data Centre systems have secure LANs for that access with an encrypted link to the Data Centre. Where people at these sites access other systems, including other sites, there are separate networks. At some Post Office Account project sites there are more complex networks which permit limited traffic to/from other controlled systems (e.g. for software distribution from the Configuration Management systems and for downloading of data to test rigs for investigating faults). In these cases, firewalls are used at the project sites to control this traffic.

There are a number of other support and Outlet Business Change sites with different types of access. These are subject to different access control policies as appropriate for the site.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

3.0 Overall Access Control Policies

This Section identifies the overall access control policies and associated procedures and controls that apply across the Horizon solution. It outlines the general policies that apply across systems and identifies where variants and exceptions are permitted. In these cases, the exceptions are defined in the appropriate sub-section of Sections 4 and 5 below. No other variants are permitted.

3.1 Introduction

The objectives in the Post Office Account Security Policy give the requirements for confidentiality and integrity of data, whether in storage or in transit, and integrity of the services and software components. The ACP defines the policies for controlling access in line with these objectives.

3.1.1 Post Office Account Human Roles

Human access to the Post Office Account information systems is specified in terms of roles. People in specified roles are permitted to carry out defined functions and access specified data. This is normally monitored by controls within the information systems, though in some cases, manual procedures are used to supplement these.

Post Office Account controls the roles people are allowed to perform, and which functions they are allowed to carry out. Users are individually identified so that they can be made accountable for their actions.

Where practical, the same or similar roles are defined for several systems to reduce complexity and make it easier to check compliance with the overall security policy.

The Access Control Policy includes all roles for users who have direct access to the Horizon operational systems and the related systems at the Data Centres. In addition, this document includes a limited number of user roles that enable others to use the system on their behalf (e.g. in response to a phone call).

Roles are normally associated with major functions. Defining separate roles allows different functions to be allocated to different individuals. However, the actual allocation of roles to individuals is done by administrative action. Some users may be permitted to carry out more than one major function, so are permitted to take more than one "role". This is not permitted in cases where security may be undermined.

3.1.2 Types of Information and its Use

Information in the Horizon system that requires protection from unauthorised access includes:

- The business data exchanged with Post Office Ltd. and its clients (e.g. reference data to support EPOSS and transaction data resulting from Post Office counter activities.)
  Business data is transferred between Post Office Ltd., Post Office Ltd. Clients and the Post Office Account Data Centres and between the Data Centres and the Post Office outlets. It is stored at the main operation systems and also in archives. Some data is also available for management services via the SMDB.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

- Post Office Account business management data - financials, service level agreements etc. Confidentiality and integrity requirements exist for much of this data. The Management Information System collects this data from the operational systems. This is then forwarded as appropriate to Post Office Account sites, Post Office Ltd. and their Clients.

- Other data supporting the business processes such as training data (special, non-sensitive, business style data used in training sessions) and on-line documentation (e.g. Post Office procedures.)

- Operational systems data such as the software, configuration information, Tivoli scripts, system management event logs etc. This information is held mainly at the Data Centre and accessed remotely from system management and support sites.

- Security information about users, keys, security audit logs etc.

Most processing of the business information, except at the Post Office Outlet, is automated and therefore not subject to human access. Most processing of system data is also automated.

All information is protected in compliance with the Security Functional Specification and Post Office Account Security Policy.

3.2 General Principles

The following general principles should be followed in controlling access to the Horizon systems.

3.2.1.1   The principle of "least privilege" must apply to restrict the access rights of users. (This may be applied through a mixture of technical and procedural controls.)

3.2.1.2   Duties of different users should be separated to minimise the damage that any one user can do to the system or the information it contains.

3.2.1.3   If a role at a particular location is allocated to a single person there should generally be at least one other person who can deputise for that person. (At small Post Office outlets where no deputy is available, and the Post Office Manager is unavailable, the Post Office Outlet will not open until emergency procedures have been invoked.)

3.2.1.4   Where possible, Post Office Account operations are automated to reduce the need for human intervention and the potential accidental and malicious security breaches that could result from human activity. E.g. applications should be designed to reduce the dependence on human interaction and jobs should be scheduled automatically in response to the receipt of files or at a particular time.

3.2.1.5   Similarly, where practical, system management tasks should be automated. This includes taking remedial action where the results of monitoring the system show this is needed. Only where action cannot be taken automatically, or human verification of an action is needed, should human intervention be required.

Note: This document covers access by system entities as well as human users, but does not define roles for them.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

3.3 Human Access

This section contains the policies for how human access to the Horizon systems is controlled. It is divided into sub-section for policies on:

- Authentication to prove the user's identity to the IT system, and hence the user's right to take on a particular role and access particular resources.

- User registration/ administration to establish and maintain the user's identity and security attributes (i.e. role, password, etc).

- Authentication of visitors.

- Authentication by telephone.

- Control of human access to resources (see also 3.5).

3.3.1 Authentication to IT Systems

3.3.1.1 All users must be authenticated to IT systems. This authentication must identify them as individuals. (The few permitted exceptions to this policy are in Section 4).

3.3.1.2 People accessing Horizon systems are required to identify themselves using hand held tokens if:

- They are at sites remote from the Data Centre and can update operational or MIS systems (for example, to perform systems management actions).

- They can access Post Office Ltd. business data (except at Post Office outlets).

- They are authorised to update system data that can affect the running of the Horizon systems. This includes roles that have UNIX root privilege, NT users belonging to the administrator's group and database administrators.

3.3.1.3 Where such tokens are used for authentication, the associated PIN must be at least 6 characters long.

3.3.1.4 Each user must have an individually allocated token except in emergencies, e.g. when a token is lost. In such cases, specific authentication will be agreed.

3.3.1.5 Where a user needs to authenticate to multiple systems/domains in one session, the first authentication (normally to the local workstation) should be with a token.

3.3.1.6 If a user who authenticates with a token to one system/domain needs to perform an additional authentication to another system/domain, the second authentication should also be a token based one, using the same token. Agreed exceptions to this must be documented.

3.3.1.7 Where passwords are used for authentication, the user should be forced to change the initial password before any other access to the system is permitted.

3.3.1.8 Passwords must expire in 30 days unless otherwise stated (in the section on the appropriate domain).

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

3.3.1.9 Re-use of the same password is not permitted for either a specified time or until at least 12 other passwords have been used.

3.3.1.10 Passwords must be a minimum of 6 characters long and be alphanumeric (i.e. a mix of letters and numbers). There cannot be more than two consecutive identical characters. The password cannot be the same as the username.

Note: The minimum password length recommended by industry best practice is 9 characters and should consist of upper case letters, lower case letters, numbers and symbols. All new systems should conform to this recommendation, however, it is recognised that some legacy systems will only be able to meet the requirements at 3.3.1.10 above.

3.3.1.11 After 3 consecutive unsuccessful attempts to log-on, the user should be locked out unless otherwise stated.

3.3.1.12 Users are authenticated with their individual usernames on first access to the system. A change to use another username will only be permitted to certain authorised operational management roles in exceptional circumstances as specified in this document.

Any change to use another username must be controlled and audited in a way that is always recorded.

3.3.1.13 In limited circumstances an operational management role may need full system administrator access. In these cases, where possible, the user should be given limited privileges on log-on with additional privileges being subject to further authorisation. In particular, no user will be allowed to log onto UNIX with root access (though some may be permitted a controlled change to root access later).

3.3.2 User Registration and Administration

3.3.2.1 People must be identified to Post Office Account information system as individuals. Users with direct access to the system should be registered as follows:

- If accessing the system via a package such as Oracle or Tivoli, they are registered with that package.

- Users who require direct access to the operating system are registered with that operating system (at the local system or MICROSOFT domain)

- Users requiring token authentication are also registered with the appropriate authentication service.

Note: The only exceptions allowed to this rule are the specific cases identified in later sections of this document. In these limited exceptional cases, the user, (e.g. an engineer) is identified as an individual using manual means prior to using the system in a way specially set up for this, and where the use of the system is suitably monitored.)

3.3.3   Authentication of Visitors to Post Office outlets and Post Office Account Sites

3.3.3.1   All visitors to Post Office Account sites who need access to operational systems must have a company identity card, which includes their photograph and pass number. For all such visits, the pass number of the visitor must be notified in advance to the relevant manager; access will not be permitted if this has not been done.

3.3.3.2   Post Office Ltd. Auditors may visit Post Office outlets and other Outlets without prior notice to the Post Office Manager.

3.3.3.3   Post Office Account visitors to Post Office Outlets must be subject to Post Office Account vetting procedures and approval by Post Office Ltd.

3.3.3.4   Other visitors to Post Office Outlets are also subject to agreed vetting procedures.

3.3.4   Telephone Authentication at Help Desks

The Help Desks receive calls from Customers, Post Office Ltd. staff at Post Office outlets and other people such as Post Office Account staff. The following categories of call have different authentication requirements:

- Category 1: Calls where the source of call would not affect the action taken. For example, the call is just a query of generally available information.

- Category 2: Where the result of the call is to cause an action which has only limited consequences e.g. to report a problem in the Post Office Outlet (which could result in an engineer call).

- Category 3: Where the consequences of misidentifying of the caller can be serious and the telephone authentication is the only authentication of the caller. For example, the wrong person may be allowed access to sensitive information, and/or be able to disrupt the service.

- Category 4: Where the consequences of the call could potentially be serious, but authentication of the user on the phone is only part of the process needed to complete an action. For example, a Post Office Manager has lost the PIN associated with the card used to boot the system, but will still also require a password to use the system.

3.3.4.1   For category 1 calls, no authentication is needed.

3.3.4.2   For category 2 calls made, for example, by Post Office Ltd. staff, at least the location of the caller should be verified, for example, the particular Post Office outlet, or Post Office Ltd. regional centre. This location must be one already known to the Help Desk for which suitable verification information is available.

3.3.4.3   For category 3 calls, the caller must be identified individually. (If the person concerned is not known individually to the Help Desk, the call must be routed via a known centre for verification. For example, calls from Post Office staff at the Outlet could be routed via a Post Office Ltd. regional centre whose staff authenticate to the Post Office Account Help Desk.)

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

3.3.4.4 For category 4 calls, the authentication process should at least verify the location of the call to one known and acceptable for this type of call.

3.3.4.5 Help Desks must maintain the information required to authenticate the callers and their Outlets/offices as required for the type of call.

3.3.4.6 If the call needs to be passed onto another internal Post Office Account help desk, the call should be forwarded only after the initial authentication has been carried out.

3.3.4.7 There are several different types of calls in each category. The authentication process for each call type must conform to these policies.

Details of the information used for different types of call must conform to these policies and be given in the appropriate Help Desk procedures.

3.3.5 Control of Human Access to Resources

Control of access to resources is achieved partly by workstation set-up and partly by administration of the resource, e.g. in the form of an access control list. Details of the way the access controls are implemented in information systems depend on the product used. They are not defined in this policy document.

3.3.5.1 All human users with access to Post Office Account Data Centre or Post Office Account managed systems on other sites must do so using controlled workstations as defined in 3.6.1.

3.3.5.2 Access controls associated with resources should define the "role" of the user, not the individual user's identity (unless there is an agreed need for individual access). The role may be represented by a group identity, for example, in products such as Riposte, UNIX ,Windows NT and Windows 2000, which support groups, not roles directly.

3.3.5.3 Access controls associated with resources should provide access to the resources as in the role definitions in Section 6.

3.4 Non Human Users

Much of the operational Horizon system is automated. Some users are therefore system based, not human users, so there are usernames and passwords for both types of users. In general, system users should be subject to the controls specified above (e.g. for password protection). This is because these usernames generally cannot be confined only to human users and they can potentially permit access to usernames intended for system users. However, some differences are permitted.

3.4.1.1 The username and password used to automate the login may be held in clear if it is only accessible to authorised operational management staff for that system and the potential damage from misuse of that username is minimised.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

3.4.1.2 The password may expire less frequently than the 30 days for human users where suitably obscure passwords are used, e.g. strong passwords consisting of upper case, lower case characters, numbers and symbols and the risk of external access to such accounts is very low.

3.5 Information and Resource Access

This Policy is concerned with protecting information contained in, and transmitted between all Horizon systems. This includes the Data Centres, Post Office Account managed systems (such as interface systems at Post Office Ltd. and other Outlets), and the systems used to access Data Centre and managed systems. Information requiring protection includes that generated during fault investigations/correction and that retained for auditing and fraud investigation.

3.5.1.1 Human access to sensitive information should be restricted to those whose role authorises them to see it.

3.5.1.2 Information in transit between systems should be encrypted for confidentiality and/or integrity according to the needs of the particular link as defined in the Security Functional Specification.

3.5.1.3 Digital signatures should be used for integrity of business information between the Post Office Outlets and other services where required. E.g. for signing automated payments at the Post Office Outlet prior to transmission via Post Office Account to Post Office Ltd. or Post Office Ltd. Clients. Some Clients may specify other protection such as encryption.

3.5.1.4 System data should also be integrity protected when required. E.g. digital signatures protect software distributed to the Post Office outlets and elsewhere.

3.5.1.5 Business information in filestore at the Post Office PCs should be encrypted.

3.5.1.6 Passwords should be stored in encrypted format and held separately from application data and executable code, except for the specific cases listed in *Non Human Access* above.

3.5.1.7 Horizon systems should prevent interference between human user roles, between applications and between human users and automated applications.

3.5.1.8 Information should be appropriately separated in filestore, database tables etc. Each data set should be accessible only to those with a need for that access.

3.5.1.9 Different applications should run in their own user names or that of the user that calls them (or at the Post Office Outlet, in the Riposte username impersonating the user).

3.5.1.10 Access to shared resources such as filestore should be controlled by:

- Access to that filestore being restricted to a specific product which is available only to authorised users, or

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

- Access to those resources being restricted to users in specified roles. (Group IDs may be used to represent roles. Access control lists using these will ensure that only authorised people can access the resource).

3.5.1.11 Information in relational databases should be accessible only via authorised client "applications" (such as Oracle Forms, Discoverer, Business Objects, Tivoli database interfaces) except where there is a proven need for lower level access. Lower level access will only be granted for agreed operational management and support functions.

3.5.1.12 System Management actions by Tivoli should be activated using pre-defined Tivoli tasks authorised for use by SMC and the Post Office Account configuration management and software distribution process. This includes collection of diagnostic information from the Post Office Outlet for application support.

3.5.1.13 Packages (such as Oracle and Tivoli) and applications above the operating system must also conform to the Access Control Policy. For example, Oracle should restrict users to the authorised tables and views. Also, access to the package's resources should use role based access controls.

3.5.1.14 For client-server applications (such as Oracle Forms ones), audit records should be generated at the server so audit logs do not rely on input from workstations.

3.5.1.15 Security audit logs must be protected from everyone except those permitted to take specified Security Event Auditor roles. Unless otherwise specified for a particular domain (such as the Post Office outlets), the security-auditing role is separate from other roles at that domain.

3.5.1.16 All systems, except Post Office counter systems, must provide read access to audit trails by authorised security auditors.

3.5.2 Key Management

Cryptography is used widely in Post Office Account as described in the Security Functional Specification for:

- Protecting information on links for confidentiality, integrity and origin authentication in line with the requirements for that link.

- End-to-end integrity and data origin authentication, potentially over multiple links using digital signatures.

- Filestore encryption at the Post Office Outlet.

- Protecting keys associated with the operation of PINPads and with the keys that protect customer PINs.

The following general policies apply for protection of keys.

3.5.2.1 CESG approved keys must be protected in line with CESG requirements.

3.5.2.2 Key material (symmetric keys, DSA private keys and DSA entropy) should be held in clear only when in physically secure environments.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

3.5.2.3   Public keys (except for the CA's public key) should be held in certificates signed by the Certification Authority.

3.5.2.4   Symmetric keys should only be stored where necessary, and be held securely.

3.5.2.5   Keys (or part keys) held in filestore must be in a separate filestore accessible only to authorised key custodians via authorised applications.

3.5.2.6   Keys used for protecting data should not be resident in filestore in clear.

3.5.2.7   Keys should be changed periodically according to CESG policy or, where commercial algorithms are employed, in accordance with industry recognised timescales. Different periods may apply to Symmetric Keys used for encrypting data, Key Encryption Keys (KEKs) used to encrypt other keys and Certification Authority keys.

3.5.2.8   New KEKs should not be distributed solely under the protection of existing KEKs.

3.5.2.9   Key material in transit electronically must be encrypted (except for CHAP keys between the routers within the Post Office Account Data Centre LAN).

3.5.2.10   Cryptographic keys and Key Encryption Keys are either installed locally at the machine where they are to be used, or are distributed electronically using an approved protocol which protects these keys in transit.

3.5.2.11   Where a key is delivered in two parts, e.g. a red key and a black key, the parts should be delivered by different routes.

3.5.2.12   The key (or part key) to be handled manually must be held in a locked safe when not in use. Access to this must be authorised and recorded in conformance with Post Office Account procedures.

3.5.2.13   The creation, handling, transmission and storage of keys must be undertaken in accordance with ISO9564. Key generation must be undertaken on standalone workstations or other hardware units within a physically secure environment.

In addition, the following policies also apply to the management of the NBS related keys:

3.5.2.14   Key generation and management must comply with ISO11568 Parts 1 to 3.

3.5.2.15   All keys that may directly or indirectly reveal a plain text PIN must be generated, handled, transcribed and stored in a way which ensures that no one individual has access to all key parts.

3.5.2.16   PINs and any cryptographic key that may directly or indirectly reveal them must never appear in plain text outside a tamper detecting hardware security device complying with the relevant section of ISO9564. Modules handling PINs or keys associated with multiple PINPads should conform to FIPS 140-1 level 3.

3.5.2.17   Devices used to generate keys associated with PIN encryption and PINPad loading must be physically secure and conform to agreed standards.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

3.6   System Set-up Policies

3.6.1   Workstation Set-up Policies

3.6.1.1   Users with interactive access to Horizon systems should use "controlled, "workstations" as defined in the following policies in this section. All such exceptions to the "Implementation Guide for NT Platforms" policy must be authorised and documented in the ACP.

3.6.1.2   Workstations from which operational systems can be updated should have floppy drives disabled or be fitted with physical locking devices. Booting from CDROM should also be disabled once a system has been configured.

In all cases, exceptions to this rule must be documented and agreed with Post Office Account Security Management.

3.6.1.3   Workstations at the Post Office display sensitive business data (e.g. about payments) as part of normal operation. All other workstations, which can display sensitive information, should be in physically secure areas.

3.6.1.4   All systems should have the required roles, groups and other privileges set up on installation. It should rarely be necessary to update these. "Guest" users must not be enabled in the installed systems, and where possible, Guest accounts should not be included. Other generic users should not be accessible for user logon except in exceptional circumstances explicitly defined in the appropriate section below.

3.6.1.5   Operating system set-up and services available at that workstation should be controlled by Post Office Account or shown to conform to Post Office Account standards.

3.6.1.6   After a workstation is booted up, a login screen should be displayed which cannot be by-passed.

3.6.1.7   The selection of tasks available on the desktop (or via secure menu system, where used) should be constrained to those available to users with that role.

3.6.2   Server Set-up

3.6.2.1   Servers should have floppy drives disabled at boot time. Booting from CDROM should also be disabled once a system has been configured. Wherever possible USB ports that are not required for the operation of the service should also be disabled.

In all cases, exceptions to this rule must be documented and agreed with Post Office Account Security Management.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

3.6.2.2 Where a server is delivered with pre-defined usernames for human users, these should be deleted, or if this is not possible, disabled) once the initial individual usernames required for administering the system have been set-up. Usernames should be disabled by changing by renaming the user account and assigning a strong password, which is extremely difficult to guess, then storing this password in a safe with appropriate manual controls for recording access.

3.6.3 Workstation Environment Related Access Controls

3.6.3.1 Users with interactive access to Horizon systems should access these systems via controlled, MICROSOFT workstations in secure environments as defined in the following policies. All exceptions to these policies must be authorised and documented in the ACP.

The following diagram shows the main types of workstation environment supported for access to the Post Office Account Data Centres and other Post Office Account managed systems:
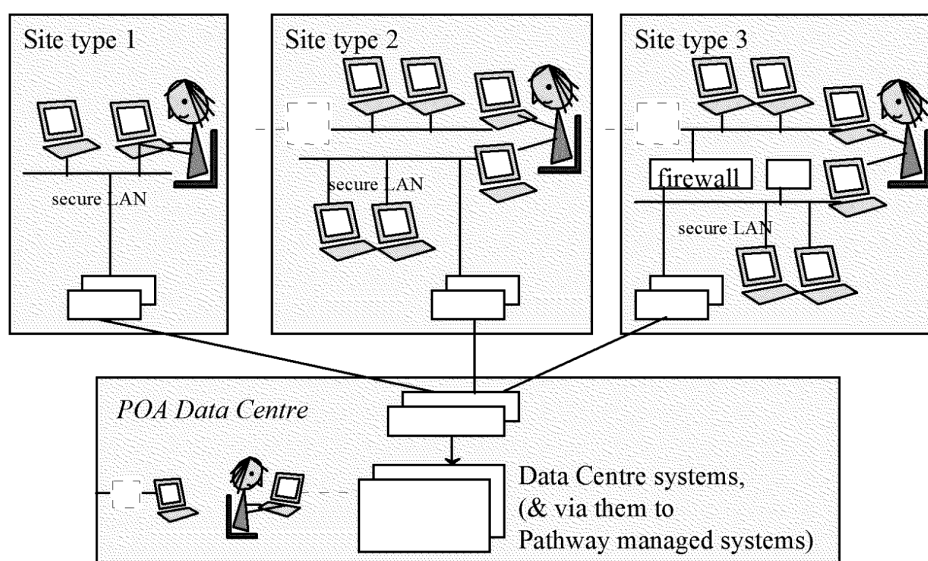
Figure 3-1 Workstation Environments Supported by Type

3.6.3.2 Workstations that have access to sensitive data or can be used to access Horizon systems (code or data) should be on separate secure LANS linked only into the Post Office Account secure network. (Site types 1 and 2 and the Data Centres)

3.6.3.3 The only permitted exceptions are:

- For authorised transfers of software and data from the controlled Post Office Account LAN at the management site at Feltham to the appropriate Data Centre system.

- For application support users linking to test rigs. In agreed circumstances, authorised application support users may access operational data to investigate a problem and may download that data to the workstation or test rigs.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

In these site type 3 cases, firewalls between the LAN on the project site and the encrypted link to the Data Centres must constrain traffic to just that authorised from identified project systems to the identified Data Centre systems.

3.6.1.4   All such users should authenticate using a token.

3.6.1.5   The secure LAN and workstations must be located in a physically secure area restricted to permitted users. This also applies to any routers, encryption boxes and firewalls connecting them to the Post Office Account Data Centres.

3.6.1.6   Where the workstation is remote from the system being accessed, encrypted links should be used.

There may be exceptions to this policy in the case of FTMS, Streamline and the TESQA links to Post Office Ltd. Clients, in any such cases the client is made fully aware the risks taken in using unencrypted links (see also 3.7.2.7 below).

3.6.1.7   Where a user also needs access to internal Horizon systems (such as the call recording and management systems and e-mail), the user must use a second workstation linked to the internal network and system required but not to the Post Office Account Data Centre. (Site types 2 and 3).

3.6.1.8   Incident tracking systems using networks outside the Post Office Account secure controlled area, for example e.g. the Fujitsu Services corporate network, may include information relating to a particular record of customer data but must not include such data, unless adequately protected, for example, by encryption.

There may be exceptions to this policy in the case of PEAK and SMBD where data is stored unencrypted.

3.6.1.9   Any external users must conform to these policies.

3.6.1.10   External support users of Horizon systems (such as Solaris and Cisco) should be permitted access to Post Office Account Data Centre systems only from approved Outlets/environments and subject to agreed network and other controls (see 4.6.3).

3.6.1.11   Where, by the nature of the role(s) to be performed, the workstation requires access to the Diskette or CR-ROM sub-systems, the workstation must be afforded additional protection through the use of anti-virus software. Where appropriate other controls such as the use of physical floppy locking devices and BIOS passwords should also be employed.

3.7   Network Access Policies

Post Office Account controls should be in place to restrict who can access particular services. This covers all traffic in and out of, as well as within, the Post Office Account Data Centres and managed systems and also within parts of the Post Office Account management systems. In addition to the workstation environment controls above, network access policies should be enforced where

appropriate by the use of a combination of access lists at routers, controls at firewalls, MICROSOFT domain controls, platform controls on use of ports and other application controls.

3.7.1   Information in Transit

3.7.1.1   Business and system data in transit to/from the Post Office Account Data Centres must be protected in accordance with [SFS]. This covers, for example:

- Transfer of data to/from Post Office Account managed systems at other Outlets such as Post Office Ltd. and Post Office Ltd. Client systems.

- Business and system management traffic to/from the Post Office outlets (which is protected using a VPN to provide authentication and encryption as well as digital signatures in some cases - see above)

- Business and system information between the Data Centres and Post Office Account management and Outlet Business Change sites

- NBS data transferred to/from the Data Centres and the NBX.

3.7.1.2   The Energis ATM network with its closed user group should be used to restrict access to the main Post Office Ltd. data (TIP and Reference data) to Post Office Account only.

3.7.1.3   All Fujitsu Services Core Services links should use VPN protection (for authentication and encryption) or in cases where that cannot be justified, CHAP authentication and CLI.

3.7.2   Control of Traffic In and Out of Data Centres

3.7.2.1   All access in and out of the Post Office Account Data Centres should be restricted to the required traffic from/to the authorised sources/destinations for business and system traffic using routers and firewalls. Such traffic should be routed only to the ports at systems, which require that traffic.

3.7.2.2   All management and support users access the Data Centres (and other managed systems) from controlled workstation environments as defined in 3.6.3 above.

3.7.2.3   All Post Office Account Corporate management, system management and support sites with access to the main operational systems should have fixed links to the Data Centres.

3.7.2.4   External support users with access to any of the Horizon systems containing sensitive or protectively marked information must access the systems via controlled workstations and environments as for Post Office Account support staff, but subject to extra controls – see appropriate section below. (Support of routers is an exception – see below).

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

3.7.2.5 All such fixed links should be protected by the use of hardware encryption devices using the Rambutan algorithm or where this is not appropriate, by the use of an agreed commercial algorithm.

3.7.2.6 Apart from links via the Energis closed user group to the main Post Office Ltd. systems (and via Post Office Ltd., to Royal Mail), all access to the Data Centre by external organisations for support or other purposes should be firewalled from the main Data Centre systems. Any exception to this must be agreed with the Post Office Account Security Manager and documented in the ACP.

3.7.2.7 Traffic to/from Post Office Account managed interface PCs/routers at other Outlets (Post Office Ltd., Post Office Ltd. Clients etc) should be restricted (by routers and firewalls) to:

- Authorised business traffic between the managed system and the particular Post Office Account Data Centre server handling that link (normally just file transfer between the systems).

- Network management traffic between the routers and the NMS.

- System management traffic between the PCs and Tivoli Management Centre

3.7.2.8 RADIUS Servers at the Data Centres authenticate traffic from managed PCs at Outlets. The Radius Servers, which used to authenticate FRIACO ISDN and ADSL network services for NBS, hold CHAP usernames and passwords for the live estate. No operational Post Office traffic should be accepted via other routes. Firewalls and Routers should also restrict where traffic can be routed to/from within the Data Centre i.e. to VPN servers the Correspondence Servers, Tivoli management servers and KMS.

3.7.2.9 When implementing a new or significantly changed Post Office Outlet, the initial connection will be to a dedicated boot server. Access to this from the Post Office outlets is via a firewall, which also restricts traffic between the boot server and the main Horizon Data Centre LAN.

3.7.2.10 Firewalls and Routers should be configured to deny access to external users (e.g. CISCO support) until this access has been agreed - see 4.6.3. When permitted, the appropriate router should be configured to restrict access to the Data Centre to the particular system(s) needing support.

3.7.3 Controlling Traffic Within Data Centres

3.7.3.1 Controls in the Data Centre should reduce the possibility of interference between systems by separating independent parts of the system, particularly where these which have different security requirements. (This may be by a combination of network set-up, router controls, controls at ports of specific systems and MICROSOFT domain structure.) For example,

- Systems concerned with Outlet Business Change should be separate from those used for operational running.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

- Security services, e.g. the Key Management Service (KMS), must be protected from unauthorised access from other systems.

3.7.3.2 Traffic originating within the Post Office Account Data Centres is generally initiated by controlled applications. These applications (and the way they are configured in the system) should restrict traffic between systems to the minimum necessary.

3.7.3.3 Additional network controls should be used where specific systems are subject to higher risks or vulnerabilities in the Data Centre network. All such special cases should be documented in the ACP.

3.7.4 Controlling Traffic at and from Post Office Account Project Sites

Post Office Account project sites include:

- Various systems and operational management sites and support sites

- The main Post Office Account management Sites

- The OBC Teams main site

- Offices used by Post Office Account Regional Managers

3.7.4.1 The main Post Office Account management sites should separate their main networks from both the Fujitsu Corporate network and from those more secure LANs used to access the Data Centre e.g. via a DMZ.

3.7.4.2 Most local users should only have access to specific LANs that provide access to local services and (via controlled connections) to the Fujitsu Corporate network.

3.7.4.3 The only permitted connections from this management site network should be:

- To the Fujitsu Corporate network via a controlled router, which restricts traffic to specifically authorised traffic only.

- To OBC users at regional offices and OBC suppliers at their sites via a controlled router and firewalls.

- To the secure LANs via a firewall which restricts data to that permitted (e.g. software from the Configuration Management system).

3.7.4.4 The only permitted connections from the secure LANs should be:

- To the Data Centres via encrypted links.

- To other secure LANs via an encrypted link (i.e. between the Post Office Account management sites).

3.7.4.5 All users with any interactive access to the Data Centres must do so via secure LANs (see also 3.6.3)

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

3.7.4.6   Separate secure LANs should be used for separate user groups/activities where sensitive data is being handled at Post Office Account management sites. For example, Security Management and Audit users should be on a separate high security LAN separate from other users.

3.7.4.7   Servers at the Post Office Account management sites that handle sensitive/RESTRICTED data or are used to update the Data Centre require stronger security and should therefore be on a secure LAN. This applies, for example, to the CM signing server, which distributes software to the Data Centre and reconciliation database.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

4.0   Specific Human Access Controls

4.1   Introduction

This Section deals with access control polices, in particular authentication policies for specialised human user roles and where exceptions to these polices are permitted.

Note that a full list of Post Office Account roles, outlining the IT access permitted to each of them, is given in Section 6.

4.2   Post Office Outlets – Operational and Installation Roles

There are no system management and support roles at the Post Office outlets. These tasks are run remotely apart from some limited tasks available to Post Office managers.

4.2.1   Post Office Normal Running

For normal functions, Post Office Managers, Clerks and Supervisors authenticate using a Riposte username and password.

On normal counter start up (once installation is complete) the Post Office Manager (or authorised other user) uses the Post Office Memory card and PIN (which is also used in protecting the filestore, as defined in the Security Functional Specification).

The following specialisations of the policies in Section 3 apply in these cases.

4.2.1.1   A password cannot be re-used for 18 months.

4.2.1.2   The password is checked to conform to quality standards as follows:

- The password cannot contain spaces;

- The password cannot be one of an agreed "excluded passwords" list.

4.2.1.3   After a period of inactivity at a Post Office counter, the session will time out but can be resumed on entry of the password. After a longer period of inactivity, the user is forcibly logged out.

4.2.1.4   The PIN used for the Post Office Manager's memory card is a 15 character alphanumeric value.

4.2.1.5   The Post Office Manager should secure the Memory card and associated PIN in separate places.

4.2.1.6   When a new Post Office user is added to the system, a full name must be supplied. This ensures that the user can be identified from the user name included in the transaction logged in the Riposte journals.

4.2.2   Customer Authentication at Post Office Outlets

For most Post Office operations, customers do not need to authenticate themselves.

4.2.3 Post Office Exceptional Cases except Installation

This subsection includes exceptional cases involving the Post Office Manager and other Post Office staff and also supports engineers, Post Office Ltd. auditors and emergency managers.

For some user groups, and some exceptional circumstances, the Post Office Manager (or other authorised person) authenticates using a one-time password with the assistance of the Horizon System Help Desk (HSHD). The Post Office system generates a value, then phones the HSHD authenticating to the HSHD as defined for that user role/circumstances (see Access Control and User Administration Processes and Procedures).

The HSHD, after authenticating the user, provides a check value that the user can type in at the Post Office counter to authenticate themselves.

The following policies apply to these exceptions.

4.2.3.1   If there is a failure on booting the counter systems after installation of new software, the Post Office Manager then reverts to the failsafe version of NT supported by HSHD and using a one-time password.

4.2.3.2   If the Manager loses his password, he (or an authorised deputy in his absence) logs into a SUPPORT username using a one-time password provided via the HSHD.

4.2.3.3   If the Manager loses his card or PIN, he obtains an emergency recovery key via the HSHD (after authenticate to the HSHD).

4.2.3.4   Support engineers (installing new hardware and running tests to check it) and Auditors use generic Riposte usernames for the appropriate role and authenticate via one-time passwords. For both engineers and auditors, the pass number is also typed in; so individual users can be identified in the log.

4.2.3.5   If a Post Office Ltd. Emergency Manager takes over a Post office when the manager is unavailable or unco-operative, he may use the emergency recovery procedure to boot up the Post Office – see 4.2.3.3.

4.2.4 Installation Roles at Post Office Outlets

On installation of a Post Office Outlet,

- The installation engineer sets up the connection to the data centre

- The Post Office Manager (POM) completes the Post Office set-up for normal working including set up of the memory card and PIN

4.2.4.1   The installation engineer must authenticate to the POM *(see Visitor Authentication)* prior to using the Auto-configuration application. Authentication to Microsoft or Riposte must be impossible at this stage.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

4.2.4.2   On first installation of the Post Office (after memory card set-up), the Manager logs in under the Set-up Manager username to create his individual username. He then logs in using this, and deletes the Set-up Manager username. On all future occasions, the POM must authenticate using his individual user name except in cases identified in 4.2.3 above.

4.3 Corporate (including Security) Management Users

Unless stated otherwise, all corporate management users are authenticated to their local Microsoft domain using a security token. They use controlled Microsoft workstations on secure LANs at Post Office Account sites linked by encrypted links to the Data Centres (see site type 1 in 3.6.3).

4.3.1 Business Management

These users may also need to authenticate to the relevant system and/or application for particular systems. This is required for Oracle applications, and for Business Object universes used to access data at Data Warehouse systems via Oracle/Business objects.

The only specialisation's and exceptions to the policies in Section 3 for these users are:

4.3.1.1   People in the following roles have access to CD writers at their workstations:

- Management support users, who write agreed warehouse data to CD for transfer to Post Office Ltd.

- The Business Function Auditor, who provides information to external auditors

- Security Management users for generation of key material.

4.3.2 Key Management

4.3.1.1   The Key Manager is responsible for the generation or other acquisition of cryptographic keys and organising their distribution.

4.3.1.2   The Key Custodian uses the local console at the platform where the key is to be installed/changed and authenticates using a token to the local system. For Microsoft, this is defined as a local role.

4.3.1.3   The Key Handler has the key on the appropriate media (e.g. floppy) for re-installation of the key during system reboot. He is not a known user of the system and does not authenticate to it.

4.3.1.4   The Key Handler role may be performed by identified, authorised (non-Post Office Account) staff at remote Post Office Account managed systems e.g. by Post Office Ltd. etc. at interface PCs at their sites.

4.3.1.5   The Cryptographic Key Manager and KMA Data Manager roles are SQL Server users, so log-on to Oracle, after Microsoft workstation, token logon. This gives access to specific functions only.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003

Version: 7.0

Date: 14/04/2005

4.4   Outlet Business Change Users

No specialisation to the policies in Section 3 have yet been identified for OBC users, except at the Post Office – see above.

4.5   System Management and Related Users

All system management, operational management and application support users have controlled Microsoft workstations for management/support activities, and a separate workstation for access to call monitoring and other systems as in 3.6.3 site type 2 and 3.

4.5.1.1   SMC/HSH technicians and other Tivoli users (e.g. Auditors, SSC application support) authenticate to Tivoli as well as the workstation logon to Microsoft.

4.5.1.2   For Post Office Key Recovery, the SMC Team Leader may also need to log onto the KMA via the specific KMS role created for this purpose.

4.5.1.3   SMC/HSH technicians also have limited read only access to some data centre systems for the purposes of fault diagnosis. Access is via SSH client on the support Terminal Server.

4.5.1.4   All network technicians access only the NMS and routers, so access for them is described in that section.

4.5.1.5   Controlled access to floppy diskette and/or CD devices is permitted in exceptional circumstances where such access is required in order to achieve the desired functionality, e.g. on AP client remote platforms where diskette is the nominated media for onward transmission of AP clients data, on Audit workstation from which extracts of audited information are delivered on CD-ROM.

4.5.2   Engineering Access

4.5.2.1   Where possible, engineering access to the machines, for example, for hardware diagnosis and repair, should be subject to the same controls as other users, as specified in Section 3.

4.5.2.2   In agreed, limited circumstances, (e.g. when the operating system cannot be booted) special access is permitted, by-passing the normal controls. In all such cases any visiting engineer must be subject to the policies for "authentication of visitors" (see Section 3) and two people must be present during such access.

4.5.3   Procedures for getting in Support Staff

A number of problems can lead to staff being required to support the system. This could be Core Services or SSC staff coming in to support the system from their normal support sites. However, it could also require support staff from other organisations such as Solaris or Cisco. Core Services is generally responsible for the call out procedures.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

4.5.3.1 All requests for technical support should be made to the Horizon System Help Desk. The identity of the caller requesting support (if by telephone) should be verified to ensure the call comes from an appropriate source, before being actioned. The Help Desk will pass on the call to the appropriate unit in line with Help Desk Procedures using the call handling system.

4.5.3.2 All support calls should be recorded in the call handling system and their progress reported there, including who was called out and the actions taken.

4.5.3.3 Routers will by default, be configured to prevent access from support organisations other than the SSC, SMC and the Core Services. When support is required from another authorised site (e.g. Solaris or Cisco), a router should be configured to allow this access, and then re-configured to disallow it after use.

4.5.4 Software Distribution and Exceptions for Fixes

4.5.4.1 All software (new software and fixes) must be registered in the configuration management system controlled by configuration librarians. It should be tested using test rigs and authorised by the CS Release Manager prior to distribution by Software Distributors.

4.5.4.2 In exceptional circumstances, where this is not fast enough, authorised code fixes may be done directly by Core Services according to agreed procedures.

4.5.5 Application Support

Application Support calls come via HSHD, from there they are forwarded to the appropriate unit. Many application support calls are routed to HORIZON SERVICE DESK for filtering known errors, before being forwarded to System Support Centre (SSC) or Core Services as appropriate for solving. Calls may sometimes be forwarded to other 3rd and potentially also to 4th line support units, which may include application suppliers.

Note that no application support users have access to Post Office counter systems except as allowed for in 4.5.5.2 below. Errors here are diagnosed using logs of events extracted via Tivoli.

4.5.5.1 All support users with access to the Post Office Account Data Centre must do so using Microsoft controlled workstations in a secure workstation environment as defined in 3.3. (For SSC, the secure environment must include a firewall to restrict traffic between the test rigs and the secure LAN, though the workstation gives access to both Data Centres and test rigs.)

4.5.5.2 SSC access to the counter estate via SSH and may download data from the Data Centres to an appropriate test rig where this is required to assist in diagnosing application problems and testing new software to fix the problem.

4.5.5.3 Support users should have only read access to the supported systems, except for:

- SSC support managers (not normal SSC support users) "correcting" data under controlled conditions. (Data may need to be corrected where it has been corrupted by faulty code.) Correction of data must be subject to agreed authorisation procedures.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

- Core Services operational management staff that will fast fix code, when authorised, under controlled conditions. Where time permits, correction of errors should be by re-issue of a new version of the software via the Configuration management system. When faster fixing is required, agreed Post Office Account authorisation procedures must be followed. For applications supported by SSC, this will start with a request by SSC.

  Remote access to FTMS Gateways and Counters is managed and supported using SSH client on a support Terminal Server.

4.5.5.4   In all cases, updates to code or data by application support staff require two staff to be present when the change is made and all such changes to be audited, identifying what has been changed (before and after values) and the individual who made the change.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

5.0 Specific System Access Controls

5.1 Introduction

This Section deals with cases where the access control policies in Section 3 are specialised for particular systems and where exceptions to these policies are permitted.

In addition to the policies in Section 3, all systems should support the roles in Section 6, with only the required functions and resources available as defined there with the human access controls defined in Section 4.

Note: the ACP does not cover internal systems such as Powerhelp and PEAK.

5.2 Post Office outlets Platforms

A multi-counter Post Office has a local LAN with Microsoft workstations, one of which is the gateway with a link to the Post Office Account Data Centres.

5.2.1 Human Users

The roles supported are Post Office staff (Post Office Manager, Counter Clerk and Supervisor), Customer (indirectly), Post Office Ltd. Auditors and Emergency Managers, Engineers (Support and Installation Engineers) and SSC (see 4.1, 4.2 and 4.4).

5.2.1.1 At no stage after leaving the factory should it be possible to logon directly to Windows NT and Windows 2000 or for a user to access Microsoft functions or data.

5.2.1.2 No operational management roles should be supported at the Post Office systems, or any other roles apart from than those listed above.

5.2.2 Factory Set-up Controls

Software is installed at the factory (though may be updated on installation) and initial configuration done.

5.2.2.1 Riposte user groups set-up should be Manager, Supervisor, Clerk, Engineer, PinPad Install, Auditor, AuditorE (used by Emergency Managers), Support (used for emergency procedures such as the Manager forgetting his password). The Engineer, Auditor, AuditorE and Support groups should be set up to require one-time password authentication.

5.2.2.2 Usernames should be set up in Riposte and Microsoft for an Engineer, an Emergency Manager, a Support user and for a number of Auditors (enough to allow an auditor at each counter of the largest Post Office) and a set-up manager associated with the relevant Riposte groups. (The Post Office Manager will introduce further users later.)

5.2.2.3 When leaving the factory, it should only be possible to run the Auto-configuration application, not log-on to Microsoft or Riposte.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

5.2.3 Post Installation Controls

5.2.3.1 After installation, special software used for installation only should not be accessible. Usernames used for installation only should be removed.

5.2.3.2 The encrypted filestore should not be accessible unless the workstation has been booted using the memory card and PIN (or agreed emergency procedures).

5.2.3.3 After a user has logged on using Riposte, all access to the system should be controlled by Riposte – the Riposte desktop should allow access to only those items available to people in the user's role. The user must not be able to call any other applications or Microsoft functions or resources. No direct access to Windows Microsoft should be possible at any time, even for engineers.

5.2.3.4 The Riposte infrastructure should not need Microsoft administrator privilege.

5.3 Solaris Systems

5.3.1 Introduction

Solaris systems and Oracle databases are used for the main operational applications (see 2.1) at the Data Centres. The systems also have data in flat files (e.g. before/after transfer to/from other systems).

5.3.2 Human Access

All Solaris systems support the operational management and support roles listed in Section 6. They also support application roles for the particular applications such as ODBC, RDMC and Business Objects.

5.3.2.1 All business users (such as the Business Support unit) should use Oracle applications – Oracle Forms, Business Objects or Discover3i.

5.3.2.2 Where the SQL*Net or Oracle access to the database could potentially give more access than that permitted for the business role, the application at the client must restrict access to that permitted. In addition, a secure controlled workstation conforming to Post Office Account policies (see 3.2) must be used and the user identified there with the correct role so that the application controls cannot be by-passed.

5.3.2.3 Users using only Oracle via applications on their controlled workstations should be registered to the Oracle application, not the underlying operating system, and authenticate using a password.

5.3.2.4 Where users need to be both UNIX and Oracle users, they should be registered in UNIX, and have Oracle use the result of the UNIX (and security token) authentication.

5.3.2.5 Oracle database administration functions should use:

- Patrol for monitoring the database

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

- Pre-defined Discover queries to examine the state of the database. (Discoverer should be configured to restrict access to the tables and views needed for the task and audit actions.)

- Pre-defined, authorised SQL*Plus for database updates (which should include auditing)

5.3.2.6   Application support users of Oracle should use:

- Pre-defined forms for correcting standard types of data problem

- Pre-authorised SQL*Plus scripts for correcting other data problems

    All pre-defined forms and pre-authorised scripts should audit the correction made.

5.3.2.7   Users who require any access to operating system facilities must do so via a secure menu system that restricts the user to functions authorised for users of that role (and audits all functions performed by that user).

5.3.2.8   Where a function called from the secure menu system requires a change of username, that change should be done automatically by the menu system and audited. Changes to username must also cause a Patrol event.

5.3.2.9   The secure menu system should have specific functions for most system management activities. However, for emergency use, the menu will include an item that provides root access and use of UNIX commands.

5.3.2.10   Computer operators access Solaris systems from the console, using the secure menu system to access a limited number of predefined jobs such as back-ups.

5.3.2.11   Engineering access when the operating system cannot be fully booted, is via "single user mode" under controlled conditions (see *Visitor Authentication* and *Engineering Access*). Single user mode should only be used when more controlled methods are not possible.

5.3.2.12   Operational management staff must always authenticate under their own names to UNIX and perform functions wherever possible without superuser/root privileges. If root is needed, the appropriate menu item on the secure menu system will be used to switch users. This will be audited and an alert sent to BMC Patrol so a record remains available even if the audit log at the UNIX machine is subsequently corrupted.

5.3.2.13   Where non-Post Office Account, e.g. Solaris staff provide 3rd line support, this may be from the 3rd party site. In this case, access must be from a controlled Microsoft workstation and controlled environment as for Post Office Account operational management - see 3.2. Call in procedures are as in 4.5.3.

5.3.2.14   As Solaris requires root access, an independent monitoring system will be used where all key strokes on the Solaris workstation are captured and echoed on a Core Services workstation.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

5.3.2.15 Application support managers can correct application data subject to authorisation procedures – see 4.5.5. For Oracle applications, this should, where possible, be via specific functions available to the Oracle SSC role. In exceptional circumstances, use of SQL*Plus scripts will be authorised after checking. For other services, this may involve updates to flat files. In all cases, corrections to the data are audited.

5.3.3 Application/Oracle Roles at the Operational Solaris Systems

5.3.3.1 Database roles with appropriate database views/tables should be used to separate what data is available to whom.

5.3.3.2 The following Oracle roles should be defined for all Oracle applications on the operational Solaris servers. Note that in some cases, people with different human roles in the list in Section 6 may have the same access to the same Oracle role.

Oracle role	Functions, and roles
MONITOR	Read only access to application data in this database - used by Auditors, application support etc
AUDITOR	As MONITOR plus access to audit information - used by auditors
CORE_SERVICES_DBA	Full dba privileges
SSC	As for MONITOR, plus limited updates, implemented by pre-authorised SQL*Plus scripts.
Management Information	Specific business support functions on OBCS and some other applications - see Section 6.

5.3.3.3 Other application roles should be defined for particular applications to support the application roles listed in Section 6, for example, Reference Data roles at RDMC.

5.3.3.4 Information available to people doing ad-hoc queries should be further constrained e.g. using Business Object universes.

Note that there are also roles for non-human users.

5.3.4 Solaris and Oracle Access Controls

5.3.1.1 The Solaris operating system should be set-up according to the access control policy in 3 above.

5.3.1.2 Automated processes should do all loading/unloading of data to/from Oracle databases. Separate interface tables should be used to restrict the damage possible due to failures during automated processes.

5.3.1.3 The set-up of the system should be regularly monitored, for example, to check for dormant accounts and to review any changes made to important system files.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

5.4 Windows NT and Windows 2000 Systems

This section deals with Microsoft workstations and servers at the Data Centres and other Post Office Account managed Microsoft systems except the Post Office outlets. Microsoft workstations at secure Post Office Account management and support sites should also conform to these policies, and the NT domain policies.

5.4.1 Generic Microsoft Policies

Microsoft systems support the operational management and support roles listed in Section 6 unless otherwise stated.

5.4.1.1 As on other systems, engineers should only have controlled access and must be accompanied by Core Services staff when using the system.

5.4.1.2 Apart from event logs etc, which are relevant to all Microsoft systems, application support users should access application databases via relevant tools, rather than just operating system facilities.

5.4.1.3 All Microsoft servers should be set up with a group and template user for the generic management and support roles (plus any others defined for the particular Microsoft system). When a user is assigned to a role these templates should be used to set up that user with the required user profile providing access only to those tools needed to carry out the role.

5.4.1.4 While use of Microsoft domains allows a user to log in once to multiple servers, some roles (such as Engineer and Key Custodian) should always be defined as requiring the user to be local to the machine.

5.4.2 NT Domain Policies

Windows Microsoft domains are used in Post Office Account to control which Microsoft servers can share Microsoft resources and which users have access to those resources. They are also used to simplify user authentication – a user need only logon once to a domain (or once to a set of domains) which have an established trust relationship that includes trust in the users of the domains.

Microsoft domains should conform to the following policies:

5.4.2.1 Microsoft domains should generally have at least one Backup Domain Controller. This should be on a separate site from the Primary Domain Controller. Exceptions to this must be agreed and are expected to be small domains with few users.

5.4.2.2 Where a set of related Microsoft systems is run by a different authority from other Microsoft systems, this should be set up as a separate domain.

5.4.2.3 Where such a domain does not share users or resources with other domains, it should be a separate domain with no trust relationship with other domains.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

5.4.2.4 Domains may span sites where all Microsoft workstations and servers in the domain are run by the same authority and are subject to the same physical and network security. (For example, the SMC system management domain spans the SMC workstations attached to a secure LAN on the secure SMC Site and the Tivoli Microsoft servers at the Data Centre).

5.4.2.5 A domain must be confined within an area of the network, which is subject to the same security policies and controls. For example, it must not include Microsoft systems on different sides of a firewall.

5.4.2.6 Where sharing of resources, but not users, is required between domains, then the trust between domains should be restricted to sharing the agreed resources/files across the domain boundary. The resource sharing must be restricted to the minimum required for the agreed functions.

5.4.2.7 Where sharing of files is required between domains on different sides of a firewall, this should be subject to special authorisation procedures as well as the policy above.

5.4.2.8 A domain should not establish trust in users registered in a domain in a less trusted part of the network.

5.4.2.9 Users should only have access to the Microsoft systems to which they are permitted access. The domain set up should prevent them accessing any other Microsoft systems.

5.4.2.10 Users should not be registered as Microsoft users at domains where their only access is at the application level, for example, from a remote client via an application protocol to a particular application that has its own logon.

5.4.2.11 Set up of Microsoft domains should assist separation of systems to reduce interference between them.

5.4.3 Correspondence Servers

5.4.3.1 Business Support and Auditor access to the operational Correspondence servers should be restricted to exceptional circumstances for limited amounts of data (as otherwise, the performance of the system could be impaired). In all cases, access should be controlled, and limited to use of a specific agreed query tool.

5.4.4 Security Servers on Microsoft

Security services on Microsoft are:

- The Key Management Application (KMA) which generates and distributes cryptographic keys to Horizon services and the Post Office outlets. An associated Certification Authority Workstation (CAW) generates public key certificates and Entropy servers that generate DSA entropy for digital signatures.

- The VPN servers used for protection of the traffic to Post Office outlets and across to Post Office Outlet LAN.

- The audit and key management workstations supporting the Post Office Account Security Manager and his staff.

- Signing servers to sign software and auto-configuration information sent to the Post Office Outlet.

(This is in addition to the software security services to protect data in transit on particular links.)

5.4.4.1 The Certification Authority Workstation (CAW) that includes the CA should be off-line – not connected to any network.

5.4.4.2 The KMA should store all keys encrypted, and the key used to encrypt these keys should be subject to the normal KEK policies – see 3.5.

5.4.4.3 Application level access to the KMA should be restricted to the agreed functions for each of the specified roles, and each role should have the least privilege needed to do the job. All security significant actions should be audited.

5.4.4.4 On-line interactive access by human users to the Microsoft server on which the KMA resides should not be generally possible. It should require approval by the Post Office Account Security Manager to permit this access (except for key handling on reboot). The access will only ever be permitted for:

- Read only access by application support staff (updates should always be via the standard Tivoli software distribution)

- Limited, authorised, system admin access by local users

- Engineers

5.5 Authentication Service for Authentication using Tokens

Authentication using tokens will be supported by an **Authentication Service** at each Data Centre (one the master, generally used for all authentications, with the other acting as a slave to provide resilience).

5.5.1.1 After installation and configuration of the Authentication Service, the only application access to the Authentication service should be by the Post Office Account Security Manager workstation at the Post Office Account management site. These must be controlled Microsoft workstations on the secure LAN (see Section 3).

5.6 Cryptographic Boxes

5.6.1 Hardware Encryption Boxes

Hardware encryption boxes are used to provide link level encryption on a number of links. These are government approved point-to-point encryption devices generally using Rambutan encryption but can operate with commercial encryption algorithms where this is agreed.

5.6.1.1 Access controls at these devices should be as specified by the manufacturer and / or informed by Post Office Account Security.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

5.6.2   Host Security Modules.

Host Security Modules (HSMs) provide a secure environment in which to translate an encrypted PIN value between domains – primarily between the Post Office Central Services domain and the NBX domain.

5.6.2.1   Access control procedures for these devices are documented in NB/PRO/007.

5.6.3   Secure Configuration Terminals

Secure Configuration Terminals are hand-held devices used to generate and encrypt keys and to load keys into HSMs.

5.6.3.1   Access control procedures for these devices are documented in NB/PRO/007.

5.7   Symmetrix discs

EMC require access to the live Central Host systems for support of the Symmetrix Remote Data Facility used to replicate disk array data between two Campuses. The disk arrays are monitored by an internal system, which regularly checks the disks against predefined thresholds such as numbers of failed read or write attempts. When a threshold is exceeded, the disk monitoring system automatically telephones the EMC support unit.

5.7.1.1   Access to EMC disc controller (and to discs) is as specified and restricted to the use of the special EMC client

5.8   Interface Systems at Business and Outlet Business Change

The Horizon system manages interface PCs at some related Outlets (Post Office Ltd., Post Office Ltd. Clients and Outlet Business Change supplier). It also manages the interfaces to the Post Office Account network (e.g. routers.)

In all cases, routers are managed by Post Office Account Network Management and interface PCs are managed using Horizon System Management.

5.8.1   Interface Systems with Interface PCs

Post Office Account has links to a number of Post Office Account managed interface PCs at Sites remote from the Post Office Account Data Centres. These include Post Office Ltd. and Post Office Ltd. Client systems. (The Post Office Ltd. TIP link is also used for Royal Mail traffic.) There may also be interface systems at Post Office Account Outlet Business Change Suppliers.

5.8.1.1   Once configured, the PCs and routers at these sites should not normally have any human access – file transfers should be automated and the PCs managed remotely using Tivoli.

5.8.1.2   The operational management role at these sites is limited to local system administrative functions only.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

5.8.1.3 The engineer role is restricted to installing or replacing the PC. The PC will not be repaired when configured into the operational system.

5.8.1.4 Business data in transit to the Data Centres is protected as defined in 3.7 above.

5.8.1.5 Where the PC is directly connected to other systems (such as the Post Office Ltd. ones), it should also be configured to restrict traffic with such systems.

5.8.1.6 Controls at the interface PCs at Post Office Ltd. (and similar) sites must ensure separation of incoming and out going files so that all files supplied by Post Office Account are read only for Post Office Ltd. access. In addition, files for different systems (e.g. TIP, Royal Mail and Reference Data) are separated.

5.9 System Management Servers

A set of Tivoli system management servers are used to manage the Post Office systems and related Data Centre Microsoft systems (mainly using Tivoli products). They also monitor other Post Office Account management systems and collect event data from other systems.

5.9.1.1 All users of Tivoli must be registered at the Tivoli server and associated with the appropriate roles, groups (and regions) to restrict their access to facilities, which they are permitted to access. (All such users have security tokens, so are also registered with an Authentication Service)

5.9.1.2 In addition to SSC and SMC/HSH roles, Tivoli servers should also support:

- Post Office Account Security Auditors with read access to audit information via the web interface – platform audit logs, Tivoli notices, and Tivoli events collected for auditing.

- Application support users with access to pre-authorised Tivoli tasks to extract diagnostic information from the Post Office.

5.9.1.3 Tivoli integrity features should also be used to protect Tivoli traffic on the link.

FUĴITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

5.10 Network and Firewall Management

5.10.1 Network Management and Routers

The Post Office Account network routers are managed using HP Open View with Cisco Works as illustrated below.
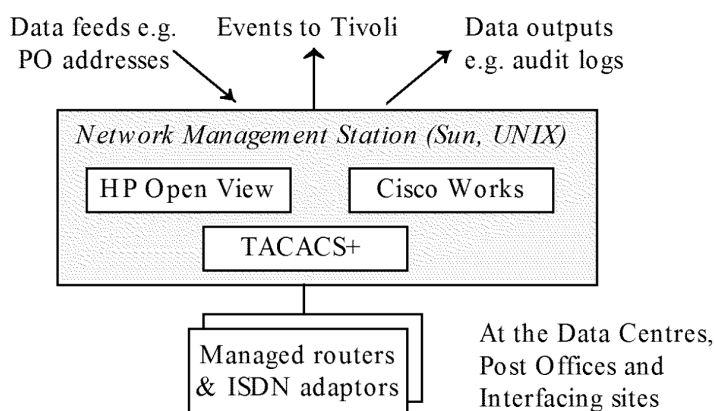

Figure 5-1 Network Management

There is a single Network Management Station (NMS) at each Post Office Account Data Centre. NMS users use controlled Microsoft workstations with tokens (see section 3) but also need to log onto UNIX for access to authorised OpenView and Cisco Works/View functions.

In addition to NMS roles, there are also Cisco router support roles. Engineers may also require direct access to routers.

There are no on-line application support roles. Support of Open View, Cisco Works etc is done off-line. Post Office Account auditors access audit information from the NMS via audit records sent through to Tivoli and extracted audit logs.

5.10.1.1   Network Management configuration must be carried out before live running and the configuration independently validated and authorised by a senior Core Services network person before use.

5.10.1.2   Even though network management workstations run 24 hours a day, all users must still be individually authenticated. (This implies that at the end of the shift, the existing user must log out and the new user log on.)

5.10.1.3   Network management should normally be done using OpenView. In agreed exceptional circumstances (for example, for fault resolution requiring use of the debug facility, in times of excessive network workload or during fault conditions), the network may be managed using router facilities directly via telnet, not via Open View, and therefore not subject to its controls. This is confined to authorised Core Services Network Managers using Telnet access to routers from a specific dedicated Microsoft system on the Operational Bridge area of the Network Centres.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

5.10.1.4   Telnet access to routers is permitted only to Core Services senior network management staff and Cisco staff supporting the routers from a remote CISCO site. All such access must be authorised by a member of the Telnet authorisation list. Manual records must be kept of this authorisation each time Telnet access is used.

5.10.1.5   All users of Telnet access to routers must authenticate using TACACS+ and their access audited at the NMS.

5.10.1.6   Cisco staff must access the router needing support via a separate gateway router dedicated for Cisco use. This gateway router must be configured to permit Cisco access only when Cisco support is needed. A different TACACS username and password must be used on each occasion, valid for the particular session only.

5.10.1.7   The standard Cisco engineers must have only read access to the routers. Only named and authorised senior CISCO staff may have the "enable" mode needed for reviewing configuration files and debugging. CISCO staff should not make changes to the routers, but advice the Network Manager of any changes required.

5.10.1.8   The only direct access permitted to routers is for engineers investigating hardware problems. In this case, access should always be done locally at the router using a console.

5.10.1.9   In normal running, the routers must not have consoles attached, though console access may be enabled. Any attempt to log-on at a console should be via TACACS+ and so be flagged at the NMS.

5.10.1.10   A faulty router must be configured out of the network before a console is attached and the router engineer logs on to diagnose and repair the fault. When the router is connected back into the system, its configuration must be checked and the new configuration authorised before the router is configured for normal use in the operational system.

5.10.1.11   Engineers are not individually known to the routers, so manual procedures must identify the engineer when he visits the site before he is given today's password. The password used for direct router console access should be changed via the NMS every 28 days and also immediately when an engineer requires access.

5.10.2   Firewall Management

Firewalls are managed using Enterprise Centres on Solaris systems (shared with Security token management), one at each Data Centre.

Enterprise Centre roles supported are Firewall Manager and Firewall Monitor. There are no on-line support roles for the Enterprise Centre application or the firewall application.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

5.10.2.1 All access to the firewalls must be via the NMS and the appropriate proprietry administration tools, Checkpoint Enterprise Manager for Checkpoint FW-1 and XXX for Cisco PIX Firewalls and Firewall Security Modules within the Core Switches, except for hardware maintenance. For routers, in normal running, firewalls must not have consoles attached – they should only be attached for hardware maintenance after the firewalls has been configured out of the system.

5.10.2.2 All configuration changes must be made via the NMS and the appropriate proprietry administration tools, Checkpoint Enterprise Manager for Checkpoint FW-1 and XXX for Cisco PIX Firewalls and Firewall Security Modules within the Core Switches and logged via Tivoli. Firewall audit logs should also be sent to the Enterprise Centre.

5.10.2.3 Firewalls should restrict traffic as in the network access policies in 3.7. (This is different for different firewalls).

5.11 Software Distribution Servers

Software distribution servers include the Configuration Management and associated signing servers on Post Office Account project Outlets and the depot/Tivoli servers at the Data Centres to which software is sent for onward transmission to other Horizon systems at the Data Centres, Post Office outlets and elsewhere.

5.11.1.1 The Configuration management system should have access controls, which conform to this policy, even though it is not at the data centre, or on a separate secure LAN.

5.11.1.2 The associated signing server should be on the secure LAN, and controls should be fully conformant with this policy.

5.12 OBC Servers at the Data Centres

The Post Office counters are delivered with a standard configuration, which needs to be personalised and updated when installed.

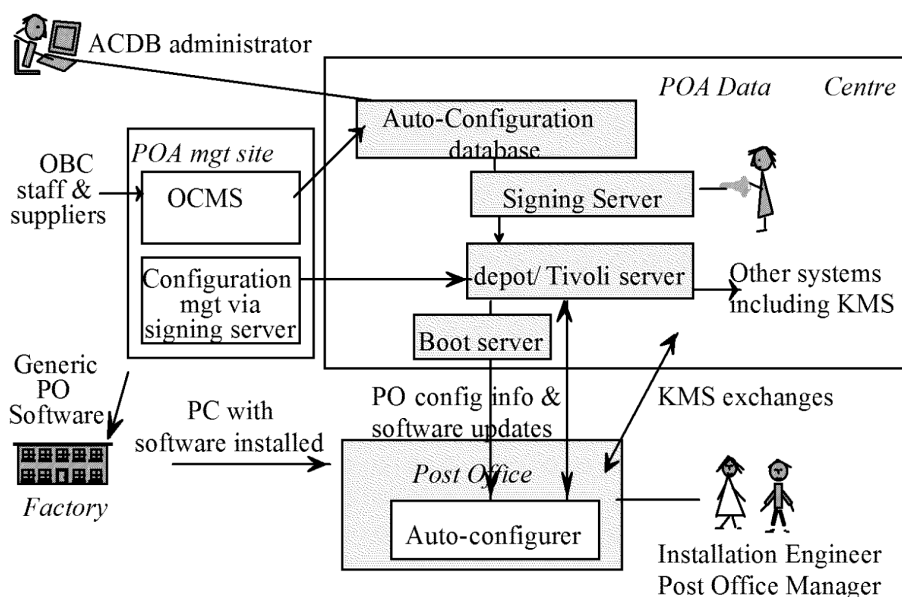The servers involved in this process are shown in the following diagram.

Figure 5-2 Interactions of Post Office Installations

5.12.1.1 The terminals should be delivered from the factory conforming to the agreed build with software, including an Auto-configurer application, installed.

5.12.1.2 Access to the ACDB should be confined to:

- ACDB administrators using controlled Microsoft workstations (Site type 1 in section 3.6.3)

- Application support using controlled Microsoft workstations (Site type 1 in section 3.6.3)

- File transfers from the OCMS database at the Post Office Account Management site via the firewall

- The normal Microsoft admin, audit and engineering access.

5.12.1.3 Access to the software depot/Tivoli software distribution system from outside the Data Centre should be confined to the feed of software and associated files from the signing server at the Post Office Account Management centre and to the managed distribution to the Post Office outlets.

5.13 Third Party Access to Aurora-Managed Consoles

Access to a third party supplier, e.g. UKME, Fujitsu Sun Support, Oracle to any of the UNIX server consoles managed by the Aurora servers in Bootle, Wigan or Bracknell will be as follows:

The following is a high-level overview of the process:

- Enable 3rd party access to the server under investigation i.e. log on to console as root and monitor output.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

- Enable 3rd party access to Aurora (enable modem and set password for 3rd party UNIX user)

- Give details of dial-up and login process to 3rd party engineer

- Monitor 3rd party access to the server under investigation (using aurora "view" mode)
  Once complete, monitor engineer logging off and disable all access (modem and UNIX user)

Monitor all engineer activities until investigation complete. if, at any point, the engineer looks to be putting the POA service at risk, either knowingly or unknowingly, take control of the console. This prevents the engineer being able to type commands at the console.

On completion check that the engineer has logged off Aurora by checking for the relevant user and if the engineer has not logged off, then force a log-off and free up the modem.

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

6.0   Roles and Permitted Access

This Section specifies all human roles with access to the Post Office Account Data Centres and the other Post Office Account managed systems such as the interface PCs at Post Office Ltd. Sites.

For each role, the following table outlines the job functions performed and also the IT functions and resources accessed to carry out these roles, including which systems are accessed. The table is ordered into:

- Main operational roles (Post Office outlet staff);

- Corporate management roles (Post Office Account business management, customer services including business support, Post Office Account security roles including cryptographic key ones and auditor roles including Post Office Ltd. and NAO auditors);

- OBC roles (help desk, ACDB roles);

- System and operational management and support roles (operational management on Solaris and Microsoft etc, SMC system management, software distribution, network and firewall management, application support and other support roles).

In the following table:

- The site type is:

  - DC for Data Centre

  - PPS for a Post Office Account project site

  - SL/PPS for secure LAN at a Post Office Account site

  - PO for Post Office

- The system is:

  - Solaris for all Solaris systems

  - HS for the Host Application Solaris system

Unless otherwise stated, users access the system via controlled Microsoft workstations, logging into the appropriate Microsoft domain.

	Horizon Access Control Policy	Ref:	RS/POL/003
		Version:	7.0
	Commercial In Confidence	Date:	14/04/2005

FUJITSU
FUJITSU SERVICES

Role (organisation)	Main Job Functions	It Functions & Data Access	Systems Accessed
Main Operational Roles			
Post Office Staff and Customers at Post Office outlets			
Post Office Manager (The person in charge of the Post Office, who may be a sub-postmaster or agent.) (Post Office Ltd.)	All the management of the Post Office system including setting up workstations, introducing users, doing accounts. Post Office Managers may allow other staff to deputise for them, and so take this role. Workstation set-up, emergency procedures, installation functions.	Key (and memory card) custodian - installing, changing and recovering keys. User management (of local post office staff). Specific management applications, for example, balancing Post Office accounts and stock unit management (including allocation to clerks). Run diagnostics to check system and peripherals are functioning correctly. All counter clerk functions.	Post Office only
Post Office Counter Clerks (Post Office Ltd.)	Run the PO applications e.g. APS, EPOSS and OBCS. Do training.	System boot-up using the memory card. (At some Post Office outlets, this may be restricted to more senior staff.) Run applications e.g. EPOSS, APS, OBCS. Stock unit balancing etc. In training mode, special training data (counter clerk also uses special training benefits/APS cards so does not need a customer present)	As above
Post Office Supervisor (Post Office Ltd.)	All Counter Clerk functions plus other functions.	As Counter Clerk plus viewing stock, users.	As above

Customers	Transactions at Post Office outlets e.g. buying stamps, collecting benefits, paying utility bills.	Customers do not access the system directly.	
Corporate Management Roles			
Post Office Account Corporate Management Roles and associated support roles *(all Post Office Account staff on secure LAN at Post Office Account management site)*			
Post Office Account Management Support	Managing the set-up of the management information services (e.g. setting up Business Object Universes and associated controls). Providing information to other Post Office Account Management users on request. Also, providing the Post Office Ltd. interfaces for management information – including provision of management data regularly and on request.	Business Object Universes (including supervisor functions); Read and update access to agreed MIS data including CONFIDENTIAL and SLAM; Data required for download to workstations for reports (Post Office Account, Post Office Ltd.)	DW; other MIS
Post Office Account Financial Management	Use of financial management information in the Common Charging System and elsewhere	Access to Common Charging System (CCS) and other financial information	DW
Post Office Account Contract Management	Use of contract management information in the Contract Management system (CON)	Access to CON service	DW
Post Office Account Business Development	Use of selected Data Warehouse information in development of the business	DW: read only access to Post Office information	DW
Post Office Account Customer Services, including Management Support *(mainly Post Office Account staff on secure LAN at Post Office Account management site)*			

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: **RS/POL/003**
Version: **7.0**
Date: **14/04/2005**

Post Office Account Customer Support Managers	Service Level agreement management	Business Objects Universe with predefined Reports for SLA's.	DW
CS User	Service Level agreement Monitoring of Outlets	SMDB Database access via Corporate LAN	SMDB
Management Support Manager	*Unit function* Support the business when there is a Post Office Account problem, for example a service breakdown. *[This includes reconciliation of data other services]*. *Role function* Authorising adjustments to business records subject to agreed procedures.	Access to services for cases needing reconciliation. Access to services such as OBCS, APS and TPS (PO transaction logs) etc when required. Also access to NBS reconciliation services via NWS User role and DRS. All update access is via specific Oracle forms applications.	HS: OBCS, APS, NBS Correspondence server, DRS.
Management Support Analyst	Investigating incidents, and adjusting business records, (but not finally authorising them.)	Access to OBCS, TPS, NBS etc as above	As above
Post Office Account Reference Data Management	Use of reference data in the Data Warehouse	Access to DW reference data	DW
Reference Data Change Manager	Kick off the transfer of validated reference data of classes 2 to 5 to TMS when all required dependencies have been met.	(Oracle role: user_change_control)	HS:RDMC

Horizon Access Control Policy

Commercial In Confidence

Ref:	RS/POL/003
Version:	7.0
Date:	14/04/2005

FUJITSU

FUJITSU SERVICES

RDMC Loader	Manually initiated load of reference data files to RDMC	(Oracle role: user_loader)	HS:RDMC
RDMC user	Query and report on reference data, so read only access	(Oracle role: user_reports)	HS:RDMC
RDMC access administrator	Sets up users and assigns them their roles	(Oracle role: user_administrator)	HS:RDMC
Post Office Account Security and Cryptographic key roles			
Post Office Account Security Manager	Maintains the records of security tokens and their PINs and users.	Maintenance and audit functions at the ACE server	ACE server
Cryptographic Key Manager	Generating or obtaining cryptographic keys and organising their distribution.	Also viewing current situation re keys (KMA) and generating certificates to certify keys (CAW)	KMA, CAW
Cryptographic Key Custodian	Initial installation of cryptographic keys where this needs to be done manually. Periodic update of these keys.	Installing keys where needed (interfacing PC (Data Centre and remote), KMA, (CAW), VPN. Always local user, not remote.	See IT functions column
Cryptographic Key Handler (Note 3)	Handling part of a split cryptographic key when this needs to be re-installed e.g. when a system is rebooted.	Loading part key (normally from floppy) during load, so no logon, no individual authentication.	As key custodian
PO Key Recovery (part of SMC team	Initiating recovery of a Post Office key from the Help Desk after a Post Office Manager has lost his	Authorised functions at KMA	KMA

leader role)	card or PIN.		
KMA Data Manager	Maintain validity of data within KMA database e.g. specify new client where keys are to be sent (but no key management roles)	Authorised functions at KMA	KMA
Auditor Roles			
Post Office Account Business Function Auditor	Overall auditing of the Post Office Account solution	(though not Post Office outlets directly, as there are records of Post Office activity at the Post Office Account central site.) The Business Function Auditor mainly uses information from the archive server and information extracted from other systems, though has limited access to other systems.	Archive server; exceptionally, correspondence servers, host applications etc
Post Office Account Prosecution Support User	Provision of audit data in support of investigations and litigation.	Information extracted from the archive server and supporting data extracted from other systems though has limited access to other systems.	Archive server and corporate problem management systems
Post Office Account Security Event Auditor	Auditing the security of the Horizon system including monitoring, investigating incidents, reporting etc	Operational and management logs of business transactions including Riposte journal for events at Post Office outlets and host application logs System logs of activities at Horizon systems such as user logon and administration and other security relevant events including system, network and firewall management. Logs at relevant Post Office Account internal systems. Archives of these at the archive server retrieved from	Most except Post Office outlets

		archive media there.	
		Manual records associated with IT access.	
		Many events are collected centrally using Tivoli (via Patrol and Openview where needed). The technician monitoring the systems management workstation will alert the Security Event Auditor of specified types of significant events. However, some event records will remain in local audit logs.	
Post Office Ltd. Auditor	Auditing operation of a Post Office	Authorised Riposte functions after authentication using one shot password	Post Office outlets only
Post Office Ltd. Emergency Manager; Post Office Ltd. Investigator	Taking the role of an Emergency Manager who may take over from the manager after suspected fraud or when a Post Office is closed down or transferred to a different manager.	Post Office start up functions Authorised Riposte functions after authentication using one shot passwords	Post Office outlets only
External Auditor	A Post Office Ltd. or NAO Auditor auditing the operation of Post Office Account	External auditors have (indirect) access via Post Office Account Auditors, rather than direct access to the Horizon systems. There are some differences in data available to different External Auditors.	None
OCMS Roles with Data Centre access			
OCMS users (Post Office Account)	Handle calls from Post Office Account suppliers and Post Office outlets forwarded from Horizon system help desk. Queries and limited updates to OCMS depending on call	Query and update access to OCMS.	OCMS

Auto-configuration user (Post Office Account)	OCMS staff managing the data going through the auto-configuration database (ACDB). This includes some update access.	Query access plus update as permitted by ACDB/client	ACDB
ACDB data administrator	Administering the central services site information in the ACDB	Query access plus update as permitted by ACDB/client	ACDB
Installation engineer	Start-up Post Office outlets	Auto-configuration application only	PO links to boot server
System and Operational Management and support			
Operational Management			
Computer Operator	Local operation of the machine such as media handling.	On Solaris, the ability to run pre-defined jobs, such as back-ups. On Microsoft, media handling only, including archive media	
Operational management/ System Administrator (Core Services)	Management of the operating system. On Solaris, any action needed concerned with replication between campuses and local archiving. Job scheduling (Solaris & Microsoft) using Maestro workstation. Code updates when required quickly (prior to update via configuration management) and authorised	Access to required operating system functions. On Solaris, this can allow use of ROOT, UNIX commands and Oracle dba functions under controlled conditions (see 5.3) Operational monitoring/management using Patrol workstations.	All Solaris; all Microsoft (except PO); all Solaris
Security Management (Core Services)	Administering UNIX/Microsoft user information, including group membership for all users; also, on	User administration and related functions	All Solaris; Microsoft (not

	Solaris, in secure menu system. Administering Oracle database administrator users and associated roles and privileges. Security monitoring		PO); Solaris
Secure menu administrator (Solaris only)	Configuration of the secure menu system, including addition of new functions	Pre-defined agreed functions	Solaris
System Monitoring (Solaris only)	Monitoring the operational system.	Patrol via an appropriate workstation	Solaris
Engineer	Hardware diagnostics and repair	Access to diagnostics and, if needed, data on suspect hardware	All systems except PO
Base Installation and configuration	Initial installation and configuration the base system - Solaris and Oracle databases. Later updates to these.	As job function for Data Centre systems and Post Office Account managed systems, except POs where there is a special installation engineer	
Dynix 3rd line support	Operational management of Solaris by UNIX staff when Core Services cannot cure problem.	UNIX, which can include ROOT access under controlled conditions	Solaris
Database monitor	Monitoring Oracle databases	Read only access; on Oracle, use of SQL*Plus, svrmgr	Solaris
Operational	Oracle database administrator for database	Dba functions for specified applications	Solaris

management/ Database administrator	structure - setting up views, space allocation etc.	(CORE_SERVICES_DBA role)	
Oracle database 3rd line support	Operational management of Oracle on Solaris when Core Services cannot cure problem.	Read only access; Oracle dba and limited UNIX functions	Solaris
Archive Administration	Managing the audit archives	Audit archives via archive client	Archive server
System Management – SMC roles			
System Management Centre	*Unit functions* System management activities are: planned system management actions, for example, the distribution of software or the implementation of new Post Office outlets. monitoring the system and taking action when this is needed. resolving technical problems passed on by the Horizon System Help Desk They also handle PO Key Recovery.		
SMC/HSH technician or technical specialist	Monitoring the system - software distribution, the auto-configuration process and other system	Tivoli/Oracle facilities for authorised functions. (No Microsoft/UNIX tools)	Tivoli servers via Tivoli client

FUJITSU

FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003

Version: 7.0

Date: **14/04/2005**

	management events. For software distribution, select targets for distribution from those authorised and report on progress. Run pre-defined, pre-allocated tasks. Raise alarms on pre-defined conditions	Pre-defined Tivoli tasks can be used for a variety of system management tasks including Riposte administration at the Correspondence servers.	
SMC/HSH technical team leader	For software distribution, authorise targets for distribution, change priorities or cancel distribution and report on progress. Other system management tasks as SMC technician. Authenticating users at the Post Office using one-shot passwords. Assisting in Post Office Key Recovery.	Tivoli/Oracle facilities for authorised functions. (No Microsoft/UNIX tools) For one-time password authentication, special security system with access to special application only For PO Key Recovery, application at KMS	Tivoli servers via Tivoli client; (KMA for PO recovery)
SMC MSS technical support	Handle receipt of software and auto-configuration information. Configure Tivoli event management – configure the view of events by others and task event relationships and add new Sentry monitors. Create Tivoli tasks and allocate to SMC technicians.	Tivoli/Oracle facilities for authorised functions. Authorised Microsoft/UNIX tools	Tivoli servers via Tivoli client

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

	System administration of the SMC workstations and Tivoli servers (Microsoft and UNIX systems) including backup/recovery. Access to the ISDN files on the boot server in order to provide live support		
SMC Security Manager	User administration – adding SMC and other users to the SMC domain and to Tivoli. Allocating users' rights e.g. roles, groups.	Tivoli and OS user and role administration	Tivoli servers via Tivoli client
	Software Distribution		
Software Distributor	Initiates transfer of software to the depot/ Tivoli at the Data Centre for distribution to the operational system after authorisation by CS Release Manager.	Functions at signing server to initiate transfer	Signing Server at Post Office Account project site
	Network Management		
Network Technician (Core Services)	Monitoring the network	Specified Open View and Cisco Works/CiscoView functions and the NMS only. (No direct UNIX access)	NMS
Network Manager (Core Services)	Monitoring the network. Updating router configuration information e.g. Post Office information e.g. Fujitsu Services Core Services address	Open View and Cisco Works network management functions, but no direct UNIX access at the NMS	NMS

	Horizon Access Control Policy **Commercial In Confidence**	**Ref:** RS/POL/003 **Version:** 7.0 **Date:** 14/04/2005

	Access Lists of permitted addresses, protocols, and ports. Updating information about routers available when needed (including confirming bringing a mended one back on line – see below)		
Network Management Configurer (Core Services)	Configuring NMS including Open View e.g. what to display to whom actions to be taken on certain events Configuring Tivoli Event Adapter	Open View configurer functions only (no UNIX access)	NMS
Network Security Manager (Core Services)	Maintain user information for those users permitted to use this system – both UNIX users and Open View users. Local auditing of network management activities at this system	User administration functions	NMS
Cisco support	nth line support of routers	Telnet access to routers	Routers
Firewall Management			
Firewall Manager	Maintains the firewall configuration and policy data	Defined as Microsoft & Enterprise centre user; Authenticated with token to Microsoft workstation, and	Checkpoint FW-1 via Enterprise

		authenticated to the Enterprise Centre application.	Manager on Solaris system Cisco PIX & FWSM via Cisco XXX
Firewall Monitor	Read access to alerts, logs and the rule base	as above	as above

Technical Help Desk and Application and other Support			
Horizon Systems Help Desk	Receiving technical queries from all IT users of Post Office Account (internal and external) and answering queries on these calls. Answering some technical queries and forwarding other calls on to the appropriate 2nd line support unit. Note, this includes forwarding calls on PO key and password recovery to SMC.	These users have no access to the main Data Centre and other operational systems. They have access to supporting services such as Powerhelp for call handling and special versions of Post Office Account (Post Office) applications (without real data etc) to assist answering calls from Post Office staff.	Internal systems only
Application support user	Supporting applications on Solaris - both Oracle applications and Access services.	Read only access to event logs and other relevant files and databases. (This does not include the Post Office counters) Tivoli server access is restricted to pre-authorised tasks to extract diagnostic info for POs Access is managed and supported using SSH client via Terminal Server. (Oracle MONITOR role on Solaris)	Most Microsoft; Solaris; test rigs

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: **RS/POL/003**
Version: **7.0**
Date: **14/04/2005**

Application support manager	Supporting applications as above, plus correcting data when required and authorised under controlled conditions.	As above, plus controlled write access to application data using SSH client via Terminal Server. (Oracle SSC role on Solaris)	as above
Other hardware and system support			
EMC	Handling problems with Symmetrix discs	Access to EMC disc controller (and to discs) using special EMC client	EMC

FUJITSU
FUJITSU SERVICES

Horizon Access Control Policy

Commercial In Confidence

Ref: RS/POL/003
Version: 7.0
Date: 14/04/2005

Notes:

This table does not include the Software distribution related roles at the Configuration Management system, as the CM is not on the secure LANs covered by the ACP. These Roles are:

- CS Release Manager (authorising software (new software and fixes), configuration information etc. for release (after testing at the test rigs).

- Configuration librarians (maintaining the library of software at the Configuration Management system and initiating signing and distribution of software after authorisation).

- The Key Handler role needs to be performed on-site whenever systems are rebooted, so is generally performed by the organisation at that site e.g. Post Office Ltd. at their Outlets.

- There are associated manual processes to authorise some of the actions above and to liase with other Post Office Account units involved in software distribution and auto-configuration. For example:

- Team Leaders and SMC Managers can authorise software distribution.

- Only SMC Managers can authorise creation of new Tivoli tasks.

All changes distributed via Tivoli first go through the standard Configuration Management system with its associated processes for change control, testing and authorising release.