POL00033119

Document Title: HNG-X Solution Architecture Outline

Document Type: Architecture

Release: N/A

Abstract: This document describes the target Solution Architecture for Project HNG-X. The document encompasses the Application as well as the Infrastructure components of the solution. Service-Oriented Architecture principles provide the overall framework for the solution.

Document Status: APPROVED

This document contains text (as listed in section 0.5) that has been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review.

This text must not be changed without authority from the FS Acceptance Manager.

Author & Dept: Author: Pete Jobson

Contributors: Dave Johns, Chris Baker, Roger Barnes, Ian Bowen, Pat Carroll, Dave Chapman, Jason Clark, Nial Finnegan, Alan Holmes, Mark Jarosz, Gareth, Jenkins, David Johns, Duncan Macdonald, Giacomo Piccinelli, Alex Robinson, Brian Ridley, Glenn Stephens, Mario Stelzner, Jason Swain, Jim Sweeting, James Stinchcombe, Lee Walton, Andy Williams, Nasser Siddiqi.

Internal Distribution:

External Distribution:

Approval Authorities:

Name	Role	Signature	Date
Amit Apte	CTO	See Dimensions for record	
Geoff Butts	HNG-X Programme Manager		
Ian Trundell	Post Office Design Authority for HNG-X		

Documents are uncontrolled if printed or distributed electronically. Please refer to the Document Library or to Document Management for the current status of a document.

POL00033119

0 Document Control

0.1 Table of Contents

POL00033119

POL00033119

0.2 Figures and Tables

0.3 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	12/06/2006	First formal issue as ARC/SOL/ARC/0001 for formal review. First draft as document reference ARC/SOL/ARC/0001. Replaces all previous informal working drafts. Significant changes in this version from previous documents are: 1.4 Service Oriented Architecture (SOA) 3.2.5 Testing in passive Data Centre 9.0 Training Appendix A – Mapping to BCSF Appendix B: Mapping to Infrastructure documents	
0.2	30/06/2006	Updated following review comments. In addition to minor typographical changes, the following changes were made. Throughout document: alignment with contract definitions for Business Capabilities and Support Services. Section 0.7: previous section 0.7 (Accuracy) deleted. Section 1.4: clarification added on wider Post Office architecture. Section 2.1.1: figure 3 updated to show SOA layering, and associated description updated. Section 2.2.2: figure 4 moved forwards, and additional sections added for Branch Presentation Tier and	

POL00033119

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		External Client Tier. Section 2.2.2.3.4: Clarification added Section 3.2.5: Clarification added. Section 4: renamed as Central and Branch Network Services to align with contract definitions. Section 5.6: Clarification added. Section 9.2: Clarification added. Appendix A: cross references added to section 2 figure 4, section 2.1 and sub-contract schedule B3.2 Appendix B: cross references sub-contract schedules B3.3 and B3.4.	
1.0	06/07/06	Issued for Approval. No changes to document content from version 0.2.	
1.1	11/08/2006	Updated following further Post Office comments.	
2.0	16/08/2006	Issued for Approval. No changes to document content from version 1.1.	
2.1	30/10/2006	Section 1 restructured and completed	
2.2	22/11/2006	Draft for review	
2.3	23/01/2007	Updated following review comments.	
3.0	12/03/2007	Issued for approval.	
3.1	29/02/2008	This document has been revised by RMGA Document Management on behalf of the Acceptance Manager to contain notes which have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. This text must not be changed without authority from the FS Acceptance Manager. This version will not require full review using the RMGA Document Control Process, as agreed between Acceptance Manager and Programme Management.	N/A
4.0	19-Jun-2009	Moved back to Approved status following changes described at version 3.1 above which are deemed not to need re-approval. No content changed.	
4.1	04/03/2010	Updated to reflect the solution design that has been implemented for HNG-X at Release 1, including approved CPs that impact on the overall architecture: • CP4305 (CCN1202) Application for PCI • HNG-X CP0010 (4364) Introduction of MoneyGram to HNG-X • HNG-X CP0022 (4405) Migration of PHU1.5 Portable Counter to HNG-X • HNG-X CP0031 (4430) Migration of Telecoms Service to HNG – X • HNG-X CP0065 - Batch 3 - Kahala - Guaranteed Delivery Dates • HNG-X CP0077 (CP4523) Definition of Branch Router Migration Strategy • HNG-X CP0098 (CP4549) Retention of Utimaco VPN	CP4305 CP0010 CP0022 CP0031 CP0065 CP0077 CP0098 CP0136 CP0140 CP0172 CP0304 CP0330 CP0342

POL00033119

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		• HNG-X CP0136 (4596) Removal of Interstage from BAL • HNG-X CP0140/CP0172 - Branch Router Wireless WAN Using Dual Service Provider • HNG-X CP0304 Extension of Branch Router Solution to include VSAT branches (Fixed and Luggable) • HNG-X CP0330 Consequences of NT Retention • HNG-X CP0342 Deferral of Auto-Fault Logging from HNG-X Release 1. Clarification added that the initial release of the HNG-X Counter will operate under Windows NT. Whilst CP 0330 (Consequences of NT Retention) is not yet approved, the change to the target operating system for the counter will not now take place at Release 1 of HNG-X, and are deferred until a subsequent release. Consequently there is no requirement to upgrade Back Office Printer to be network connected in large branches. References added for ARC/SOL/ARC/ -0005 (HNG X Architecture - Counter Training Offices) and ARC.NET/ARC/0003 (Branch Router Architecture) Help data is now delivered to the counter as part of reference data. The Online Help service has been removed from the Branch Access Layer. Addition of section 0.5 containing the Acceptance by Document Review Table.	
4.2	2nd Aug 2010	Updated following comments	N/A
5.0	2nd Aug 2010	Issued For Approval	N/A

POL00033119

0.4 Review Details

Review Comments by :	19/03/2010
Review Comments to :	pete.j GRO & RMGADocumentManageme GRO
Mandatory Review	
Role	**Name**
Post Office Design Authority for HNG-X	Ian Trundell
Solution Design	Steve Evans **Counter, BAL/OSR** Mukesh Mehta **Estate Management** Jerry Acton **Systems Management** Karen Morley **Counter Infr. and Packaging** Adam Spurgeon **Host Dev Management** Andy Beardmore **Host Online Systems** Roger Barnes **Host Batch Systems** Duncan MacDonald **Host Reference Data** Andy Williams **Agent and Web Services** Sarah Selwyn **Cryptography** Mark Wright **Scheduling** Gary Maxwell **File transfer** Mike Croshaw **Time Sync** **Alan Holmes Audit**
Infrastructure Design	Pat Lywood (or nominees)
Head of Service Introduction	Role Unfilled
Security Architect	Stephen Cottrell
Information Governance	Bill Membery
Capacity and Performance Specialist	Dave Chapman
Optional Review	
Role	**Name**
Security & Risk Team	CSPOA.Security GRO
Test Design	George Zolkiewka
Service Network	Ian Mills
Head of Service Operations	Tony Atkinson
LST	John Rogers
LST Manager	Sheila Bamber
POL Test Manager	James Brett (POL / JTT)
SV&I Manager	Chris Maving
VI & TE Manager	Mark Ascott
Service Director	Gaetan van Achte
SSC	Steve Parker
Business Continuity	Adam Parker
HNG-X Service Change and Transition	Graham Welsh
Data Centre Migration	Vince Cochrane
Integration Team Manager	Vijesh Pandya
Programme Manager	Geoff Butts
Integrity Testing	Michael Welch
Operational Security	Donna Munro
Core Division	Ed Ashford
Core Division	Andrew Gibson
Applications Engineering Manager	Graham Allen
Test Manager	Debbie Richardson
HNG-X Architect (Branch Database)	Andy Beardmore
HNG-X Architect (Business Applications),	Gareth Jenkins
HNG-X Architect (Counter / BAL)	Andy Thomas
HNG-X Architect (Estate Management)	Patrick Carroll
HNG-X Architect (Network)	Mark Jarosz
HNG-X Architect (Online)	Andy Williams*
HNG-X Architect (Platforms and Storage)	Jason Clark
HNG-X Architect (Reference Data)	Duncan MacDonald
HNG-X Architect (Support Services)	Alan Holmes
HNG-X Architect (System and Estate Management)	Ian Bowen
Issued for Information – Please restrict this distribution list to a	

POL00033119

minimum	
Position/Role	**Name**
Acceptance Manager	David Cooke

Note: See RMGA HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

(*) = Reviewers that returned comments

0.5 Acceptance by Document Review

The sections in this document that have been identified to POL as comprising evidence to support Acceptance by Document review (DR) are listed below for the relevant Requirements:

POL NFR DR Acceptance Ref	Internal FS POL NFR Reference	Document Section Number	Document Section Heading
ARC-402	ARC-402	1.4	Layered Architecture
ARC-400	ARC-400	2.1.2	Counter Applications: Solution
ARC-400	ARC-400	2.2.2	Data Centre Applications and Services: Solution

0.6 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	1.0	13/6/06	Fujitsu Services RMGA HNG-X Document Template	Dimensions
			Sub schedules B3.2, B3.3, B3.4 and B6.2.	HNG-X contract
ARC/APP/ARC/0001			HNG-X Reference Data Architecture	Dimensions
ARC/APP/ARC/0002			HNG-X Integration Architecture	Dimensions
ARC/APP/ARC/0003			HNG-X Counter Architecture	Dimensions
ARC/APP/ARC/0004			HNG-X Branch Access Layer Architecture	Dimensions
ARC/APP/ARC/0005			HNG-X Online Services Architecture	Dimensions
ARC/APP/ARC/0007			HNG-X Batch Application Architecture	Dimensions
ARC/APP/ARC/0008			HNG-X Branch Database Architecture	Dimensions
ARC/APP/ARC/0009			HNG-X Counter Business Applications Architecture	Dimensions
ARC/NET/ARC/0001			HNG-X Network Architecture	Dimensions
ARC/NET/ARC/0003			HNG-X Branch Router Architecture	Dimensions
ARC/PER/ARC/0001			HNG-X System Qualities Architecture	Dimensions
ARC/PPS/ARC/0001			HNG-X Platform and Storage Architecture	Dimensions
ARC/SEC/ARC/0003			HNG-X Security Architecture	Dimensions
ARC/SOL/ARC/0005			HNG-X Architecture	

POL00033119

Reference	Version	Date	Title	Source
			- Counter Training Offices Dimensions	
ARC/SOL/ARC/0006			HNG-X Architecture - Global Users	Dimensions
ARC/SVS/ARC/0001			HNG-X Support Services Architecture	Dimensions
ARC/SYM/ARC/0001			HNG-X System and Estate Management Architecture	Dimensions
PA/PER/033			Horizon Capacity Management and Business Volumes	Dimensions
DES/SEC/HLD/0002			HNG-X Crypto Services HLD	Dimensions
SVM/SEC/POL/0003			RMGA Information Security Policy	Dimensions
DEV/GEN/SPE/0007			Platform Hardware Instance List	Dimensions

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

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

0.7 Abbreviations/Definitions

Note that some of the Abbreviations below are also defined in Schedule 1 (Definitions). Where abbreviations in this CCD are also defined in Schedule 1, the definition from Schedule 1 has been used, though in some cases it has been clarified further for the purposes of this CCD.

Abbreviation	Definition
ACD	Active Directory Domain Controller
ADSL	Asynchronous Digital Subscriber Line. A new network method of connecting Post Office Ltd. Branches to the data centres.
AP-ADC	Automated Payment – Advanced Data Capture
API	Application programming interface
APOP	Automated Payment Out-pay
APS	Automated Payments Service
Branch	A post office or any other location where Post Office (whether directly or by means of Agents) transacts business with Customers Within the HNG model, a Branch is a logical entity that can be composed of several physical locations at which business is transacted. Each branch is identified by a unique Branch Code
Budman	Budman and Cashman are two MS Access based systems used in Cash Centres
Bureau	Bureau de Change The Application referred to in paragraph 4.3 of Schedule 18 and "Bureau Application" shall be construed accordingly
Business Capabilities and Support Facilities	The business capabilities and support functions that are described in Sub-schedule B3.2 The facilities provided to Post Office to allow the trading of products in the Branches

POL00033119

Abbreviation	Definition
	and deliver data to 3rd parties.
CA	Certification Authority
Cardholder Data	Data extracted or derived from a Payment Card that relates to the holder of the card
Cashman	Budman and Cashman are two MS Access based systems used in Cash Centres
CLI	Calling Line Identity. Service that allows a customer to see the number of the caller before answering the call.
CMS	CMS is the Royal Mail Customer Management System – Siebel-based. POLSAP enables Post Office to come out of CMS by carrying out the equivalent functionality within SAP
CSM	Content Switch Module. A network device that allows incoming requests for service to be load balanced across a number of platforms.
CTO	Counter Training Office
DCS	Debit Card System
DMZ	De-Militarized Zone. Physical or logical sub-network that contains and exposes an organization's external services to a larger un-trusted network
DNS	Domain Name System
DR	Disaster Recovery
DRS	Data Reconciliation Service - A new service introduced as part of network banking. Its main component is a new database running on the host.
DVLA	Driver and Vehicle Licensing Agency
DWDM	Dense wavelength division multiplexing, or DWDM for short, refers to optical signals multiplexed within the 1550 nm band
DWH	Data Warehouse
EDG	External Data Gateway
EDGE	EDGE is a new modulation scheme that is more bandwidth efficient than the Gaussian pre-filtered minimum shift keying (GMSK) modulation scheme used in the GSM standard. It provides a promising migration strategy for GPRS.
EFTPoS	Electronic Funds Transfer at Point of Sale: a term used to describe the debiting of Customers' accounts, usually through EPOS systems, for goods or services they purchase. The application delivering EFTPOS functionality under this Agreement is the Debit Card Application, which is referred to as DCS.
EMC	Company that provides fast an resilient disk storage configurations
e-pay	Company that interfaces to the mobile phone companies for ETU. The third party, providing services to or for the benefit of Post Office, that facilitates the handling and authorisation of ETU messages (including, without limitation, ETU Requests and ETU Authorisations).
ETU	E-Top-Ups. Ability to credit money to a mobile phone account. As applicable in accordance with this Agreement, the Application referred to in paragraph 4.2 of Schedule ~~18~~B4.2 and/or the Electronic Top-Up Business Capability, and "ETU Application" shall be construed accordingly.
FS	Fujitsu Services

POL00033119

Abbreviation	Definition
GPRS	The General Packet Radio Service is a new non-voice value added service that allows information to be sent and received across a mobile telephone network.
GPS	Global Positioning System – used as a source of Greenwich Mean Time
GSM	Global System for Mobile Communications
HDD	Hard Disc Drive
HR SAP	External SAP system (See SAP below) that aggregates transaction value and volume for the purposes of postmaster remuneration.
(Baseline) Horizon	The existing solution being re-architected
HNG	Horizon Next Generation replacing current Baseline Horizon solution
HNG-X	Horizon Next Generation – Plan X
HSM	Hardware Security Module, an appliance used for certain cryptographic services.
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISDN	ISDN, which stands for Integrated Services Digital Network, is a system of digital phone connections which has been available for over a decade
KEL	Known Errors Log
LFS	Logistics Feeder Service: the Horizon Application referred to at paragraph 2.4 of Sub-schedule B4.2
MID	Merchant Identifier issued by Streamline Merchant Services to identify the Branch from which a transaction originated
MIS	Management information system
MPLS	Multiprotocol Label Switching (MPLS) is a mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next
MSF	The Time from NPL- a radio signal broadcast from the Anthorn VLF transmitter near Anthorn, Cumbria which serves as the United Kingdom's national time reference – also know as MSF
MSI	MicroSoft Installer
NBS	Network Banking Service: The Horizon Application referred to at paragraph 2.6 of Sub-schedule B4.2
NPS	Network Persistent Store
NTP	Network Time Protocol. A protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks
OBC	Operational Business Change
OMDB	Operational Management Database.
Operational Services	Those services that are needed to run the Horizon system that are not directly supporting the Post Office business. Examples include software distribution, audit, security management etc. The services referred to in Table A of Sub-schedule B3.1
PAF	Postal Address File. A service to allow post codes and addresses to be looked up (the PAF Database).

POL00033119

Abbreviation	Definition
PAN	Primary Account Number
PAN Manager	Processor Area Network manager used to manage configuration and virtualisation of blades/resources within a bladeframe
PCI	Payment Card Industry. A set of security controls defined by the Payment Card Industry organisation.
PCI-CE Domain	A security domain in Tier 3 of the security architecture that adheres to the demands of PCI standards
PDF	Package Definition File
PO	Post Office
POL FS	SAP based system providing financial accounting for the Branch based business. This is the production system. There are other SAP systems in the Data Centre to support development and test.
POL MIS	Otherwise known as POL MI. This is the Post Office Management Information system.
Pseudo Counter	A platform loaded with the counter automation application that is located at the Data Centre to support test transactions
PSTN	The public switched telephone network
RAC	Real Application Cluster. A multi-node Oracle database
RDDS	Reference Data Distribution System
RDMC	Reference Data Management Centre
RDP	Remote Desktop Protocol, a remote access network protocol developed by Microsoft.
RDS	Post Office Reference Data System
RDT	Reference Data Team - the Post Office and Fujitsu Customer Services teams use the RDT environment to validate and verify the Reference Data associated with business changes.
RMG	Royal Mail Group
SAN	Storage area network . An architecture to attach remote computer storage devices to servers in such a way that the devices appear as locally attached to the operating system
SAP	Integrated suite of applications providing financial accounting and other business functions.
SAPADS	SAP Advanced Distribution System: Post Office ' s Advanced Distribution System (based on the SAP package) that interfaces to LFS
SAS	Secure Access Server
SDC01	Fujitsu Location at Grays in Essex
Sensitive Authentication Data	The full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.), Encrypted PIN blocks.
SOA	Service Oriented Architecture
SSN	Secure Service Network. Part of the network that is behind a firewall/IPS

Post Office

POL00033119

Abbreviation	Definition
Stratum	A measure of each level in a hierarchy of time sources
Streamline	Merchant Acquirer for DCS.
Strong Authentication	The process in which the identities of networked users, clients and servers are verified without transmitting passwords over the network
SU	Stock Unit
SYSMAN	The systems management environment.
TCY02	Fujitsu Location at the Isle of Dogs
TES	Transaction Enquiry Service
TACACS+	Terminal Access Controller Access-Control System Plus is a Cisco proprietary protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services. Used for Branch Router access from the data centre
TESQA	Transaction Enquiry Service Query Application
TID	Terminal Identifier issued by Streamline Merchant Services to identify the terminal from which a transaction originated
TNS	Transparent Network Substrate
TPS	Transaction Processing System
Two Factor Authentication	Two-factor authentication means using any independent two authentication methods
Type A Reference Data	Type A Reference Data is reference data that is received on the automated feed from POL RDS. All other types (non-type A reference data) is received via non-automated feeds or declared locally within the HNG-X solution (meta data)
VPN	Virtual Private Network
VSAT	A Very Small Aperture Terminal is a two-way satellite ground station
XML	Extensible Markup Language

0.8 Changes Expected

Changes
Subsequent to the baseline, the document could be updated to remove terms such as legacy systems and updated Horizon systems, so that it described the target HNG-X solution “as is”.
Any changes to the counter operating system (and potentially the hardware used) will be subject to a separate Change Proposal and are beyond the scope of this document which covers the initial HNG-X release.
The IDS / IPS solution is currently being reviewed and this document will be updated if needed when a revised strategy is agreed.
Changes may be introduced as part of Release 2 and subsequent development of the solution.

POL00033119

0.9 Copyright

POL00033119

1 Introduction

This document outlines the solution architecture delivered by Project HNG-X. It covers applications and infrastructure.

1.1 Scope

This document describes the solution architecture for the HNG-X applications. It includes:

- Applications that provide Business Capabilities
- Applications that provide Support Facilities
- The solution architecture for the HNG-X infrastructure.

Appendix A shows how the components described in this document align to Business Capabilities and Support Facilities.

This document covers topics that go across both applications and infrastructure: Systems and Estate Management; Availability; Performance and Scalability; Security; and Training.

The document does not include:

- Operational Services
- Development, testing, migration, or any other aspect of solution delivery.
- Business Impact Analysis or risk associated with any architecture or design of the system

This document is a contract controlled document. Any changes to components or component usage explicitly described in this document (or other documents and artefacts of the Solution Baseline Documentation Set which have been agreed as requiring PO approval) must be jointly approved.

1.2 Background

Post Office Ltd operates in both the retail and financial services industries. The Post Office's main channel to market is a network of approximately 14,000 branches, which serve up to 28 million customers a week. Post Office has also been expanding the use of the Internet and Call Centres as part of a comprehensive multi-channel strategy.

Post Office branches are supported by a set of IT systems known as "Horizon".

The objective of the HNG-X programme is to substantially reduce support and maintenance costs by developing a replacement for Horizon.

HNG-X is a straight replacement for Horizon. It does not aim to provide additional business capabilities. However, it may include a limited number of extra features that are important to the Post Office and can be easily incorporated into the systems.

1.3 Solution Outline

Horizon is expensive because it stores customer transaction data at the Counter. This data has to be kept secure, and securing it makes the Counter application complicated. It can also cause performance problems, and makes maintenance procedures more complicated and expensive.

HNG-X will store customer transaction data in the Data Centre. The data will be stored in a new Branch Database, and accessed through new Branch Access Layer systems. The HNG-X Counter system will

POL00033119

only store operational data, such as reference data. This will make it easier and cheaper to keep the data secure.

The HNG-X Counter system will be based on Java technology. It will use the current Counter hardware. The Counter operating system will initially be deployed under Windows NT, and may subsequently be upgraded to a more recent / supportable operating system such as Linux or Windows XP[1]. The Counter will communicate with the Data Centre using encrypted messages for business transactions although the Virtual Private Network (VPN) originally used in Horizon will be retained whilst the counter remains on Windows NT.

The branch Network will use a combination of low-cost ADSL, ISDN, VSAT and mobile communications. Routers will be installed in all Branches before the new HNG-X systems are implemented.

New Data Centre applications will be based on Java, the Interstage application server and Oracle database. The existing Horizon Data Centre systems will be retained, and modified to work with the new systems.

The infrastructure and systems within the HNG-X Data Centre will be highly resilient. There will be a stand-by Data Centre for disaster recovery, which will be a copy of the live Data Centre. Data replication technology will keep a mirror of the live data at the stand-by Data Centre, to guarantee that no data is lost if there is a catastrophic site failure.

The Solution will be developed using the following principles:

- The solution will be designed to address the ongoing operational costs of providing the service.
- Where appropriate, it will utilise existing solution building blocks.
- It will use packaged applications and standard components unless suitable products are not available
- The Solution will not customise a packaged application other than via configuration capabilities supported by the vendor, unless agreed by PO Ltd.
- Where applicable, the solution will utilise IT industry standard components, industry standards and widely used technologies, unless agreed otherwise with PO Ltd
- Internal HNG interfaces shall exploit, wherever possible, established or emerging standards where these are appropriate, stable and are (or are likely) to be adopted widely by the IT industry.
- For the new development parts of the solution, the architecture will be designed to simplify application development, service management and maintenance.
- Where technically feasible, and it does not introduce additional cost, components will be designed for reuse.
- For the new development parts of the solution, the architecture will be designed using Service Oriented Architecture principles.
- From a compliance perspective, e.g. DVLA and passports etc it also operates in a government environment

[1] Whilst HNG-X CP0330 (Consequences of NT Retention) is not yet at an approved state, the initial version of the HNG-X counter at Release 1 will only operate under Windows NT.

POL00033119

1.4 Layered Architecture[2]

The HNG-X solution adopts Service Oriented Architecture (SOA) principles. (SOA) is an approach to designing, implementing, and deploying information systems so that components, called "Services" can be distributed across a network. Applications are created from a composition of these services and importantly, the services can be shared among many applications.

The HNG-X solution can be thought of as a series of layers.

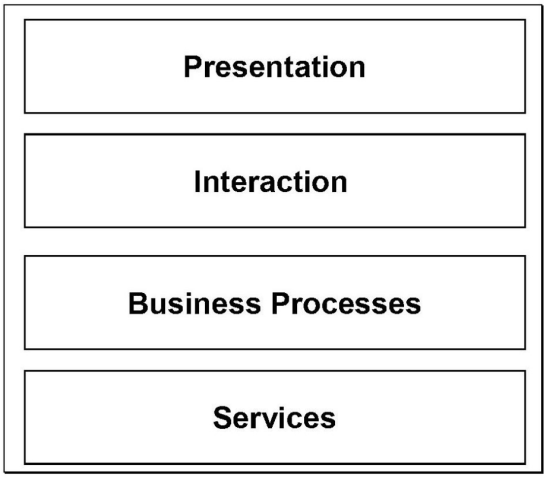


Figure 1 – Layered View of the Application Architecture

The **Services** layer is made up of services that carry out business functions:

- Storage and processing of transaction data (Branch Data and Reports)
- Product and operational data storage and distribution (e.g. Reference Data, Bureau)
- Business reporting (e.g. POL-MIS, POL-FS, POL-HR, FRTS, DRS, TES)
- Interfaces into Clients (e.g. Enquiry and Data Delivery)
- Interfaces into service providers (e.g. Authorisation and Reconciliation, LFS)
- Interfaces for Post Office central support staff (e.g. Enquiry and Administration)
- Internal Services (e.g. PAF, APOP, Message Broadcast, Audit)
- Branch Services (e.g. Stock Unit Mgt, User Mgt, Help Desk)

The services are combined into **Business Processes**:

- Customer Interaction / Sale of Products and Services (e.g. Stock, Mails, Bureau, Banking, AP-ADC)
- Branch Back-office Processes (e.g. for End of Day, Pouch Collection and Delivery, Mails Despatch, Transaction Correction, Balancing)
- Central Batch Processes (e.g. Data Aggregation and Distribution, Reconciliation, Reporting, Reference Data Mgt)

[2] This section comprises text that has been identified to POL as evidence to support Acceptance by Document review (DR) for Requirement ARC-402.

POL00033119

The business processes **Interact** with people:

- Counter/Branch Staff: Data Capture Sequences, Receipts and Reports, Basket Management, Peripheral I/O (e.g. scales, PIN pads, barcode readers)
- Post Office Central Staff: Enquiries and Administration
- Service Desk Staff: Alerts, Incident Management and Reporting
- Operational Support Staff: Diagnostics, Configuration and System Management

The interactions are supported by a **Presentation** layer:

- Counter/Branch Staff: Counter GUI comprising
  - Modern graphical screen representation
  - Touch Screen and keyboard input
  - Menus, Pick lists, Data capture forms, messages and prompts, etc.
  - Reference Data driven transaction sequences
  - Context Sensitive Help

This layered architecture supports two reuse patterns.

- Some services, such as PAF, are simple "atomic" services. The process layer makes a single call to the service and processes the results.
- Other services require more interaction with the process layer. The process makes a series of service calls to achieve a meaningful business result. Both the process layer and the service layer keep track of where they are within the process.

The underlying services could be reused in other parts of Post Office's multi-channel architecture.

1.5 Document set

Section 2 describes the business applications within HNG-X. It covers the application that runs on the Counter, and the applications and services that run in the Data Centre.

Other architecture documents cover these business applications in more detail.

- *HNG-X Counter Business Applications Architecture* (ARC/APP/ARC/0009) covers the business applications on the Counter. *HNG-X Counter Architecture* (ARC/APP/ARC/0003) covers the overall counter architecture.
- *HNG-X Branch Database Architecture* (ARC/APP/ARC/0008) covers the new central database which holds branch data.
- *HNG-X Branch Access Layer Architecture* (ARC/APP/ARC/0004) covers the new application server layer that provides access to the Branch Database and to other online services.
- *HNG-X Online Services Architecture* (ARC/APP/ARC/0005) covers the online services that are accessed through the Branch Access Layer.
- *HNG-X Batch Application Architecture* (ARC/APP/ARC/0007) covers the batch systems that provide bulk transaction processing and reporting.
- *HNG-X Reference Data Architecture* (ARC/APP/ARC/0001) covers systems that create and distribute reference data to the branches and to data centre systems.
- *HNG-X Support Services Architecture* (ARC/SVS/ARC/0001) covers supporting systems such as audit and file transfer.

POL00033119

- *HNG-X Integration Architecture* (ARC/APP/ARC/0002) gives an overview of the composition of and interfaces between all the business applications.

Section 3 describes the computer platforms and data storage infrastructure within the HNG-X counter and data centre. Detail for the counter is given in *HNG-X Counter Architecture* (ARC/APP/ARC/0003), and for the data centre in *HNG-X Platform and Storage Architecture* (ARC/PPS/ARC/0001).

Section 4 describes the networks that support HNG-X. It covers the networks within the branch, the wide area network that connects the branches, the networks within and between data centres, networks to Post Office and external organisations, and support and tests networks. More detail is given in *HNG-X Network Architecture* (ARC/NET/ARC/0001) and HNG-X Branch Router Architecture (ARC/NET/ARC/0003) .

Section 5 describes the systems required to operate, manage and monitor the HNG-X solution within the data centre and across the branch estate. More details are given in *HNG-X System and Estate Management Architecture* (ARC/SYM/ARC/0001).

Section 6 describes how HNG-X will achieve the required levels of availability, including disaster recovery. This is covered in more detail in *HNG-X System Qualities Architecture* (ARC/PER/ARC/0001).

Section 7 describes how HNG-X will cope with required volumes of data, how it can perform and scale. This is covered in more detail in *HNG-X System Qualities Architecture* (ARC/PER/ARC/0001).

Section 8 describes how HNG-X will be made secure. This is covered in more detail in *HNG-X Security Architecture* (ARC/SEC/ARC/0003).

Section 9 describes how training facilities will be made available within HNG-X. More detail is given in *HNG-X Architecture Counter Training Offices* (ARC/NET/SOL/0005)

POL00033119

2 Business Applications

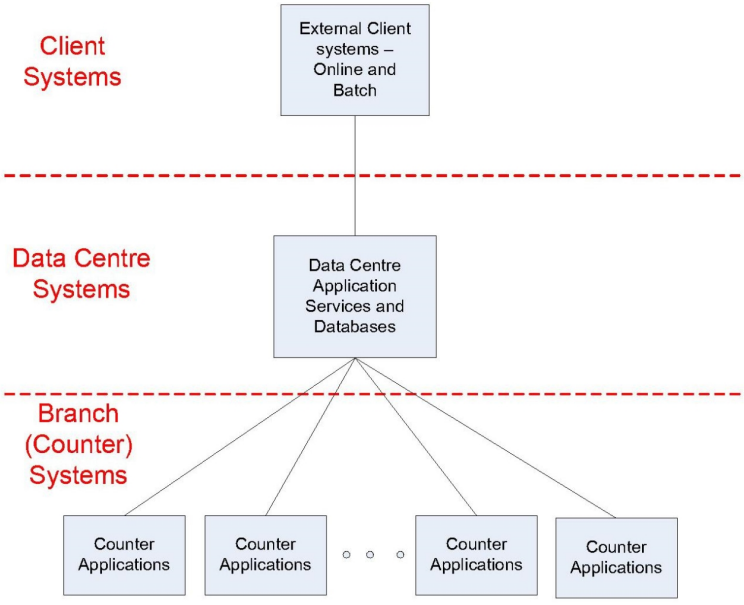


Figure 2 – Overall Application Architecture

2.1 Counter Applications

2.1.1 Assumptions

The main assumptions are that:

1. All transaction data is stored centrally; No network = No Branch trading.

2.1.2 Solution[2]

All Horizon counter business applications are replaced by a single bespoke application that better aligns with the serviceability and cost requirements of HNG-X. In addition to internal analysis, this choice was formally endorsed by an architectural analysis from both Forrester and the Gartner Group.

The technology platform for all the Business Applications on the counter is Java.

[2] This section comprises text that has been identified to POL as evidence to support Acceptance by Document review (DR) for Requirement ARC-400.

POL00033119

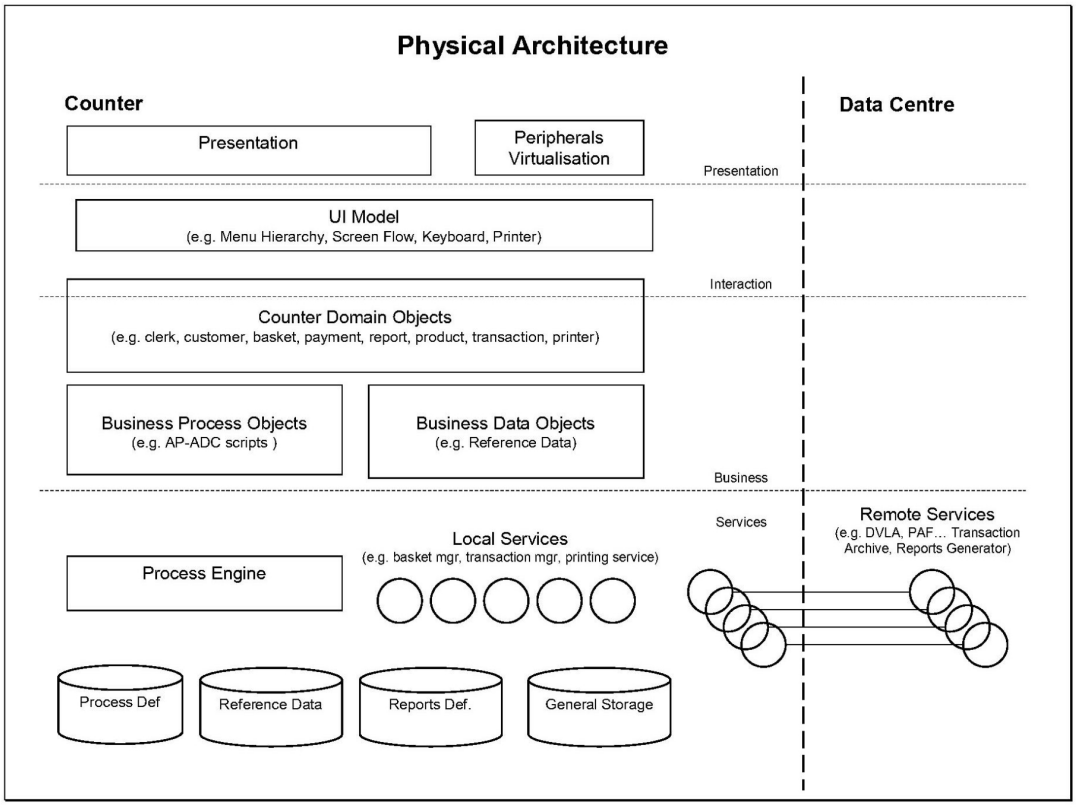


Figure 3 – Counter - Application Architecture

The architecture for the counter application system is based on the Service-Oriented Architecture (SOA) model. Atomic capabilities are encapsulated in self-contained service units. Complex business capabilities are recreated by aggregation and orchestration of atomic capabilities.

The model applies to local as well as remote capabilities.

A 4-layer approach is used for the realisation of the overall Counter system (see Figure 3 – Counter - Application Architecture

).

The Presentation layer:

> This layer comprises the Presentation and Peripheral Virtualisation components. This allows the UI style to be separated from the underlying business logic.

The Interaction Layer

> This layer comprises the UI Model and a limited subset of Counter Domain Objects that support the channelling of Business Capabilities and Support Facilities to the presentation layer.

The Business layer:

> This middle layer comprises the Counter Domain Objects, Business Process Objects and Business Data Objects. All business functionality is handled at this layer. A data driven counter

POL00033119

architecture model will be developed, using presentation and services layers as appropriate. In particular, use of a data driven architecture enables support of an AP-ADC type facility and a new Postal Services capability.

The Services layer:

The lower layer comprises the Process Engine and a set of Local and Remote Services. The process engine is used by the Business layer to support the more complex transactions that are built up as sequence of process steps. Local services are provided for common functions such as report rendering. Remote services provide access to the Data Centre for online transactions, posting of transactions at end of the customer session, user and session management, requests for report data, application help pages, etc.

This layer includes a set of local data retrieval capabilities to support the higher level layers. All transaction data is held centrally, including any recovery data needed for online transactions. The Reference Data is refreshed daily, with different distribution techniques for the common data that is shared across all Branches, and the Branch specific data. Other data, such as Reports definitions are more static, typically only updated when new functionality is provided.

Business applications are realised through process definitions that execute within the process engine. These combine the atomic building blocks provided in the Business and Services layers to provide potentially complex business capabilities. Much of these applications are data driven, based on Post Office controlled Reference Data.

2.1.2.1 Usability

Consistency of User Interface across all business applications is provided through the presentation layer components.

A new Style Guide and Construct Catalogue for HNG-X counter applications will be provided. In addition to the separation of the UI presentation from application logic, the Reference Data will contain detailed definitions of UI components so that as much as is practical of the presentation aspects of the User Interface is separated from the application logic.

2.2 Data Centre Applications and Services

2.2.1 Assumptions

1. Service Level Targets for availability reflect revised agreements

2.2.2 Solution[1]

The Data Centre applications derive from a combination of new and legacy applications (Figure 4). New applications cover mainly back-end functionalities required by the counter applications. Legacy applications cover mainly interfaces to existing client systems.

The Legacy Host database applications (TPS, APS, LFS, DRS and TES) are to remain largely intact. The online interfaces from the counter (i.e. Banking, Streamline and ETU) will be modified to provide a Web Service interface in place of Riposte messaging, together with a simplification of the security mechanisms.

[1] This section comprises text that has been identified to POL as evidence to support Acceptance by Document review (DR) for Requirement ARC-400.

POL00033119

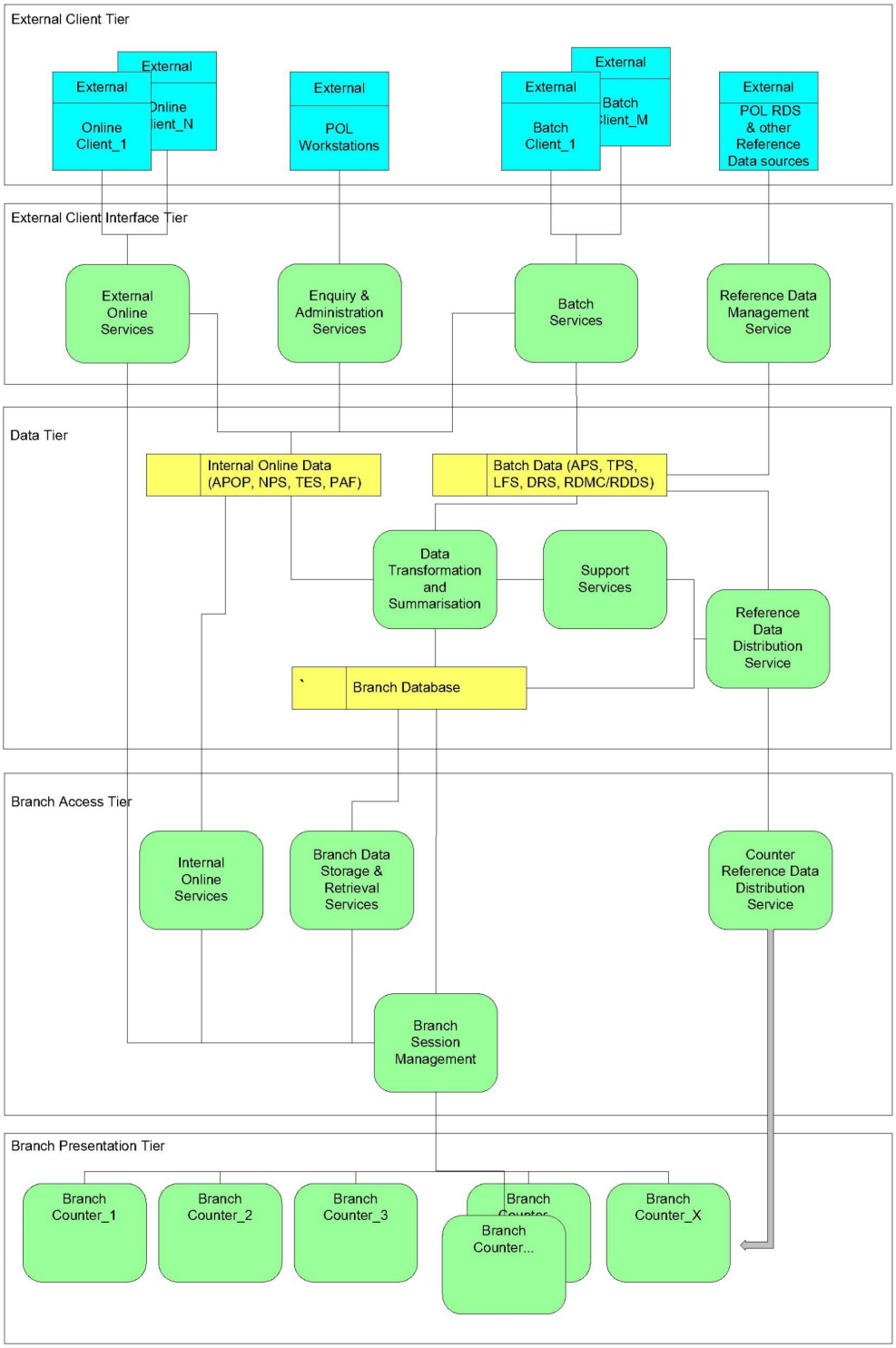


Figure 4 – HNG-X Data Centre Application Architecture

POL00033119

2.2.2.1 Branch Presentation Tier

This tier comprises the Branch Counters. The counter application architecture is described in section 2.1.

2.2.2.2 Branch Access Tier

This tier provides support to Branches for access to the central data storage tier and to the external Clients for online transactions. This tier comprises a number of services that are accessed by the Branch Counters through the Branch Access Layer servers.

2.2.2.2.1 Branch Session Management

This system component is responsible for the initial authentication of users within the Branch estate and also responsible for the authentication of all other business communications between the Branch estate and the Data Centre following the initial authentication.

The Branch User data is held persistently within the Branch database.

The Branch session management application acts as a proxy for other Branch services routing requests to individual services as needed. This layer also provides the main security in separation of CTO transactions from Live transactions (see section 9).

2.2.2.2.2 Branch Data Storage and Retrieval Services

The largest single function performed by the Branch access tier is the capture of transaction and settlement information resulting from completion of customer sessions and other activities within the Branch estate. This XML data needs to be parsed to determine its type and then acted upon. The following list gives an example of the different types of message that may be received:

- Transaction & Settlement data
- LFS Pouch Information
- Declaration data (Stock, Cash, Stamp, Bureau)
- Report Request
- SU and Branch Rollover Information
- Existing Reversal requests
- Transaction Corrections
- Transaction Recovery data
- Messages sent to Branches
- Branch specific Reference Data

The interactions that the Branch Communication application must have with the Branch database for each of these communication types differs significantly as does the volume and nature of the data that needs to be returned in response to the initiating communication. This tier will be designed to provide service isolation between different types of service requests, and in particular be optimised so that settlement transactions are not adversely impacted by other slower running transactions such as reporting.

2.2.2.2.3 Internal Online Services

A number of online Branch transactions are supported within the Data Centre. These are:

- APOP
- PAF

POL00033119

- Training

The PAF and APOP legacy services remain largely unchanged.

The Training service is a new service introduced for HNG-X. It provides a simulation of online services for use in CTO branches where use of the equivalent Live online service is not permitted.

2.2.2.2.4 Counter Reference Data Distribution Service

This service replaces the loader agents that currently distribute Horizon Reference Data via the Correspondence Servers.

The system management capabilities (SYSMAN) will be utilised to distribute the common set of Reference Data to the counter estate. Branch-specific Reference Data will be loaded through the Branch database.

2.2.2.2.5 Horizon Online Service Routing

This Branch Access Layer component provides a routing capability for Horizon PCI Banking and Debit / Credit card transactions, routing the transactions to the appropriate Online Authorisation agent.

This replaces the agents that currently handle these transactions via the Correspondence Servers. This new service is implemented to provide protection for Cardholder data and sensitive authentication data as required by the Payment Card Industry standards.

[This component is not shown in the figure 4, since it is a transient state only whilst the branches are migrating to HNG-X and is not part of the target architecture.]

2.2.2.3 External Client Interface Tier

2.2.2.3.1 External Online Services

There are a number of Client specific "Agents" that provide dedicated interfaces to their respective Clients. The changes being made at this layer for HNG-X are described below.

2.2.2.3.1.1 DCS Authorisation Agents

The Debit and Credit card Authorisation Agent will be replicated and modified to use NPS instead of Riposte for data persistence and audit and to remove digital signature checking on requests and signing on responses. The Authorisation Agent also handle reversals, using status data held within NPS. Note that (as in Horizon) there will be no guaranteed delivery mechanism if it can't send the reversal immediately. Resilience will be provided with similar mechanisms to the banking agents through heartbeats stored within NPS. The Authorisation Agent supports an interface from the BAL that query the operational status.

The DCS Agent will use existing MID/TID data – with appropriate transfer from a revised MID/TID database.

The DCS Agent will use Hardware Security Modules (HSM) to encrypt the PAN and related cardholder data.

The DCS Agent will support transactions that originate from both HNG-X and Horizon counters. The latter will interact with the DCS Agent through the Horizon Online Service Routing component in the Branch Access Layer, rather than Riposte. This eliminates the storage of Track 2 data in the Riposte Message store, and returns the encrypted PAN to the counter.

POL00033119

2.2.2.3.1.2 ETU Authorisation Agents

The ETU agent will be replicated and modified to use NPS instead of Riposte for data persistence and audit and to remove digital signature checking on requests and signing on responses. The Authorisation Agent also handles reversals, using an additional table in NPS for persistence of transaction status, together with a guaranteed delivery mechanism for reversals. Resilience will be provided with similar mechanisms to the banking agents through heartbeats stored within NPS. The Authorisation Agent supports an interface from the BAL that query the operational status.

The ETU Agent will use TID only, with appropriate transfer from a revised MID/TID database.

2.2.2.3.1.3 DVLA Agents

No change is required to these agents other than a technology refresh of the platform. The DVLA agent will be shared between Horizon and HNG.

2.2.2.3.1.4 Banking Application Agents

These Authorisation Agents will be enhanced to have an interface to the Branch Access Layer web servers in addition to their interface supporting the Routing Agents. Messages will be handled in XML format on the new internal interface. Within the Authorisation Agents, the Horizon digital signature capability will be removed, together with any usage of Riposte code once all branches have migrated to HNG-X.

The Routing function will be performed within the Branch Access Layer.

The Banking Agents will use Hardware Security Modules (HSM) for cryptographic functions.

The Banking Agents will support transactions that originate from both HNG-X and Horizon counters. The Banking Agents support Horizon transactions via Riposte and the Routing Agents, Horizon-PCI transactions via the Horizon OSR and HNG-X transactions via the HNG-X OSR. The use of the Online Service Routing component in the Branch Access Layer, rather than Riposte eliminates the storage of Track 2 data in the Riposte Message store, and returns the encrypted PAN to the counter.

2.2.2.3.1.5 *Moneygram, Service Hub and other online services*

Additional online services such as the Moneygram Authorisation service and Service Hub Web Services are being introduced over time onto Horizon and the associated services are carried forward to HNG-X. No change is required to these agents other than a technology refresh of the platform. These agents will be shared between Horizon and HNG-X counters.

2.2.2.3.1.6 *Help Desk*

The Help Desk service enable calls to be logged by branch staff through the counter instead of the telephone. This service has not been implemented at release 1 and is not expected to be implemented in future. Whilst an internal Fujitsu provided service, the external server system is outside the data centre and hence this is classified as an external online service.

2.2.2.3.2 Enquiry and Administration Services

Enquiry and administration capabilities are provided to Post Office Workstations located with Post Office central systems. These include:

- APOP (Enquiry and Administration)
- TES (enquiry only)

POL00033119

There are no functional changes planned to APOP, but there will be a technology refresh of the solution as part of the move to the new Data Centre.

The TESQA service provides a query capability for Banking transaction data. The PAN and associated cardholder data is held in encrypted form in accordance with the PCI requirements to protect Cardholder data. TESQA provides a mechanism to decrypt an individual PAN. Access to TESQA will use SSL.

2.2.2.3.3 Reference Data Management Service

Reference data is provided by Post Office to control the Horizon / HNG-X systems, and this data is held and managed from the database application:

- RDMC Reference Data Management Centre

The baseline assumption of HNG-X is that the Type A Reference Data received on the automated feed from POL RDS will be unchanged. RDMC will be enhanced to allow the new postal services Reference Data to be handled, plus other new forms of non Type A Reference Data. The precise form of any new data Types will be identified during the detailed design stage. The Non Type A data will continue to be delivered via the Fujitsu RDT team who use the RDMC Workstation to load the data, and enable distribution of verified and authorised changes.

In addition to the functional changes for the new Reference Data types, there will be a technology refresh of the solution as part of the move to the new Data Centre.

Help text is implemented by downloading the data to the counters. This is similar to Horizon. The Help data is authored by Post Office, and is loaded by RDT as Reference Data for distribution to counters.

This service incorporates the RDT environment where Reference Data changes are verified prior to being released through to the Live service. New Reference Data proving rigs will be provided to allow proving of Reference Data on the HNG-X system.

2.2.2.3.4 Batch Services

The legacy Horizon database applications primarily provide batch services to external Clients, though some of these also provide a separate online capability. These database applications are as follows:

- APOP Automated Payment Out-pay Database
- APS Automated Payment Service
- DRS Data Reconciliation Service
- DWH Data Warehouse
- LFS Logistics Feeder Service
- TES Transaction Enquiry Service
- TPS Transaction Processing Service

There will be minimal change to legacy applications. APS, LFS, DRS and TPS will incorporate new harvesters / loaders that will extract transactions and deliver data from / to the Branch database rather than the message store.

The DRS and TES applications provide storage for Cardholder data which is held in encrypted form in accordance with the PCI requirements once the Horizon PCI counter changes have been rolled out, and the data retention period for DRS (90 days) and TES (180 days) has elapsed.

The TES service provides storage for “Banking” transaction data in accordance with the PCI requirements to protect Cardholder data. This includes storage of encrypted PAN and associated cardholder data. TESQA provides a mechanism to decrypt an individual PAN.

POL00033119

The TES does not store sensitive authentication data, but will hold clear PANs until Horizon-PCI roll-out and data retention period (180 days) has elapsed. The DRS does not store sensitive authentication data once the Horizon PCI counter changes have been rolled out, and the data retention period for DRS (90 days) has elapsed.

The APOP database is moved to share the Linux platform with NPS,

No other rationalisation is proposed to the Data Centre applications as part of HNG. A phase II rationalisation programme is not deemed to be part of Project HNG-X and must be separately justified at a later stage.

The Data Warehouse will be simplified by replacing the service level measurement for Reference Data delivery to the counter, with a report based on data within the Branch database.

2.2.2.3.4.1 Near Real Time services

A subset of the batch services operate in near real time.

- Track and Trace – provides data on parcels etc received by Branches
- LFS – receives Replenishment Delivery Notices.
- RDMC – receives Spot Rates data for Bureau service

A new T&T client interface will be provided between the Branch database and NPS. The existing Horizon T&T EDG facing Agents will be used for the interface between NPS and EDG.

The legacy LFS processes will be modified to deliver the data into the Branch database instead of Riposte. The Replenishment Delivery Notices will be accessed on demand from the Branch.

The Spot Rates data for Bureau de Change transactions will be delivered by the new HNG-X Branch specific Counter Reference Data Distribution Service.

2.2.2.4 External Client Tier

This tier comprises the batch and online Client systems that interface with the Data Centre systems.

2.2.2.4.1 Online Clients

There are a number of clients providing online services which are directly connected to the data centres, for example: Banks (A&L, CAPO and LINK), Streamline, e-pay, DVLA, and MoneyGram. There are also a number of online clients which are accessed over the Internet, for example: BT, Neopost and PostcodeAnywhere.

2.2.2.4.2 POL Online Workstations

Workstations within Post Office central systems have access to enquiry and administration services for TESQA and APOP respectively.

As part of the changes for PCI, the TESQA displays a hashed version of the PAN rather than displaying the PAN in clear, TESQA provides a mechanism to decrypt an individual PAN, and access to TESQA will use SSL.

2.2.2.4.3 Batch Clients

There are a number of batch clients providing input to, or taking output from the Data Centre systems. These include the batch reconciliation interfaces for online clients; EDG data for Automated Payment Clients, APOP, Track & Trace; SAPADS which provides and receives LFS data; POL FS; and other Post Office systems POL MIS, HR SAP.

POL00033119

2.2.2.4.4 POL RDS and other Reference Data Sources

Reference data is supplied from POL RDS and other Client systems.

2.2.2.5 Data tier

The application databases are covered in the Information Management section of this document. There are in addition, application services that operate within this tier of the architecture.

2.2.2.5.1 Data Transformation and Summarisation

These processes are new and replace the functionality provided in Horizon by the harvesting and Loader Agents. Various processes are scheduled as either batch or near real time processes to copy, transform and summarise data between the Branch database and the legacy databases.

2.2.2.5.2 Support Services

There are interfaces from the business applications to supporting services. These include:

- Audit service
- File transfer Service
- MID/TID management service
- Estate and System Management services.

The Audit application remains largely unchanged apart from various modifications to the configuration of audit collection points throughout the estate. [These changes cannot be specified at this time - the Audit application will be unchanged other than modifications required by the HNGX Project architecture which will be specified in the design phase.] An audit conversion tool will be provided to convert existing audit data from Riposte to another readable/searchable format. The Audit system provides storage for Banking and Debit / Credit card transaction data in accordance with the PCI requirements to protect Cardholder data. This includes storage of encrypted PAN and associated cardholder data. The Audit workstation has the ability to decrypt an individual PAN. The Audit does not store sensitive authentication data for transactions performed using the new authorisation services interfaces, which includes Horizon transactions. However, the audit system does store such data in encrypted form for historical transactions performed using the Horizon authorisation interfaces where messages were transferred using Riposte.

The Audit solution is described in greater detail within the Security section of this document.

Aspects of the File Transfer service are referred to in various sections of this document. The HNG-X solution assumes a reduced set of direct Client/3rd party connections compared to Horizon, but in general for those interfaces that are retained, there is an equivalent service and Client/3rd parties are unaware of the source of transaction data originating from Horizon and HNG Branches.

The other services will be updated as appropriate to support the changes within the HNG-X solution. See Infrastructure / Estate Management sections of this document for further details.

2.2.2.5.3 Reference Data Distribution Service

This tier of the Reference Data comprises the database application:

- RDDS Reference Data Distribution Service

This system takes the Reference Data once it has been released by RDMC, and prepares it for distribution to the Branch estate and other Data Centre systems.

Changes are required to RDDS to handle distribution of Reference Data to the new counter business application. Data will be handled in one of three ways:

POL00033119

1. Changes to Branch Specific Data (e.g. name and address, which products are sold in that Branch etc) will be distributed to the User and Session Management database. This will be picked up overnight or on log-in by the counters.
2. Common Reference Data required by counters will be packaged for distribution by SYSMAN on a nightly basis
3. Reference Data required by Data Centre (e.g. account mappings for products) will be distributed in the same way as for existing legacy Data Centre applications.

2.3 Information Management

2.3.1 Assumptions

1. The rate of report requests is reduced significantly by the removal of unnecessary reports and consolidation of reports. Reports will be grouped in to a small number of categories, such as “Last Post”, “End of Day” and “Adhoc”.

2.3.2 Solution

A number of separate application databases provide the Information Management components of the solution.

The Branch transaction data for HNG-X will be centralised into a single database repository (the Branch database) within the Data Centre, thereby replacing the Riposte message repository.

The relationship between the application databases is shown in Figure 5 (the direction of the arrow represents the main Data Flow).

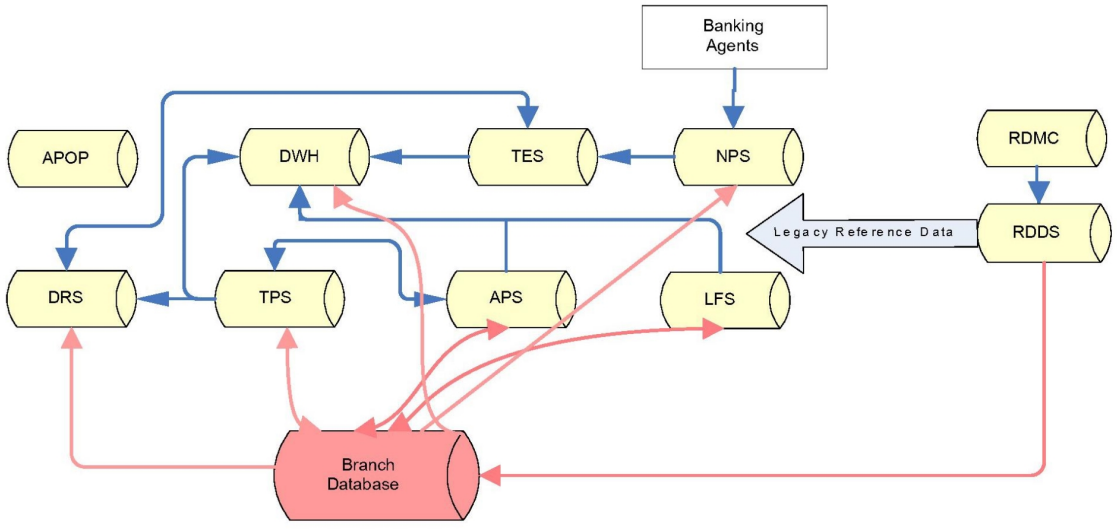


Figure 5 – Application Database Architecture

POL00033119

The database technology platform for all the business applications will be Oracle running on Red Hat Enterprise Linux (RHEL) or Solaris.

The existing legacy databases will be retained. Rather than these legacy databases receiving their transactional information from the Riposte harvesting agents, they will access the new Branch database directly. Conversely, Transaction Corrections, messages and LFS Pouch information required by the Branches will be transferred through the legacy databases and delivered to the Branch database such that it is available to on-line counters.

Reconciliation will be simplified through the centralised transaction model, no transactional information will be held at the counter, eliminating the need to reconcile the branch to the data centre.

The Branch database will be constructed as a single database. This database must support a high commit rate as well as a high volume of database queries, and must have high availability. [See section 6.] Oracle Real Application Cluster technology will be used for the Branch database (this is already in use on Horizon for NPS database). Maximum Availability Architecture will be used to provide data protection and availability by minimising or eliminating planned and unplanned downtime at all technology stack layers including hardware, storage or software components. This architecture involves primary and standby Branch Databases.

POL00033119

3 Infrastructure – Platforms & Storage

This section describes both the platforms and the storage aspects of the solution architecture. Separate views are provided for the Data Centres and the Branch domains.

3.1 Platform Builds

The definition for each platform supports a set of common requirements for use in HNG-X. Each platform must support the application software for HNG-X, be managed using prescribed systems management tools and uphold the security standards Post Office Ltd. required for any platform to be connected to the HNG-X network.

The objective of the platform design process is to produce a set of baseline standard build configurations fulfilling the requirements for HNG-X infrastructure platforms.

Figure 6 and the text below describes the breakdown for various components used in the standardised platform design which enables common approach to be used for all platform types.

Each platform is split into a number of build levels, each one applied cumulatively to the previous level.

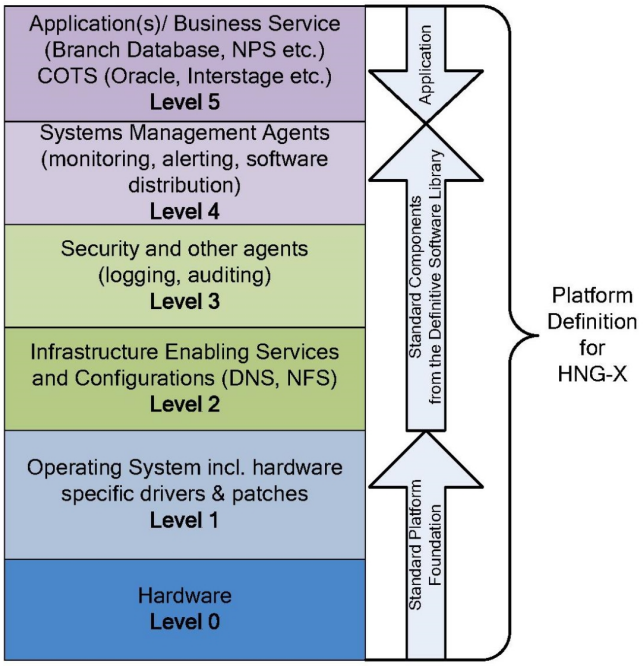


Figure 6 – Platform Definition Multiple Layers

In detail the Component levels of each platform consist of:

- Level 0 - Baseline Hardware Configurations Required for HNG-X Platforms
- Level 1 - Base Operating System build and low level system software
- Level 2 - Base Infrastructure Services
- Level 3 - Security configuration and software

POL00033119

- Level 4 - Standard Common Base Software configuration applied to all platform types
- Level 5 - Application support software applied to specific Platform Types

Level 0 - Baseline Hardware Configurations Required for HNG-X Platforms

This is a set of minimum hardware specifications required to support HNG-X platform builds. It includes a definition of the Base hardware and low level software such as BIOS and firmware levels

Level 1 - Base Operating System Build and Low Level System Software

This level consists of the Base Operating System build, specific low level hardware dependent support utilities, such as disk management tools and device drivers required to run the Operating System, plus Service Packs and Security patches as designated by the HNG-X security Policy. .

Level 2 - Base Infrastructure Services

This level includes standard infrastructure services such as file server, Domain Naming Server, Directory Services, Dynamic Hosting Configuration Protocol. Etc.

Level 3 - Security Configuration and Software

The component level is made up of platform security configuration and security applications applied to the level 3 build. This will be common to all platform types and will consist of security software such as specific system configuration and application of Group Policies. This will ensure each platform conforms to the HNG-X security policy.

Level 4 - Standard Common Base Software Configuration (Applied to all Platform Types)

These components consist of common software items that are applied to all platform types. These will include items such as agent software for Systems Management tools and performance management.

Level 5 – Application Support Software (Applied to Specific Platform Types)

This build level splits systems into groups of platform types, such as Database Servers, Agent Servers or Infrastructure Management Servers. It will provide software that is applied for specific platform roles such as Database Management or Application Servers. This is the final infrastructure platform level ready to receive application code and will complete a full platform

3.2 Platform Architecture

3.2.1 BladeFrame

In order to standardise on a single hardware type FTS / Egenera BladeFrame technology is used. This technology allows single vendor management and a common approach to platform deployment, management and consumption of compute power. It also provides the capability to scale up or out without the typical constraints of traditional systems.

Each pBlade server is a stateless unit of CPU and Memory which when combined with cBlade and sBlade presentation of SAN and network provides a server capability. Each pBlade server is a hot swap commodity item making future upgrades easier and also allowing reorganisation due to changing

POL00033119

demands. Due to the logical management of configuration via the Processor Area Network service (PAN Manager), a standard approach to presenting server platforms is provided which allows good return on investment.

BladeFrame provides inherent high availability in both local resilience and cross site failover. Each Frame has separate standby pBlades capable of automatic recovery should another fail. PAN Manager automatically manages the failover on all servers affected by the outage. By using SAN based system, boot and data storage, the stateless servers can be brought back online very simply. Cross site failover is provided by replicating the system, boot and data to an opposite Frame pair in the passive data centre. SAN based hardware replication over dedicated SAN links provides a robust and simple recovery method. BladeFrame hardware is configured identically to enable rapid recovery in the event of a disaster. Passive data centre equipment provides test services during normal operations.

Certain specific services run in an active / active model across both data centres, each is capable of supporting 100 percent of the estate. SSN and ACD are two such examples of this configuration on BladeFrame whilst VPN is configured on discrete servers.

3.2.2 Discrete

BladeFrame is the preferred hardware platform to be used, however discrete hardware will be used where application requires a specific OS (e.g. DAT) or there is a specific security reason (e.g. VPN) or performance reasons where a bottleneck could be created (e.g. Backup). The amount of discrete server types and instances has been kept to an absolute minimum.

3.2.3 Operating Systems

Three supported operating systems have been defined for use within the estate. They are:-

- Windows 2003 Server (Enterprise and Standard, 32Bit and 64Bit)
- Red Hat Enterprise Linux (Release 4, 32Bit and 64Bit)
- Solaris 10 (Discrete platforms only)
- Windows XP, Windows 2000 and Microsoft NT operating systems exist on some legacy services. These systems must be retained in order to support the use of Microsoft NT on the counters.

3.2.4 Virtualisation

Hardware virtualisation is the preferred BladeFrame deployment model making efficient use of hardware through virtual Blades (vBlades). A vBlade is configured on an underlying pBlade which is running a XEN derivative hypervisor within the BladeFrame. This allows a single pBlade to be carved up into multiple vBlades sharing the physical resources available to the pBlade.

Discrete servers also make use of virtualisation in order to provide support to out dated operating systems such as Windows NT4 and the VPN service. The hypervisor used is hosted by Windows 2003 Server and is Microsoft Virtual Server 2005.

For Live, memory is not over specified in allocation of platforms to pBlades, but can over specify for test configurations where performance not critical. CPU has been specified to always allow one core to be dedicated to the Hypervisor with the remainder divided up according to the requirement.

POL00033119

3.3 Data Centre

This section is subdivided into a number of areas: Operational Model, Business Systems, POL-SAP, Storage and Audit and Supporting Systems.

3.4 Operational Model

The platforms of HNG-X are arranged in two Data Centres each capable of providing the production service. The configuration of the physical platforms is such that in normal operations, the active Data Centre provides Counter facing service whilst the passive Data Centre provides Test and Release service. Some services operate in a Active Active model in normal operations. These are considered key infrastructure services such as VPN.

The Disaster Resilience model for the HNG-X solution is based on an *active* Data Centre paired with a *passive* Data Centre. The active site usually delivers all business applications and services. The passive site is usually used for testing and switches into active triggered by disaster recovery procedures. More details can be found in section 6 (Availability).

To enable failover to the passive Data Centre some base level infrastructure platforms operate in an Active Active model. This includes platforms AD, Sysman, DNS, NT Domain controllers and such.

Limited service Orchestration for Test is achievable in the active Data Centre in the event of the passive Data Centre being unavailable.

3.4.1 Business Systems

The table below lists the platforms for the business systems at the Live Data Centre.

#	Name	Function
1	Database Servers	Database servers for all of Branch data and accounts. Also supports NPS and legacy Horizon databases (APOP, TPS, APS, LFS, DRS, TES, RDMC and RDDS).
2	Central Agents	Central online services such as PAF, APOP and Training.
3	Banking and Client File Transfer	Batch feeds to Banks, Streamline and e-pay
4	Other Client Agents	Online feeds to Streamline, e-pay, DVLA, Moneygram , Help Desk and other online services such as those provided by the Service Hub. All Client Agents will be implemented as virtualised platforms independently of each other, with the exception of the Service Hub where all services hosted on a single virtualised platform.
5	Banking Agents: NBS	Online feeds to the banks. There are three types (A&L, CAPO and LINK) and these use different platforms (required for security reasons).
6	Branch Access Layer Servers	Branch Access Layer Servers support all Branch counter business application interactions.
7	TES Application Server	Application services for Post Office staff accessing the Data Centre
8	PO File Transfer	Batch feeds to Post Office systems.

POL00033119

3.4.2 POL SAP

The POL-SAP system provides SAP financial services to Post Office and is hosted across both Data Centres in a three Tier SAP Landscape. Initially this was a hosting only contract for POL-FS but a recent service consolidation has increased the service catalogue to include POL-FS, SAP-ADS, Budman, Cashman and CMS. POL-SAP is providing hosting and application support and development.

The POL-SAP system is hosted on standard Linux based platforms utilising Oracle Application servers and databases. It uses the standard tiered storage model to provide a robust financial capability.

3.4.3 Storage and Audit

Generally physical storage is provided by a multi tiered EMC based architecture. Enterprise class EMC Symmetric storage arrays provide the highest storage availability and performance. These are arranged in two tiers to provide some operational cover to the highest tier during upgrades of firmware. Next is Clarion and Centera storage. As one transcends the storage arrays greater impact will result from component failure and therefore business and system data is located accordingly.

Storage is consumed by Service Class arranged by performance, availability, resilience, integrity, and recoverability. Each platform is mapped to an appropriate class taken from the platforms requirements. This varies from zero data loss and immediate recovery to long term archive storage. Figure 7 shows the main storage tiers with the classes overlaid.

Celerra NAS storage is not shown on Figure 7 for clarity but should be regarded as a presentation technology for other physical hardware Tiers. Due to the characteristics of NAS storage, it will be unable to participate in all Service Classes.

Some Discrete server platforms do not consume SAN storage and therefore have local storage and are not represented in Figure 7.

POL00033119

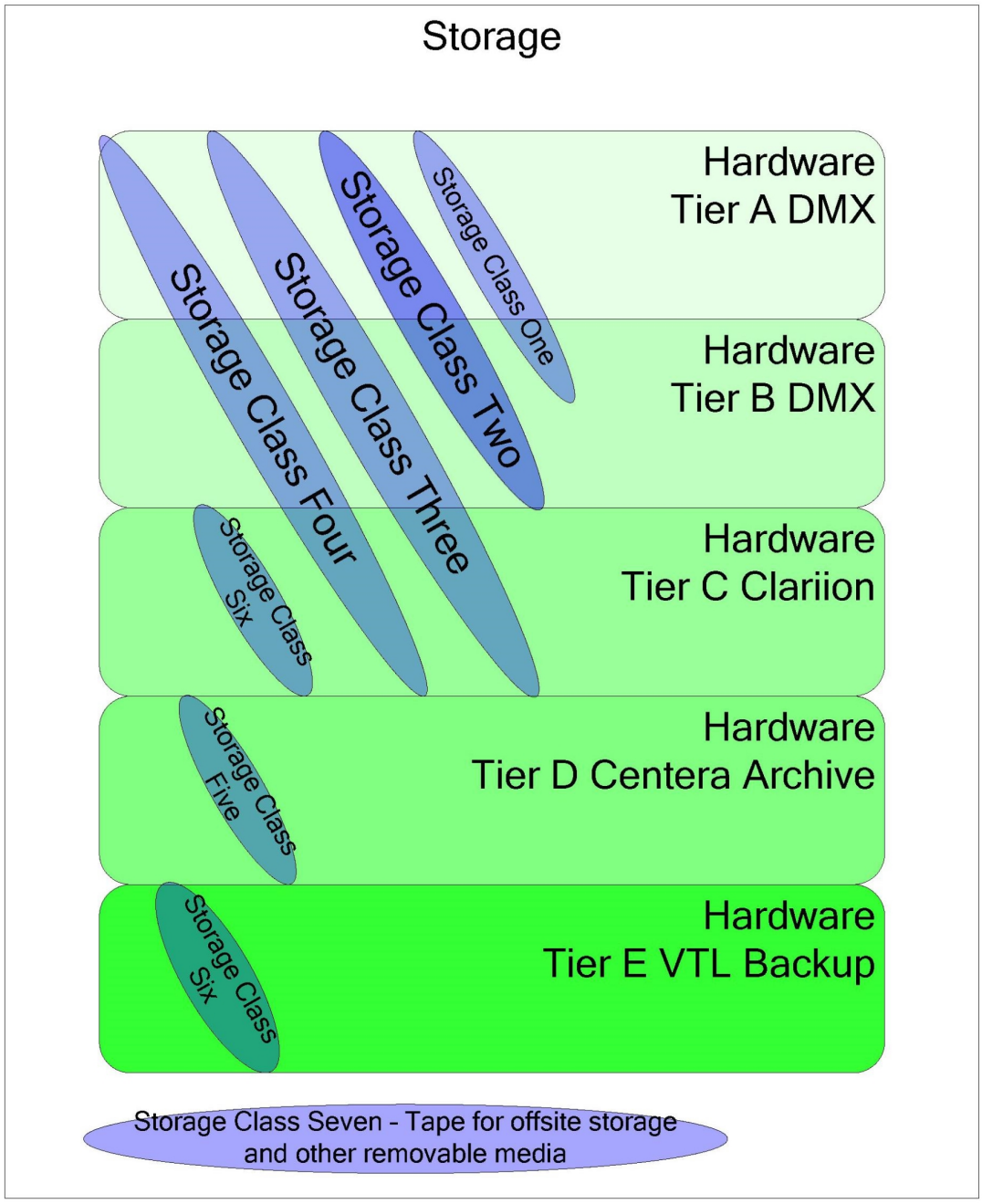


Figure 7 – Logical and Physical Storage

Business critical data with high availability requirements are located on Storage Class One and replicated via a synchronous link to the second Data Centre. This guarantees that no transactions will be lost.

Data that does not require such a high level of protection and availability will be hosted on more cost effective storage. Where required this data will be replicated to the second Data Centre via an asynchronous link or a scheduled replication mechanism.

POL00033119

Historical and audit data will be placed on dedicated Centera storage arrays and the contents are replicated to the passive Data Centre.

Both Data Centres will contain all the appropriate management systems to allow for the management of all storage platforms from either Data Centre. Additional phone home capability is built into the storage system enabling proactive support.

3.4.4 Supporting Systems

The table below lists the supporting services included in the solution. For some platforms there are additional systems at the DR site that are not used for testing as they hold a copy of the live data to allow failover on DR.

#	Name	Function
1	Estate Management	Servers and systems supporting the estate management databases and processes
2	Systems Management	Servers and systems supporting Systems Management databases and processes. Remote Management, Event Management, Software Distribution, Provisioning, Network Management are examples of Systems Management.
3	Support Services	Servers and storage providing audit capabilities
4	System Qualities	Capacity Management servers, Backup and Recovery
5	Infrastructure Services	Directory Services, Backup and Recovery, DNS, Domain Management, User Account Management, Patch Management
6	Security Services	Servers and Systems providing authentication, access and assurance for security

3.4.5 Testing in passive Data Centre

When the second passive Data Centre is not used as a disaster recovery location it will be used to support HNG-X testing. Where necessary, additional hardware is deployed in the second passive Data Centre to enable testing under close to live conditions without interfering in any way with the Live Data Centre operation. Testing will make use of virtualisation technology to support multiple concurrent test streams. In the event of a disaster the second passive Data Centre will be re-configured as the active Data Centre with live data and all testing will cease. On restoration of the Live Data Centre the passive Data Centre will resume its role of supporting HNG-X testing based on an earlier checkpoint. During the period the passive Data Centre is used as live no HNG-X test activities will be undertaken.

Due to the architecture used to implement the solution, a limited test capability exists in the live Data Centre should the passive Data Centre be non operational. This capability will be realised in the event that critical updates need to be deployed to the live system during a prolonged passive Data Centre outage. Careful consideration will be needed at the live data centre as live systems will require reconfiguration during quiet periods to enable this capability.

3.5 Branch Platform Infrastructure

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

POL00033119

The normal configuration for a Counter position is:

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

A single back office printer is provided for each Branch. This is connected to one of the PC's.

Initially the HNG-X counter application will operate under Windows NT. Any changes to the operating system (and potentially the hardware used) will be subject to a separate Change Proposal and are beyond the scope of this document which covers the initial HNG-X release.

The Branch is connected to the Data Centre via a Branch router (see Network section).

For mobile counters the normal configuration is:

- PC Base Unit (1GHz Pentium 4 Celeron with 256Mbytes of memory and integrated support for multiple serial connections) packaged in a mobile form factor.
- Integrated touch screen.
- LIFT Keyboard incorporating a Magnetic Swipe and Smart Card reader (serial connection for card reader)
- BAR Code Scanner (Serial Connection)
- Slip and Tally Roll Printer (Serial Connection)
- PIN Pad (Serial Connection)

The mobile counters are connected to the Data Centre via a Branch router (see Network Section).

POL00033119

4 Network Services

The following diagram provides an overall view of the HNG-X Network services. It represents the target solution after Migration of all services from existing Horizon data centres has been completed and the Horizon Data centres have been de commissioned.

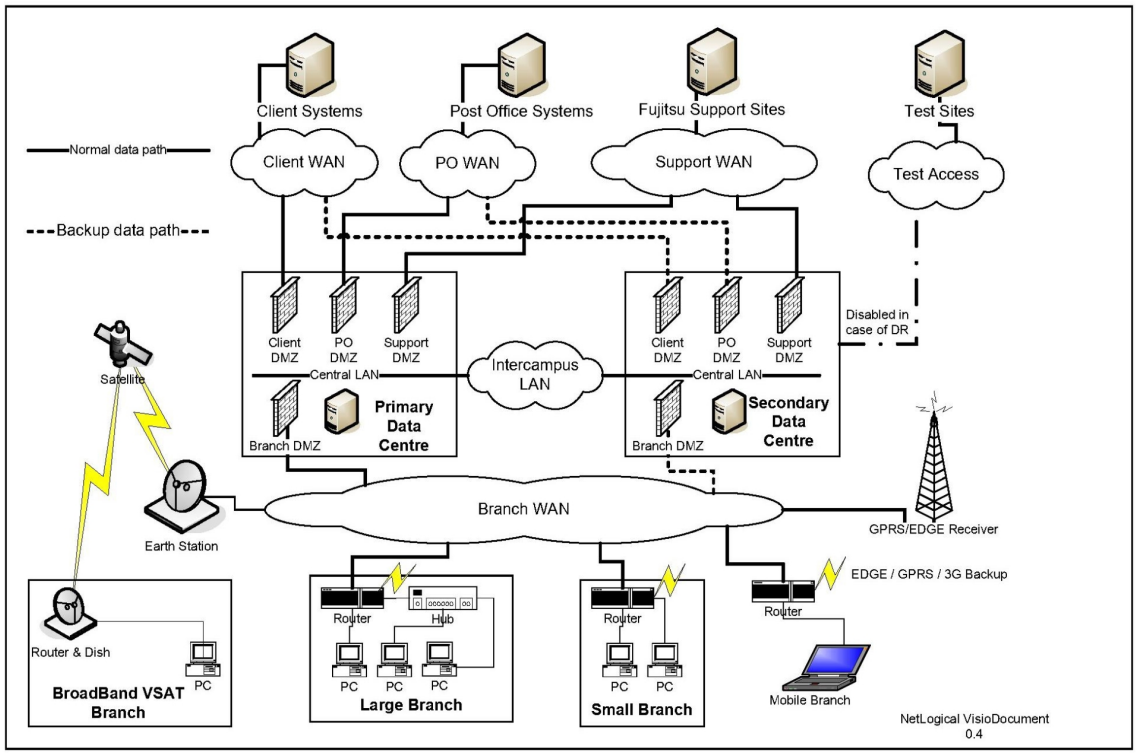


Figure 8 – Central and Branch Network Services

The Network services may be subdivided into the following topology areas;

- Data Centre (LAN, Inter Data centre services and Application Services).
- WAN services; These provide for connecting Post Office Client sites, Post Office Data centres and Fujitsu sites (Support, Test and Application workstations) to the HNG-X Data centres. Internet connectivity is provided as some Post Office Services are reached via the Internet.
- Branch network; This includes Branch connectivity to the Data centres and within Branch Networking

The approach used for Network Management is based on HP Open view for monitoring, SYSLOG repositories for event storage and Cisco works for Configuration backup. Alerts are forwarded into the Enterprise Management System. The Branch Router is an exception to this model as it is directly managed by the Enterprise management Framework (SYSMAN3) as an Agent less node.

A common approach based on TACACS+ is used for authenticating access to Network Appliances, auditing access plus changes and authorization of commands based on user types.

POL00033119

4.1 Data Centre

4.1.1 Inter Data centre networks

This LAN service between the two HNG-X Data Centres carries IP traffic and Fibre Channel SAN traffic. It is based on a DWDM service and this service needs to be highly resilient since it is used to replicate state which is required in the event of DR. The DWDM service has the following Resilience and Availability characteristics;

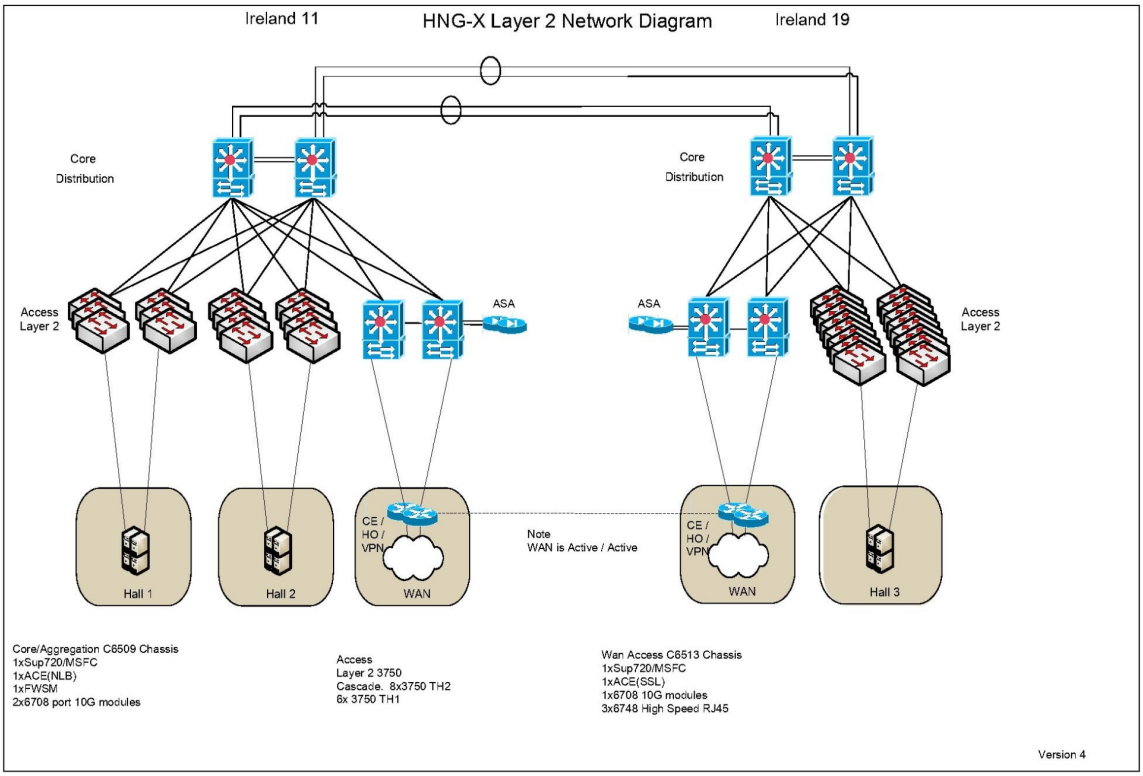
a) There are two DWDM devices each Data Centre and the SAN extension and IP Network topology is such that it is sufficient for a single device to function to provide an Inter Campus service.

b) Between both HNG-X Data Centres there is a pair of fibre optic cables. The radial distance of each of these is < 100 km (in order to meet latency requirements for synchronous SAN extension) and the two fibres are kept separate along their runs with no common interconnection points.

4.1.2 Data Centre LAN

The Data Centre network follows the Classic Cisco Three-layer hierarchical model referred to as Core, Distribution and Access layers.

The following diagram illustrates these layers and how they are realised on network appliances.



A summary of how each layer is created and the functions it provides follows;

POL00033119

Core / Distribution Layer;

- Created on fully redundant Enterprise Class Cisco multilayer switches
- IP Routing at very high speed between Servers on different IP subnets
- Provides Inter- Campus traffic; Layer 3 / 2 switch traffic between HNGX Data Centres (IRE1x)
- Application service; Network Load Balancing and IP endpoint virtualisation across data centres
- Firewall Services – internal firewall

Access layer (Servers);

- Server connectivity (shown as Hall1, Hall2 and Hall3 on diagram) is provided by a scaleable collection of Access Layer 2 switches.
- The Access Layer 2 switches have fully resilient connections to Core / Distribution layer

Access layer (WAN);

- Created on fully redundant Enterprise Class Cisco multilayer switches
- Location of "Handoff Routers" to provide all external connectivity(*)
- Application service; SSL offload for Branch counter traffic
- Firewall services – external Firewall
- Creation of the Utimaco VPN layer so that all traffic between counters and the data centre is IPSEC protected.

(*) In some cases clients connect directly to HNG-X data centres (for example Vocalink, EDS and Moneygram)

4.1.3 Application services

The network provides the following services to the HNG-X Applications; - SSL offload, Load balancing and Virtualisation.

SSL offload is used to terminate SSL sessions initiated from the counters. SSL provides for encryption of the application payload and for one way authentication of the Data Centre to the Counters. Specifically Client Authentication where the counters authenticate to the Data centres is not used. SSL Offload is provided by a pair of redundant Cisco ACE blades in the Access Layer (WAN) Cisco multilayer switches.

Virtualisation enables Client applications to target a single endpoint (IP address and port) irrespective of which servers and / or data centres provide the service. This removes the need for multiple endpoints and significantly simplifies client failover as the client does not need to be concerned with multiple service endpoints.

Load balancing distributes the workload across available servers based on probing of application ports to determine available servers.

A pair of redundant Cisco ACE blade in the Core / Distribution Cisco switches is used to provide Load balancing and Virtualisation services.

4.2 WAN services

The functions of the Wide Area Network service are to provide;

POL00033119

- Network Connectivity between HNG-X Data centres and locations for Post Office Clients as well as Post Office Data Centres.

(Note some Post Office Clients provide the WAN connectivity into HNG-X data centres, these being Vocalink, EDS and Money gram)

- Network Connectivity between HNG-X Data centres and Fujitsu Support sites (including Test locations)
- Network Connectivity between HNG-X data centres and the Internet

The general approach to providing connectivity to HNG-X data centres from an external location (Node) is based on connecting the Node (with suitable resilience and capacity) into an MPLS cloud from Cable & Wireless. This MPLS cloud provides a private HNG-X network with any to any connectivity between all connected nodes. Typically the connectivity is limited to between the HNG-X data centres and individual Nodes as opposed to being provided between distinct Nodes.

In addition Fujitsu locations at "TCY02" and SDC01 are connected to this MPLS cloud via a HNG-X dedicated service known as the IP Gateway. This service is primarily used for Branch traffic but supports a general method for traffic to traverse from Fujitsu to HNG-X networks. This is exploited for example when providing connectivity from support sites in India. Rather than connect the support site to the C&W MPLS cloud which may be expensive, existing connectivity between India and Fujitsu is used to provide connectivity into the IP Gateway location. The IP Gateway is used to complete the traffic path to the HNG-X data centres.

A common approach (Handoff Router Model) is used in HNG-X data centres for all external connectivity where HNG-X provides the Wide area network. These "Handoff Routers" are connected to the Access layer (WAN) switches.

Single high capacity WAN circuit tails are provided into each HNG-X data centre. Resilience is achieved by triangulation through the other data centre using the Inter Data Centre network.

4.2.1 Post Office Clients and Post Office Data Centres

The following PO Clients and POL Data centres follow the general approach to providing WAN connectivity based on the C&W MPLS cloud mentioned in the previous section. All WAN connections are provided by Fujitsu:

- DVLA for online authentication of car tax.
- e-pay for mobile phone top up (ETU) transactions
- Alliance & Leicester for banking transactions
- POL data centres at Huthwaite (Live) and DR (Sungard and Maidstone)

The following WAN connections to HNG-X data centres are provided by third parties:

- Voca LINK for banking transactions
- CAPO for banking transactions
- Moneygram for money transfer

POL00033119

Streamline for debit / credit card (DCS) transactions is provided over X.25 circuits from TNS with ISDN dial up (initiated from HNG-X) for File transfer.

The specific configuration of each Client connection and how they are used is defined in the relevant Technical Interface Specification (TIS) and Application Interface Specification (AIS).

4.2.2 Support WAN

This provides access for the Fujitsu support communities to the HNG-X Services, platforms and appliances. This access covers Business support and application / network / platform support roles. The following models are supported;

- RED LAN model; A dedicated workstation managed by HNG-X (provisioning, eventing and maintenance is provided). The path to the HNG-X data centres consists of HNG-X components and HNG-X WAN services only. This model provides for the most flexible access and high availability.
- Corporate Workstation LAN only; A Fujitsu Corporate workstation is used to access HNG-X data centres. All WAN conveyance is provided by a HNG-X WAN. This model is used to cover the case where the amount of data exchanged is too large (based on agreed volumes) for the Fujitsu corporate WAN. To support this model a local handoff gateway (back to back Firewalls) is created at the relevant location. Traffic travels locally over the Corporate network and then over a HNG-X WAN to reach the HNG-X data centres . Access is restricted to Remote Desktop (no copy / paste and file transfer) onto HNG-X Secure Access Servers.
- Corporate Workstation; This is a special case of the Corporate Workstation LAN only model where part of the WAN conveyance takes place over the FJ corporate network. As stated this limits the voume of traffic sent over the WAN.
- Out of Hours Access; this is a Corporate Workstation model where the initial access is over the Fujitsu corporate VPN.

The selection of the relevant support model is made on the basis of support role and associated requirements.

To provide for Data Exchange between HNG-X and Fujitsu corporate workstations a Corporate Data exchange proxy is provided in HNG-X.

4.2.3 Internet Access

This is required for Counter Services that are reachable over the Internet. These being;

- Neopost (Kahala)
- BT Broadband Checker
- postcodeanywhere.co.uk

In addition the Test service for Moneygram is accessed via the Internet. The Internet service is also used for EMC support access.

In all cases connections are initiated from HNG-X data centres to the internet reachable endpoints.

POL00033119

4.3 Branch LAN and WAN

Within each Branch there is a single LAN onto which all Counters are connected. The network in small Branches (1 or 2 counters) consists of a Router which connects to the Counter PCs. Larger Branches (3+ counters) use one or more hubs are also used to provide the LAN connections. Each Mobile Counter has its own router.

Each Branch has its own IP subnet used for the LAN connections, with each PC having direct access to the Data Centre via the router. The Branch routers support ADSL, ISDN, PSTN and EDGE / GPRS / 3G connections in a single device. The majority of branches will use ADSL with EDGE/GPRS/3G used as a backup. For a small number of Branches that are out of distance from the nearest exchange, VSAT is used. The router will automatically switch to the backup network (subject to availability) on failure and revert to the Primary network when restored. The Router has 2 SIM cards fitted and will choose between providers (Orange or Vodafone) to optimise Wireless WAN availability. The Branch Router provides a NTP time source (in broadcast mode) to all counters in the Branch.

ISDN is supported in "dial on demand" mode both as a Primary network type and back up network, To enable the data centre to initiate communications to ISDN branches, "dial out prod" is provided where the data centre "prods" the Branch Router (with a call to the branch that is rejected) to cause the Router to establish a connection.

PSTN is only supported in an "always on" mode – that is the connection is kept open whilst this network type is the selected as the best choice by the Branch Router.

The counters within a branch communicate over a VPN. The Utimaco product used on Horizon is used for this purpose whilst the HNG-X counters are deployed on Window NT. However, unlike Horizon communication is direct between each counter PC and the central VPN servers, and not routed via the gateway counter.

All Branch WAN services are delivered into Fujitsu Locations at SDC01 and TCY02 and from there delivered into HNG-X data centres using the IP Gateway. The Branch WAN services are;

- Cable & Wirless for dialled PSTN and ISDN
- FJ Core services for ADSL based on the the IPStream Home service from BT
- Wireless WAN based on Orange and Vodafone

4.4 Testing Access

The test access network allows testers access to the Data Centre systems at the DR site for testing. In the event of a disaster, when the site has to be used for running the live system, this access is disabled.

POL00033119

5 Systems & Estate Management

The size and topology of the Post Office Branch estate requires proactive and comprehensive system management such that every Branch and individual Counter Position is under management and is being supported in successfully performing business transactions.

Similar considerations apply to the applications running in the Data Centres. Any anomaly can potentially have effects over large parts of the Branch estate.

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

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

5.1 Software Distribution and Management

5.1.1 Receipt

Software to be distributed, and optionally installed, on target systems will be delivered from Software Change Management to Systems Management through a formal Release Management mechanism. Such software will be pre-packaged so that it can be delivered and optionally installed in a fully automated manner. Where such automation is not possible the procedures will still be followed to include documentation of any manual intervention that may be required.

Reference data updates, received for distribution, will not be sourced through the above mechanism, but will be received in a fully automated manner which will include targeting information.

On receipt of Software packages the Release Note will be used to create targets for the packages and to control any optional distribution parameters.

5.1.2 Distribution

Software distribution will be supported in either of two modes of operation:

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

It should be noted that the above does not imply the direction of software transfer, but only the origin of the transfer request.

The software is optionally installed and a permanent record is kept of its distribution and installation against the end system in the central system management inventory. All end systems in the Data Centre and the Branch estate can be updated through this service, although the pull mechanism is not considered necessary in the case of Data Centre Systems.

Two other types of device are supported via this system:

1. Peripheral devices that provide an API to update their firmware from the end system to which they are attached are also supported on this solution. Pin Pad's are an example of this class of device.
2. Branch Routers will have both configuration data and firmware updated; in this case only 'push' distribution will be supported.

POL00033119

Both of the modalities described in items 1. and 2 above have associated scheduling and targeting criteria. The targeting criteria is the statement of what end systems need to be updated and will allow such groups as single end systems, nominated sets of Branches (for pilot roll out of new facilities); and generic rules (such as all end systems who do not have the software already installed).

The scheduling criterion is the time at which the installation on the end system is actioned. Most software installations are invasive to the business and hence their schedules are chosen to be out of business hours. In the push mode the scheduling criteria is implemented by the central management systems.

The pull operation is driven by a local schedule on the end system. The local schedule will allow a variety of options and associated functions including:

1. At user log on
2. At fixed time of day and day of the week
3. At end system swap out. This is the automatic upgrade of a new end system from the software baseline present on that end system (i.e. at cold build) to the baseline of the live end system it replaces. Support will be available to counter and pin pads.

The local schedule will itself be capable of remote update using the push operation.

While the Branch Estate utilises the Windows NT Operating System it will be managed by additional integrations inside the current Management environment; in this case user logon requests are not supported and the schedule is policed centrally on receipt of the transfer request.

The payload will typically contain software items but for the counter estate may now constitute Reference Data. The payload will be applied using installation technology appropriate to the end system that provides the minimum deployment costs while preserving the key attributes including accuracy, non invasive to user operation, unattended operation, end to end integrity, and resilience and recovery. Installation technology will include such candidates as MSI, PDF or where necessary bespoke scripts.

The installation of software is generally performed wholly on the end system but there are some situations where software installation may not be performed wholly on the end system. In particular, it may be important for Post Office staff that new functionality is available at all Counter positions in a Branch at the same time to avoid confusion over which positions have what functionality. For Reference Data, this will be supported through the use of a “soft launch” control, where new functionality will activate only when all Counter positions have been upgraded.

There may be updates that require Branch wide installations (changes that need to be made to all Counters in a physical Branch at the same time). However the need to use this type of update is expected to be extremely rare and limited to circumstances where infrastructure changes need to be applied to all Counter positions to allow inter-working (e.g. an update to change the way software caching works where it has not been possible to make it backwards compatible).

The software distribution solution will provide management reports via Web based displays or standard tooling (such as SQL or Crystal Reports) to generate ad hoc reports and/or service level reports.

All of the above in this paragraph 5.1 will be used to deploy updates to the live estate according to the nature of the payload. It is anticipated that the great majority of updates to the Branch estate can (after a successful completion of a pilot) be applied counter by counter thus minimising the operational deployment costs. While the NT Operating System is in use on the Counter only Reference data will use the ‘pull’ technique.

5.1.3 Integrity checks

The security policy on the Branch estate requires that the software on each Counter is regularly validated to check that it has not been tampered with. Software distribution will provide the software baseline definition and schedule the periodic check.

POL00033119

This will be available for New and Migrating Platforms in the Campus Estate and Branch Routers, but only existing facilities will be offered on the Windows NT Counter.

5.2 Distributed Monitoring

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

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

1. Whether each business service is working fully, partially or not at all.
2. The state of resilience features that make up that service – for example resilience may be currently reduced due to an earlier failure.
3. Indicators that the service may have problems – for example higher business error rates than expected or volumes being processed are lower.
4. Indicators that the components that make up the service may have an issue – for example processor usage is much higher than expected.

Wherever possible an “end to end” view of the service will be directly monitored together with the individual components. To achieve this view, system management agents can generate 'health-check' transactions that exercise the Data Centre and Branch components of the application, and report when it encounters problems. Special features in the business applications support this (for example to ensure that these requests are not to be passed outside the HNG-X system).

The monitoring will include the ability to view each Branch in the estate, to display whether it is available or not and whether the network connection(s) to the Branches are working..A single integrated view will be provided, although the different toolsets may be used for different operations.

5.3 Event Management

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

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

However in the case of business applications at the Branch, events may also be sent to the central system via application infrastructure to the Branch database. This is used to report business application issues. This ensures reporting on business applications is kept independent of the platform and operating system on which it is being run. Instrumentation will be introduced on the central business application systems to forward into the systems management environment information pertinent to systems received via the business application route.

The central event management system will provide facilities that include:-

- Web based user interface to view the reception of events
- Links to Known Error Log repositories so that the significance of the event may be determined

POL00033119

- Links to automatically perform automated actions based on configurable criteria
- Links to automatically raise entries in the incident management system for events based on configurable criteria
- Medium term storage of events for trend analysis
- Movement of selected classes of events to long term storage coupled with their removal from the online repository

These facilities are deployed to support a typical workflow view of the actions on event reception

1. Automatic resolution, which is triggered when a problem is recognised and has an associated automatic action. Automatic resolution may, for example, include raising a call to get hardware changed.
2. Operator intervention, which can be needed to resolve a known issue. Both the event and the KEL (known error log) are displayed together for the appropriate operator.
   [DN: There is currently no KEL database facility provided in the Campus. The event subsystem is capable of providing a call to a KEL function (api), passing any parameters from the event.]
3. Operator investigation, for an unknown issue.
4. Operator investigation for events recognised as a systemic issues in the estate (e.g. present on multiple systems or multiple instances on the same system). These events are combined with other events to present a single view to the operator. Systemic issues may be either known or unknown issues.
5. Known issues that do not require immediate investigation out of Working Hours are held until the next working day for resolution.
6. Audit, when an event is recognised as only needing recording for audit or information reasons and no other action being required.

All actions undertaken with specific events (whether automatic or manual) are audited

Typically the lifecycle of an issue progresses from initial identification, through investigation and the raising of a KEL or the rapid deployment of automated recovery actions / event filtering. Subsequently the problem is either fixed by a new code issue or by some form of reconfiguration or Reference Data alteration.

5.4 Remote Operations and Secure Access

All access by operations to manage IT systems will be fully audited.

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

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

1. Access to Data Centre resident Secure Access servers from Fujitsu Services locations during Working Hours or from support staff home locations out of Working Hours using secure workstation or lap top builds and encrypted communications.
2. Two factor authentication at the Secure Access servers.
3. Onward access from the Secure Access Servers to Data Centre platforms and counters using 3rd party COTS product management interfaces and audited access to all Windows, Unix and Network platforms direct via IP or proxies.
4. A Support Framework to allow 3rd-line-written tooling to be incorporated into the new system.
5. Role based privileges for support access on platforms operating systems, hosted applications and database schemas.

POL00033119

5.5 Application manageability

The manageability of any distributed solution is not only constrained by the quality and agility of the system management tools but also behaviour of the application itself. Manageability compliance and guidelines for application providers delineate the framework for a solution that can be proactively managed. As such the Manageability compliance standards will form part of the architecture.

Areas covered in the manageability compliance include:

- Exception handling such as:-
  - Uniform use and documentation of events
  - Autonomous behaviour – " act locally but think globally"

- Diagnosability such as:
  - Standard use of tracing
  - Diagnostic files

5.6 Estate Management and Auto-Configuration

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

5.6.1 Operational Business Change

To deliver this policy, a cooperating set of facilities are provided to support the Operational Business Change (Branch Change) Service.

Fujitsu Services actions in response to the OBC include:

- To acknowledge and enter the OBC change into a scheduling system
- To schedule requests to parties, external and internal, to provision the OBC change (for example this may include hardware, communications suppliers and engineering services)
- To schedule the timely update of any Data Centre applications configurations that are impacted by the OBC change. This may for example require adding or removing Branch data
- The timely and automatic generation of any new or changed personalisation data for the Branch router and/or counter affected by this OBC
- The automatic installation of the personalisation data at the time of any physical installation of the counter and/or Branch router associated with this OBC
- The provision of estimation and invoicing to Post Office
- The ability to report on the progress and/or change to an existing OBC schedule in accordance with agreed policy
- The update of the central branch configuration repository such that the support staff always have an accurate view of the status of a Branch.
- To respond to and action (where feasible) amendments to the OBC request by Post Office

POL00033119

5.6.2 Counter spares

A spare installation is architecturally a replay of the existing personalisation data for the failing Counter Position. As such it re-uses the same enabling software solution to installing a new Counter Position, the only distinction being that the software fixes applied to the spare will be specific to the Branch and Counter Position in which it is being installed rather than a generic set.

5.7 Capacity Monitoring

The system will be effectively capacity managed. To support this following services are provided:

- Immediate alerting on performance issues that could jeopardise the live service.
- Lower priority alerting for performance issues, which while not jeopardising the live service, indicate a problem that needs to be investigated.
- Medium and long term trending to allow potential problems to be forecast in advance

All new platforms in the architecture and where appropriate existing platforms that are not currently managed will have the performance monitoring software installed.

5.8 Scheduling

Scheduling for all central systems (both business applications and operational services) will wherever possible use a single scheduler which will include the following architectural attributes :-

- Operate on all the major operating systems in use in the HNGX solution
- Integrate with the enterprise management system for alerting
- Operate within the time synchronisation service
- Provide role based management user interface
- Allow the definition of schedule with associated activities and timer based controls

5.9 Time Synchronisation

Time will be distributed through the HNG-X network using the NTP3 protocol and the Microsoft Active Directory (AD) derivative, it will be arranged in a hierarchically as follows:

- Stratum 0

  a) 4 Dedicated NTP servers with attached MSF/GPS time sources to provide time to:

- Stratum 1

  b) Unix platforms
  c) AD Domain Controllers
  d) All network infrastructure
  e) Estate Time Servers, peered radius servers, these will serve:

- Stratum 2

  f) All AD Clients including subdirectory controllers but excluding Unix AD clients, these will optionally be served by the stratum 0 servers in the event of failure.
  g) The Branch Routers, these will serve:

- Stratum 3

  h) All Post Office counters.

POL00033119

Time synchronisation is supported within a single Time Zone.

POL00033119

6 Availability

6.1 Principles

The solution for availability and DR is:

- One Data Centre will be used to support the Business Capabilities and Support Facilities (the "Live Data Centre") with a second Data Centre providing DR (the "DR Data Centre").
- The DR Data Centre will under usual operation be used for testing, except where it needs to be used for business continuity tests.
- Some "Live" elements of the solution will be operational at the DR Data Centre where this is required to support DR or WAN diversity.
- Each Data Centre shall have the capability in normal operation with no failures or a single failure having occurred:
    - To support the Contracted Volumes as defined in the CCD entitled "Horizon Capacity Management and Business Volumes" (PA/PER/033); and
    - To support Fujitsu Services' obligations in respect of Service Levels set out in Schedule C1.
    - The exception list of areas which constitute potential Single Points of Failure are formally described in ARC/PER/ARC/0001.
- Each Data Centre will be configured such that no single point of failure within the Data Centre will cause the Business Facilities to fail.
- Data is replicated from the Live Data Centre to the DR Data Centre to ensure that in the event of disaster there is:
    - No loss of transactions received from the Branch estate where those transactions have been committed to the Branch database.
    - No loss of the audit trail
- Switchover to backup systems within the Data Centre and for the network connections within the Data Centre:
    - for real-time elements of the Business Capabilities and Support Facilities, support is automated.
    - for non-real time elements may be automated or manual.
- Switchover from the Live Data Centre to the DR Data Centre will be manually initiated.
- In the event that the DR Data Centre needs to be used to run the live service or if the DR Data Centre itself is unavailable, there will be no significant test environment. In this scenario, limited testing (sufficient to test minor fixes needed to keep the live service operational) will be available at a Fujitsu development site. However such testing facilities will not be sufficient to test releases.
- The required failover times from the decision to invoke DR are covered in the HNG-X System Qualities Architecture document (ARC/PER/ARC/0001). There are three broad categories as follows:
    - Branch Logon, Basket Settlement Banking and Debit/Credit Card – 2 hours
    - Other Branch services (e.g. DVLA, PAF, APOP) – 5 hours
    - Remaining services (e.g. SAP) – 48 hours
- Business Continuity Testing will take place:
    - Resilience (e.g. failure of a server) during normal Working Hours.
    - DR (i.e. failover to DR site) out of Working Hours.

POL00033119

6.2 Disaster Resilience

The diagram below shows how the approach to DR is handled in the Data Centres.

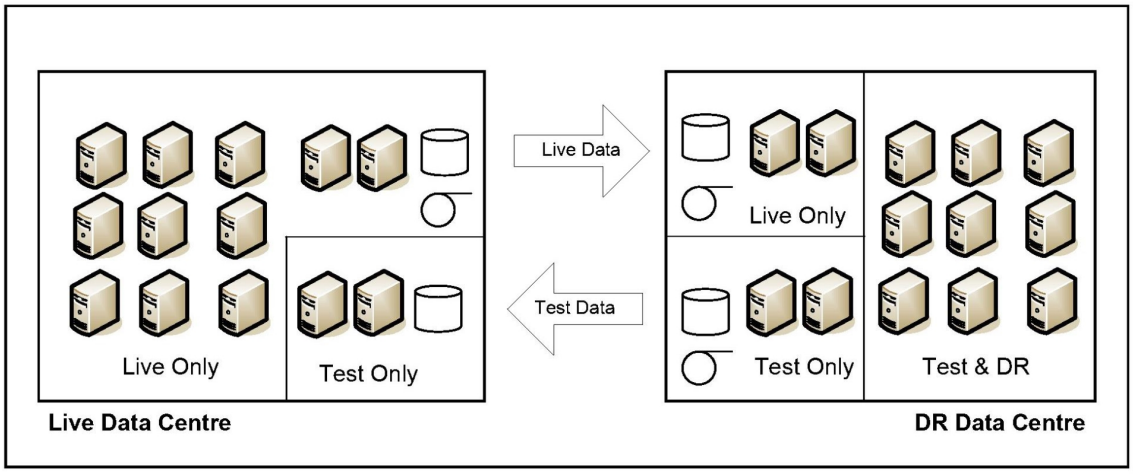


Figure 9 – Data Centre DR

To support the live system there is:

- At the Live Data Centre the main servers, LAN, storage and backup facilities dedicated to live use.
- At the DR Data Centre dedicated to live use:
  - A copy of the data stored at the live site.
  - Backup facilities (so that the data is backed up in both Data Centres).
  - Copies of the live system configurations so that in the event of disaster, the test system can be re-configured into live.
  - Hardware Cryptography Modules with live keys in them to support banking and debit card services.
  - WAN triangulation.
  - Infrastructure operational servers (such as AD, VPN, Radius)
- At the DR Data Centre, normally used for testing:
  - Servers and LAN that in the event of disaster will be used by live.

To support testing there is:

- At the DR Data Centre dedicated to test use:
  - Storage and backup facilities.
  - Copies of the test system configurations so that following business continuity tests, the test system can be restored.
  - Hardware Cryptography Modules with test keys in them to support banking and debit card services.
  - 3rd party emulators and test injectors

POL00033119

- Test WAN links

- At the Live Data Centre dedicated to test use, in the event of a disaster at the DR Data Centre:
  - Storage and servers to allow limited DR testing to be performed. (Note that not all test data will be copied to the live site – just that sufficient to support the test objectives).

The need to have test facilities on the live site is under review and these may be moved to the test site, with appropriate emulation of intercampus network.

To support this approach, Hardware and network changes must follow the Change Control Procedure to ensure that the resilience properties of the solution are maintained.

The business continuity plans will include the following steps:

- Relevant people and organisations are informed that invoking DR may take place (e.g. operations, testers).
- The decision to invoke DR is taken.
- Live server configurations are applied to "DR & Test" servers to convert them from test to live systems (including using live Storage rather than test storage).
- Live network configuration applied to LAN components
- Live network configuration applied to WAN components
- Services restarted

6.3 Resilience

Each Data Centre in its own right must be fully resilient for the business applications. To achieve this there are two main areas that need to be considered: servers and LAN/WAN.

For the servers, there are three general approaches that are used:

- Active server, with dedicated standby. This would typically be used to support online Branch services where it is not possible to have both servers simultaneously connected to a third party (e.g. banking).
- Multiple active servers, with sufficient capacity so that failure of a single server does not cause capacity issues. This would typically be used to support online Branch servers where it is possible to have multiple servers active (e.g. Branch Access Layer servers, Branch database servers).
- Active server with the standby server shared with a number of other systems. This would typically be used for batch services, where the time to reconfigure the standby server to take on the personality of the failed server (which may take a few minutes) would be acceptable (e.g. a file transfer server).

The method of detecting that an active server has failed and how this is recovered will vary depending on the application on that server. For example, Oracle used by the Branch database in a RAC configuration itself detects that one of the servers has failed, and initiates recovery; the failure of a Branch Access Layer server is detected by the network (which polls the servers) and traffic is directed to the working servers.

For the LAN and WAN, all components are doubled up to provide resilience (and for the WAN diverse routing is used to ensure that a single incident does not break both connections). These are used in one of two ways:

- Active/Active where network traffic is spread across the components. On the failure of one, all traffic is routed through the other.

POL00033119

- Active/Passive where network traffic normally uses one component, but switches to the other on failure.

For both servers and the LAN/WAN there are a number of factors that need to be considered to determine the optimum solution namely cost, complexity, impact of failures and failover time. The approach used for each component of the solution will be determined as part of the design work.

POL00033119

7 Performance and Scalability

This section outlines the volumes that the solution needs to be support and how scalability needs to be supported. Performance targets for specific components will be set as part of the detailed design work.

7.1 Volumes

The volumes that the solution needs to support will be documented in an updated version of "Horizon Capacity Management and Business Volumes" (PA/PER/033).

They are not covered further here.

7.2 Scalability

To ensure that the solution is able to adapt to changing transactions volumes, it is important that it is scalable – both upwards and downwards.

There are two broad approaches to scalability:

- Scale Wide – Where multiple instances of a particular component can be run in parallel and therefore resources can be added or removed by changing the number. An example would be adding more servers to the Branch Access layer.
- Scale High – Where multiple instances cannot be run in parallel and therefore the capability of the component needs to be changed. An example would be a banking agent where the platform can be upgraded to provide more processing power.

In some cases to Scale Wide, application or other infrastructure changes may be required (e.g. more banking interfaces). Where this is the case it is usually more economic to Scale High.

The table below describes the possible scaling strategies for the 3 key components of the system that are performance critical:

#	Area	Scaling Approach
1	Online 3rd Party Interfaces: Banking Debit/Credit Card ETU DVLA PAF	Primary approach is to Scale High providing more processing power for the agent platforms or where a number of agents share a platform to split this across multiple platforms. This avoids needing to change the 3rd party solution. It would be possible to Scale Wide if the number of instances is increased although this is likely to require other changes in the system (e.g. to increase number of Processing Interfaces for banking). For Web Services (DVLA, PAF) where the service is already load balanced across a small number of stateless platforms, scaling wide is a relatively simple option. Reductions in workload are unlikely to result in a reduction in these systems as they are expected to be small servers. The number of platforms is dictated through the security policy and therefore cannot be reduced.
2	Branch Access Layer Servers	Primary Approach is to Scale Wide by adding additional platforms It should also be possible to Scale High by making each platform more powerful although this is likely to be less cost effective.

POL00033119

#	Area	Scaling Approach
		If the workload reduces, this layer can be reduced by removing platforms subject to resilience considerations.
3	Branch Database	If the current servers are not powerful enough then either adding additional platforms or making the platforms more powerful is possible. If the workload reduces then this layer can be reduced by removing platforms or down grading them to smaller servers.

POL00033119

8 Security

8.1 Assumptions

Where the system provides encryption or signing, AES or TDES encryption keys and RSA signing/encryption keys will be used.

8.2 Solution

8.2.1 Security Strategy

The security strategy for HNG-X is risk based and uses the Prevention => Containment => Detection => Response model.

This strategy applies to both infrastructure and software development and provides defence in depth protection to the HNG-X system through the application of layered security controls.

This security architecture has been developed with the aim of ensuring that there are no single points of failure and that each area of risk has more than one technical or management control working together to mitigate that risk.

Item	*Description*
Prevention	Use a combination of security controls such as physical, network, platform and application access control, system hardening and vulnerability management to reduce vulnerability.
Containment	Constrains the spread of malware or malicious activity using various techniques and controls such as network segmentation, anti-malware controls and physical, network and platform access control.
Detection	Quickly detect the presence of malicious activity or malware in any domain of HNG-X through the use of anti-malware, intrusion detection and security event management controls.
Response	Automatic or manual incident response to mitigate the activity using pre-configured activities, intrusion prevention and incident response procedures.

To reduce complexity and implementation times, the approach taken for security applications and services is to use internal Fujitsu services when appropriate and to buy and integrate COTS products rather than develop them internally.

Specific exceptions to this rule have been made in the area of cryptography and key management where the Horizon solution has been redeveloped for the cryptographic API, (referenced in DES/SEC/HLD/0002), and a key management solution has been developed in the absence of commercial alternatives.

8.2.2 Principles

A set of principles must be established to guide the secure design, development, test, implementation and operation of the HNG-X system. These principles must be;

- Balanced between the 'text book' view of Information Security and the business requirements of the HNG-X system
- Carefully considered

POL00033119

- Objective

The extent to which each principle should be applied is decided through risk assessment, with controls being selected and implemented based on the identified vulnerabilities, threats and risks.

The controls themselves can be chosen from a wide range including policy and procedure, standards, guidelines, management controls such as staff vetting and technical controls.

Item	Description
Principle 1	Use a risk-based approach
Principle 2	Least privilege access control
Principle 3	Detect anomalous activity
Principle 4	Maintain systems
Principle 5	Ensure compliance
Principle 6	Defence in depth
Principle 7	Reduce security by obscurity
Principle 8	Fail secure
Principle 9	Simple is good
Principle 10	Close the loop

These principles are explained in more detail in the HNG-X Security Architecture document ARC/SEC/ARC/0003.

8.2.3 Tiers and Domains

To reduce the likelihood of a compromise and to ensure that a compromise of one Platform Instance does not immediately result in the compromise of the entire estate and campus, a security tier and domain model has been created. This model groups together platforms based on type, perceived vulnerability and risk rating.

It is a pragmatic model and therefore some groupings have been made on the basis of expediency rather than from a purist information security viewpoint.

There are three tiers in this model, adopting the standard architecture for web applications, with the most exposed platforms in Tier 1 and the least exposed in Tier 3. Exposed, in this context, means the type of connection the platform instance has with the outside world, (if any)

8.2.4 Security Tiers

There are three tiers defined in this architecture, which are used to specify the security rules and requirements that apply to systems in each tier.

Tier	Description
Tier 1	Systems that directly connect to or from an external entity such as Link, Streamline, Royal Mail or other third-parties, or are in an environment considered to be 'hostile'. This includes the Branch and the Internet. Systems in this Tier must be hardened to a standard compliant with the HNG-X Information Security Policy {SVM/SEC/POL/0003}. Systems in this Tier must be patched in accordance with the HNG-X Information Security Policy {SVM/SEC/POL/0003}.

POL00033119

Tier	Description
	Inter-domain communication is not permitted.
Tier 2	Systems that are on a secure network and have a secure build. Systems in this Tier must be hardened to a standard compliant with the HNG-X Information Security Policy {SVM/SEC/POL/0003}. Systems in this Tier must be patched in accordance with the HNG-X Information Security Policy {SVM/SEC/POL/0003}.
Tier 3	Systems that do not connect externally, (other than through an agent or other proxy), and are only accessed through a management server. These systems are generally those that are on the Data Centre network. Systems in this Tier must be hardened to a standard compliant with the HNG-X Information Security Policy {SVM/SEC/POL/0003}. Systems in this Tier must be patched in accordance with the HNG-X Information Security Policy {SVM/SEC/POL/0003}.

8.2.5 Security Domains

There are a number of defined security domains with the HNG-X security model; therefore data traffic will always be either intra-domain traffic or inter-domain traffic.

- Intra-domain traffic – Data traffic moving between systems in the same domain.
- Inter-domain traffic – Data traffic moving between systems in different domains.

There is a third class of traffic consisting of data moving into and out of the HNG-X infrastructure.

Intra-domain traffic may be unrestricted because the systems share a LAN segment, or may be restricted through the implementation of logical separation, (using VLANs), or physical separation, (using separate network segments in the same domain).

Inter-domain traffic must pass through an enforcement point that restricts data flow based on its source, destination, protocol, port, type or content/format. This can be a firewall, router or other in-line control point, such as an IPS system. (i.e. The control is physically part of the data path)

There can be multiple Security Domains in a Tier, but there can only be one Tier per Security Domain. This is because the rules defining what is allowed and what is restricted apply to a Tier, therefore they have to be consistent and it is not possible to have a security domain partly in Tier 1 and partly in Tier 2

A network segment however, whether it is a logical or physical network segment, must be entirely in a domain and cannot span domains. There is no restriction on the number of network segments, firewalls or other network security controls that can be in a security domain.

For example, in the Client Agents Domain, each Banking Agent can be separated from every other Banking Agent through the use of physical separation, using firewalls or separate LAN segments, or through the use of logical separation using VLANs. This is dependent on the requirements of the contract with the external party.

The security domain model can therefore be viewed as a method of logically grouping network subnets.

Domains can also span physical locations. For example, the Key Management Domain contains Data Centre systems as well as workstations in remote locations such as Bracknell and Lewes.

POL00033119

In the event that a database or application, nominally in one tier, shares a platform with another database or application in a different tier, then the most restrictive set of permissions shall apply. This is particularly relevant to the Solaris Main Host that supports a number of Oracle Databases, some of which contain cardholder data and some of which don't. The Solaris Main Host has therefore been placed in the Core PCI-CE Domain in Tier 3, despite the fact that a number of Databases hosted on it do not store Cardholder Data.

The use of this domain model ensures that network segmentation can be implemented to tightly control communication to, from and between HNG-X platform instances.

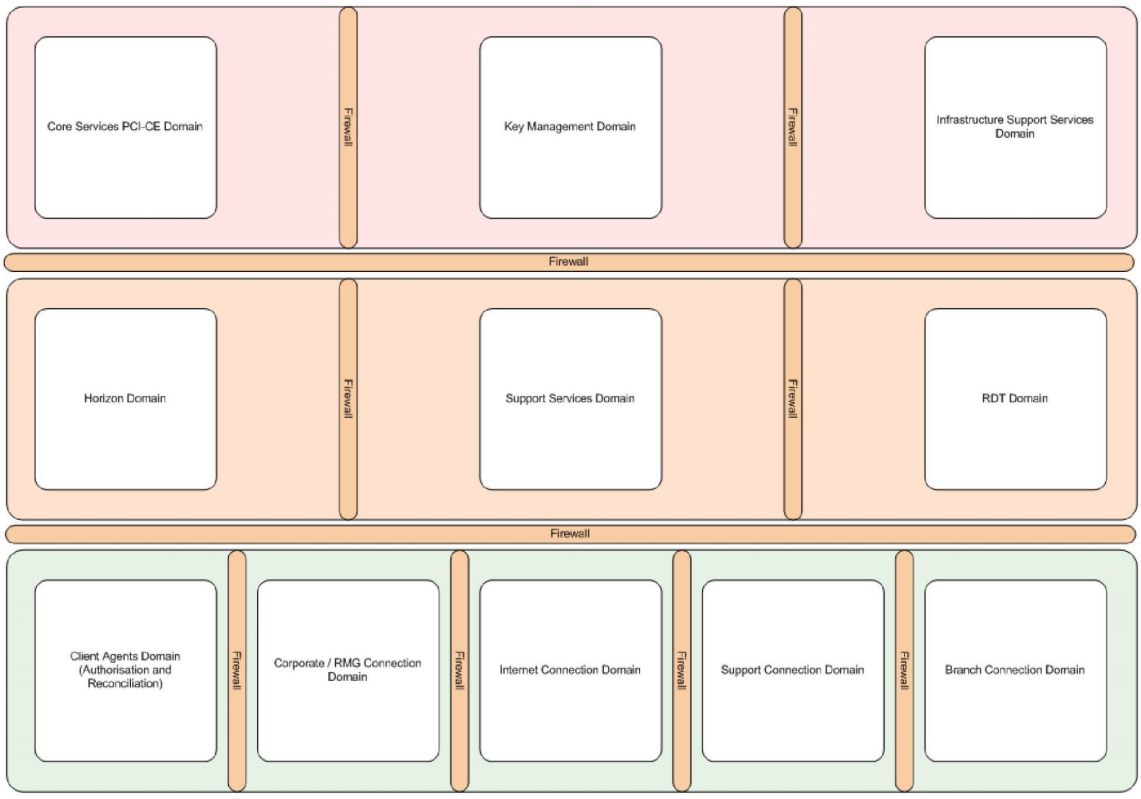


Figure 10 - Security Tiers and Domains

The domain model is an overlay for each environment. This means that there is no need for separate Test domains to be added to the model, as each test environment, (ST, V&I, SV&I, RV Mig, RV Acc, VOL, LST), will overlay the security domain model in the same way as it is overlaid onto the Live environment.

Separation between environments is controlled using a combination of preventive and detective controls such as access control, firewall rules, BladeFrame configuration, switch configuration and event monitoring.

The HNG-X Platform Hardware Instance List {DEV/GEN/SPE/0007} contains a definitive mapping of platform instances to security domains.

POL00033119

8.2.6 ISO27001 / PCI

The solution has been architected using the control objectives in ISO27001 as a guideline. In addition, an ISO27001 Information Security Management System (ISMS) is being implemented as part of the operational security management process.

The solution also meets the requirements imposed on Fujitsu by Post Office Ltd in relation to the Payment Card Industry Data Security Standard.

A security policy document has been written (SVC/SEC/POL/0003) that covers the correct operation and management of the HNG-X system.

8.2.7 Security Services

8.2.7.1 Data Integrity and Confidentiality

The HNG-X system makes extensive use of cryptography and digital signatures for the protection of data, both in storage and during transit.

Messages from the Counter to the Data Centre are protected by a combination of the retained Utimaco VPN from Counter to Data Centre and the use of SSL from the Java virtual machine on the Counter, to the Data Centre. These transaction messages are also digitally signed using a non-managed session key, created at Counter user logon, the Public Key portion of which is then sent to the Data Centre and signed by a managed signing key.

Connections to third parties are protected through the use of encryption where the contractual agreement requires it.

The approved cryptographic algorithms, associated key lengths and data retention periods are covered by the Security Architecture (ARC/SEC/ARC/0003).

In accordance with CCN1202 which described the requirements for the PCI Data Security Standard, a number of approaches are adopted in the solution for the protection of Sensitive Authentication Data and Cardholder Data.

In regard specifically to Card PANs

1) The first 6 and the last 4 characters will be in clear. The remaining characters will be overwritten using a character such as 'x' as a replacement for each character. This algorithm is used for all 13-19 digit PANS.
    a) For Example: *1234567890127890* will become *123456xxxxxxxxx7890*
    b) For Counter receipts, this will be printed in the form *xxxxxxxxxxxx7890* as per Visa and MasterCard requirements.
2) The first 6 and the last 4 characters will be in clear. The remaining characters will be replaced with the equivalent number of characters from a base 64 hash of the PAN and a seed value. The first character of the hash characters will be a non-numeric character to facilitate the distinction between hashed and non-hashed PANs.
    a) e.g. *123456Yg20xAWIE7890*
3) The PAN will be encrypted.

Banking, Debit and Credit Card transactions will be processed, transmitted and stored using the mechanisms described above.

POL00033119

- Option 1 will be used for writing to log files, receipts, or for report files when the details of the PAN are not required.
- Option 2 will be used for the storage of the PAN where it is **not** necessary to obtain the clear-text PAN.
- Option 3 will be used for the storage of the PAN where it is necessary to obtain the clear-text PAN. Systems using this option are considered to be part of the Cardholder Environment.

The algorithm to produce the hash from the PAN will be implemented within each application that needs to use it and will use a seed value to provide extra strength to the algorithm. The seed value will be a randomly generated 80 bit value, which will be concatenated with the PAN to make a dictionary-style attack much more difficult.

Network connected hardware security modules (HSM) will be deployed to perform encryption and decryption of authorisation messages and data used for the creation of reconciliation files. These modules are Atalla 10150 and 8150 NSPs (Network Security Processor) from Hewlett Packard. Access to the HSM will be tightly controlled by the implementation of firewall rules, restricting communication to the authorisation agents and the reconciliation platforms only. Monitoring of the HSMs is done by the SYSMAN3 system, but uses a different port to that used for transaction processing.

A Key Server / Key Client will be implemented to manage the distribution of key material throughout HNG-X. Keys themselves are encrypted under a Key Server master public key and are stored in the Network Persistent Store (NPS) database. Communication between the Key Client and the Key Server is protected through a combination of firewall rules and the use of a RSA public/private key exchange.

Key management for the Identity and Access Management service is done automatically by the system, however there are manual authorisation steps, performed by the CS Security Team, that ensure that all user access is tightly controlled and monitored.

Key management for the interface with Financial Institutions is a largely manual process and will be conducted in HNG-X as it is in Horizon. This is a well understood process that is performed a number of times every year for the replacement of key material.

8.2.7.2 Identity and Access Management

There is a significant change between Horizon and HNG-X as the authentication of users is now performed by a directory service. This includes UNIX and Linux operating systems as well as Microsoft Windows. This is achieved using Active Directory as a master directory service with the implementation of a pluggable authentication module (PAM) onto non-Microsoft platforms. This enables the non-Microsoft platforms to appear as objects in Active Directory and facilitates access management from a central point.

All users of the HNG-X system will be individually identified, through a process controlled by the CS Security Team. Every administrative user will use strong two-factor authentication when logging on to the system and it will not be possible to directly access any HNG-X system without such a token.

Non-administrative user's access to the HNG-X system will be controlled through applications (such as Tivoli) and will not have direct access to underlying platforms.

All access into the HNG-X system that is non-application controlled (i.e. is interactive) will be provisioned through the deployment of a number of systems administration servers (SAS Servers). These servers act as a control point for all interactive access into the HNG-X system. The SAS servers will be sited in a dedicated DMZ in each Data Centre with firewall rules in place to control the access each server has to other platforms. Access to the SAS servers for support purposes is via encrypted RDP sessions from a workstation or remote support laptop.

Third parties can also use this support route on creation of a dedicated user for the purpose. An exception to this is the deployment of the EMC Secure Remote Support Gateway platform (RSG) which

POL00033119

is a dedicated support platform for storage hardware and software. This will be sited in a dedicated DMZ with network access restricted to storage equipment only through the use of firewall rules and functionality available to users of the RSG controlled through the use of a dedicated policy server.

Application and database access will be controlled by the application or database itself. However, from a support perspective, to access an application or database requires that the user has already authenticated using strong authentication. The management of such users will be a manual process, performed by the relevant support groups and overseen by the CS Security team.

Users of the Counter business application will be access-controlled via tables in the Branch Database. Access to the underlying Counter operating system (Windows NT4) will continue to be controlled as in Horizon with local administrative users on each Counter.

8.2.7.3 Event Management

Event monitoring and management will be deployed to ensure that security related events are used for incident response and reporting. These events will be captured, forwarded, alerted from and stored by the Tivoli event management system.

"Events of interest" will be identified and will raise alerts when they are detected. The Fujitsu service desk will deal with each incident on the basis of a pre-prepared list of actions.

The list of events that are considered to be "interesting" will be fine-tuned during the development, testing, pilot and live operation phases of the programme.

In addition to the alerting process, longer term trend reporting will be implemented and detailed analysis of event data will take place for the purposes of improving the service and identifying potential security weaknesses.

Log information from all platforms will be captured by the Tivoli system. This includes logs from the Counter, logs from network devices (via the implementation of a syslog server) and logs from all Data Centre platforms.

8.2.7.4 Vulnerability Management

Through the implementation of a comprehensive vulnerability management process, the risk of successful attacks by malicious individuals or through the use of malicious code will be reduced.

The vulnerability management process has multiple strands, consisting of vulnerability scanning and assessment, anti-malware, patching and system hardening.

Vulnerability scanning will be performed on a regular basis using a combination of external and internal scanning by both the Fujitsu CS Security Team and by third parties. This process will ensure that the existence of any known vulnerabilities is identified and quickly resolved.

Sophos anti-virus software will be deployed, within the Data Centre, on all platforms running a Microsoft operating system. This software will be regularly updated and will detect spyware in addition to viruses, Trojans, worms and other malware.

Patching will be conducted on a regular cycle and will be scheduled to ensure the most vulnerable systems are patched first. Vulnerable in this context means those systems with a connection to a public or third party network.

System hardening is also implemented to reduce the levels of potential vulnerability in the HNG-X system. The Microsoft security configuration tool with the Bastion Host template has been used to harden the Windows 2003 platform foundation. For the purposes of a platform foundation, the Solaris and Red Hat Linux platform foundations are considered to be sufficiently robust through the standard installation. Even here however, unnecessary software has been removed and the security settings adjusted to provide extra resilience to attack.

POL00033119

In addition to the system hardening process, there are multiple levels of security control within the HNG-X system and therefore additional hardening is not considered to be necessary. Where additional hardening is required it will be identified through risk assessment and adjustments made to the platform type as necessary.

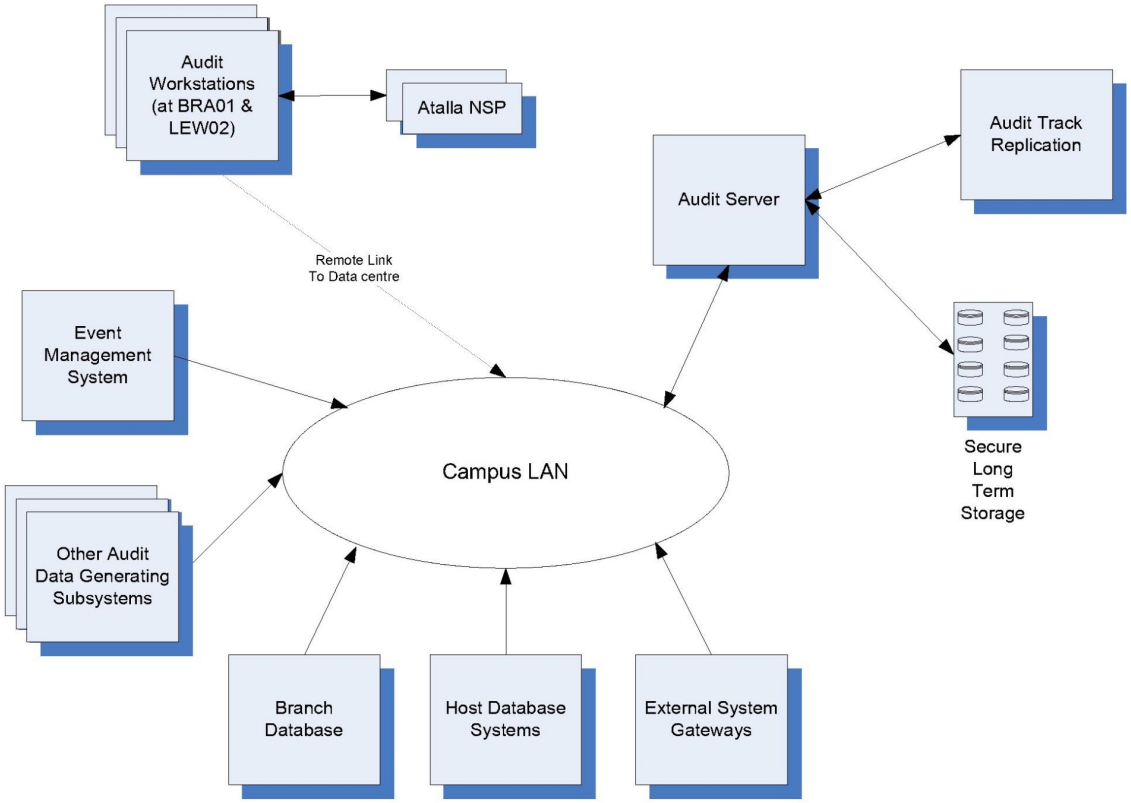
8.2.8 Security Measures Considered but not Justified

It has been agreed with Post Office that there is insufficient justification for the following security measures:

#	Control Name	Justification
J1	AV on counters	AV on the counters is expensive and of limited value as there is no easy infection method
J2	Special controls on mobile equipment	Combination of application username/password, network controls router firewalls and IDS are felt to be sufficient for the small number of such devices currently in use. However the threat assessment should be reviewed as part of the rural program as the number of such devices increases.
J3	Encryption on network connections between the two Data Centres	The connections are high speed (Gbit/s) point to point connections.
J4	Encryption of online transactions for credit/debit cards to Streamline	Streamline doesn't support encryption of this traffic
J5	Encryption of counter disks	Transaction data no longer held in counter.
J6	General encryption of any sensitive data within the databases at Data Centre	Access controls and physical security provide sufficient protection.
J7	Encryption of network for online authorisations to DVLA	Not supported by DVLA

POL00033119

8.3 Audit



The Audit system is responsible for gathering Audit Tracks generated by other subsystems and securing them on the local Centera array. This data is subsequently replicated to the Audit Server at the other date centre to ensure that two copies of all Audit Tracks are maintained.

As well as gathering and storing audit data on EMC Centera, the Audit Server provides services to retrieve data from the Audit Archive. These services are utilized by the Audit Workstations.

The Audit Workstation provides facilities for authorised Fujitsu Services staff to securely access the Audit Server in order to retrieve Audit Track data from the Audit Archive and to either select or prepare Audit Track data for presentation to Post Office or in support of internal audit activities. The Audit workstation is dedicated to this task & provides no other services.

POL00033119

9 Training

9.1 Assumptions

The HNG-X solution will support training from CTO (Counter Training Offices) based on the following assumptions.

1. The need to have a solution that looks and behaves in a very similar way to the Live system (i.e. not script based – though scripts will be used to provide a simulation for some internal and external clients).).
2. As new products etc are introduced, that the solution is updated to ensure the training is relevant. This may include AP-ADC transactions or products that require software changes.
3. Post Office will allocate Branch codes within the Live estate that will be dedicated for CTO use only. This will require full management of CTO Branches within the Estate Management and Reference Data system.

9.2 Solution

The main features of HNG-X training solution are shown in the diagram below:

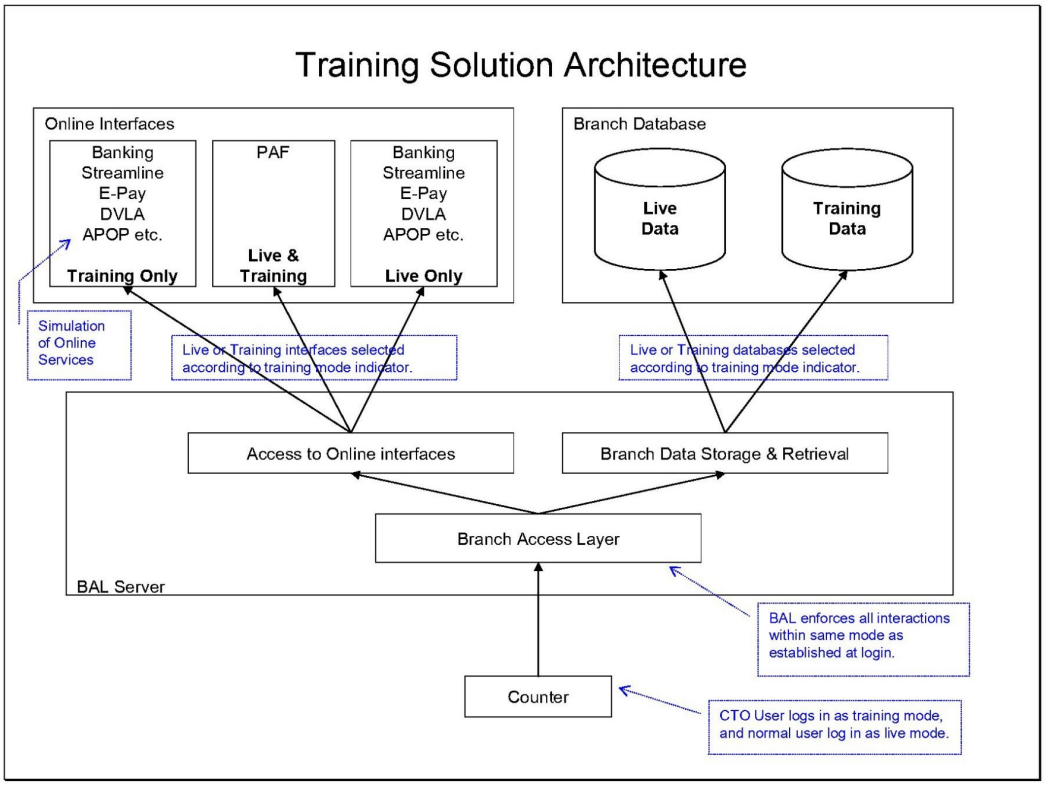


Figure 11 – Training Solution Architecture

POL00033119

The Training solution will share the Data Centre elements of the solution with the Live service.

CTO Branches will be created as "standard Branches" within the Live estate. They will have their own Branch Code (aka FAD Code) which indicates that they are Training Branches.

These Branches are connected to the Live Data Centres through the standard network connections. Mobile CTOs would be handled in the same way as normal mobile Branches (e.g. need a network connection). However, some Mobile CTOs are "multi-counter" and so will require a portable hub to connect the counters to a single branch router

CTO Branches will be managed as "standard Branches". Faults and failures of equipment will be handled through the standard break-fix service. Updates to the Reference Data (including Bureau spot rates and margins) for CTO Branches would happen automatically as the Reference Data for Live Branches is changed. Updates to code in the CTO Branches would happen automatically as the code is changed for the Live system. The CTO Branches will see the real help pages for the solution and pick up any changes.

The counter will operate with the standard HNG-X counter hardware, including agreed mobile solution. The standard peripherals will be supported for the CTO hardware including the following peripherals: Touch screen, Bar Code reader, Horizon Keyboard, Counter Ithaca Printer, Training PIN Pad. The training counters will be connected by LAN through the shared single Branch router, and there will be a shared back office printer.

Each CTO counter training session will run in its own virtual office – even though there are multiple counters within a CTO Branch.

The "training service" comprises the counter software, application server layer, Branch database and simulators for online components. There is a facility that can be used by the trainer to reset the "training state" of a counter back to a default state. The "training service" will only be available from CTO Branches.

There will be separate services to simulate online interfaces where appropriate. Note that the diagram above only provides examples of the services for which simulation is available – fuller details are provided in the relevant design specifications. Some services (e.g. PAF) will be shared between Live and Training. The system will operate as the Live system with the exception for the pre-defined simulation responses.

The training part of the Branch database holds the training transaction data. Reports will reflect transactions performed during the training session and Stock levels reported will be adjusted accordingly.

All capabilities will be supported as per the current Live Reference Data for that Branch. Post Office will be responsible for ensuring that any products that must not be used within a CTO are not available within the Reference Data.

A more complete description of the solution for Counter Training Offices is contained in ARC/SOL/ARC/0005.

9.3 Security

The following points describe the security controls for the training solution in CTO Branches.

- Each CTO Branch is treated as a standard Branch from a network/physical perspective.
- The CTO hardware build and associated security controls are as for any other Live counter.
- Application control (defined centrally) dictates that the Branch is a CTO Branch.
- At logon, a User Session is established using the same technical controls as for Live Branches. This session will be "marked" as a training session. All further communication between counter

POL00033119

and Data Centre is protected by the standard session controls which will include the training marker.

- The Branch Access layer will ensure that all online requests are handled as Live or training mode as appropriate. Strong controls will be in place to ensure a clean separation of services used.
- The PIN Pad used in CTO Branches has a training key. Transactions performed with these PIN pads would be rejected by the Live Banking online services.
- The training data will be cleanly separated from the Live data within the Branch database, so there is no risk of leakage. The training marker on the session will indicate where transactions are to be stored within the Branch database.
- The Training "marker" will also be stored with the transaction data within the Branch database.
- Training data will not be passed to external clients, Post Office systems or the audit stream.

POL00033119

A Appendix A – Mapping to BCSF

The following table provides a mapping between the architectural components described in Figure 4 within Section 2 and the BUSINESS CAPABILITIES AND SUPPORT FACILITIES described in Sub-schedule B3.2. The counter architecture is described in section 2.1.

BUSINESS CAPABILITIES AND SUPPORT FACILITIES	How supported by architecture
Point of Sale Capability	Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service.
In / Out Payment Capability	Counter, Branch Session Management, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service.
APOP Facility	Counter, Branch Session Management, Internal Online Services, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service.
Banking Capability	Counter, Branch Session Management, External Online Services, Branch Data Storage & Retrieval Services, Enquiry Services, Batch Services and Reference Data Service.
DVLA Licensing Capability	Counter, Branch Session Management, External Online Services, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service
Electronic Top-Up Capability	Counter, Branch Session Management, External Online Services, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service.
Bureau de Change Capability	Counter, Branch Session Management, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service.
Postal Services Capability	Counter, Branch Session Management, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service.
Payment Management Capability, cash, cheque, vouchers	Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service
Payment Management Capability, Debit or Credit Cards	Counter, Branch Session Management, External Online Services, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service
Cash and Stock Management Capability	Counter, Branch Session Management, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service
Branch Management Capability Stock unit balancing	Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service
Branch Management Capability Branch accounting	Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service
Branch Management Capability printing of Client summaries	Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service
Branch Management Capability	Counter, Branch Session Management, Branch Data

POL00033119

BUSINESS CAPABILITIES AND SUPPORT FACILITIES	How supported by architecture
Branch reports	Storage & Retrieval Services and Reference Data Service
Branch Management Capability Reversals and Refunds	Counter, Branch Session Management, External Online Services, Internal Online Services, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service
Branch Management Capability Transaction Corrections	Counter, Branch Session Management, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service
Branch Administration Facility User log on / off	Counter, Branch Session Management.
Branch Administration Facility User / password management	Counter, Branch Session Management, Branch Data Storage & Retrieval Services
Branch Administration Facility Stock Unit creation / allocation	Counter, Branch Session Management, Branch Data Storage & Retrieval Services Batch Services
Branch Administration Facility provision of secure inactivity time-out facilities	Counter, Branch Session Management
Branch Management Capability generic User help system	Counter, and Reference Data Service
Branch Support Facility Sales Prompts	Counter, and Reference Data Service
Branch Support Facility Bulk Input of transactions.	Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service
Transaction Management Facility (TES)	Enquiry Services
File Management Facility	Batch Services
Reference Data Facility	Reference Data Service
PAF Facility	Counter, Branch Session Management, Internal Online Services
Message Handling Facility	Counter, Branch Session Management, Branch Data Storage & Retrieval Services
Audit Facility	Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Support Services
Reconciliation Facility	Data Transformation & Summarisation and Batch Services
Training Facility	Counter, Branch Session Management, Internal Online Services, Branch Data Storage & Retrieval Services and Reference Data Service

POL00033119

B Appendix B: Mapping to Infrastructure documents

The following table provides a mapping between the architectural components described in this document and Sub-schedules B3.3 and B3.4.

HNG-X INFRASTRUCTURE	How supported by architecture
Branch Infrastructure	The Branch Infrastructure is described in section 3.5.
Central Infrastructure	The central Infrastructure is described in section 3. The DR capability and the use of the DR site for testing is covered in section 6.2.
Branch Telecom Infrastructure	The Branch network Infrastructure is described in section 4.3
Central Telecom Infrastructure	The central Telecom Infrastructure for the Data Centres and intercampus is described in section 4.1 The client and Post Office WAN is described in section 4.2.1 The Support WAN is described in section 4.2.2 Testing access is described in section 4.4.
Security	Security is described in section 8
Business Continuity	Business continuity is described within section 6