Document Title:	Horizon Solution Architecture Outline
Document Reference:	ARC/SOL/ARC/0001
Release:	N/A
Abstract:	This document describes the ~~target~~ Solution Architecture for the Horizon system. 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~~ Draft This document contains text (as listed in section 0.4) 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,~~ Torstein Godeseth (last update) , Requirements, Solution Design & Architecture Contributors: Pete Jobson, 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.
External Distribution:	
Information Classification:	See section 0.9 for details.

Approval Authorities:

Name	Role	Signature	Date
~~Torstein Godeseth~~Simon Wilson	~~Chief Architect~~Fujitsu Post Office Account CTO	See Dimensions for record	
~~Adrian Eales~~Sally Rush	Post Office Ltd ~~Domain CTO - Retail~~Horizon Chief Architect		
~~Dionne Harvey~~Rajivsinh Rathod	Post Office Ltd Head of IT Contract Management		

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.

0 Document Control

0.1 Table of Contents

LIST OF FIGURES

LIST OF TABLES

0.2 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 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	N/A

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		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.	
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 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.	CP4305 CP0010 CP0022 CP0031 CP0065 CP0077 CP0098 CP0136 CP0140 CP0172 CP0304 CP0330 CP0342
4.2	2nd Aug 2010	Updated following comments	N/A
5.0	2nd Aug 2010	Issued For Approval	N/A

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
5.1	18-Aug-2011	Updated template and preliminary revision to reflect post roll-out status.	
5.2	23-Aug-2011	Updates to Horizon Release 5.0. Including the incorporation of changes for the following change proposals: CP0367- Implementation of Transaction Acceptances (PING) CP0409 - Changes for LIS5 2008 CP0461 – Link PCI and Accreditation (Amendment to CP0409/CT0815) CP0487 – POLSAP Interfaces CP0491 - AEI Near Real-Time Development CP0492 - POca Card Fulfilment Service development CP0502 - HNG-X Changes for A&L PCI Compliance CP0506 - Deployment of Configuration managed DXC builds. CP0545 - DXI SSL Scanning CP0565- (To remove the Horizon OMDB Server from the Horizon Online environment) CP0633 – Implementation of PAF Replacement Service	See Summary
5.3	30th July 2013	Minor updates following responses to comments	
6.0	30th July 2013	Base-lined	
6.1	21st Jan 2015	Update Platforms and Storage to include Belfast Refresh changes to HNG-x	
6.2	3rd Feb 2016	Change Streamline to GlobalPayments (CP0631) Implementation of Post Office Data Gateway Change from A&L to Santander Channel Integration, introduction of POMS Switch and Horizon Business Server AMEX as a method of payment Generic Pass-through HBS -> CDP Collect & return and Access Point Paystation Barcoding all parcels RDT PODG to replace DXC Horizon Anywhere	CP0631 CP0659 CP0688/701 CP0699/743/759/764/800/887/998/1026 CP1089/1143 CP1194 CP0882/1472 CP1519 CP1543 CP1653
7.0	7th Apr 2016	For Approval	
7.1	30-Oct-2018	Removal of references to Moneygram	CT2543a (to be ratified by CCN1648)
7.2	20-Feb-2020	CP1941 – EUM Full Implementation CP1955 – Credence to Azure Cloud CP2039 – Horizon to CFS Implementation CP2099/2106/2123/2241 – HNGT Lite CP2102 - POLSAP to TransTrack Migration Phase 2 CP2118 - Replacing POLSAP Interfaces with Equivalents from CFS	CT2251 CT2239 CT2284 CTs2408 / 2418/ 2441 / 2566 / 2573 CT2372 CT2456

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		CP2229 - POLSAP to TransTrack Migration Phase 3	CT2548
		CP2242 - POLSAP Application Separation	CT2561 / CCN1655
		CP2355 & CP2367 – Flexible cash planning interfaces to Arrow	CWO0063 / CWO0074
		CP2270/2318 – Agent Portal/BDAS	CT2601 / CT2636 / CCN1658
		CP2304 – Decommission HNG-X Components	CWO0095
		CP246~~8~~9 – Belfast Exit (Remove APS/TPS) R20.55	CWO0180 / CCN1669
7.3	18-Mar-2020	Dave Haywood:	CT1848
		Reviewed security content.	CP2304 / CWO95
		CT1848 Horizon Data Centre Refresh	
		CP2304 Decommission HNG-X Components	
		Change SSL references to TLS	
		Remove references to Utimaco VPN	
		Change counter OS to Windows 10	
		Add Windows 10 and Windows 2012 R2 to server types	
		Update security section	
7.4	20-Mar-2020	Updates to Section 4:Network Services to describe Verizon MPLS.	CT2543 (to be ratified by CCN1648)
7.5	25-Mar-2020	Updated following Comments	
7.6	29- Apr-2020	Updated following further comments. GDPR added.	
8.0	19-May-2020	Approved	
8.1	30-Jun-2023	Introduced Post Office Cloud as part of the environment for HNG-X.	CCN1678
		Added Self-Service kiosks and Connected Devices (HIH) as part of the environment for HNG-X	
		Introduce Apache Camel and JBOSS as technologies in use.	
		Introduction of PBS and resulting changes to the architecture.	CWO0230 / CCN1672
		General tidying of the document to reflect the current environment.	
8.2	27-Sep-2023	Revisions following internal review.	

Commented [POL1]: CCN1678 refers to this document: "This document to be reviewed and updated to recognise the shift in responsibilities from Fujitsu Services to Post Office, for security of the Post Office Cloud hosting infrastructure and provision of foundational security mechanisms, for those elements of the HNG-X System migrated to Post Office Cloud"

Need IT Architects/Cloud Engineers to review and approve

Commented [POL2]: CCN1672a - Introducing the Payment and Banking Service into the Agreement

0.3 Review Details

Review Comments by :	
Review Comments to :	Torstein Godeseth & Post Office Account Document Management
Mandatory Review	
Role	**Name**
Business Architecture: Counter	Steve Porter
Business Architecture: Host Batch Systems, NPS	Pete Jobson
Business Architecture: Scheduling and Time Sync	John Bradley
Network Architect	Ravi Saini; Steve Freke
Security Architect	Dave Haywood; Stephen Wallis

Storage Architect	Gareth S Jones <GRO>
Service Architect	Phil Boardman
POL Horizon Chief Architect	Sally Rush <GRO>
Optional Review	
Role	**Name**
POL Head of IT Contract Management	Rajivsinh Rathod <GRO>
POL IT Document Specialist	Steven Vouthas <GRO>
POL Security Architect	Dave King <GRO>
POL Lead Solution Architect	Bob Booth <GRO>
POL Solution Architect	Dmitry Barsukov <GRO>
POL Solution Architect	Krishna Kumar Paramasivam <GRO>
Business Architecture: Crypto, Web Svcs	Colin Simpson; Rajni Doel
Business Architecture: Host Ref Data, Branch DB, RDT, APOP	Gareth Seemungal
Business Architecture: TWS	Shaun Wood
Business Architecture: Estate Management	Dave McLaughlin
Business Architecture: Counter/BAL	Jon Hulme; Paul Braisher; Geoff Haydock
Business Architecture: File Transfer, Audit	Gerald Barnes
Business Architecture: PODG	Susan Brindley; Sandip Patil
Business Architecture: HBS, SSK	Paul Braisher; Andy Kendrick
Business Architecture: Agent	Adrian Barclay
Solutions Architecture and Business Requirements	Steve Evans; Kevin Stothard
CISO	Steve Browell
CTO	Simon Wilson
Service Architecture Manager	Alex Kemp
Network Operations Manager	Chris Harrison
Business Continuity	Sidharth Singh
Security Operations Team	CSPOA.Security GRO
Network Architect	Shubhashish Bhattacharya
Systems Management, Integration & SCM Manager	Jerry Acton
Infrastructure Operations Manager	Andrew Hemingway; Rob Tickner
Test Delivery Manager	Joan Duhaney
Test Manager	Mark Ascott
SSC Manager	Adam Woodley; sscdm GRO
Release Management and Operational Change Manager	Tomi Okelola
Senior Programme Manager, HNG-X	Jon Dowell
Information Security Management	Farzin Denbali; Chris Stevens
Unix Team	Andrew Gibson
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	**Name**

Note: See POA Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

(*) = Reviewers that returned comments

0.4 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

0.5 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	~~1.0~~	~~13/6/06~~	Fujitsu Services ~~RMGA~~POA 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 - Counter Training Offices Dimensions	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
DES/APP/STD/3433			HNG-A UI Style Guide	Dimensions
DES/SEC/HLD/0002			HNG-X Crypto Services HLD	Dimensions
DEV/GEN/MAN/0003			HNG-X UI Construct Catalogue	Dimensions
DEV/GEN/SPE/0007			Platform Hardware Instance List	Dimensions
PA/PER/033			Horizon Capacity Management and Business Volumes	Dimensions

Reference	Version	Date	Title	Source
SVM/SEC/POL/0003			POA Information Security Policy	Dimensions
SVM/SEC/REP/3936			Post Office Account GDPR One Trust Assets	Dimensions
SVM/SEC/REP/3954			Post Office Account GDPR One Trust Processing Activities	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.

0.6 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.~~
~~AEI~~	~~Application, Enrolment and Identity~~
Amex	American Express Card suppliers and transaction clearing house
AP-ADC	Automated Payment – Advanced Data Capture
API	Application programming interface
APOP	Automated Payment Out-pay
APS	Automated Payments Service
Arrow	A system managed by Accenture that supplements CWC in the forecasting of cash stocks across the estate.
AWS	Amazon Web Services. AWS is used for Post Office Cloud.
Bladeframe	An alternative term for the Fujitsu Primergy BX900 Chassis Blade Server
Branch	A post office or any other location where Post Office (whether directly or by means of Agents) transacts business with Customers Within the Horizon 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 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. Following ~~stringent PCI rules,~~the introduction of PBS the only cardholder data data that is retained is the ~~encrypted~~truncated PAN and ~~hashed versions of the~~tokenised PAN
~~Cashman~~	~~Budman and Cashman are two MS Access based systems used in Cash Centres~~

Abbreviation	Definition
CDP	Common Digital Platform. A system that provides a number of on-line services to satisfy the needs of some AP-ADC scripts. The system is delivered and supported by Accenture.
CFS	Core Finance System that delivers Branch Ledgers and Client settlement functions
~~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.~~
Credence	See POL MIS
~~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
CWS	Collect and Return Service.
CWC	Cash Web Community. Software systems delivered by Transtrack for cash planning and tracking
~~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 service introduced as part of network banking. Its main component is a 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~~
DXI	Internet Data Exchange Proxy. The DXI provides a facility to transfer information to and from the Internet domain in a secure manner. It provides TLS interception and AV/AVM scanning if required.
~~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.~~
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).
Eternus	Fujitsu Storage Solution
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.
~~Forgerock~~ForgeRock	ForgeRock is a multinational identity and access management software company headquartered in San Francisco, U.S.A. The company develops commercial open source identity and access management products for internet of things, customer, cloud, mobile, and enterprise environments. POL's Forgerock system is delivered and managed by Accenture
FAD	A unique 6 digit code assigned to a Post Office Branch by Post Office. A 7th digit is sometimes added as a check digit. The check digit can be numeric or "X"'

Abbreviation	Definition
	Acronym for Financial Accounting District
FAD Hash	A number generated by passing the FAD through a hashing algorithm and used to assign branches to a specific partition in the Branch Database. A given FAD will always generate the same FAD Hash value. There are 128 possible values to the FAD Hash.
FS	Fujitsu Services
GDPR	The **General Data Protection Regulation** (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. Since Brexit a UK variant has been introduced which differs in minor ways from the EU version.
GlobalPayments	Merchant Acquirer for Payment Transactions
~~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~~UTC (Coordinated Universal Time).
~~GSM~~	~~Global System for Mobile Communications~~
~~HAW~~	~~Horizon Anywhere~~
HBS	Horizon Business Server
~~HDD~~	~~Hard Disc Drive~~
~~Horizon~~HIH	~~Post Office branches are supported by a set of IT systems known as "Horizon".~~Horizon Integration Hub
HNG	Horizon Next Generation – a project that replaced the message-based Horizon solution with an on-line Horizon solution.
HNG-A	Horizon Anywhere. This is the replacement for the HNG-X counter using Windows running the original HNG-X counter Business Application and using the same peripherals.
HNG-X	Horizon Next Generation – Plan X. HNG-X was a project that replaced the Horizon message-based branch network with the Horizon on-line branch service. All references to HNG-X within this document refer to the Horizon On-line service.
HSM	Hardware Security Module, an appliance used for certain cryptographic services.
IDS	Intrusion Detection System
IPS	Intrusion Prevention System. IPS is not deployed currently.
~~ISDN~~KB	~~ISDN, which stands for Integrated Services Digital Network, is a system of digital phone connections which has been available for over a decade~~Knowledge Base – records information about the system useful to Operations in understanding how the system behaves.
KEL	Known Errors Log. Note that 'KEL' is no longer used. See KB above.
Kiosk	A stand alone system operated by a member of the public that processes certain Post office Ltd transactions.
LFS	Logistics Feeder Service: the Horizon Application referred to at paragraph 2.4 of Sub-schedule B4.2 – this is a sub-set of functionality provided by the Branch Database
MDM	Master Data Manager. Reference data management service operated by Accenture
MID	Merchant Identifier issued by GlobalPayments 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 former Horizon Application ~~referred to at paragraph 2.6 of Sub-~~

Abbreviation	Definition
	~~schedule B4.2~~facility that provided the Banking Business Capability;
NPS	Network Persistent Store
NRP	Network Reverse Proxy
NTP	Network Time Protocol. A protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks
OBC	Operational Business Change
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
P2PE	Point to point encryption.
PAF	Postal Address File. A service to allow post codes and addresses to be looked up (Provided within the Branch Database).
PAN	Primary Account Number
PAN Manager	Processor Area Network manager used to manage configuration and virtualisation of blades/resources within a bladeframe and BX900
PBS	Payment and Banking Service. The service introduced using P2PE (OnGuard) solution provided by Worldline.
PCI-DSS	Payment Card Industry - Data Security Standard. A set of security controls defined by the Payment Card Industry organisation.
PCI-CE Domain	PCI Cardholder Environment. 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
POC	Post Office Cloud. Based on AWS.
PODG	Post Office Data Gateway
~~POL SAP~~POLSAP	A SAP Financial system that no longer exists. Definition retained as used in list of changes.
POL MIS	Otherwise known as POL MI or Credence. This is the Post Office Management Information system.
POMS	Post Office Managed Switch. ~~A switch that can be installed in a Post Office Ltd Branch, connected to the Branch Router that allows devices other than Horizon Counters to use the Horizon Network to connect into the Horizon Data Centre (and potentially other locations).~~This is no longer supported by Fujitsu. The definition is retained as it is used in the list of changes.
~~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.
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
RTS	Retail Transaction Service. A service running on the HBS
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

Abbreviation	Definition
SAP	Integrated suite of applications providing financial accounting and other business functions.
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. Note that with the introduction of PBS Sensitive Authentication Data is not stored in Horizon.
SOA	Service Oriented Architecture
SSN	Secure Service Network. Part of the network that is behind a ~~firewall/IPS~~DMZ.
Stratum	~~A measure of each~~A level in a hierarchy of time sources
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 GlobalPayments to identify the terminal from which a transaction originated. Also used on the interface to e-pay (ETU)
TLS	Transport Layer Security
~~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 MDM. All other types (non-type A reference data) is received via non-automated feeds or declared locally within the Horizon solution (meta data)
VPN	Virtual Private Network
VSAT	A Very Small Aperture Terminal is a two-way satellite ground station. The definition is retained as it is used in the list of changes.
XML	Extensible Markup Language

0.7 Changes Expected

Changes
a. Decommission of DRSv1 b. Decommission of TES and TESQA c. APOP migration to POC d. Removal of RHEL 4/5 Windows 2003 e. IDS moving from McAfee to Fortigate f. Audit PCI data move to POC CDE g. Replacement of PODG by POETS h. Changes because of NBIT

POL00337615

i. Potential changes because of BIN8

a.j.

0.8 Information Classification

The author has assessed the information in this document for risk of disclosure and has assigned an information classification of FUJITSU RESTRICTED - COMMERCIAL IN CONFIDENCE.

1 Introduction

This document outlines the solution architecture delivered by the Horizon Online service~~.~~ (HNG-X). It covers applications and infrastructure.

The document has been expanded to describe some systems external to HNG-X in order to provide context useful in understanding Fujitsu's responsibilities.

Some systems originally within HNG-X have been migrated to Post Office Cloud (POC).

Wordline now support authorisation for card payments and banking transactions; these functions were previously supported from within HNG-X.

1.1 Scope

This document describes the solution architecture for the Horizon applications as at ~~HNG-X Release 20~~June 2023. It includes:

- Applications that provide Business Capabilities
- Applications that provide Support Facilities
- The solution architecture for the Horizon infrastructure.
- Outlining POC capabilities and responsibilities
- Outlining the functions carried out by Worldline (as part of PBS).

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.

The HNG-X Scope is assumed to be the Counter Business Application and components ~~that reside in, or are directly connected to, the Belfast Data Centres. It is assumed that systems that reside in the cloud are out of scope and that this document will be replaced when the Belfast Data Centre moves to the cloud.~~for which Fujitsu has responsibility for managing or maintaining.

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 10,500 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~~HNG-A".

1.3 Solution Outline

Horizon stores customer transaction data in the Data Centre. The data is stored in a Branch Database, and accessed through Branch Access Layer systems. The Horizon Counter system only stores operational data, such as reference data. This makes it easier and cheaper to keep the data secure.

The ~~Horizon~~ HNG-A ~~Counter~~ counter system is based on Java technology. ~~It uses Windows™ based Counter hardware.~~ The c~~C~~ounter communicates with the Data Centre using encrypted messages for business transactions, HNG-A counters run on a Windows ~~10~~ platform using a TLS mutually authenticated connection to the data centre.

As the system has evolved, in the Horizon Data ~~Centre~~Centres, the major changes are:-

- Interstage is being phased out,
- Apache Camel has been introduced,
- JBOSS has been introduced.

Additionally some applications ~~are based on Java, the Interstage~~ have been moved to Post Office Cloud (POC) and therefore use infrastructure and services provided by AWS. Note that where applications do not run in the Horizon Data Centres Fujitsu is not responsible for supporting the infrastructure or networking, but for some applications covered in this document, Fujitsu does provide application ~~server and Oracle database.~~ support.

The infrastructure and systems within the Horizon Data Centre are highly resilient. There is a stand-by Data Centre for disaster recovery, which is a ~~copy of the live Data Centre.~~ capable of supporting the primary data centre workload in DR. Data replication technology keeps 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.

Where components run outside of the Horizon Data Centre, Fujitsu is not responsible for the infrastructure that supports the applications and responsibility for resilience and disaster recovery lies with other suppliers.

The Solution has been developed using the following principles:

- ~~The solution was designed to address the ongoing operational costs of providing the service.~~
- Where appropriate, it utilises existing solution building blocks.
- It uses packaged applications and standard components except where suitable products are not available
- The Solution does not customise a packaged application other than via configuration capabilities supported by the vendor, unless agreed by PO Ltd.
- Where applicable, the solution utilises IT industry standard components, industry standards and widely used technologies, unless agreed otherwise with PO Ltd
- Internal Horizon interfaces 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 is designed to simplify application development, service management and maintenance.
- Where technically feasible, and it does not introduce additional cost, components are designed for reuse.
- ~~For the new development parts of the solution, the architecture is designed using Service Oriented Architecture principles.~~
- From a compliance perspective, (e.g. DVLA and passports etc) it operates in a government environment and must also be compliant with banking (PCI), Security, Service delivery and Quality standards

1.4 Layered Architecture[2]

The Horizon 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 Horizon solution can be thought of as a series of layers.

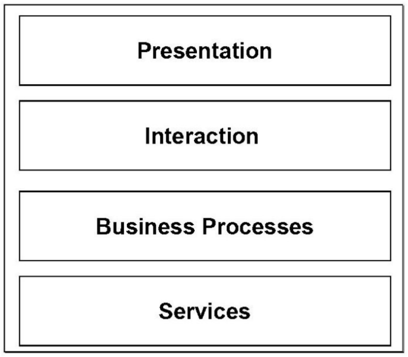


Figure 1 Layered View of the Application Architecture

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. DRS, TES)
- Interfaces into Clients (e.g. Enquiry and Data Delivery)
- Interfaces into service providers (e.g. Authorisation and Reconciliation, Logistics)
- 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)

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)

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

ARC-402 reads "Where technically feasible, and does not introduce additional cost, components will be designed for reuse. Fujitsu Services will consider re-use as part of its design process and will seek to develop solutions that are economic as well as re-usable."

- Central Batch Processes (e.g. Data Aggregation and Distribution, Reconciliation, Reporting, Reference Data Mgt)

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~~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 Horizon. 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.

- ~~*HNG-X Integration Architecture* (ARC/APP/ARC/0002) gives an overview of the composition of and interfaces between all the business applications.~~
- *Post Office Account GDPR One Trust Assets* (SVM/SEC/REP/3936) provides a full breakdown of GDPR assets broken down by HNG-X business capability and by the support tools that are required to deliver the HNG-X Service
- *Post Office Account GDPR One Trust Processing Activities* (SVM/SEC/REP/3954) describes the nature of the processing of GDPR assets broken down by HNG-X business capability and by the support tools that are required to deliver the HNG-X Service

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 Horizon. ~~It covers the networks within the branch, the wide area network that connects the branches,~~It 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 Horizon 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 Horizon achieves 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 Horizon copes 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 Horizon is made secure. This is covered in more detail in *HNG-X Security Architecture* (ARC/SEC/ARC/0003).

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

2 Business Applications

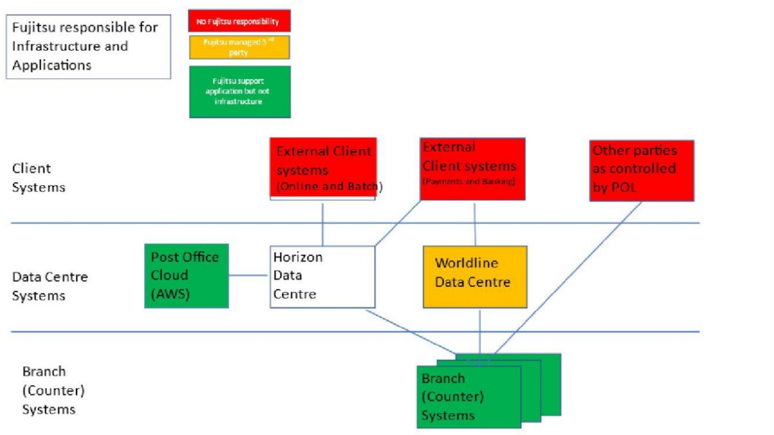

Fujitsu responsible for Infrastructure and Applications
No Fujitsu responsibility
Fujitsu managed 3 rd party
Fujitsu support application but not infrastructure
Client Systems
External Client systems (Online and Batch)
External Client systems (Payments and Banking)
Other parties as controlled by POL
Data Centre Systems
Post Office Cloud (AWS)
Horizon Data Centre
Worldline Data Centre
Branch (Counter) Systems
Branch (Counter) Systems

Figure 2 Overall Application Architecture

The above diagram illustrates a number of ways in which the environment surrounding Horizon has evolved:-

- Branch Counters are now able to use a browser to directly connect to third parties (this is shown as the box “Other parties as controlled by POL”
- Branch counters connect directly to the Worldline Data Centre as part of PBS
- Some functionality is now provided in Post Office Cloud.

2.1 Counter Applications

~~Note for HNG-A counters the counter application architecture is identical to the HNG-X counters. They originate from the same source components.~~

2.1.1 Assumptions

The main assumptions are that:

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

Note that at the time of writing the original document it was particularly important to emphasise this as prior to the introduction of HNG-X Branches were able to trade even if they had no network connection. The assumption is still true even though it is a statement of the obvious.

2.1.2 Solution[1]

All Horizon counter business applications are a single bespoke application that aligns with the serviceability and cost requirements of Horizon. 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.

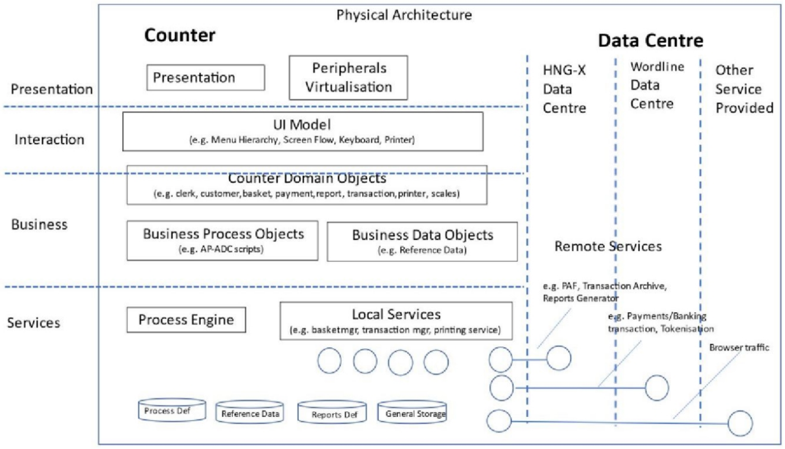


Figure 3 Counter - Application Architecture

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):

The Presentation layer:

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

ARC-400 reads “The Solution shall use packaged applications and standard components unless suitable products are not available. For this requirement and elsewhere the term 'The Solution' refers to 'The HNG-X Solution'.”

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 architecture model has been 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 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~~The Style Guide (DES/APP/STD/3433) and Construct Catalogue (DEV/GEN/MAN/0003) for Horizon counter applications ~~have been provided.~~drive consistency.

In addition to the separation of the UI presentation from application logic, the Reference Data contains 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~~

None.

2.2.2 Solution[1]

The Data Centre applications ~~derive from a combination of new and legacy applications (~~are shown in tiers in Figure 4~~). New applications cover mainly back-end functionalities required by the counter applications.~~ .

The ~~Legacy Host database applications (RDMC, RDDS, DRS and TES) remain largely intact but are candidates for future rationalisation. The online interfaces from the counter include Banking, GlobalPayments ETU and a range of Web Service interfaces.~~ key for the diagram is:-

🟥 No Fujitsu responsibility

🟧 Fujitsu managed 3rd party

🟩 Fujitsu support application

🟦 Fujitsu supported component

🟨 Fujitsu supported database

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

ARC-400 reads "The Solution shall use packaged applications and standard components unless suitable products are not available. For this requirement and elsewhere the term 'The Solution' refers to 'The HNG-X Solution'. "

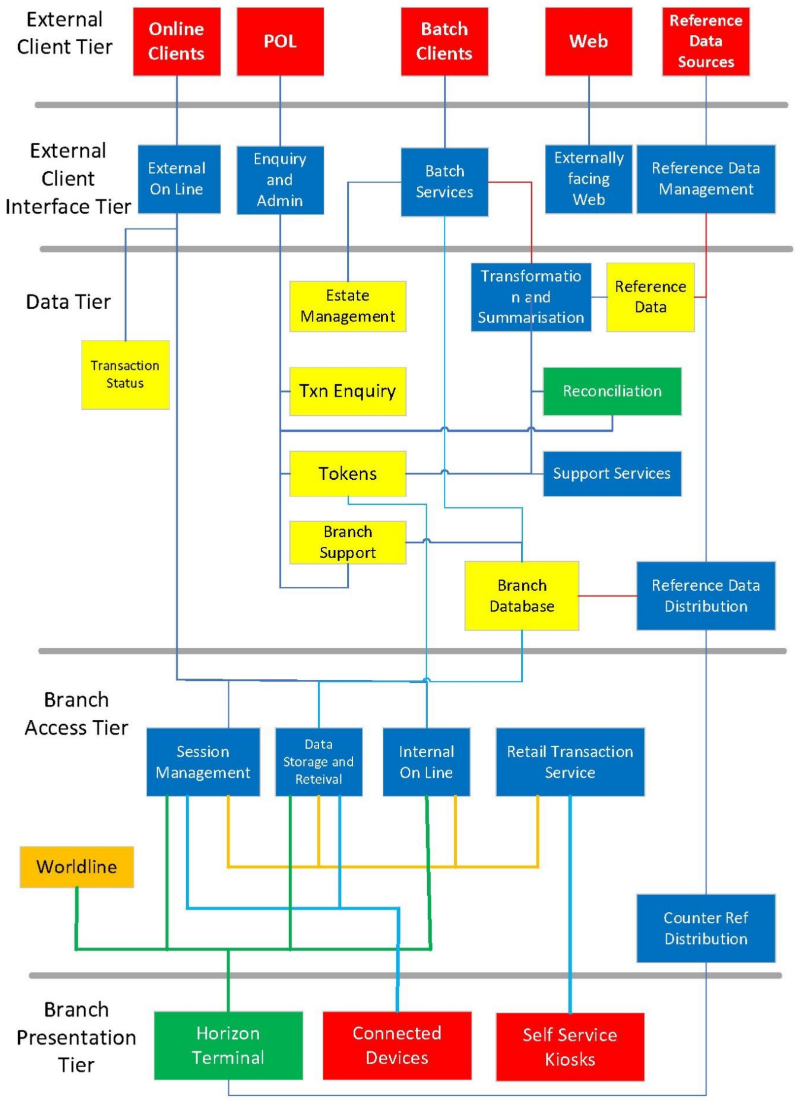


Figure 4 Horizon Data Centre Application Architecture

2.2.2.1 Branch Presentation Tier

~~This tier comprises the Branch Counters.~~

2.2.2.1.1 Horizon Terminals (HNGA)

The counter application architecture is described in section 2.1.

2.2.2.1.2 Self Service Kiosks (SSKs)

Self Service kiosks (SSKs) can connect to RTS and access a subset of the services available to HNGA counters. The application architecture for these devices is out of scope as they are not supported by Fujitsu Services.

2.2.2.1.3 Connected Devices (HIH)

Devices attached to the Horizon Integration Hub (HIH) can connect to the BAL and access a subset of the services available to HNGA counters. The application architecture for these devices is out of scope as they are not supported by Fujitsu Services.

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.

This tier supports access from SSKs and HIH devices allowing them to access a subset of the services used by HNGA counters.

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,

of users within the Branch estate (including SSKs and HIH devices which are set up with fixed user identities) and the Data Centre.

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 (Counter Training Office) 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~~is parsed to determine its type and then acted upon. The following list gives an example of the different types of ~~message~~messages that may be received:

- Transaction & Settlement data
- LFS Pouch Information
- Declaration data (Stock, Cash, Stamp, Bureau)
- Report Request
- Stock Unit (SU) and Branch Rollover Information
- Existing Reversal requests

- Transaction Corrections
- Transaction Acknowledgements
- 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 is designed to provide service isolation between different types of service requests, and in particular is 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~~
- Counter Help Service (CHS) Training

The Training service 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

Common and Branch-specific Reference Data is loaded through the Branch database.

2.2.2.2.5 Worldline C3/Axis

HNGA Counters call the Worldline C3/Axis system to request authorisation for Banking and Debit/Credit Card transactions.

~~2.2.2.2.5~~2.2.2.2.6 ~~Horizon Business Service~~ Retail Transaction Service (RTS)

A middleware layer that presents transaction business logic to ~~third party kiosks~~SSKs and interfaces with the Branch Access Tier in a manner that is very similar to a Horizon Counter. This means that as far as any Horizon and Post Office Ltd Reconciliation processes are concerned, these transactions are handled in the same way as Horizon Counter transactions. ~~HBS~~RTS supports only a sub-set of POL business transactions.

~~Another function of the HBS is to deliver help to HNG-A Counters in HTML format via the CHS Service.~~

~~The HBS also provides a pipeline for and on-line interface between the Counter and the Common Digital Platform (CDP)~~

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.

See ARC/APP/ARC/0005 for further details of items covered at high level in this section

2.2.2.3.1.1 ~~DCS Authorisation Agents~~Section deleted

~~The Debit and Credit card Authorisation Agent uses NPS for data persistence and audit. The Authorisation Agent also handles reversals, using status data held within NPS. Note that there is no~~

~~guaranteed delivery mechanism if it can't send the reversal immediately. Resilience is provided with similar mechanisms to the banking agents through heartbeats stored within NPS. The Authorisation Agent supports an interface from the BAL that queries the operational status.~~

~~The DCS Agent uses MID/TID data – with appropriate transfer from a MID/TID database.~~

~~The DCS Agent uses Hardware Security Modules (HSM) to encrypt the PAN.~~

~~The DCS Agent can support transactions that originate from Horizon counters.~~

2.2.2.3.1.2 ETU Authorisation Agents

The ETU agent uses NPS for data persistence and audit. 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 is provided ~~with similar mechanisms to the banking agents~~ through heartbeats stored within NPS. The Authorisation Agent supports an interface from the BAL that queries the operational status.

The ETU Agent uses TID only, with appropriate transfer from a MID/TID database.

The TID is a unique terminal identifier issued by POL's Merchant Acquirer.

2.2.2.3.1.3 ~~DVLA Agents~~Section deleted

~~The DVLA Web Service provides the Counters with the ability to query the DVLA for information relating to Vehicle Licences. The Counters call a service exposed by the Branch Access Layer (BAL). Within the BAL the Session Management component handles authentication and authorisation of the call and the Online Service Router delegates the call to the internal DVLA Web Service.~~

2.2.2.3.1.4 ~~Banking Application Agents~~Section deleted

~~The Banking Agents use the NPS for data persistence and audit. The Counters make banking requests to the BAL service that uses its Online Service Routing function to pass these requests to the relevant banking agent. The Banking Agent also handles reversals, using status data held within NPS. Resilience is provided with similar mechanisms to the banking agents through heartbeats stored within NPS~~

~~The Routing function is performed within the Branch Access Layer.~~

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

2.2.2.3.1.5 Not used

2.2.2.3.1.6 Generic Web Services

The Generic Web Service Framework capability can be used to introduce ~~one or more~~ Generic Web Service Agents under the Client Take-on Process. An agent includes the whole Horizon 'pipe' to support online requests to a Third Party Service provider (i.e. AP-ADC scripts using the GenericOnline ADC data type, the BAL/OSR routing configuration, the Generic Web Service Agent and the DXI and network configuration including boundary firewalls),

2.2.2.3.1.7 ~~Horizon Business Server~~Section deleted

~~As well as providing middleware business logic and settlement capability to third party self-service kiosks, the HBS provides a common interface for online communication to the Common Digital Platform.~~

2.2.2.3.1.8 Smart Metering Service (SMS)

Middleware which runs on the HBS which interfaces to British Gas to support the British Gas offering on Smart Meters.

2.2.2.3.1.9 CDP Adaptor

Middleware which runs on the HBS which interfaces to CDP allowing AP-ADC scripts to access services on the CDP (Common Digital Platform).

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)

The APOP service supports the authorisation of the sale and encashment of Postal Orders and other Voucher based and Out-Pay AP services. The APOP Workstation provides query and reporting functionality on Voucher status as well as the ability to administer vouchers and respond to exceptional voucher states.

~~The TESQA service provides a query capability for Banking transaction data. The PAN is held in encrypted form. TESQA provides a mechanism to decrypt an individual PAN. Access to TESQA uses TLS. No other cardholder data is stored.~~

Note that following the introduction of PBS there is no useful information contained in TES.

Horice is an Internet accessible website that offers service Monitoring and parameterized queries of near realtime live data. It is used by Fujitsu and Post Office.

2.2.2.3.3 Reference Data Management Service

Reference data is provided by Post Office to control the Horizon system, and this data is held and managed from the database application:

- RDMC Reference Data Management Centre

Type A Reference Data is that reference data received on the automated feed from the POL MDM service. The data Types supported by the Horizon service are identified in *HNG-X Reference Data Architecture* (ARC/APP/ARC/0001). The Non Type A data are delivered via the Fujitsu SSC team who use the RDMC Workstation to load the data, and enable distribution of verified and authorised changes.

Help text is implemented by downloading the data to the HBS Server where it can be accessed via a browser from the counters.

This service incorporates the **RDT environment** where Reference Data changes are verified prior to being released through to the Live service. Reference Data proving rigs are provided to allow proving of Reference Data on the Horizon system.

The HNG-X Development Team is responsible for delivery of certain types of reference data which is outside the scope of operational business change – a particular example might be reference data to support new functionality

2.2.2.3.4 Batch Services

The 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:

- Branch Database
- APOP Automated Payment Out-pay Database
- DRS Data Reconciliation Service
- TES Transaction Enquiry Service

The Branch Database provides a store and forward function to transfer the following batch data:

- Accounting and reconciliation data to CFS
- Flexible Cash Planning data to CWC
- Cash on Hand to Arrow
- Raw transaction data to Credence
- AP Transactions to Clients in Batch files via the Post Office Data Gateway. Client agreements dictate the frequency of file production
- Bureau transactions to First Rate Travel services

In addition, the Branch Database provides the capability of loading batches of transaction files from external devices and forwarding the information on to POL's clients

~~The DRS and TES applications provide storage for Card data, the PAN is held in encrypted form and the data retention period for DRS (90 days) and TES (180 days) has elapsed. .~~

~~The TES service provides storage for "Banking" transaction data. This includes storage of encrypted PAN. TESQA provides a mechanism to decrypt an individual PAN. No track-2 cardholder data is retained~~

There is no useful information stored in TES now that PBS has been implemented.

DRSv2 runs in Post Office Cloud with the application supported by Fujitsu. Post Office provide the infrastructure that it runs on.

DRSv1 continues to run in Belfast pending decommissioning.

The APOP database is the repository for Voucher state and Voucher history information. It also contains the configuration data that determines how Vouchers may move between different states.

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~~to a service running in Post Office Cloud; Lambda function used
- ~~NRT Agent~~Banking Undo – provides ~~AEI~~ data on banking transactions which need to ~~Cogent via~~be 'undone' to a ~~Web~~ service running in Post Office Cloud; Lambda function used
- NRT Agent – no longer used – but still supported.
- LFS – receives Planned Orders and Replenishment Delivery Notices.
- RDMC – receives Spot Rates and Margins data for Bureau service and Post Office Memo distribution
- Branch full notifications to the Collect & Return web service
- Pre-Advice files delivered to Royal Mail

~~The T&T agent takes parcel information from the NPS and transfers this to a Web Service that resides on a Smartpost application that is provided by CSC via the Huthwaite dedicated connection.~~

~~The~~Smart Meter reversalsThe NRT Agent is configurable to recognise settled transactions and to send these to configured Web Service end-points. Currently ~~the only application to use such a service is the delivery of AEI information to Cogent~~there are no applications using the service.

The LFS service loads planned orders and replenishment delivery notices from CWC into the Branch Database and takes Pouch Collection/Delivery and Cash Declaration data from the Branch Database and passes these details onto both CWC and Arrow.

The Spot Rates and Margins data for Bureau de Change transactions is delivered by the Branch specific Counter Reference Data Distribution Service.

When a branch has too many local collect items on hand then it can signal that it is full by pressing the branch full button. This signal to the collect & return web service to prevent parcels being delivered to this branch for a short period of time.

Postal services data is sent to Royal Mail in files of transactions on a regular near-real-time basis. This supplements the Track & Trace data.

Identity and training information is exchanged on a regular basis between the Branch Database and POL's ~~Forgerock~~ForgeRock system.

2.2.2.3.5 Externally Facing Web Services

The only instance of an externally facing Web Service with any Fujitsu involvement is CWS.

CWS runs in Post Office Cloud. The application is supported by Fujitsu.

CWS exposes an interface, usable from 3rd party Web sites, which displays a list of PO branches in a requested location. This allows customers of those Web sites to select a Post Office branch from which they can collect a parcel once it has been delivered.

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 (Santander, CAPO and LINK), GlobalPayments,~~ e-pay and DVLA.

There are also a number of online clients which are accessed using ~~the Generic Web Service over the Internet, for example: National Express, The Health Lottery, Neopost, PostcodeAnywhere and POca Card Fulfilment~~GWS, SMS or the CDP Adaptor.

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 uses TLS.

Note that with the introduction of PBS there is no useful information in TES/TESQA and the functionality to decrypt PANs is of no value. TESQA is awaiting decommissioning.

Post Office can access Horice using web browsers.

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;
- APS data for Automated Payment Clients,
- APOP,
- Track & Trace~~;~~ – data is fed to an agent running in Post Office Cloud;
- Banking Undo – data is fed to an agent running in Post Office Cloud;
- Cash Logistics data;
- CFS;
- ~~and~~ other Post Office systems including Credence~~,~~ and Arrow.

2.2.2.4.3.1 Post Office Data Gateway

PODG is a generic reference-data driven system that is used to deliver file-based information between two end points. These end points can be either external to the Fujitsu data centre, internal to the Fujitsu data centre or a mixture of the two. PODG allows copies of file, auditing and transformations to occur in on files as they transit through the gateway.

PODG is the architectural pattern of choice for all file based interfaces

2.2.2.4.4 POL MDM and other Reference Data Sources

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

2.2.2.4.5 External Web Sites

External Web sites can access CWS. See section 2.2.2.3.5 for further detail.

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

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~~other 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 (~~PODG) (Post Office Data Gateway)
- MID/TID management service
- Estate and System Management services.

The Audit service gathers transaction, event and ~~event~~other data from various subsystems for later retrieval and presentation. The data is immutable for 7 years and is retained for as long as POL instructs.

The Audit system provides storage for Banking and Debit / Credit card ~~transaction data to protect Card data.~~transactions. This includes storage of encrypted ~~PAN~~PANs for transactions carried out before the introduction of PBS. The Audit workstation has the ability to decrypt an individual PAN. The Audit does not store sensitive authentication data for transactions performed using authorisation services interfaces, which includes Horizon transactions. However, the audit system does store such data in encrypted form for historical transactions performed using the Riposte™ authorisation.

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

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.

Data is handled in one of three ways:

1. Changes to Branch Specific Data (e.g. name and address, which products are sold in that Branch etc) are distributed to the User and Session Management database. This is polled-for on a regular basis by each individual counter.

2. Common Reference Data required by counters is delivered in the same way as branch-specific data.
3. Reference Data required by Data Centre (e.g. account mappings for products) is distributed in the same way as for existing legacy Data Centre applications.

2.2.2.5.4 Databases in the Data Tier

Database	Notes
Branch Database (BRDB)	The Branch Database is built on a set of blades using Oracle's Real Application Cluster technology. It provides a centralised data-store for all counter transactions and events for branches with data being retained for a period that sufficiently covers the reporting and support requirements for the branches. BRDB is partitioned by FAD Hash to support rapid IO. There are 128 partitions, with each branch assigned to one partition. BRDB operates as a four node cluster.
Branch Support (BRSS)	The Branch Support Database (BRSS) is built using Oracle's Real Application Cluster technology. The Branch Support Database is populated with transactional, reporting and control data replicated from the Branch Database on a near real-time basis. The separate support database (single instance) is made available for third line support to protect the performance of the BRDB. The data is retained in the BRSS for longer (typically one year) duration as compared to the data retention in BRDB. The reason for this is to satisfy the requirement of support streams to be able to access such data over an extended period of time. Much of the data stored in BRSS can be accessed using Horice. BRSS is used as the data source for Branch Hub (a Post Master Management Information System), with BDAS (BRSS Data Access Server) acting as the middleware component, connecting BRSS and Branch Hub.
Tokens (APOP)	A generic voucher database supporting a number of Post Office services hosted on an Oracle database on the NPS platform. System configuration in the form of reference data dictates, for each APOP service: • What data can be persisted • What queries can be performed • The valid types of transaction (i.e.: sell, encash, spoil, archive) • Who/what can access and perform transactions • Reporting APOP is hosted on the NPS platform
Reconciliation DRS	A legacy Oracle database awaiting decommissioning. Its role has been taken over by DRSv2 (see below). Hosted on the DAT platform Note that manual refund transactions for Credit/Debit card transactions do not get forwarded to DRSv2 but may show up in DRS thus it does have some residual value.
Reconciliation DRSv2	A PostgreSQL Database in AWS The database supports the Data Reconciliation Service which compares

	the Financial Institution's view of a transaction outcome and the Counter's view of the transaction outcome and reports any discrepancies between these views. It also generates reports based on the Financial Institutions view for the purposes of settlement.
Estate Management EMDB/MTA	Estate Management is a suite of databases and applications generating, storing, transferring and supplying data. The data includes items such as IP addresses, number of counters, open/closed state MIDs and TIDs. Consumers of this data include BRDB, the certificate signing service, ETU authorisation agents and external 3rd parties, e.g., Ingenico and GlobalPay SQL Server 2005/ Windows 2003 on the EST platform
Transaction Status NPS	Database built using Oracle Real Application Cluster. NPS provides a data-store for the ETS message parts and HNG-X Key Management APOP is hosted on the same platform
Transaction Enquiry TES	A legacy Oracle database awaiting decommissioning. It has no role since PBS has been implemented. Hosted on the DAT platform
Reference Data RDMC/RDDS	Oracle databases hosted on Solaris Hosted on the DAT platform RDMC is the repository for all HNG-X reference data. RDDS is responsible for delivering reference data to target systems. Software is developed using Unix scripting, Pro*C and PL/SQL. Predominantly daily batch systems.

2.3 Post Office Cloud

2.3.1 Post Office Responsibilities

Provision of: -

- AWS Subscription
- Network (the connection to the HNG-X data centres is via Verizon.
- Platform provisioning
- IAM
- Foundation services (AD, F/W, Load balancers, EM)
- POL CCoE (the team responsible within POL).

2.3.2 Fujitsu Responsibilities

Application Support for Fujitsu provided applications listed in section 2.3.3

~~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 are grouped into 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 Horizon is centralised into a single database repository (the Branch database) within the Data Centre.~~

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

~~**Figure Application Database Architecture**~~

~~The database technology platform for all the business applications is Oracle running on Oracle Enterprise Linux (OEL) or Solaris.~~

~~The existing legacy databases are shown in yellow in the above diagram. These legacy databases receive their transactional information from the Branch database directly.~~

~~The Branch database is constructed as a single database. This database supports a high commit rate as well as a high volume of database queries, and has high availability. [See section .] Oracle Real Application Cluster technology is used for the Branch database (as are all on-line databases – NPS and APOP). Maximum Availability Architecture has been 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.~~

.

2.3.3 Applications and Services

2.3.3.1 IBM Workload Scheduler (IWS)

IWS is a fully automated batch job scheduling application that manages the operational batch schedules and automates most of the operator activities. It prepares jobs for execution, resolves dependencies, creates the execution environment, launches and tracks each job.

Fujitsu uses IWS to schedule all applications running in Post Office Cloud for which it is responsible. These are discussed below

2.3.3.2 Collect and Returns (CWS)

CWS is an externally facing website allowing Royal Mail customers to identify Post Office branches which they can have parcels delivered to.

2.3.3.3 Data Reconciliation Service (DRSv2)

DRSv2 is used to reconcile payment and banking transactions carried out on HNGA counters and Amex payment transactions carried out on SSKs.

It is also used to reconcile ETU transactions carried out on HNGA counters and SSKs.

A feed of transactions as carried out on the counters and SSKs and recorded in the BRDB is fed into DRSv2 along with files providing the relevant financial institutions' view of the transactions.

DRSv2 provides reports to POL to assist in settling with clients and to identify reconciliation issues.

2.3.3.4 Track and Trace (T&T)

Fujitsu is responsible for a lambda function which reaches back to the BRDB to collect details of tracked items. The function forwards these to an agent which interfaces to Royal Mail/Parcelforce to deal with them.

Fujitsu has **no responsibility** for the agent that interfaces to Royal Mail/Parcelforce.

2.3.3.5 Banking Undo (BUN)

Fujitsu is responsible for a lambda function which reaches back to the BRDB to collect details of banking transactions which need to be undone. The function forwards these to an agent which interfaces to the Wordline data centre to deal with them.

Fujitsu has **no responsibility** for the agent that interfaces to Worldline.

2.3.3.6 HIH

Fujitsu has **no responsibility** for HIH.

HIH can connect to the BAL and record transactions in the BRDB.

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 (Fujitsu Hosted DCs)

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

The objective of the platform design process is to produce a set of baseline standard build configurations fulfilling the requirements for Horizon 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.

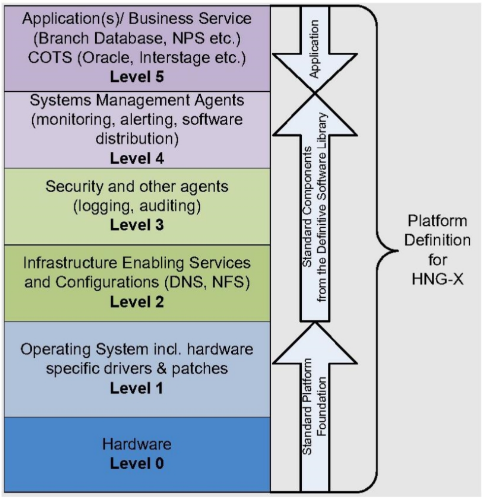

Application(s)/ Business Service (Branch Database, NPS etc.) COTS (Oracle, Interstage etc.)
Level 5
Systems Management Agents (monitoring, alerting, software distribution)
Level 4
Security and other agents (logging, auditing)
Level 3
Infrastructure Enabling Services and Configurations (DNS, NFS)
Level 2
Operating System incl. hardware specific drivers & patches
Level 1
Hardware
Level 0
Application
Standard Components from the Definitive Software Library
Standard Platform Foundation
Platform Definition for HNG-X

Figure 6 Platform Definition Multiple Layers

In detail the Component levels of each platform consist of:

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

This is a set of minimum hardware specifications required to support Horizon 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 Horizon security Policy.

Level 2 - Base Infrastructure Services

This level includes standard infrastructure services such as file server, Domain Name 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 is common to all platform types and consists of security software such as specific system configuration and application of Group Policies. This ensures that each platform conforms to the Horizon 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 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 provides 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 complete a full platform

3.2 Platform Architecture

3.2.1 Fujitsu Primergy BX900 Chassis Blade Server

The BX900 employs the use of a standards based converged I/O fabric for internal communication between Blades or pNodes and the outside world. It does this by utilising a pair of Brocade switches or cNodes. The pServer Operating System connects directly to the storage fabric and external network which provides it with a high I/O capability. The Operating System deals with SAN multipath management, World Wide Names (WWNs), Network link detection failures and MAC address allocation. The following figures demonstrates the relationship and key components of the network and storage concepts for the BX900 environment.

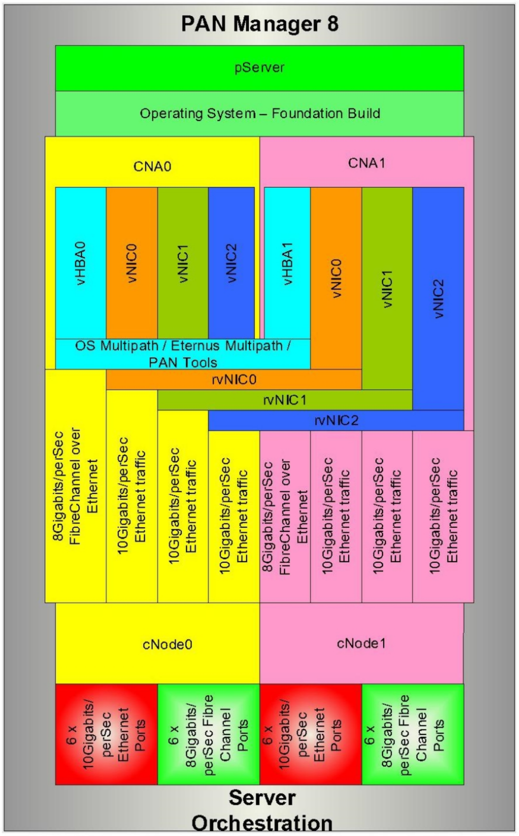

PAN Manager 8
pServer
Operating System – Foundation Build
CNA0
CNA1
vHBA0
vNIC0
vNIC1
vNIC2
vHBA1
vNIC0
vNIC1
vNIC2
OS Multipath / Eternus Multipath / PAN Tools
rvNIC0
rvNIC1
rvNIC2
8Gigabits/perSec FibreChannel over Ethernet
10Gigabits/perSec Ethernet traffic
10Gigabits/perSec Ethernet traffic
10Gigabits/perSec Ethernet traffic
8Gigabits/perSec FibreChannel over Ethernet
10Gigabits/perSec Ethernet traffic
10Gigabits/perSec Ethernet traffic
10Gigabits/perSec Ethernet traffic
cNode0
cNode1
6 x 10Gigabits/ perSec Ethernet Ports
6 x 8Gigabits/ perSec Fibre Channel Ports
6 x 10Gigabits/ perSec Ethernet Ports
6 x 8Gigabits/ perSec Fibre Channel Ports
Server Orchestration

Figure 7 Primergy BX900 Logical Overview

PAN Manager runs outside of the chassis and connects to the Blades in two ways. First there is an in-band redundant connection through a single channel on each of the Converged Network Adapters (CNAs). Secondly through the Master Management Boards (MMBs) straight into the iRMC out of band integrated Remote Managements Cards. The in-band connection requires the host operating system to run a PAN Agent software stack in order to provide PAN Manager administrative control over the pNode. PAN Manager is able to monitor the health of the pNode and send control commands to the pServer via this agent. It is recommended by Egenera that the PAN Agent is always deployed although it is not a mandatory requirement. PAN tools are deployed as part of the software stack contained within the agent. This contains SAN multipath drivers as well as configuration scripts for the network card configuration. It is possible to use the native OS multipath drivers or the Eternus multipath driver.

Pan Manager Software has been chosen with this domain architecture as an appropriate Server Orchestration tool.

PAN Manager manages the converged infrastructure introduced by the BX900/S2 and VDX2730 Connection Blades. PAN Manager runs on the PAN OPServer which is a virtual machine running on a VMware cluster to provide high availability. These are used for the Oracle databases.

BX900/S2-SBAX3: The BX900/S2-SBAX3 is ~~be~~ managed by the ~~existing~~ Belfast Refresh PAN Manager infrastructure. These are used for the non-Oracle workloads.

Figure 8 shows the components that ~~will be~~are managed by PAN Manager.

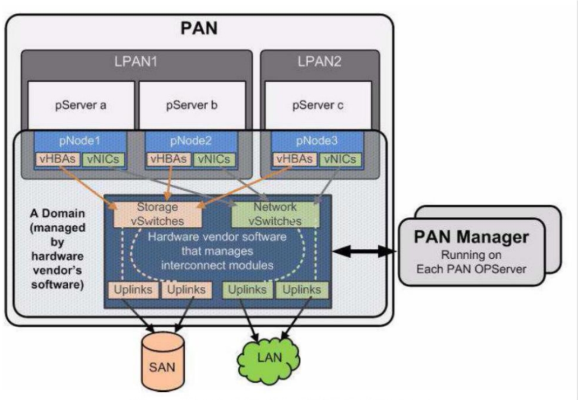


Figure 8 Logical Model of PAN Architecture

3.2.2 Discrete

Primergy BX900 is the preferred hardware platform used, however discrete hardware is used where application requires a specific OS (e.g. DAT) or there is a specific security reason or performance reasons where a bottleneck could be created (e.g. Backup). The amount of discrete server types and instances has been kept to a minimum.

3.2.3 Operating Systems

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

- Windows 2012 R2
- Windows 10
- Windows 2003 R2 Server (Enterprise and Standard, 32Bit and 64Bit)
- Red Hat Enterprise Linux (Release 4, 5, 6 32Bit and 64Bit)
- Oracle Linux (Release 6 32Bit and 64Bit)
- Solaris 10 (Discrete platforms only)
- Windows XP on some legacy services

3.2.4 Virtualisation Technologies

Oracle virtualisation is introduced through the use of Oracle Virtual Manager on the BX900 and is described in High Level Design DES/INF/HLD/2347. This is only used for RDT.

Hardware virtualisation is the 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.

For Live, memory is not over specified in allocation of platforms to pBlades, but can ~~over specify~~be for test configurations where performance is 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.

3.3 Data Centre

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

3.4 Operational Model

The platforms of Horizon 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 an Active / Active model in normal operations. These are considered key infrastructure services.

The Disaster Resilience model for the Horizon 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 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, DRS, TES, RDMC and RDDS).
2	Central Agents	Central online services such as APOP and Training.
3	Banking and Client File Transfer	Batch ~~feeds to Banks, GlobalPayments, Amex and~~feed e-pay
4	Other Client Agents	Online ~~feeds~~ feed ,to ~~GlobalPayments,~~ e-pay~~, DVLA, Help Desk and other~~ Other online services such as those provided by the Generic Web Service. All Client Agents are implemented as virtualised platforms independently of each other, with the exception of the Generic Web Service where all services are hosted on a pair of virtualised platforms.
5	~~Banking Agents: NBS~~ Not used	~~Online feeds to the banks. There are three types (Santander, 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; this is pending decommission.
8	PO File Transfer	Batch feeds to Post Office systems.
9	Branch Reporting	Provides an API (to the BDAS platform) from which Branch Hub accesses Branch Reports.

3.4.2 Storage and Audit

Storage is provided by using Eternus multi-tiered architecture using DX8700 S2 arrays.

The storage model uses two arrays in each data centre to enable separation of Platform data in order to allow operational changes to be carried out separately on each array. Platforms data is separated in such a way as to provide additional redundancy between Branch Data Base and Branch Database Standby in this way for example. Should there be a failure of one DX8700 array in a data centre, it is possible to provide services from the other to the redundant platforms.

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.

NAS storage is not shown on Figure 9 for clarity but should be regarded as a presentation technology for other physical hardware Tiers. Due to the characteristics of NAS storage, it is 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 9.

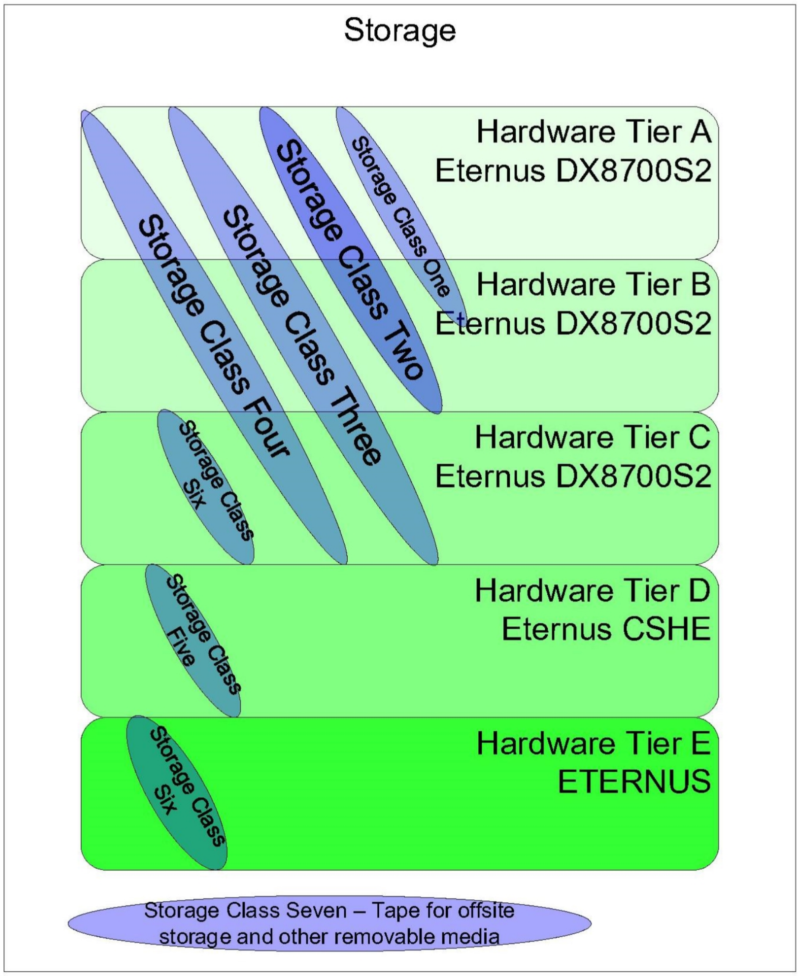


Figure 9 Logical and Physical Storage

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 are lost.

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

Historical and audit data will be placed on dedicated Eternus CS1500 storage arrays and the contents are replicated to the passive Data Centre using the Audit application software.

Both Data Centres 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.

3.4.3 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

Table 1 Supporting Services

3.4.4 Testing in passive Data Centre

When the second passive Data Centre is not used as a disaster recovery location it is used to support Horizon 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 makes use of virtualisation technology to support multiple concurrent test streams. In the event of a disaster, the second passive Data Centre is re-configured as the active Data Centre with live data and all testing ceases. On restoration of the Live Data Centre the passive Data Centre resumes its role of supporting Horizon testing based on an earlier checkpoint. During the period the passive Data Centre is used as live no Horizon test activities are 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 is realised in the event that critical updates need to be deployed to the live system during a prolonged passive Data Centre outage. Careful consideration is needed at the live data centre as live systems will require reconfiguration during quiet periods to enable this capability.

Testing of Reference Data is performed using the Reference Data Test rigs that operate within the Live Data Centre.

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.~~ All hardware is supplied and supported by a third party

The normal configuration for a HNG-A Counter position is:

- PC Base Unit
- Touch Screen
- LIFT Keyboard incorporating a Magnetic Swipe and Smart Card reader
- BAR Code Scanner
- Slip and Tally Roll Printer Weigh Scales (serial connection – normally shared between two counters with both counters having a separate connection).
- PIN Pad
- Optionally a Bureau de Change Rates Board

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

The Horizon HNG-A counters run on PC systems running Windows™. ~~The HNG-A application has been specified to require at least 40Gb hard disk, 2GB memory and a processor capable of running Windows 8.1.~~

~~For mobile counters the normal configuration is:~~

- ~~PC Base Unit.~~
- ~~Integrated touch screen.~~
- ~~LIFT Keyboard incorporating a Magnetic Swipe and Smart Card reader~~
- ~~BAR Code Scanner~~
- ~~Slip and Tally Roll Printer~~
- ~~PIN Pad~~

The ~~mobile counters are connected to the Data Centre via a Branch Router (see Network Section). Note~~ specification for ~~HNG-A additional~~ the hardware ~~e.g. tablets may be~~ required to ~~be supported by~~support the ~~counter~~HNG-A application ~~but~~is provided in ~~this case the specification of the peripherals and base unit will not change.~~ BP/DES/003.

Self-service kiosks may be provided by third ~~party hardware manufacturers~~parties.

HIH devices may be provided by third parties.

4 Network Services

The following diagram provides an overall view of the Horizon Network services. The Verizon network is included on the diagram for context.

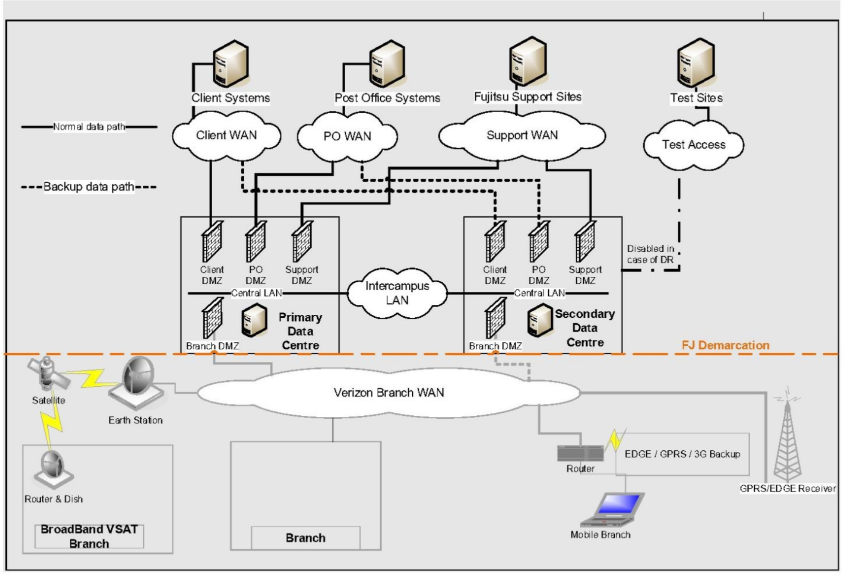


Figure 10 Data Centre Lan and WAN handoff Topology; Network Services

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

- Data Centre (LAN, Inter Data centre services and Application Services).
- WAN services; Branch Handoff routers provide the interconnectivity and demarcation into the Verizon managed Branch WAN. Further Support Hand Off routers provide for connecting Fujitsu sites (Support, Test and Application workstations) to the Horizon Data centres. Internet connectivity is provided as some Post Office Services are reached via the Internet.

The approach used for Network Management is based on ~~HP Network Mode Manager~~CA Spectrum monitoring, SYSLOG repositories for event storage and Cisco Prime for Configuration backup. Alerts are forwarded into the Enterprise Management System.

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.

4.1 Data Centre

4.1.1 Inter Data centre networks

This LAN service between the two Horizon 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 Horizon 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.

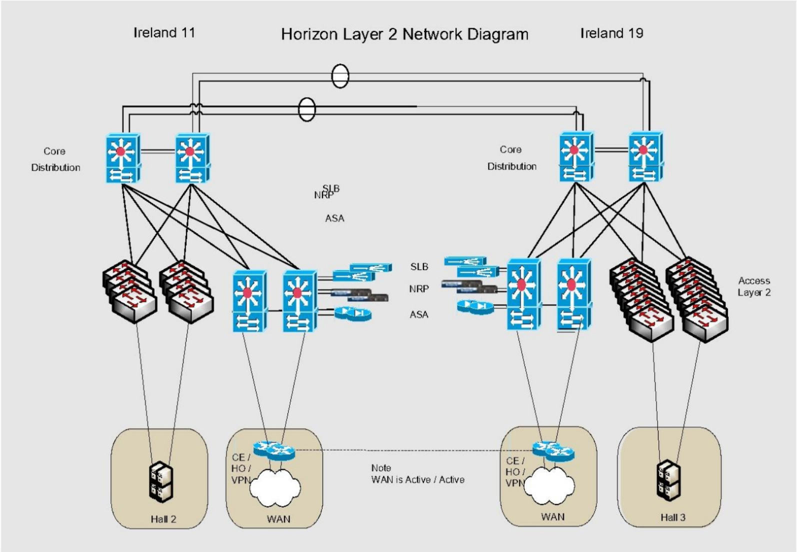


Figure 11 Network - Access, Distribution & Core Layers

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

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 Horizon 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 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(*)
- Network Reverse Proxies; TLS offload for Branch counter and SSK traffic
- Firewall services – external Firewall

(*) In some cases clients connect directly to Horizon data centres (for example ~~Vocalink and JP Morgan)~~Epay).

4.1.3 Application services

The network provides the following services to the Horizon Applications; - TLS offload, Load balancing and Virtualisation.

TLS offload is used to terminate TLS sessions initiated from the counters~~.~~, SSKs and some third parties. TLS 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. TLS Offload is provided by a pair of redundant Network Reverse Proxies at the Access Layer.

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 Citrix Netscalers 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;

- Network Connectivity handoff between Horizon Data centres and Verizon for WAN connectivity to locations for Post Office Clients as well as Post Office Data Centres~~.~~ (including POC).

~~(Note some Post Office Clients provide the WAN connectivity into Horizon data centres, these being Vocalink, EDS)~~

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

A common approach (Handoff Router Model) is used in Horizon data centres for all external connectivity where either Fujitsu or Verizon provide the Wide area network. These “Handoff Routers” are connected to the Access layer (WAN) switches.

WAN handoff router 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 follow the general approach to providing WAN connectivity based on the Fujitsu MPLS cloud.

- DVLA for ~~online authentication of car tax.~~transferring files via PODG
- e-pay for mobile phone top up (ETU) transactions
- ~~Santander for banking transactions~~

The Following WAN connections to Horizon data centres are provided by Verizon.

- POL data centres also known as POL BackOffice connectivity
- ~~AEI connectivity~~

The following WAN connections to Horizon data centres are provided by third parties:

- ~~Voca LINK~~VocaLINK for ~~banking transactions~~
- ~~CAPO for banking transactions~~
- ~~Debit/Credit card payment file transfers to Globalpayments are provided by~~transferring files via PODG ~~File transfers as are the~~ .

Payment ~~confirmation~~ files from ~~Globalpayments~~Global Pay and Amex are received via PODG and transferred to ~~Fujitsu. Payment confirmation~~the Debit Card Server (DCS) . Historically these files ~~for Amex payments come directly from Amex rather than from Globalpayments. The~~contained PCI sensitive data and so the interface between the Debit Card Server and PODG is via HTTPS rather than a file-share since this ~~keeps~~kept the PODG Service outside of the PCI domain

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

The Support WAN provides access for the Fujitsu support communities to the Horizon Services, platforms and appliances. This access covers Business support and application / network / platform support roles. The following models are supported:

- RED LAN model; ~~A~~a dedicated workstation managed by Horizon (provisioning, eventing and maintenance is provided). The path to the Horizon data centres consists of Horizon components and Horizon WAN services only. This model provides for the most flexible access and high availability.
- Corporate Workstation LAN only; ~~A~~a Fujitsu Corporate workstation is used to access data centres. All WAN conveyance is provided by a Horizon 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 WAN to reach the Horizon data centres . Access is restricted to Remote Desktop (no copy / paste and file transfer) onto Secure Access Servers.
- Corporate Workstation; ~~This~~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 volume 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 Horizon and Fujitsu corporate workstations a Corporate Data exchange proxy is provided.

4.2.3 Internet Access

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

- Neopost (Kahala)
- postcodeanywhere.co.uk
- ~~POca Card Fulfilment~~
- Generic Web Service clients
- SSK Certificate Revocation List Lookup.

In all cases connections are initiated from Horizon data centres to the internet reachable endpoints.

[Note an exception to this rule was implemented to support Smart Metering (SMS) from Paystation but this system has never been used]

4.3 Not used

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[2].

5 Systems & Estate Management

[2] Note: “Test” does not include RDT

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 (though not by Fujitsu) 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 is delivered from Software Change Management to Systems Management through a formal Release Management mechanism. Such software is pre-packaged so that it can be delivered and optionally installed in a fully automated manner. Where such automation is not possible the procedures are followed to include documentation of any manual intervention that may be required.

Reference data updates, received for distribution, are received in a fully automated manner which includes targeting information.

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

5.1.2 Distribution

5.1.2.1 Branch Counters

Counter software is distributed by a third-party. Please refer to DES/GEN/SPE/2731 Counter Packaging Specification which describes the Fujitsu expectations on ~~CC~~EUC tower in terms of packaging.

5.1.2.2 Horizon Data Centre

This is a Fujitsu responsibility.

5.1.2.3 Post Office Cloud

Post Office responsibility.

5.1.3 Integrity checks

5.1.3.1 Branch Counters

Fujitsu ~~are~~is not responsible for the Windows 10 counter build, software distribution or application integrity. This is now the responsibility of ~~Computacentre.Distributed~~ EUC tower.

5.1.4 Monitoring

5.1.4.1 Branch Counters

Fujitsu is not responsible for monitoring the Branch estate.

5.1.4.2 Horizon Data Centre

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 is 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 Horizon system).

~~The monitoring includes 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 is provided, although the different toolsets may be used for different operations.

5.1.4.3 Post Office Cloud

Kibana dashboards are used for monitoring applications.

5.2 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[3], 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 at the originating end system, at a domain gateway or at reception in the central event management system. Certain domains 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 and ensures that reporting on business applications is kept independent of the platform and operating system on which it is being run. Instrumentation has been 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 provides facilities that include:-

- Web based user interface to view the reception of events

[3] Note that since EUC tower took responsibility for the Counter estate Fujitsu only collects selected events from the counters to include them in the audit trail. Fujitsu does not monitor these events.

- Links to ~~Known Error Log~~Knowledge Base repositories so that the significance of the event may be determined
- 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~~KB (knowledge base) 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~~issue 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~~KB 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.

5.3 Remote Operations and Secure Access

All access by operations to manage IT systems are fully audited.

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

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

1. Access to Data Centre resident Secure Access servers from Fujitsu Services locations during 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.

5.4 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 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.

5.5 Estate Management and Auto-Configuration

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

Fujitsu’s role in opening new branches or adding new terminals is to

- allocate an IP addresses for each device
- for a new branch, request the MID values from Global Pay
- allocate TIDs for each device.

5.5.1 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 internally and with the Merchant ~~Aquirer~~Acquirer to provision the OBC change
- To schedule the timely update of any Data Centre applications configurations
- 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 implement new file-delivery sources, destinations and routes using PODG.

5.6 Capacity Monitoring

5.6.1.1 Branch Counters

Fujitsu has no responsibility for monitoring Capacity of Branch Counters.

5.6.1.2 Horizon Data Centre

The system is effectively capacity managed. To support this, the following services are provided:

- Immediate alerting (Tivoli) on performance issues that could jeopardise the live service.
- Lower priority alerting (Tivoli) for performance issues, which while not jeopardising the live service, indicate a problem that needs to be investigated.
- Medium and long term trending by Metron Athene
- Aggregated data extracts of volume and performance metrics by a Capacity Management Service
- Live monitors and query support via a portal that is delivered and supported by SCC (HORIce~~)~~)).

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

5.6.1.3 Post Office Cloud

Managed by Post Office.

5.7 Scheduling

Scheduling for all central systems (both business applications and operational services) wherever possible uses a single scheduler which includes the following architectural attributes~~ :~~:

- Operates on all the major operating systems in use in the solution
- Integrates with the enterprise management system for alerting
- Operates within the time synchronisation service
- Provides role based management user interface
- Allows the definition of schedule with associated activities and timer based controls.

5.8 Time Synchronisation

Time is distributed through the Horizon network using the NTP3 protocol and the Microsoft Active Directory (AD) derivative; it is arranged 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
    Verizon PE nodes in Belfast (Serving Branch Estate)
    e) Estate Time Servers, peered radius servers, these 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.

6 Availability

6.1 Principles

The solution for availability and DR is:

- One Data Centre is 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 under usual operation is used for testing, except where it needs to be used for business continuity tests.
- Some "Live" elements of the solution are operational at the DR Data Centre where this is required to support DR or WAN diversity.
- Each Data Centre has 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 is 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 is 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 is no significant test environment. In this scenario, limited testing (sufficient to test minor fixes needed to keep the live service operational) is available at a Fujitsu development site. However such testing facilities are not sufficient to test releases.
- The required failover times from the decision to invoke DR are covered in the Horizon 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
- Business Continuity Testing takes place:
  - Resilience (e.g. failure of a server) during normal Working Hours.
  - DR (i.e. failover to DR site) out of Working Hours.

6.2 Disaster Resilience

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

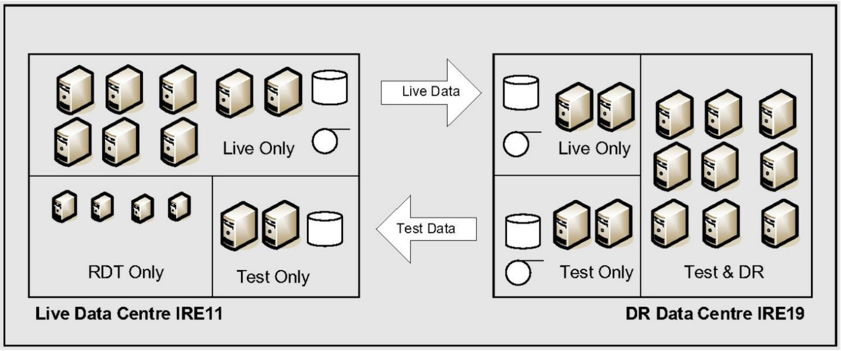


Figure 12 Data Centre DR

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)).
- 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
  - 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).

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 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.

Note: Reference Data Test (RDT) systems are considered as Live systems from a DR perspective and will failover to the DR site.

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~~ETU).
- 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.
- 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 were considered to determine the optimum solution namely cost, complexity, impact of failures and failover time. The approach used for each component of the solution was determined as part of the design work.

7 Performance and Scalability

This section outlines the volumes that the solution supports and how scalability is supported. Performance targets for specific components were considered as part of the detailed design work.

7.1 Volumes

The volumes that the solution needs to support are 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) 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. If the workload reduces, this layer can be reduced by removing platforms subject to resilience considerations.

#	Area	Scaling Approach
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.
4	HBS	Enhanced hardware (to date)

Table 2 Scaling Strategies

8 Security

8.1 Assumptions

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

8.2 Solution

8.2.1 Security Strategy

The security strategy for Horizon 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 Horizon 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 Horizon 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.

Table 3 Security Strategies

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 was established to guide the secure design, development, test, implementation and operation of the Horizon system. These principles are:

- Balanced between the ‘text book’ view of Information Security and the business requirements of the Horizon system
- Carefully considered
- Objective.

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

The controls themselves were 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

Table 4 Security Principles

These principles are explained in more detail in the Horizon 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, GlobalPayments,~~ 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 Horizon Information Security Policy {SVM/SEC/POL/0003}. Systems in this Tier must be patched in accordance with the Horizon Information Security Policy {SVM/SEC/POL/0003}. 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 Horizon Information

Tier	Description
	Security Policy {SVM/SEC/POL/0003}. Systems in this Tier must be patched in accordance with the Horizon 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 Horizon Information Security Policy {SVM/SEC/POL/0003}. Systems in this Tier must be patched in accordance with the Horizon Information Security Policy {SVM/SEC/POL/0003}.

Table 5 Security Tiers

8.2.5 Security Domains

There are a number of defined security domains with the Horizon security model; therefore data traffic is 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 Horizon 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.

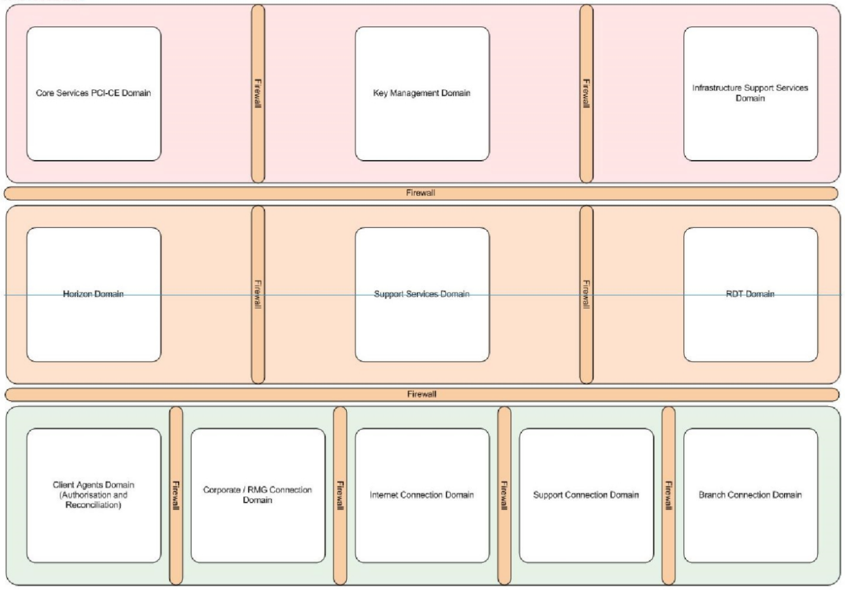
~~For example, in the Client Agents Domain, each Banking Agent can be separated from every other Banking Agent through the use of physical separation, using firewalls or separate LAN segments, or through the use of logical separation using VLANs. This is dependent on the requirements of the contract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

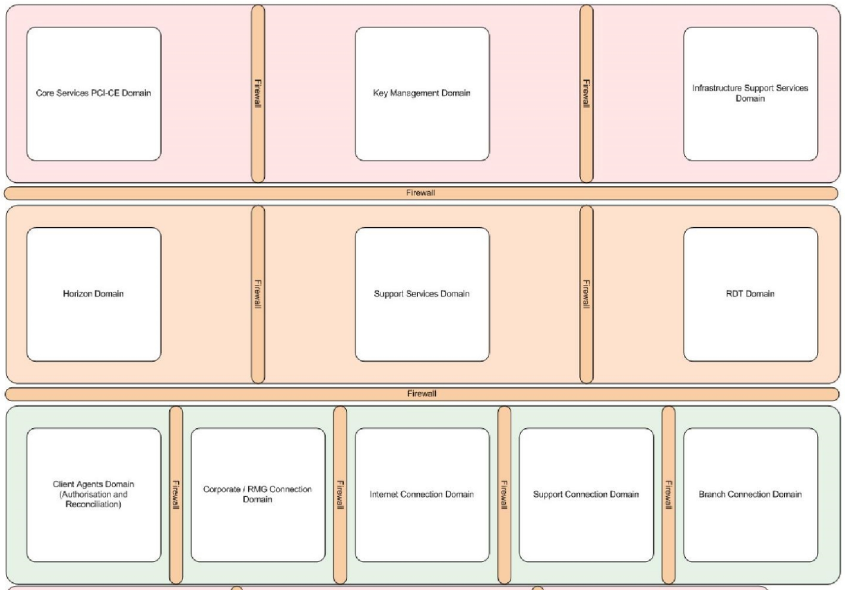
The security domain model can therefore be viewed as a method of logically grouping network subnets.

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 Stevenage.

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 applies. This is particularly relevant to the Solaris Main Host that supports a number of Oracle Databases, some of which~~ contain~~, historically, contained card PAN data and some ~~of~~ which ~~don't~~didn't. The Solaris Main Host ~~has~~was 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 Card PAN Data~~.

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


Core Services PCI-CE Domain
Firewall
Key Management Domain
Firewall
Infrastructure Support Services Domain
Firewall
Horizon Domain
Firewall
Support Services Domain
Firewall
RDT Domain
Firewall
Client Agents Domain (Authorisation and Reconciliation)
Firewall
Corporate / RMG Connection Domain
Firewall
Internet Connection Domain
Firewall
Support Connection Domain
Firewall
Branch Connection Domain


Core Services PCI-CE Domain
Firewall
Key Management Domain
Firewall
Infrastructure Support Services Domain
Firewall
Horizon Domain
Firewall
Support Services Domain
Firewall
RDT Domain
Firewall
Client Agents Domain (Authorisation and Reconciliation)
Firewall
Corporate / RMG Connection Domain
Firewall
Internet Connection Domain
Firewall
Support Connection Domain
Firewall
Branch Connection Domain

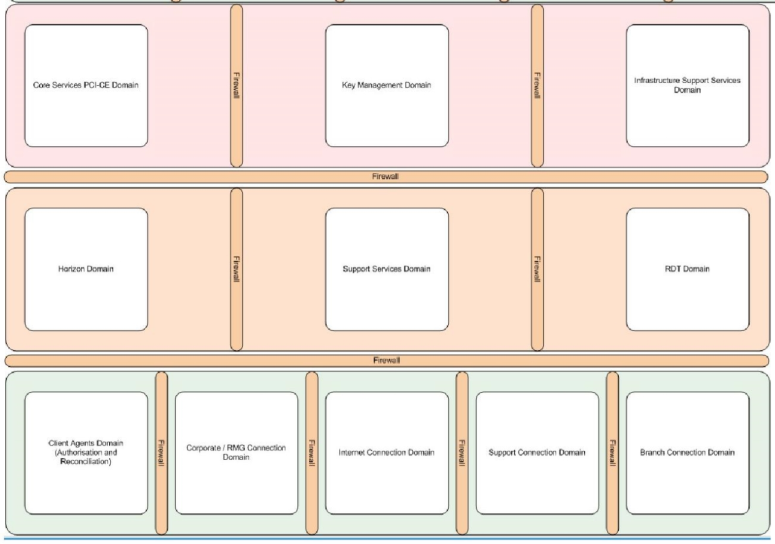

Core Services PCI-CE Domain
Firewall
Key Management Domain
Firewall
Infrastructure Support Services Domain
Firewall
Horizon Domain
Firewall
Support Services Domain
Firewall
RDT Domain
Firewall
Client Agents Domain (Authorisation and Reconciliation)
Firewall
Corporate / RMG Connection Domain
Firewall
Internet Connection Domain
Firewall
Support Connection Domain
Firewall
Branch Connection Domain

Figure 13 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 (SV&I, LST) overlays 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 /~~ BX900 configuration, switch configuration and event monitoring.

The Horizon Platform Hardware Instance List ~~{~~(DEV/GEN/SPE/0007~~}~~) contains a mapping of platform instances to security domains.

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 implemented as part of the operational security management process.

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

For HNG-A Counters:

- Any PCI compliance required at the OS and hardware level is the responsibility of Post Office and the EUC tower.
- Any intrusion detection services are the responsibly of the EUC. This is not a requirement for Fujitsu or the Horizon application, but should be considered as part of the overall security approach~~ and necessary areas to comply with PCI regulations.~~.

8.2.7 Security Services

8.2.7.1 Data Integrity and Confidentiality

The Horizon 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 TLS 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 Card Data.

In regard specifically to Card PANs, the following options are ~~in use~~available:

1) The first 6 and the last 4 characters are in clear. The remaining characters are overwritten using a character such as ‘x’ as a replacement for each character. This algorithm is used for all 13-19 digit PANS and is referred to by PCI-DSS as a Truncated PAN.
   a) For Example: *1234567890127890* becomes *123456xxxxxxxxx7890*
   b) For Counter receipts, this is printed in the form *xxxxxxxxxxxx7890* as per Visa and MasterCard requirements.

2) The first 6 and the last 4 characters are in clear. The remaining characters are 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 is a non-numeric character to facilitate the distinction between hashed and non-hashed PANs.
    a) e.g. *123456Yg20xAWIE7890*
3) The PAN is encrypted.
4) A tokenised value for the PAN is generated by Worldline.

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

- Option 1) is used for writing to log files, receipts, or for report files when the details of the PAN are not required.
- Option 2) is ~~used for~~no longer in use
- Option 3) is no longer in use. With the ~~storage~~implementation of ~~the PAN~~PBS where it is ~~not~~ necessary to obtain a PAN in clear this will requested from Worldline. Note that some pre-PBS PANs are stored encrypted in audit data however
- Option 4) is used where it is advantageous to know the same card has been used across multiple transactions. It is also used for Travel Money card top-ups where a top-up is made against the ~~clear-text PAN.~~token value and the real PAN is retrieved by Worldline from its vault.
- ~~Option 3) is 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 is implemented within each application that needs to use it and uses a seed value to provide extra strength to the algorithm. The seed value is a randomly generated 80 bit value, which is concatenated with the PAN to make a dictionary-style attack much more difficult.~~

~~Network connected hardware security modules (HSM) are deployed to perform encryption and decryption of authorisation messages and data used for the creation of reconciliation files. These modules are Atalla 10160 and 8160 NSPs (Network Security Processor) from Hewlett Packard. Access to the HSM is 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 is implemented to manage the distribution of key material throughout Horizon. 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. 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

The authentication of users is 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 Horizon system are individually identified, through a process controlled by the CS Security Team. Administrative users use strong two-factor authentication when logging on to the system.

Non-administrative users' access to the Horizon system is controlled through applications (such as Tivoli) and they do not have direct access to underlying platforms.

All access into the Horizon system that is non-application controlled (i.e. is interactive) is 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 Horizon system. The SAS servers reside within 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 may use a dedicated SAS support route on creation of a user for the purpose.

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 been authenticated using strong authentication. The management of such users is a manual process, performed by the relevant support groups and overseen by the CS Security team.

A separate RDT PODG Instance provides a facility to transfer information to and from the production environment. It provides a way of delivering operational change into Horizon and a way of getting Management information, statistics and diagnostic information out of Horizon in a secure manner.

Users of the Counter Business Application are access-controlled via tables in the Branch Database.

8.2.7.3 Event Management

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

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

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

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

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

Vulnerability scanning is performed on a regular basis using a combination of external and internal scanning by both the Fujitsu CS Security Team (using McAfee Vulnerability Manager) and by third parties engaged by Post Office. This process ensures that the existence of any known vulnerabilities is identified and quickly resolved.

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

Patching is conducted on a regular cycle and is 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 Horizon system. The Microsoft security configuration tool with the Bastion Host template has been used to harden the Windows 2003 platform foundation. The CIS standards were used to harden the Windows 2012 Server and Red Hat 6 builds. For the purposes of a platform foundation, the Solaris and Red Hat (4, 5) Linux platform foundations are considered to be sufficiently robust through the standard installation. Unnecessary software has been removed and the security settings adjusted to provide extra resilience to attack.

In addition to the system hardening process, there are multiple levels of security control within the Horizon 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 was agreed with Post Office that there is insufficient justification for the following security measures:

#	Control Name	Justification
J3	Encryption on network connections between the two Data Centres	The connections are high speed (Gbit/s) fibre optic point to point connections.
~~J4~~	~~Encryption of online transactions for credit/debit cards to GlobalPayments~~	~~GlobalPayments doesn't support encryption of this traffic~~
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~~

Table 6 Security Measures Considered But Not Justified

8.3 Audit

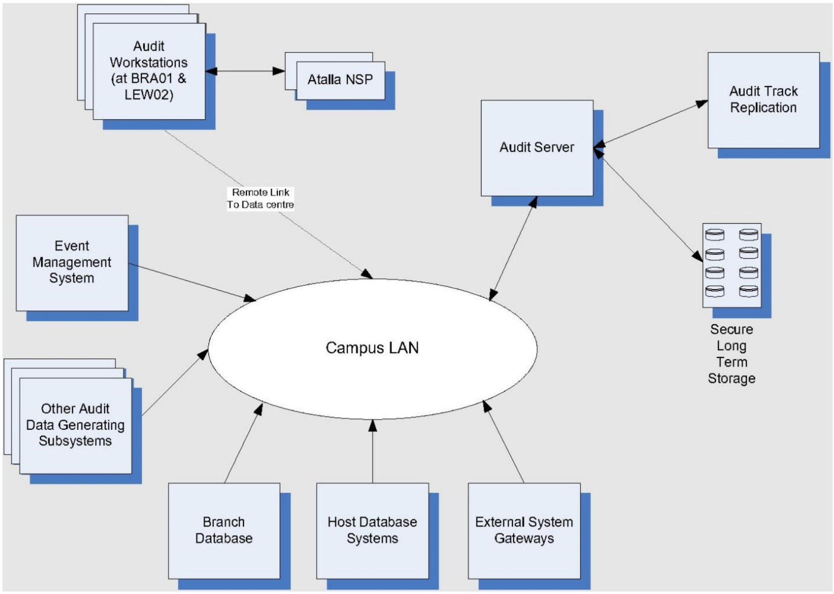


Figure 14 Audit

The Audit system is responsible for gathering Audit Tracks generated by other subsystems and securing them on the local Eternus 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, 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.

9 Training

9.1 Assumptions

The Horizon solution supports 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 Horizon training solution are shown in the diagram below:

Note that in the diagram, in the boxes "Training Only" and "Live Only", Banking and Globalpayments are no longer supported as these calls were removed with the introduction of PBS.

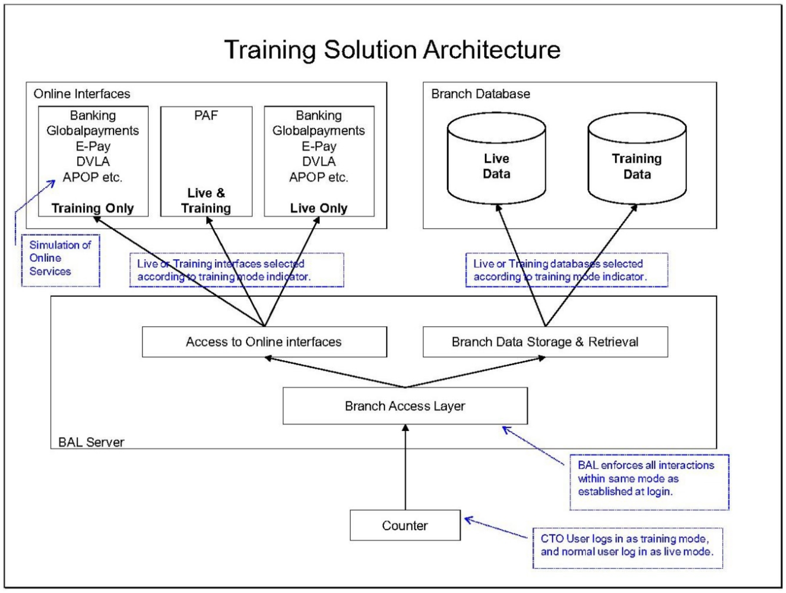

Training Solution Architecture
Online Interfaces
Banking
Globalpayments
E-Pay
DVLA
APOP etc.
Training Only
PAF
Live &
Training
Banking
Globalpayments
E-Pay
DVLA
APOP etc.
Live Only
Branch Database
Live
Data
Training
Data
Simulation of Online Services
Live or Training interfaces selected according to training mode indicator.
Live or Training databases selected according to training mode indicator.
Access to Online interfaces
Branch Data Storage & Retrieval
Branch Access Layer
BAL Server
BAL enforces all interactions within same mode as established at login.
Counter
CTO User logs in as training mode, and normal user log in as live mode.

Figure 15 Training Solution Architecture

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

CTO Branches are created as "standard Branches" within the Live estate. They 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 are handled in the same way as normal mobile Branches (e.g. need a network connection). However, some Mobile CTOs are "multi-counter" and so require a portable hub to connect the counters together~~via the Verizon network.

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

The counter operates with the standard counter hardware~~, including agreed mobile solution. The standard peripherals are 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 are connected by LAN through the shared single Branch router, and there is a shared back office printer.~~ excluding the PIN pad. Training branches use a simulator in place of a PIN pad.

Each CTO counter training session is 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" is only available from CTO Branches.

There are 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) are shared between Live and Training. The system operates 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 reflect transactions performed during the training session and Stock levels reported are adjusted accordingly.

~~All capabilities are supported as per the current Live Reference Data for that Branch.~~Post Office control what on-line services are available to CTOs by specifying the reference data that drives the responses provided by the simulator. Post Office is 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 and Data Centre is protected by the standard session controls which will include the training marker.
- The Branch Access layer ensures that all online requests are handled as Live or training mode as appropriate. Strong controls are in place to ensure a clean separation of services used.

- ~~The~~There is no PIN Pad ~~used~~ in a CTO~~Branches has a~~. CTO's use a simulator to allow training ~~key. Transactions performed with these~~on transactions that use a PIN ~~pads are rejected by the Live Banking online services.~~
- Pad.The training data is cleanly separated from the Live data within the Branch database, so there is no risk of leakage. The training marker on the session indicates where transactions are to be stored within the Branch database.
- The Training "marker" is also stored with the transaction data within the Branch database.
- Training data is not passed to external clients, Post Office systems or the audit stream.

Appendix 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.

Para ref in Schedule B3.2	BUSINESS CAPABILITIES AND SUPPORT FACILITIES	How supported by architecture
2.2	Point of Sale Capability	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service.
2.3	In / Out Payment Capability	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service.
2.4	APOP Facility	HNGA Counter, Branch Session Management, Internal Online Services, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service.
2.5	Banking Capability	HNGA Counter, Worldline, Branch Session Management, ~~External Online Services,~~ Branch Data Storage & Retrieval Services, Enquiry Services, Batch Services and Reference Data Service.
2.6	DVLA Licensing Capability	HNGA Counter, Branch Session Management, External Online Services, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service
2.7	Electronic Top-Up Capability	HNGA Counter, Branch Session Management, External Online Services, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service.
2.8	Bureau de Change Capability	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service.
2.9	Postal Services Capability	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service.
2.10	Payment Management Capability, cash, cheque, vouchers	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service
2.10	Payment Management Capability, Debit or Credit Cards	HNGA Counter, Worldline, Branch Session Management, ~~External Online Services,~~ Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service
2.11	Cash and Stock Management Capability	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service
2.12.1.1	Branch ~~Management Capability~~ManagementCapability Stock unit balancing	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service
2.12.1.2	Branch Management Capability	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services and

Para ref in Schedule B3.2	BUSINESS CAPABILITIES AND SUPPORT FACILITIES	How supported by architecture
	Branch accounting	Reference Data Service
2.12.1.3	Branch Management Capability printing of Client summaries	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service
2.12.1.4	Branch Management Capability Branch reports	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service
2.12.1.5	Branch Management Capability Reversals and Refunds	HNGA Counter, Branch Session Management, External Online Services, Internal Online Services, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service
2.12.1.6	Branch Management Capability Transaction Corrections	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service
2.13	Additional Branch Reporting	Not explicitly shown on the diagram. Supported by a feed from BRSS to POL.
3.2.1.1	Branch Administration Facility User log on / off	HNGA Counter, Branch Session Management.
3.2.1.2	Branch Administration Facility User / password management	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services
3.2.1.3	Branch Administration Facility Stock Unit creation / allocation	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services Batch Services
3.2.1.4	Branch Administration Facility provision of secure inactivity time-out facilities	HNGA Counter, Branch Session Management
3.2.1.5	Not used	n/a
3.2.1.6	Branch ~~Management Capability~~ Administration Facility ~~generic User help system~~Save and recall sessions	HNGA Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service.
3.2.1.7	Branch Administration Facility Postal Services reference data	RDMC, RDDS
3.3.1.1	Branch Support Facility generic User help system	Counter, and Reference Data Service

Para ref in Schedule B3.2	BUSINESS CAPABILITIES AND SUPPORT FACILITIES	How supported by architecture
3.3.1.2	Branch Support Facility Sales Prompts	Counter, and Reference Data Service
3.3.1.3	Branch Support Facility Bulk Input of transactions.	Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Reference Data Service
3.4	Transaction Management Facility (TES)	Enquiry Services Note that with the introduction of PBS there is no useful information in TES. Note TES is no longer supported (post Payment and Banking Trigger Point PBS5 - Completion of Migration to Payment and Banking Service - Payment and Banking Service.
3.5	File Management Facility	Batch Services
3.6	Reference Data Facility	Reference Data Service
3.7	PAF Facility	Counter, Branch Session Management, Internal Online Services
3.8	Message Handling Facility	Counter, Branch Session Management, Branch Data Storage & Retrieval Services
3.9	Audit Facility	Counter, Branch Session Management, Branch Data Storage & Retrieval Services and Support Services
3.10	Reconciliation Facility	Data Transformation & Summarisation and Batch Services
3.11	Training Facility	Counter, Branch Session Management, Internal Online Services, Branch Data Storage & Retrieval Services and Reference Data Service
5.1	POca Card Issuing (no longer supported)	n/a
5.2	Channel Integration Capability	RTS, Session Management
5.3	Not used	n/a
5.4	Smart Metering Capability	HNGA Counter, Branch Session Management, External Online Services, Branch Data Storage & Retrieval Services, Batch Services and Reference Data Service
6.1	Generic Web Services (GWS)	External Online Services
6.2.1.1	Client File Delivery Paystation transactions posted to branch accounts	Batch Services
6.2.1.2	Client File Delivery Paystation transactions collated with HNGA counter transactions	Batch Services
6.2.1.3	Client File Delivery Delivery of AP transaction data to Post Office Clients	Batch Services

Para ref in Schedule B3.2	BUSINESS CAPABILITIES AND SUPPORT FACILITIES	How supported by architecture
6.2.1.4	Client File Delivery Delivery of collated transaction data to POL MI Services	Batch Services
6.2.1.5	Not used	n/a
6.2.1.6	Client File Delivery AP transactions summarised and delivery of Client Transaction summaries.	Batch Services
6.3	Post Office Data Gateway	Batch Services
6.4	Common Digital Platform Adaptor	External Online Services

Table 7 ~~Architectural~~Architecture Component To Business Capabilities And Support Facilities Mapping

Appendix 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.

CONTRACT SUB SCHEDULE AND REFERENCE	HORIZON INFRASTRUCTURE	How supported by architecture
B3.4 Paragraph 2	Branch Infrastructure	The Branch Infrastructure is described in section 3.5.
B3.3 Paragraph 1.2	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.
B3.3 Paragraph 1.3	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.
B3.3 Paragraph 2	Security	Security is described in section 8
B3.3 Paragraph 3	Business Continuity	Business continuity is described within section 6

Table 8 Architectural Component to Sub-Schedules B3.3 and B3.4 mapping