FUJ00088336

Document Title:	HNG-X Technical Security Architecture
Document Type:	Architecture (ARC)
Release:	
Abstract:	Describes the Technical Security Framework for HNG-X
Document Status:	APPROVED
Author & Dept:	Jim Sweeting
Internal Distribution:	N/A
External Distribution:	See Reviewers Details

Approval Authorities:

Name	Role	Signature	Date
Jim Sweeting	Security Architect		
Dave Johns	CTO		
Phil Day	Programme Manager		

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

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.

FUJ00088336

0 Document Control

0.1 Table of Contents

FUJ00088336

FUJ00088336

FUJ00088336

0.2 Figures and Tables

FUJ00088336

0.3 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	09/11/2006	First draft	
0.2	24/11/2006	Draft version for review.	
1.0	22-Oct-2006	First formal release for approval.	
1.1	19-02-2007	Updated for PCI including changes for monitoring and Branch Access Layer	
1.2	16-01-2008	Updates PCI section Updated Security Tiers and Domains section Updated Migration Section	
1.3	6-03-2008	Significant rewrite and update following POL and Group Review comments. Applied updated format	
1.4	11-06-2008	Revised and issued for review.	
1.5	08-01-2009	Draft for issue by Acceptance by Document Review. Document now contains Acceptance by Document Review Table.	
2.0	08-01-2009	Document Approved	

0.4 Review Details

Review Comments by :	
Review Comments to :	Jim Sweeting & PostOfficeAccountDocumentManagement@ GRO
Mandatory Review	
Role	Name
Post Office	Paul Halliden
Post Office	Dave King
Post Office	Connie Penn
Solution Design	Adam Cousins (Counter & BAL/OSR) David Harrison (Host & RefData) Peter Ambrose (Legacy Web Svcs, Agents & Audit) Gavin Scruby (Estate Mgmt) Peter Ambrose (Crypto)
Infrastructure Design	Geof Slocombe (or nominees)
HNG-X Service Transition	Graham Welsh
Information Governance	Brian Pinder
Test Design	Peter Robinson
Test Design	John Halfacre

FUJ00088336

System Qualities Architecture	Dave Chapman
Architect	Pat Carroll
Architect	Andy Williams
Architect	Ian Bowen
Architect	Terry Jack
Architect	Mark Jarosz
Architect	Nasser Siddiqi
Architect	Alan Holmes
Architect	Dave Haywood
Architect	Jason Clark
Architect	Jason Swain
Architect	Lee Walton
Development	Adrian West
Service Network	Alex Kemp
Service Support	Peter Thompson
System Test	John Rogers
SV&I Manager	Sheila Bamber
Tester	Hamish Munro
SSC	Mik Peach
Business Continuity	Tony Wicks
Data Centre Migration	Brian Ridley
Security	Peter Sewell
Security	Bill Membery
Core Services	Ed Ashford
Core Services	Mark Walsh
Core Services	Andrew Gibson
Lead Architect	Dave Johns
Optional Review	
Role	**Name**
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	**Name**
Requirements Manager	David Cooke

(*) = Reviewers that returned comments

FUJ00088336

0.5 Acceptance by Document Review

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

POL NFR DR Acceptance Ref	Internal FS POL NFR Reference	Document Section Number	Document Section Heading
SEC-3058	SEC-3259		Whole document
SEC-3063	SEC-3260	2.4	Security Tiers and Domains
SEC-3063	SEC-3260	4	Networks
SEC-3069	SEC-3261	6.1.3	Security: Data Integrity and Confidentiality Service : Data Integrity
SEC-3069	SEC-3261	6.2.2.2	Application and Business System Authentication and Authorisation
SEC-3073	SEC-3262	3.1	Platforms: System Layers
SEC-3073	SEC-3262	6.2.2.2	Application and Business System Authentication and Authorisation
SEC-3111	SEC-3271	2.3.2	Principle 2–Least Privilege Access Control
SEC-3111	SEC-3271	4	Networks
SEC-3117	SEC-3117	3.1.2	Platforms: System Layers: Data
SEC-3129	SEC-3276	6.4.2	Vulnerability Management Service: Architectural Overview
SEC-3133	SEC-3277	3.1.1.1	Platforms: System Layers: Application: Data Centre
SEC-3137	SEC-3137	3.1.1.1	Platforms: System Layers: Application: Data Centre
SEC-3140	SEC-3278	6.2	Identity and Access Management Service
SEC-3140	SEC-3278	3.1.2	Platforms: System Layers: Data
SEC-3140	SEC-3278	3.1.3	Platforms: System Layers: Operating System
SEC-4140	SEC-3278	4.4.1	Networks: Branch Network: Counter
SEC-3142	SEC-3279	4.3.3	Internet Access
SEC-3150	SEC-3280	4.1	Network Segmentation
SEC-3150	SEC-3280	4.3	Remote Access
SEC-3152	SEC-3281		Whole document
SEC-3156	SEC-3282	4.2	Intrusion Prevention and Detection
SEC-3160	SEC-3283	4.1	Network Segmentation
SEC-3162	SEC-3284	2.3.10	Principle 10 – Close the Loop
SEC-3162	SEC-3284	4.2	Intrusion Prevention and Detection
SEC-3162	SEC-3284	6.3	Event Management Service
SEC-3167	SEC-3167	4	Networks
SEC-3167	SEC-3167	6.1.4	Secure Communications

FUJ00088336

SEC-3168	SEC-3168	6.1	Data Integrity and Confidentiality Service
SEC-3169	SEC-3169	4	Networks
SEC-3174	SEC-3288	2.4.2	Security Domains
SEC-3174	SEC-3288	4.1	Network Segmentation
SEC-3174	SEC-3288	6.1.2	Data Integrity and Confidentiality Service: Service Overview
SEC-3176	SEC-3289	4.1	Network Segmentation
SEC-3199	SEC-3295	6.1.3	Data Integrity and Confidentiality Service: Data Integrity
SEC-3199	SEC-3295	6.2	Identity and Access Management Service
SEC-3211	SEC-3299	6.2	Identity and Access Management Service
SEC-3211	SEC-3299	3	Platforms
SEC-3213	SEC-3300	3.1.1.1	Platforms: System Layers: Application: Data Centre
SEC-3216	SEC-3216	6.1.2.2	Pin Pads
SEC-3218	SEC-3218	6.1	Data Integrity and Confidentiality Service
SEC-3219	SEC-3219	6.1.5	Data Confidentiality
SEC-3231	SEC-3304	3.1.2.1	Platforms: System Layers: Data: Data Centre
SEC-3231	SEC-3304	6.1.6	PCI PAN Protection
SEC-3231	SEC-3304	6.5	Payment Card Industry Solution - Debit/Credit Card System
SEC-3231	SEC-3304	6.6	Payment Card Industry Solution - Network Banking System
SEC-3233	SEC-3307	3.1.2.1	Platforms: System Layers: Data: Data Centre
SEC-3233	SEC-3307	6.1.6	PCI PAN Protection
SEC-3233	SEC-3307	6.5	Payment Card Industry Solution - Debit/Credit Card System
SEC-3233	SEC-3307	6.6	Payment Card Industry Solution - Network Banking System
SEC-3235	SEC-3235	3.1.1.1	Application : Data Centre
SEC-3235	SEC-3235	3.1.3	Operating Systems
SEC-3235	SEC-3235	6.1	Data Integrity and Confidentiality Service
SEC-3236	SEC-3310	6.1.4.1	Public Networks
SEC-3236	SEC-3310	6.5	Payment Card Industry Solution - Debit/Credit Card System
SEC-3236	SEC-3310	6.6	Payment Card Industry Solution - Network Banking System

0.6 Associated Documents (Internal & External)

FUJ00088336

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	1.0	13/6/06	Fujitsu Services Post Office Account HNG-X Document Template	Dimensions

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

0.7 Abbreviations

Abbreviation	Definition
ACL	Access Control List
AES	Advanced Encryption Standard
AIS	Application Interface Specification
ARQ	Audit Record Query
BDK	Base Derivation Key
BKLK	Basic Key Loading Key
BSK	Base Derivation Key
CA	Certificate Authority
DCS	Debit Card System (Including Credit cards)
DCSM	Debit Card Management Service
DES	Data Encryption Standard
GKLK	Global Key Loading Key
HIDS	Host-Based Intrusion Detection System
HLD	High Level Design
HSM	Hardware Security Module
IK	Initial Key
IP	Internet Protocol
IPSEC	IP Security
LLD	Low Level Design
LPAN	Logical Processing Area Network
MAC	Message Authentication Code
NAS	Network Attached Storage
NBS	Network Banking System
NSP	Network Security Processor
OID	Object Identifier
PAM	Pluggable Authentication Module
PAN	Primary Account Number
PAN	Processing Area Network (In Section 3)
PCI	Payment Card Industry

FUJ00088336

PCI DSS	Payment Card Industry Data Security Standard
PED	PIN Encrypting Device
PKI	Public Key Infrastructure
POL-FS	Post Office Limited – Financial Service
POL-MIS	Post Office Limited – Management Information Service
SAN	Storage Area Networking
SLA	Service Level Agreement
SRP	Secure Remote Password
SSH	Secure Shell
SSL	Secure Sockets Layer, (also referred to as HTTPS)
TDES	Triple DES Encryption Standard
TIS	Technical Interface Specification
TLS	Transport Layer Encryption
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

0.8 Glossary

Term	Definition
IPSEC	A suite of standards used for providing confidentiality and integrity of network traffic.
Cardholder Data	PCI Term defined as; the PAN or the PAN plus any of the following: • cardholder name • expiration date • Service Code • start date • issue number;
ISO27001	International Standard for Information Security Management.
Salt	A string, (usually randomly generated), that is added to a clear-text value, about to be hashed or encrypted, to make it more difficult post-hash or post-encryption, to establish what the clear-text value was.
Sensitive Authentication Data	PCI Term defined as; Security related information used to authenticate cardholders appearing in plain text or otherwise unprotected form. This information can be any of the following: • Card Validation Code • Card Validation Value

FUJ00088336

	• Full Track • PINs • PIN blocks (including encrypted PIN blocks);

0.9 Changes Expected

Changes
No further changes are expected to this Architecture document except those resulting from the approval of CPs.

0.10 Accuracy

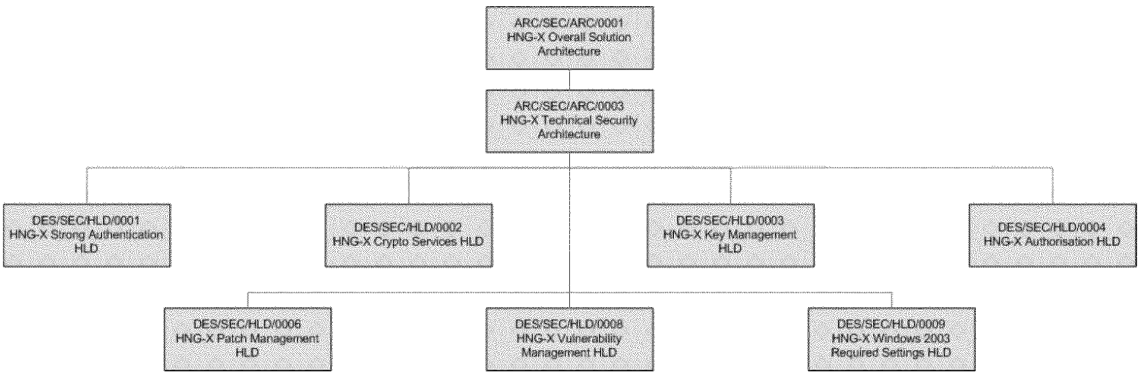
Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.11 Copyright

FUJ00088336

1 Scope

This document is a **Topic Architecture** and is part of the first level of decomposition beneath ARC/SOL/ARC/0001 – the HNG-X Overall Solution Architecture.



This document describes the technical security framework proposed for HNG-X. As applicable to the technical security solution, it covers the principles, process and standards that should be used during the design, development and operation of the HNG-X system.

This document uses the Open Group description of an architecture which is:

> **"The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time."**

When correctly implemented, security is not a block on business activity and progress, but is a business enabler allowing change to take place as quickly as the business requires, but in a secure and controlled fashion.

It is very important therefore that a set of guiding principles are agreed and established, and embedded into the planning, change management and operational processes of HNG-X.

The security architecture has been designed in accordance with the SOA principles defined in the HNG-X Overall Solution Architecture document, {ARC/SOL/ARC/0001}.

This architectural document is expected to be revised and updated throughout the lifespan of the HNG-X system.

FUJ00088336

2 Architectural description

2.1 Requirements

Requirements are documented in Section 12 Requirements Traceability.

2.2 Security Strategy

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

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

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

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

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

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

2.3 Principles

A set of principles must be established to guide the secure Design, Development, Test, Implementation and Operation of the HNG-X system. These principles must be;

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

II. Carefully considered

III. Objective

FUJ00088336

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

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

These principles are explained in more detail in the following sections;

2.3.1 Principle 1 - Use a Risk Based approach

Security controls must be selected on the basis of risk assessment. This risk assessment is largely conducted by the CS Security Team and the Security Architect, however it is an ongoing process and design and development groups are also expected to use a risk analysis process, with guidance if required, to establish the controls that should be implemented.

2.3.2 Principle 2 – Least Privilege Access Control

Both internal and external access must be controlled within the HNG-X infrastructure. This includes segmentation of the Data Centre LAN, the BladeFrame and the use of role based access control.

Support users will be authenticated using strong, two-factor, authentication. Application designers and developers are responsible for conducting a risk assessment, (as per Principle 1), to establish the access controls that their applications must enforce. The risk analysis, decisions and implications must be clearly documented.

Access rights must be validated on initial access to the Horizon-Online system to ensure that attempted unauthorised access is detected and prevented.

Access must be provided using the principle of “that which is not explicitly granted is denied” or a “default deny”, (otherwise known as the, “least privilege”, stance), by only granting the permissions necessary to carry out the action being performed. These permissions include application, platform, network and management, (through policy and process), or any combination necessary to perform the action.

This approach assumes that, subject to risk assessment and given the limitations of an operating system or other software, any entity such as a user, an application, a device or an object within application code has no permissions to perform any action before permissions are granted. This assumes that the default configuration of all systems is to deny access. It is very important to ensure that the permissions matrix is developed correctly to ensure that all entities have the access they need to perform their function.

Assumptions must not be made about what is secure and what is not without a corresponding risk assessment exercise. This includes access to and from other applications and systems, as well as network level access. A system should not accept or make connections to another without appropriately validating its identity.

A security domain model has been designed to effectively segregate the HNG-X infrastructure, such that systems with a similar criticality level are grouped together and systems exposed to a similar level of risk are grouped together.

Traffic passing between security domains must be controlled to only allow the relevant protocol and port necessary for the service being accessed.

2.3.3 Principle 3 - Detect Anomalous Activity

Following the security strategy outlined in 2.2 above unusual activity must be prevented, contained, detected and responded to as defined in the Information Security Policy {SVC/SEC/POL/0003}.

This will include the long-term analysis of performance data as well as the use of tools such as event log and audit trail monitoring, intrusion detection and prevention and performance monitoring.

FUJ00088336

2.3.4 Principle 4 - Maintain Systems

To reduce the number of vulnerabilities available to exploit, systems within HNG-X should be maintained through the regular updating, tuning and patching of operating systems, appliances and applications.

Hardening of systems by removing unnecessary services and setting user, object and filestore permissions appropriately also ensures that the number of vulnerabilities is reduced. The hardening process will also include the changing of default settings, where necessary, such as passwords of any kind and excessively permissive user and file system rights.

Specific hardening steps will be defined during the design phase of the project.

NOTE: The hardening process must be appropriate to the intended use of the Platform and should not take away any essential capability of the system that is needed by the application.

2.3.5 Principle 5 - Ensure Compliance

Compliance with all relevant policy, legislation, regulation and standards is essential. This is provided to the Architecture, Design and Development teams in the form of requirements that must be analyzed and met in an appropriate fashion.

2.3.6 Principle 6 - Defence in Depth

Use a layered approach to security to provide multiple controls for prevention and detection. These controls will include application, platform, network and management controls. Controls and their relevance will be established by risk assessment, the results of which must be documented.

Both external and internal services and infrastructure should not be considered to be secure just because they have gained access. It is always a possibility that an internal system has been compromised and if data is accepted unquestioningly, a large scale incident may occur. Therefore assumptions on the integrity and validity of data should not be made just because the data has been received from what is considered to be a secure source. i.e. if data is transmitted between systems in the HNG-X Data Centre, an appropriate level of data validation should still take place.

Where risk assessment has indicated it is necessary, input and output data must be validated using an appropriate means. This is to ensure the integrity of data and to prevent security breaches caused by unexpected data being sent or received, including through the transmission of unexpected quantities of data.

2.3.7 Principle 7 - Reduce Security by Obscurity

Security achieved purely through the use of information hiding is not acceptable. A risk assessment conducted at anytime during the architectural, design, development or operational stages of the programme is an acceptable way to identify where this is being done.

If information hiding is necessary due to technical or other limitations or constraints, then additional security controls must be considered and implemented to provide additional protection.

This is particularly relevant to the area of clear-text passwords, required by an automated process. If automatically obtained clear-text passwords are necessary, then additional access controls should be implemented to increase security.

2.3.8 Principle 8 - Fail Secure

System failure should not allow the system to be compromised. Within the limits of the technology and availability requirements, any component of the system that fails due to error or malicious activity should fail secure. This failure event must be detected as early as possible so that suitable containment and remediation activities can be carried out.

FUJ00088336

In this particular case, (due to the nature and purpose of the HNG-X system), consideration must be given to availability as an overriding principle, to ensure that a minor failure does not cause some or all of Branch Trading to be suspended.

In the event of error messages being generated, either on screen or in log files, these must reveal minimal information to non authorised users.

A system failure or error must not reveal sensitive information as defined by the HNG-X Security Policy. {RS/PRO/0002 to be superseded by SVM/SEC/POL/0003 when approved}

This includes Sensitive Authentication Data and Cardholder Data as defined by the PCI Data Security Standard v1.1

2.3.9 Principle 9 - Simple is Good

The solution must be designed to be, "as simple as it needs to be, but no simpler."

This involves the analysis during each design and development phase to establish what is critical functionality and what is a "nice to have"!

2.3.10 Principle 10 - Close the Loop

Ensure that there is a feedback loop such that events and alerts are generated, incidents are raised and remedial actions are generated. This follows the security strategy of prevention, containment, detection and response.

2.4 Security 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)

2.4.1 Security Tiers

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

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

FUJ00088336

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

2.4.2 Security Domains

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

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

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

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

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

The following figure illustrates the security tiers and domains in diagrammatic form.

FUJ00088336

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 dependant 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 to assist in the development of firewall and Router access lists.

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

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

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

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

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

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

The following table describes the purpose of each security domain;

#	Name	Description
1.	Core PCI-CE Domain	HNG-X Database Platform Types that store, process and

FUJ00088336

		transmit encrypted and hashed PANs.
2.	Key Management Domain	HNG-X Platform Types that manage cryptographic material.
3.	Infrastructure Support Services Domain	HNG-X Platform Types that manage and control the infrastructure, such as Active Directory and DNS Servers.
4.	Horizon Domain	Virtualised retiring Horizon Platform Types
5.	Support Services Domain	HNG-X Platform Types responsible for the management of Audit Data.
6.	RDT Domain	Reference Data Team testing environments
7.	Client Agents Domain	HNG-X Platform Types responsible for communication with Post Office clients.
8.	Corporate / RMG Connection Domain	HNG-X Platform Types responsible for communication with the Fujitsu Corporate network and with the Royal Mail network.
9.	Internet Connection Domain	HNG-X Platform Types responsible for communication across the Internet.
10.	Support Connection Domain	HNG-X Platform Types responsible for managing support connections
11.	Branch Connection Domain	HNG-X Platform Types responsible for Branch communication and management

2.5 Control Objectives

The control objectives used in this document come from ISO27001 – The International Standard for Information Security Management Systems and are employed as a method of providing a consistent approach to solving security issues.

The control objectives of ISO27001 are as follows:

1) Security Policy Management
2) Corporate Security Management
3) Organisational Asset Management
4) Human Resource Security
5) Physical and Environmental Security
6) Communications and Operations Management
7) Information Access Control Management
8) Systems Development and Maintenance
9) Information Security Incident Management
10) Business Continuity Management

FUJ00088336

11) Compliance Management

The standard lists a number of suggested controls under each of these sections but the implementation, or otherwise, of these controls is decided by risk assessment. The risk assessment is conducted as one of the activities of the Information Security Management System (ISMS). The creation of the ISMS is the main purpose of the standard.

The security requirements of HNG-X are mapped to the relevant control objectives as documented in Section 12 Requirements Traceability.

FUJ00088336

3 Platforms

The definition of a platform in this document is taken from HNG-X Architecture - Platforms and Storage (ARC/PPS/ARC/0001);

Platform Foundation: the combination of HNG-X approved hardware and a HNG-X approved operating system for the purpose of hosting an HNG-X application, service or function in the HNG-X data centre; the platform foundation is provisioned through an automated process

Platform Type: a type of server hosting a business application or infrastructure service that is part of the HNG-X solution and hosted in the HNG-X data centres, a platform can have multiple **Platform Instances** and is built from a Platform Foundation

Each **Platform Instance** is managed using Tivoli Systems and Event Management software as defined in;

- HNG-X System And Estate Management Overall Architecture {ARC/SYM/ARC/0001}
- HNG-X System And Estate Management Monitoring {ARC/SYM/ARC/0003}
- HNG-X System And Estate Management Remote Access And Diagnostics {ARC/SYM/ARC/0004}
- HNG-X Estate Management Component Architecture {ARC/SYM/ARC/0005}
- HNG-X Provisioning and Platform Software Lifecycle {ARC/SYM/ARC/0007}

All events from each Data Centre **Platform Instance** system event log are captured by the Tivoli software and sent to a central aggregation point.

The Tivoli system maintains the integrity and confidentiality of the data in this central store through a combination of platform and application access, and other, security controls. In addition, the audit system collects events from the Tivoli system on a scheduled basis, and adds them to the Centera audit data store.

Software installations and updates for operating systems and applications are performed using the HNG-X System and Estate Management Software Distribution and Asset Management {ARC/SYM/ARC/0002}.

This mechanism is fully audited through the use of formal change management, configuration management and release management processes in conjunction with the technical access controls and auditing facilities within the Tivoli product itself.

It is therefore possible to trace the path of a single piece of software from its initial entry into the Dimensions system to its installation on an end-point platform instance or instances.

3.1 System Layers

Each Horizon-Online system or device can be further subdivided into four additional layers and by using these it is possible to define both the functions that take place at that layer and the security strategy for each layer.

The four layers are;

1) Application
2) Data
3) Operating System
4) Network

These layers are defined as below;

FUJ00088336

3.1.1 Application

This is the data processing and presentation layer utilising the services provided by the software and by the other three layers of the model.

Application development in HNG-X uses a variety of tools and languages, most notably Java, C++ and PERL. The principles in this document are intended as guidance for the development community and should be used in conjunction with the guidance expressed in documents such as HADDIS {DES/GEN/STD/0001} and other Best Practice guides from Vendors such Microsoft and Sun.

3.1.1.1 Data Centre

The strategy for the application layer is to prevent security incidents by ensuring that data is entered correctly, processed correctly and is validated, following the security principles defined in section 2.3 Principles. This will be achieved through strict control of the application development process and specific application security testing.

Exceptions detected by the application will be logged and an alert will be raised, by the Tivoli systems management subsystem, when appropriate criteria have been met.

Dependent on each application design, different levels of logging will be possible to facilitate the troubleshooting and debugging process. This facility will be developed to ensure that sensitive data, (either related to the PCI-DSS or to the Data Protection Act), is dealt with appropriately and in accordance with the Information Security Policy {SVM/SEC/POL/0003}.

The Tivoli system will be configured to forward events from the local system event log by default. Where necessary it will also be configured to collect events from other application logs, (such as bespoke text files).

Any passwords stored or transmitted must be encrypted or otherwise obscured by using symmetric, (AES 256, TDES), or asymmetric encryption, (RSA 1024/2048), or by using a salted hash algorithm, (minimum of 80 bits).

NOTE: The use of debug traces and detailed event logs is permitted, however passwords must be overwritten with asterisks '' if they are also written to the log.*

The principle strategy for this layer is prevention and, following the principle of Least Privilege, applications must only run in a user context that provides them with the access permissions they need. Unless explicitly required, (the reasons for which must be documented in detail in the design), accounts used by applications must not be capable of interactive logon. (i.e. They must not be usable by human users), nor must they be capable of network access. This applies to both COTS and bespoke software and applications.

Database access control also required individual role-based accounts for each class of user, both for controlling the actions a user can perform and for ensuring all administrative and other actions are traceable to an individual to provide a valid and informative audit trail.

The main classes of database users will be;

1) Application – Accounts used by applications for database access to either Oracle or SQL Server Databases.
2) System Administrators – Operational support users with responsibility for managing the database systems.
3) Database Administrators – Operational support users with responsibility for specific databases.
4) Non-administrative Database support users - Operational support users with responsibility for specific databases.

During the detailed design stage, an analysis will be performed by the designers and developers to assess the rights needed for each COTS product and bespoke software component/application to ensure they do not have excessive rights. This analysis will be documented in detail, with reasons for the decisions. Where this analysis establishes that administrative or super-user rights are required, the use of such rights is permitted.

FUJ00088336

The hardening process will set the rights and permissions required by the platform, according to the relevant roles and users.

Java applications requiring database access, (such as the Branch Access Layer); will be developed to use Java prepared statements and all database access permissions will be granted following the principle of Least Privilege. The combination of these two controls will prevent SQL Injection-style attacks from being successfully attempted, even if a malicious attacker could gain access to the network to execute this type of attack in the first place.

In addition to the logical network access controls such as Utimaco VPN, SSL and firewall access lists to reduce the risk of unauthorised connection to the network, (thereby reducing the risk of being able to inject messages into the network that have not come from an authorised Counter), transaction message validation will be implemented in the Branch Access Layer and the Authorisation Agents to mitigate the risk of replay attacks.

The validation will consist of the verification of unique transaction numbers, time verification and the validation of the transaction message digital signature. The digital signature is provided using a key pair created during the initialisation of the authorised session and is therefore unique to that particular session. This also mitigates the risk of an attacker gaining access to the private key and being able to sign their own transactions as this only has a very limited lifetime. In the event that a duplicate transaction number is received, it will be rejected by the BAL and the Authorisation Agent. Any modification of a transaction number will invalidate the digital signature resulting in the rejection of the transaction and the raising of an alert.

This will ensure that transaction messages can only originate from a valid Counter during an authorised session and that a transaction message cannot be submitted more than once.

During the Hydra phase of the Migration, when the BAL will be accepting messages from both Horizon and HNG-X Branches, the Horizon digital signature mechanism will be retained for Horizon transactions to ensure that they originate from a valid Horizon Branch. This is also necessary as a replacement for the MAC functionality on EMV transactions that do not involve a PIN entry. (For clarity, swiped transactions and EMV transactions that involve PIN entry can generate a MAC for the transaction).

3.1.1.2 Branch

3.1.1.2.1 Windows NT

There are a number of stages in the process of moving from the existing Riposte Windows NT Counter to the HNG-X Counter. These are as listed below;

1. Horizon PCI Counter Update
    1.1. This is a Counter change package that will be implemented once the HNG-X Data Centres have gone live with the Branch Access Layer. This change is being implemented to cease the retention and encryption of Track 2 data for Debit and Credit card transactions and to hash the PAN in accordance with Post Office requirements for the PCI-DSS.
2. Horizon HNG-X Application Update
    2.1. This is a Counter change package that implements the new Horizon-Online Counter Java application as a complete replacement of the Riposte product.
    2.2. Full details of the steps involved in this process are in the Counter Architecture document {ARC/APP/ARC/0003}
3. Utimaco VPN Update
    3.1. This is a Counter and Data Centre change package that changes the operation of the Utimaco VPN product on the Counter and in the Data Centre. This change is being implemented to reduce the vulnerabilities and risks surrounding the continued use of the Windows NT operating system on the Counter.

FUJ00088336

3.2. In the event of a Counter operating system upgrade, the Utimaco product will be retired. Requirements for a replacement will be analyzed and designed once such an upgrade has been scoped.

4. Proposed Counter Hardware and Operating System Update (Currently scheduled for HNG-X Release 2)

The Counter business application replaces the MSGINA.DLL used as the login screen on Microsoft Windows Operating Systems. The appropriate application and system access rights will be established and applied, and the underlying operating system will be hardened to ensure that the users of the business application cannot bypass it and access the operating system itself.

3.1.1.2.2 Windows XP

A Windows XP Counter is not in scope for Release 1 of HNG-X

3.1.1.3 Remote

Support users will be provided with access to the operating system as described in the Remote Support section of this document, Section 5 - Manageability

3.1.2 Data

3.1.2.1 Data Centre

The Data Layer is responsible for the storage, integrity and management of application, platform and network information.

There are a number of different classes of data within the Horizon-Online system. These are as follows;

1. Transaction Data from Counters

   1.1. This is data produced as a result of transactions conducted on the Counter. This includes debit and credit card transactions, banking transactions, voucher transaction and others conducted on behalf of a third-party such as bill payments and car tax.

   1.2. For compliance with Post Office requirements in relation to sensitive authentication data and cardholder data as defined by the PCI-DSS, the following requirements will be met for Horizon-Online Counters. [FOR THE AVOIDANCE OF DOUBT, THESE CHANGES DO NOT APPLY TO DATA ALREADY COLLECTED BY THE AUDIT OR OTHER DATA CENTRE SYSTEMS. NEITHER DO THEY APPLY TO HORIZON COUNTERS PRIOR TO THE HORIZON PCI CHANGE.]

      1.2.1. No full track, (magnetic stripe or chip), images will be stored post-authorisation.

      1.2.2. No PIN or PIN Block information will be stored post-authorisation.

      1.2.3. No CVV2, CVC2 or CID information will be stored. (This data is used for card not present transactions which the Horizon-Online system does not currently perform)

      1.2.4. PANs will be hashed, encrypted or otherwise obfuscated by overwriting.

   1.3. This transaction data is also collected by the Audit sub-system, (as defined in the HNG-X Support Services Architecture ARC/SVS/ARC/0001). Currently Fujitsu Services are contractually required to retain such data for 7 years.

2. Event Log Data

   2.1. This is data written to the Platform operating system event log or to text files, which is then collected, filtered where necessary and forwarded to the Tivoli event management system.

   2.2. This event log data is also collected by the Audit sub-system, (as defined in the HNG-X Support Services Architecture ARC/SVS/ARC/0001). Currently Fujitsu Services are contractually required to retain such data for 7 years.

FUJ00088336

3. Personal Data

3.1. Personal data is defined by the Data Protection Act 1998 as that data which when used on its own, or in conjunction with other data, can identify a living individual.

3.1.1. In this Act "sensitive personal data" means personal data consisting of information as to;

3.1.1.1. The racial or ethnic origin of the data subject,

3.1.1.2. His political opinions,

3.1.1.3. His religious beliefs or other beliefs of a similar nature,

3.1.1.4. Whether he is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),

3.1.1.5. His physical or mental health or condition,

3.1.1.6. His sexual life,

3.1.1.7. The commission or alleged commission by him of any offence, or

3.1.1.8. Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

3.1.2. In respect of Horizon-Online, there is no defined policy requirement to store any of these data.

The data requested and stored through the use of Post Office created AP transactions is currently unknown by, and not under the control of, Fujitsu Services.

3.2. The Horizon-Online system collects such data during a number of transactions, particularly those involving the recording of personal data as a requirement of the transaction such as Moneygram, DVLA and the Broadband service.

3.3. Applications and house-keeping procedures should be developed, (under change control), to ensure that such data is only retained for the length of time defined in the HNG-X Security Policy.

3.4. This personal data is also collected by the Audit sub-system, (as defined in the HNG-X Support Services Architecture ARC/SVS/ARC/0001), except where the requirements of a service specifically exclude its collection. Currently Fujitsu Services are contractually required to retain all such data for 7 years.

Databases and Database applications will be designed following the principles outlined in this document and the best practices described in HADDIS {DES/GEN/STD/0001}.

3.1.2.2 Branch

The existing Windows NT Counter retains a significant quantity, (currently 84 days), of encrypted Branch transaction data within its local Riposte message store. The encryption key is protected by the Postmasters POLO card which is required for initial start-up and logon of the Counter. Part of the Counter migration process results in the removal of the POLO authentication method once the Counter is updated to the HNG-X application. This means that the sole authentication method on the Counter is now the Branch employee username and password. This also removes a security protection layer for the Counter hard-drive. As a consequence, although the data in the Riposte message-store is still encrypted, the Riposte message-store will be deleted within a short time period following the Counter upgrade. This will be a matter of days, but is dependent on events within each individual Branch during the migration period.

Horizon-Online Counters will retain no sensitive data. All recovery data is maintained by the Branch Database and any event or diagnostic logs will contain only sanitised information.

Disk cache on HNG-X Counters will not be encrypted on the grounds that the management of such encryption outweighs any potential exposure of single PANs stored in the cache.

FUJ00088336

This is only considered to be a risk in the event that a Counter crashes, or has its power supply terminated whilst operating, hence leaving cached data on the disk. The Counter will be developed to flush the cache at the conclusion of each business day.

3.1.2.3 Remote

Data that must be sent to a third-party, including Royal Mail and Post Office, must only be sent using approved methods and media, as defined by the HNG-X Information Security Policy {SVM/SEC/POL/0003}.

The confidentiality, integrity and availability of such data must be considered and formally documented prior to the data being extracted and sent.

This is particularly important when considering transmission of the following;

1. Personal information
2. Cryptographic key material
3. Network trace files
4. Database dumps or extracts
5. Event logs
6. Diagnostic logs. (Distinct from event logs as diagnostic logs usually contain a greater quantity of low-level detail)
7. Raw transaction data.
8. Encrypted data such as PANs.

This list is not exhaustive and analysis will be done during the design and development phases of the HNG-X project to ensure that the risk of leakage of sensitive information is reduced to a minimum.

The protection of remote data ceases to be the responsibility of the Horizon-Online system, once it has left the Data Centre or Fujitsu premises.

There is no other remote data within the scope of this document.

3.1.2.4 Oracle

Oracle databases, (such as the Branch Database), will be configured in a secure fashion following the guidance contained in the Oracle Database Security Checklist Guide. {DES/PPS/MAN/0002}

Database user accounts will be created as described in 3.1.1.1 above. Privileges for such accounts will be managed using database access controls and will be guided by;

1) The purpose and design of the database
2) HADDIS {DES/GEN/STD/0001}
3) Oracle Database Security Checklist Guide. {DES/PPS/MAN/0002}

3.1.2.5 SQL Server

SQL Server databases, (such as the Estate Management Database - EMDB), {DES/SYM/HLD/0031}, will be configured in a secure fashion following the guidance contained in the Microsoft SQL Server 2005 Security Best Practices guide. {DES/PPS/MAN/0003}

Database user accounts will be created as described in 3.1.1.1 above. Privileges for such accounts will be guided by;

1) The purpose and design of the database
2) HADDIS {DES/GEN/STD/0001}

FUJ00088336

3) Microsoft SQL Server 2005 Security Best Practices guide. {DES/PPS/MAN/0003}

3.1.2.6 File

Data held on file store will be secured, as appropriate, using a combination of the following security controls;

1) File / Disk Encryption
2) File / Directory permissions
3) Group / Role and User access control

In addition to the above controls, file system auditing using native OS facilities or alternative software will be implemented on specific platform types where this has been determined to be necessary through risk assessment

3.1.2.7 Removable Media

Any date transferred to removable media for storage or transport must be appropriately secured in line with the HNG-X Information Security Policy {SVM/SEC/POL/0003}.

Removable media includes, but is not restricted to, CD, DVD, Memory Stick, other USB connected devices such as hard drives and any other method of transporting data.

On receipt of removable media, the contents must be checked for malicious code and the integrity of the data thereon must also be verified.

3.1.3 Operating Systems

A definitive list of the Platform Types and their associated operating systems is maintained in the Platform Hardware Instance List {DEV/GEN/SPE/0007}.

Following the security strategy of prevention, containment, detection and response, a specific Horizon-Online build, (the **Platform Foundation**), has been created.

The Platform Foundation will then be suitably hardened by following a policy of removing unnecessary software from the system, applying the latest relevant patches, and setting appropriate permissions contained in the following documents;

1) Windows Server 2003 Security Guide {DES/PPS/MAN/0004}
2) Red Hat Enterprise Linux 4 Security Guide {DES/PPS/MAN/0006}
3) Solaris 10 System Administration Guide - Security Services {DES/PPS/MAN/0005}

The aim of the hardening process is **not** to produce a highly secure platform foundation, but is intended to reduce the surface area for attack by following the simple steps outlined above.

Additional hardening and security will be applied as necessary on systems that are risk-assessed as needing it. In particular, systems which interface with third parties, particularly where a connection is made with a public or otherwise insecure network, will be additionally hardened.

The regular implementation of security patches is extremely important for any organisation wishing to manage the security of its systems, as defined in section 6.4 Vulnerability Management Service. In the Horizon-Online system, critical security patches will be obtained, evaluated, tested and deployed on a regular basis, (to be defined in the security policy document {SVM/SEC/POL/0003}. This will include development, test and live systems to ensure that ongoing application development is using the same baseline as the live system.

Specific host-based intrusion detection software is not being implemented as the security controls that are being deployed, (as outlined in this document and throughout the Horizon-Online solution), are considered sufficiently comprehensive to ensure that unauthorised modification of data or application files is a very low risk.

FUJ00088336

The subsequent design documents will be;

- DES/PPS/HLD/0002 Red Hat Linux AS High Level Design for HNG-X
- DES/PPS/HLD/0012 Solaris 10 High Level Design for HNG-X
- DES/PPS/HLD/0001 Windows Server 2003 High Level Design for HNG-X
- DES/SEC/HLD/0009 Windows 2003 Server Required Settings High Level Design for HNG-X

Any application passwords stored or transmitted at this level of the architecture will be encrypted or otherwise obscured by using symmetric encryption algorithms such as AES 256 or TDES, asymmetric encryption such as RSA, (with a minimum 1024 bit key size), a seeded hash algorithm or by using a recognised and approved authentication method such as Kerberos. This is in addition to any network layer protection for data transmission, (such as SSL, SSH, IPSEC or TLS).

Operating system users will have their passwords protected by the native OS security controls and mechanisms. It is not intended that these be changed or enhanced beyond the requirement to use two-factor authentication for human users and have very long complex passwords for service accounts.

A comprehensive monitoring, auditing and performance management regime is also implemented for each Platform Type as defined in the following documents;

1) Monitoring HNG-X System and Estate Management Monitoring {ARC/SYM/ARC/0003}
2) Auditing HNG-X Support Services Architecture {ARC/SVS/ARC/0001}
3) Performance Management HNG-X System Qualities Architecture {ARC/PER/ARC/0001}

3.1.3.1 Windows Server 2003

The Windows 2003 platform foundation has been hardened by using an adapted version of the Windows Security Tool and a modified Bastion Host template.

A risk analysis will be conducted as part of the design process and those systems established to be at a higher risk of exploitation, will be further hardened. This exercise will be documented in a specific risk analysis document which will then be lodged in the Dimensions document management system.

These systems are principally expected to be those that interface with external parties such as Authorisation Agents, Reconciliation Platforms, the Branch Access Layer and Proxy Servers.

3.1.3.2 UNIX and Linux Platforms

As with Windows 2003 platform types, Solaris and Linux operating systems will be further hardened following a risk analysis exercise during the design process. It is not expected that this exercise will result in significant changes to the existing platform foundation builds as the default install of Red Hat Linux and Solaris 10 are considered to be sufficiently secure for the Horizon-Online environment. This is due to the additional logical and physical access control and auditing measures in place.

3.1.3.3 Windows XP

There are a number of workstations within the HNG-X system that will use the Windows XP Professional operating system. These workstations must meet the following requirements as a minimum;

1) Be a member of the HNG-X Active Directory Domain
2) Send Event logs to the Tivoli Event Management system
3) Use the patching system or otherwise be patched with the latest OS patches in compliance with the HNG-X Security Policy {SVM/SEC/POL/0003}
4) Be connected to a network DMZ that only permits the appropriate traffic to pass between the Workstation and the Data Centre.

FUJ00088336

Workstations that do not meet these requirements will not be permitted to connect to the HNG-X network and will only be provided with restricted access to the SAS Servers.

3.1.3.4 Windows NT 4

Windows NT 4 remains in HNG-X for retiring platforms. This includes correspondence servers, Utimaco VPN Servers, Generic Agents and the existing Counter.

For Data Centre platforms, these will consist of a Windows 2003 Virtual Server running an image of the Horizon platform. Full details of this design are contained in the HNG-X Virtualisation High Level Design {DES/PPS/HLD/0004}

For Counters, there will be a number of changes, both pre and post the HNG-X application rollout.

The initial change to the Counter will be the deployment of the Horizon PCI change. This will be implemented once the Data Centres in Ireland are Live, and will send all authorisation messages via a BAL OSR instance. This change will remove Track 2 data from the audit trails and Riposte message stores and will encrypt and hash the PAN as necessary.

The second change to the Counter will be the deployment of the HNG-X application. This will result in the removal of the Layer 7 cryptography product, Riposte application, Riposte message store and POLO.

The Utimaco VPN is being retained, though in a simplified form, as a result of a risk analysis and vulnerability tests conducted on a standard Horizon Counter spare. The results of this risk analysis showed very clearly that without the VPN, the Counter is extremely vulnerable to compromise as a result of the operating system in use, the patch status of the operating system, lack of anti-malware software and the extensive use of Windows shares for software distribution and update purposes.

3.1.4 Network

The network layer enables network services for the other three layers. This includes data storage provided through SAN or NAS.

Security Controls for this layer follow the security strategy for HNG-X, namely to ensure that;

1) Attacks originating from outside the HNG-X infrastructure will be prevented, contained and detected through the use of a secure perimeter consisting of firewalls and intrusion detection / prevention.
2) Attacks originating within the HNG-X infrastructure will be prevented, contained and detected using network segmentation, access control lists, firewalls, intrusion detection and intrusion prevention security controls.

Further details of the HNG-X network security controls are in Section 4 Networks.

3.2 Data Backup

Data backups are an essential component of HNG-X and are potentially critical in ensuring data availability in the event of data corruption or system failure. The backups themselves must also be protected with an appropriate level of security. This should be determined through risk assessment of the system or service in question. This includes data written to be removable / portable media including Tapes, Hard Drives, WORM Media, Memory Sticks, DVDs/CDs or Floppy Diskettes.

The HNG-X system must be designed to ensure that any sensitive data, (as defined in HNG-X Information Security Policy {SVM/SEC/POL/0003}), is protected adequately when written to backup media for storage or transportation.

The use of encryption will be implemented as dictated by policy requirements or where risk assessment deems it necessary, in particular to meet the requirements of the PCI-DSS and ISO27001.

The overall backup solution is described in HNG-X Backup and Recovery HLD {DES/SYM/HLD/0015}

FUJ00088336

3.3 BladeFrame

The majority of platform instances in the Horizon-Online system will be virtualised instances, running on Fujitsu-Siemens BladeFrame technology. This technology uses a Hypervisor layer to control both the definition and allocation of processing, memory and virtual networking resources for each platform instance.

Fujitsu Services Defence and Security Business Unit conducted a penetration test of a BladeFrame in early 2007. The results of this are confidential but are available to readers of this document if required, subject to appropriate authorisation.

The results of this penetration test were positive and revealed no fundamental flaws in the BladeFrame architecture.

Due to the use of the BladeFrame as a technology, it is extremely important that the definition and configuration of each BladeFrame is rigorously checked and tested. Horizon-Online relies heavily on virtualisation and therefore correct configuration becomes more important than normal. When virtual hosts are using virtual networks and rely on virtual access permissions, then the definition, configuration and management of these is critical to the secure and efficient running of the system.

To assure that appropriate security controls have been implemented, the testing phase of the HNG-X project will include specific security-testing of the BladeFrame configuration.

The PAN Manager software will be accessible only from the SAS Servers in the Data Centre, which require strong two-factor authentication on logon. Individual user and role permissions will be managed by the PAN Manager application and an audit trail of all activity will be written to the Tivoli event management system in real-time. In addition PAN and LPAN security domains will be implemented to separate virtual platform instances in line with the Horizon Online Security Domain model.

The high level design for Bladeframe is covered in DES/PPS/HLD/0025

FUJ00088336

4 Networks

The network architecture provides facilities to securely transmit data, to provide remote access and to segment networks. In addition analysis and reporting facilities are provided to report against SLAs and to enable base-lining and trending to be performed.

The following facilities are supplied by the service;

- Provides secure network capabilities.
- Provides secure remote access facilities.
- Provides network segmentation.
- Enables network analysis and reporting.
- Controls and manages network access control.

Detailed information on the HNG-X network infrastructure is contained in the HNG-X Network Architecture {ARC/NET/ARC/0001}.

4.1 Network Segmentation

Within each Data Centre, the HNG-X network is segmented following the Security Domain model defined in Section 2.4.2 - Security Domains. The security domain model provides a framework for the network architecture and designs, such that the flow of data around the network is controlled following the principle of least privilege as described in Section 2.3.2 Principle 2 – Least Privilege Access Control.

The purpose of network segmentation is to reduce the scope of any potential attack. By restricting the 'attack surface' to a limited number of systems, any damage caused as a consequence of an attack, can be kept to a minimum.

The network segmentation is achieved using a combination of physical and virtual controls. Dependent on the Security Domain and any specific contractual agreements with third parties, the network segmentation is enforced using VLANs, Stateful Inspection Firewalls, ACLs and physical separation.

Each different network media type is authenticated using a dedicated RADIUS server instance for network device access, with the Branch Router using different CHAP credentials per interface, and each human support user accessing a network device is authenticated using the Identity and Access Management Service.

Network segmentation will also be used to provide separation between environments. Each Test environment will be separated from all other test environments, as well as from the Live environment. This will be enforced through the use of Firewall and Router access control lists, VLAN restrictions and user and network access control. These controls will be monitored using the event management system to verify that access control lists and configuration settings are not changed in a way that may allow a network path from one environment to another except under strictly controlled conditions.

The Horizon-Online network infrastructure will use RFC1918 compliant IP addresses for private networks and will use formally allocated IP addresses where required. (Such as for the Internet access connection). Legacy Horizon systems will continue to use their existing Horizon IP addresses until the platform type in question is retired.

Access to the Hardware Security Module (Network Security Processor) appliances will be tightly controlled through access permissions at a network and platform levell. These permissions will restrict the platforms that can access the HSMs through IP address, protocol and port. The HSMs will be monitored by the Tivoli system through a port that does not provide any transaction processing capability.

FUJ00088336

The management of key material and assurance of the configuration of the HSMs will be the responsibility of the CS Security Team. This will continue to operate following tried and tested procedures as for Horizon.

Access to the Key Server will also be tightly controlled through access permissions at a network and platform type level and will be strictly audited.

All encrypted traffic will be initiated from a firewalled subnet, (either Post Office Client, Red LAN connection or any other source), and will be allowed through an external network control point, (firewall or router access control list), into a DMZ, prior to being decrypted. This is to ensure that only the correct traffic type is allowed into the data centre before being decrypted and inspected. The decrypted traffic will then also be controlled using firewall rules on the internal firewalls and routers.

4.2 Intrusion Prevention and Detection

Network-Based Intrusion Prevention is deployed in the HNG-x infrastructure at the interface between the Branch Network and the Data Centre network. This is to prevent malicious traffic from the Branch estate from entering the Data Centre and to provide notification of any occurrence to the Security Event and Information Management service.

This capability will be provided using McAfee Intrushield IPS appliances as defined in the McAfee Intrushield IDS/IPS Appliance LLD {DEV/INF/LLD/0051}

Network-based intrusion detection is also deployed throughout the HNG-X Data Centre infrastructure. This will provide notification of an attempted compromise of systems within the Data Centre, through malicious activity or malicious code.

The appliances will allow the monitoring of multiple physical network segments from a single appliance. The appliances are designed to prevent traffic flowing between sensor ports. i.e. It is not possible for the appliance to act as a Router and connect networks, thereby bypassing other security controls.

In addition to raising alerts of malicious activity, the IDS sensors will send feed event logs into the secure event management service, to provide an audit trail and to enable additional event correlation with Firewall, Router and other network device logs.

To reduce processing overhead on core HNG-X systems, Host Based IDS, (HIDS), is not being deployed. The inherent security of the platform foundation builds, the hardening process, the implementation of file and process auditing, the network security controls and the implementation of Sophos anti-virus on Windows platforms significantly reduces the need for HIDS.

Traffic types that will not be inspected by the IPS are;

- SSH traffic originating from the SAS servers to the Counters.
- SSH traffic originating from the SAS servers to the Campus, (Data Centre), servers.
- SSH traffic originating from the network management group connecting to the Branch Router.

Any use of other support tools such as SCP or SFTP will also be logged to ensure an audit trail is available in the event of an incident.

For the purposes of this document it is assumed that this is acceptable to Post Office Information Security, as the encrypted traffic is tightly access-controlled and is only permitted between specific end-points. Access control is enforced at both the platform level and the network level through the use of strong authentication and restrictive firewall rules.

Initially the intrusion prevention features of the appliances will be disabled to ensure that valid traffic isn't blocked. As there will be a limited set of messages coming from the Counter / Branch, the intrusion

FUJ00088336

prevention facility will be tuned during the migration and early months of full operation to further protect the Data Centre. Tuning will be based on the number and type of events noted during this period.

The Horizon-Online Tivoli Event Management system will be refined during this phase to ensure that any false positives and false negatives are reduced to a minimum.

The Incident Management Policy and PCI Incident Management Policy documents will be updated accordingly.

Additionally, intrusion attempts will be detected through the use of the Tivoli event management system and specifically, alerts raised as a result of failed attempts to logon or to access data with invalid permissions.

Distributed denial of service attacks are a considered to be a low risk for the Horizon-Online system as it operates as a closed network system and therefore the possibilities of attack from Internet, (the most significant threat source), although present, are very low. However, to ensure that such attacks do not originate from within the Horizon-Online infrastructure or through connections to and from third-parties, all edge routers and firewalls are implemented with denial-of-service protection configured. In addition, the segmentation of the Horizon-Online WAN and Data Centre LAN means that a successful denial of service attack will be extremely difficult to perform.

As part of the testing of the Horizon-Online solution, denial of service attacks will be simulated against appropriately configured firewalls and routers.

4.3 Remote Access

4.3.1 Fujitsu Corporate Access

The connection between the Fujitsu Corporate network and the Horizon-Online infrastructure will be carefully designed and secured to ensure that each environment is properly protected. This connection will be used for both support and reporting purposes.

The network design is detailed in the HNG-X Transit LAN High Level Design {DES/NET/HLD/0015}

Controlled facilities for Data Transfer will be provided as described in the Corporate Data Exchange Proxy HLD {DES/NET/HLD/0018}.

This facility will be used for the controlled transfer of data between the corporate network and the Horizon-Online network. This will include the transfer of report and SLA/OLA data and the transfer of configuration and release management information for system provisioning.

These connections are terminated in the Corporate/RMG Security Domain.

4.3.2 Client Access

Connections to Post Office Clients for Authorisation, Reconciliation, Reporting and other services will continue to be provisioned in line with the appropriate Technical Interface Specification and Application Interface Specification documents.

The general principles outlined in this document still apply to the development of a TIS or AIS.

These connections are terminated in the Client Agents Domain.

4.3.3 Internet Access

Internet access will also be provided to the HNG-X infrastructure. This will be used by any service that needs to exchange information with a service connected via the Internet. Utilising the Internet in this way will reduce costs as dedicated network connections are not then needed.

FUJ00088336

Services using this approach are at a higher risk of being exploited by malicious code or through other means with consequent effects on the Confidentiality, Integrity and/or Availability of the data or service in question, therefore a full risk assessment must be conducted on any service that needs an Internet facility as part of the solution design.

The Internet service as deployed through this architecture is not intended to support the hosting of publicly accessible services with no incremental change. The architecture is designed to ensure that if such services are required in the future, then incremental change will be required to support them. The changes to be made will be identified through the solution design process and will be detailed in this document and in the relevant detailed design documents.

A DMZ will be provisioned that provides network separation, data isolation and content inspection of traffic going to and from the Internet. This will be achieved through a combination of tight firewall controls and proxy services for interactive access and for content inspection.

The proxy service will be a Secure Computing Webwasher appliance configured to inspect http, https and ftp traffic, depending on the requirements of the service.

This service will initially only be used to;

1) Support outbound HTTPS connections for the Moneygram Test Web Service and for the Kahala/Telecoms Broadband Service.

2) Support EMC remote support and monitoring

Both of these connections are provisioned to only allow outbound access. i.e. All connections are initiated from the Horizon-Online infrastructure.

All existing and future services requiring access to or from the Internet will use this service.

These connections are terminated in the Internet Connection Security Domain

4.3.4 Post Office and Royal Mail Access

Post Office / Royal Mail will be treated as another client of the HNG-X system and access provisioned through the definition of a Technical Interface Specification (TIS) and an Application Interface Specification (AIS).

These connections are terminated in the Corporate/RMG Connection Security Domain.

4.3.5 'Red' LAN Access

This access is provided from remote sites as an extension of the Data Centre network, (as distinct from the Fujitsu Corporate Connection which provides a gateway between the Data Centre Network and the Fujitsu Corporate Network.

Effectively, platform instances, (usually workstations), on these network segments are classified as being part of the Data Centre. These workstations are those used by ISD, SSC and CS Security for Audit and Key Management purposes.

Any workstations or systems on such networks are restricted, at a network level, by firewall rules so that only authorised traffic can ingress to the Data Centre. Unauthorised traffic blocked by the firewall will cause an alert to be triggered through the Tivoli Management System.

These connections are all terminated in the Support Connection Security Domain.

FUJ00088336

4.4 Branch Network

4.4.1 Counter

The Branch is assumed to be an insecure environment and therefore application transaction traffic between the Counter and the Data Centre is encrypted using 128 bit SSL encryption, generated using standard Java VM APIs.

The SSL connection terminates on a Cisco ACE blade in the Data Centre. The key pair is generated on the blade and the certificate signing request is sent to the sub-CA using an auto-enrolment protocol. Receipt of this certificate signing request triggers an alert that notifies the Operational Security Manager that a new signing request has been received. On validation of the details in the signing request, the certificate is signed and returned automatically to the Cisco ACE Blade. The certificate is then ready to be distributed to the Counters as and when they connect to the Data Centre.

To ensure that the certificate can be correctly validated by the Counter, both the Root CA and Sub-CA certificates must exist in the Counter Java Certificate Store. The Counter spare will be built with these certificates already installed, but the existing Counters must be updated using the Tivoli software distribution mechanism. This can be done prior to, or concurrently with, the distribution of the HNG-X application Counter update.

The SSL connection validates the identity of the Data Centre using the Data Centre SSL certificates and the HNG-X Root and Sub-CA public keys installed into the key/certificate store on the Counter.

The SSL connection is established prior to the application login prompt appearing for the user, which ensures that any authentication information is encrypted. For all Counter-based logon, the password is not transmitted across the network in the clear as the logon mechanism uses the SRP protocol {RFC2945}. The design of the Counter logon solution is defined in HNG-X End-to-End Key Usage Overview High Level Design {DES/APP/HLD/0094}.

4.4.2 Branch Router

An SSH tunnel will be created between the Data Centre and the Branch Router for management access. This tunnel will be initiated when required for management purposes. It will not be possible to connect to the Branch Router for management purposes using anything other than an SSH tunnel from the WAN side of the Router.

Local access to the router from the Branch LAN is not permitted although access to Router log files stored on one of the Counters will be provided through an engineering menu function.

The design of the Branch network is detailed in the Branch Router Topic Architecture {ARC/NET/ARC/0003} and in SYSMAN3 - Branch Router Management {DES/SYM/HLD/0036} and Branch Router Autoconfig High Level Design {DES/SYM/HLD/0037}

Connections from the Branch are terminated in the Branch Connection Security Domain.

4.4.3 Utimaco VPN

The Utimaco VPN will be retained for HNG-X, with minor modifications, until the Windows NT Counter is replaced. This follows a risk analysis that revealed the relative ease with which a Counter could be ***accidentally*** compromised which would then allow compromise of the Data Centre.

The retained VPN will be implemented differently to the existing implementation, however the level of risk mitigation provided by the VPN is still considered to be above the Horizon-Online risk threshold, due to the following controls;

FUJ00088336

- All transaction traffic is protected by a 128 bit SSL connection from Java Virtual Machine to Data Centre. This connection uses the TDES algorithm and a certificate certified by the Horizon-Online certificate authority. This connection is independent of the Utimaco VPN
- No sensitive data is retained on the Counter post-migration. (Following a defined point of no return, the existing data on the Counter will be deleted. This data is already encrypted and, as the key material has been removed with the removal of the POLO card, there is no way of decrypting it in the branch. In addition, the message store will be securely overwritten as part of the Migration process. Though there is a small risk of the data store being obtained in the period between the migration of a Counter to the HNG-X application and the final deletion of the data store, this time interval is planned to be a few days at most and the risk is therefore considered to be acceptable.)
- Only encrypted traffic is allowed through the external layer of firewalling, (first line of defence into the Data Centre), and is decrypted in a DMZ before passing through the IPS and additional firewalls prior to reaching any Data Centre applications.
- No Delivery Server exists in Horizon-Online, therefore the simple compromise route between the Counter and the Data Centre has been removed. (The Horizon Delivery Server utilises Windows NT shares for data exchange, which are notoriously easy to exploit.)
- Anti-Virus software is implemented on all Windows 2003, 2000 and XP platform instances in the Data Centre.
- VPN Keys are managed as part of the Horizon-Online key management regime and are therefore tightly controlled.
- VPN PIN values will be increased in length for HNG-X as compared to Horizon Online. The exact length and complexity of the PIN will be decided during the design phase and may be subject to constraints imposed by the Utimaco software.
- VPN Keys on the Counter are protected using file access permissions, with the PIN value for the VPN key being stored, (in obfuscated form), in the Registry. The PIN is also protected through the use of permissions and access to both the VPN key and PIN are monitored and logged.
- During installation of a VPN key, existing VPN functionality is used to change the PIN value to a random value which is then stored in the registry and protected as in the previous bullet.

The VPN servers will continue to run on a Windows NT4 platform and will be virtualised onto discrete hardware in the Data Centre. This will ensure that the rules defined in section 4.1 regarding encrypted traffic can be adhered to. The detailed design for this solution is in the VPN on HNG-X NT High Level Design {DES/MIG/HLD/0006}

FUJ00088336

5 Manageability

5.1 Platform Support

5.1.1 SAS Servers

Management of all platform types and instances will be provided and controlled using the Systems Admin Servers, (SAS). This provides a common platform for providing access to tools and platform instances that can be enforced through the use of network and platform level access control.

SAS Servers are implemented in their own network segment, with firewall rules configured to restrict traffic flow from the SAS Servers, based on Customer Service requirements. The individual rules will be identified in the SAS Server design {DES/SYM/HLD/0017}.

Access control for the SAS servers is provided by the Identity and Access Management service. Each SAS server is a member of the Active Directory domain and each user of the service will need a strong authentication token to access the system. All access to the SAS Server is audited, though command line auditing of SSH sessions has been removed.

Following the principle of Least Privilege, access permissions will be implemented to ensure that support tools and scripts are only available to those users entitled to use them. Each user of the SAS server will have a secured personal directory which will confidential data such as SSH private keys. Group/Role directories will also be created that contain software products, (applications and scripts), that are accessible by all members of the same group.

This route will be used by all internal support groups for maintenance of the Horizon-Online infrastructure.

5.1.2 Aurora

The Aurora solution, {DES/SYM/HLD/0020}, provides console level access, via a serial line connection, to the following Data Centre platforms - Fujitsu-Siemens BladeFrame Control Blades, Solaris servers and Network Equipment.

This is used for 3rd party support purposes and as a last-resort access in the event of critical system or network failure.

Access to the console is only permitted by either;

1) Using strong, two-factor, authentication to connect to the console via SSH from the SAS Servers or;

2) Using the connected dial-in modem. (This modem is only enabled when required.)

All users accesses to the Aurora system are tightly controlled using access permissions at both a file-system and application level, and every action is logged to the Aurora system logs and collected by both the Event Management system and the Horizon-Online Audit system.

5.1.3 EMC

For support of the storage fabric within Horizon-Online a remote monitoring and management solution is being deployed. This will use the services of EMC to allow 24 x 7 response to developing or actual problems with the storage devices.

The full design of this solution is outlined in the following documents;

1) HNG-X Storage Infrastructure LLD {DEV/INF/LLD/0004}.

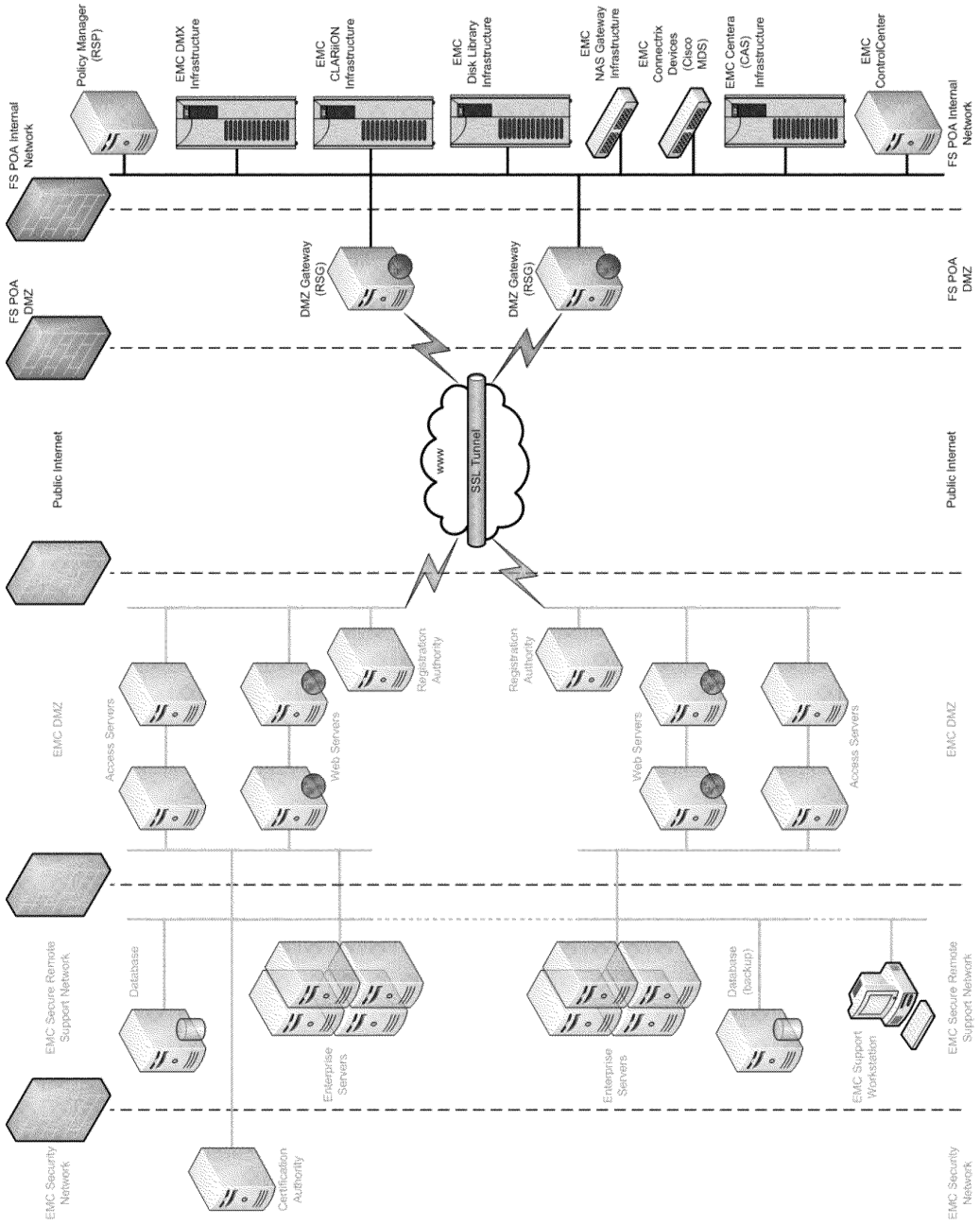
2) HNG-X EMC Secure Remote Support Gateway {DEV/INF/LLD/0030}

3) HNG-X Internet LLD. {DEV/INF/LLD/0047}

FUJ00088336

These documents contain detailed information on the functional and security design of the solution.

At an architectural level, the solution allows EMC access to the storage devices only, for fully audited and Fujitsu-controlled support purposes. The following diagram illustrates the solution.



All connections between the Data Centres in Ireland are initiated from within the Data Centre in an outbound direction. Any connection made is fully encrypted and authenticated using SSL encryption and a certificate installed on the Remote Support Gateway by EMC.

FUJ00088336

The connections are managed using the EMC Policy Server which controls the level of access that is allowed for each EMC support user. This control extends to mandating that every connection in to the storage hardware must be individually approved.

The Remote Support Gateways are securely configured within a DMZ and access to and from these devices is managed through a combination of firewall rules and the Policy Manager. This includes the application of IP level restrictions on the storage hardware that can be accessed and the protocols that can be used.

Every user access and action will be fully logged and auditable.

Only secure protocols will be allowed for data communication between the Secure Remote Support Gateway and EMC and between storage hardware and the Secure Remote Support Gateway.

The Remote Support Gateway platform itself must be fully hardened.

5.1.4 Out of Hours

Remote out-of-hours access to the HNG-X Data Centres will be provisioned using IPSEC VPN technology, dedicated laptops and two-factor authentication. The existing Horizon laptops will be reused and users will utilise the Horizon-Online strong authentication solution.

Access is controlled through a combination of network controls that restrict access to specific Laptop IP addresses and logical access controls that only allows users accessing via the Fujitsu Corporate VPN solution that have a strong authentication token.

Once connected, the only access provided is an HTTPS-protected RDP session onto the SAS Servers.

This access will not be restricted through a time schedule and is expected to develop into a 24hrs remote support capability.

5.1.5 SSH Access

Access to the Counter will be provided through the implementation of an SSH service running on the Counter which can then be accessed from the Secure Access Servers in the Data Centre.

The SSH server on the Counter or on a Data Centre platform is configured to only accept connections originating from the SAS servers.

The existing SSH configuration for Horizon Windows NT Counters will be reviewed as part of the design process. It is not expected that this will result in any changes to this mechanism, until the Counter operating system is replaced.

A file transfer capability will be provided for retrieval of data by the SSC. This will use the corporate proxy server to provide a secure, auditable and access controlled file transfer mechanism.

SSH access will be controlled through the use of Public/Private key authentication. A combination of Host Key Authentication and Firewall rules will ensure that only authorised systems can communicate. Firewall rules will be configured to ensure that the SSH and SCP traffic can only be initiated from the SAS servers to the Data Centre platforms and from the SAS Servers to the Counters.

Although the capability exists to use a Kerberos-enabled SSH solution for those systems running the Vintella PAM software, this is not an option for the Windows NT Counters and it is considered a preferable solution to have a single consistent approach to the implementation, rather than two different approaches.

All support user access will be audited to ensure an audit trail of administrator activity is available. This auditing will take place at the SSH server, not at the client. SSH will be configured to use a single Bash shell and to prevent the spawning of additional, non-logging, shell processes. For clarity, this is not intended to prevent the spawning of additional processes, just to ensure that any such activity is logged.

SSH connection chaining will not be allowed. (i.e. Hopping from one platform to another. Connections must always be from the SAS to the platform instance, not from platform instance to platform instance)

FUJ00088336

5.1.6 SUDO

On UNIX and Linux systems, for general support use, a SUDO shell will be implemented so as to restrict the use of the Root user.

The SUDO application allows close control of the administrative privileges and commands that a user can access, without needing to be a root user. Each command issued by the user is also logged to the system event log for alerting, reporting and later forensic analysis if required.

Event monitoring will be configured to alert on changes to service states and configuration files.

5.2 Third Party Access

Third party access will be provided using a number of different methods, depending on the specific requirements of each individual case.

The solution for each of these access types will be defined in the relevant architecture and design documents.

In each case, the security principles will be followed and the designs will ensure the access provided is secure.

FUJ00088336

6 Security

6.1 Data Integrity and Confidentiality Service

6.1.1 Service Description

The information integrity and confidentiality service ensures that sensitive and personal information is protected in an appropriate fashion for the appropriate length of time in both transit and storage. In conjunction with the identity and access management service the service controls the visibility of information throughout the HNG-X infrastructure and beyond.

The following facilities are supplied by the service;

- Provides Key and Certificate Management
- Enables data integrity.
- Enables secure communications.
- Enables data confidentiality
- Enables PCI PAN protection
- Enables PIN protection

6.1.2 Service Overview

The Data Integrity and Confidentiality service ensures that confidential or sensitive data is adequately protected within the Horizon-Online system.

A Root Certificate Authority and subordinate Certificate Authority will be created to manage and create Public Key Certificates for a number of purposes. This is not a full implementation of a PKI as one is not required for Horizon-Online.

The Root CA will be an Enterprise Root CA using Microsoft Software that will create the Root CA Key Pair. This is a self-signed key pair and the Live and Test environment will use different Root CAs. The private key of this key pair is then used to sign other certificates to verify their authenticity. The public key of this key pair is distributed to the subordinate CAs and to any other end-point that requires it.

The Root CA certificate will be configured with a life-span of 30 years (until 2038).

The sub-CA certificate will also be configured with a life-span of 20 years (until 2028).

In the event of a compromise or suspected compromise, the appropriate certificate will be revoked and a new key pair will be created, signed and distributed.

The Root CA key pair will be generated by the CS Security Manager and the resulting Certificate will be deployed over the network, to the relevant end-points. The end-points are defined in detail in the HNG-X Key Management High Level Design {DES/SEC/HLD/0003} document.

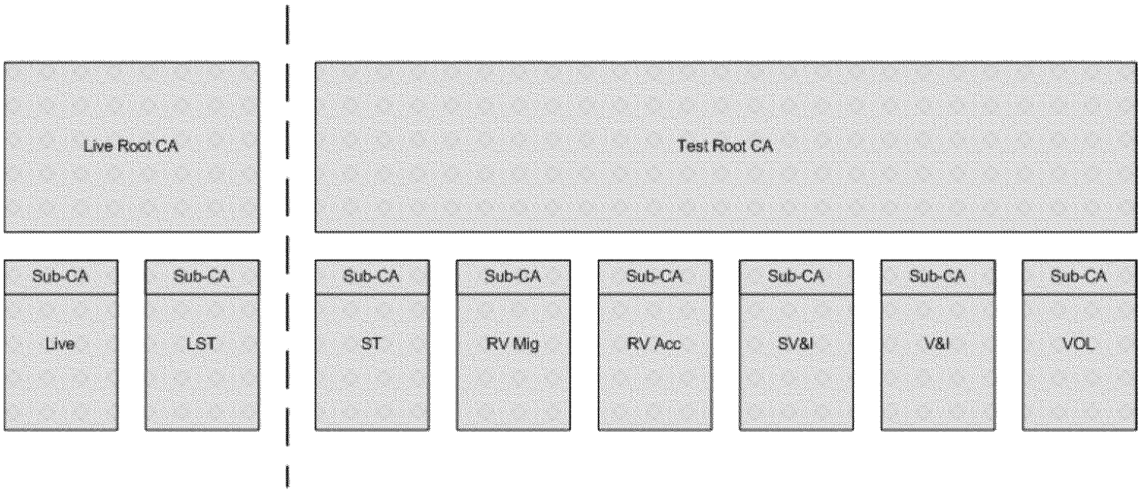
The Root CA will be an offline CA, stored in a physically secured location in BRA01 and LEW02.

FUJ00088336

Once the Root CA key pair has been generated, it will be backed up to removable media, (CD or DVD), and copies will be kept in secure storage in Bracknell and Lewes. The hard drive of the Root CA may also be removed and securely stored in a safe.

The Live environment and the LST test environment will share the same Root CA, but will have a dedicated sub-CA.

All other test environments, (ST, VOL, SV&I, V&I, RV Mig and RV Acc), will share a testing Root CA and will also have a dedicated sub-CA per environment. Therefore, different certificates will be configured onto the Counter and the SSL termination point, depending on which environment the Counter is accessing.



The Live and LST environments share a Root CA as LST is the final testing stage before deployment into the Live environment and therefore it is occasionally necessary to test Live key material prior to use. It will not be possible for test data to be used in the Live environment however, as previously stated, it will be possible for Live data to be used for Test purposes, (on the LST rig only), under very specific circumstances. If this is required, rigorous management and technical controls will be applied and will be defined in the appropriate policy, procedure and technical design documentation.

In addition to the other security controls mentioned in this document, OID restrictions will be applied both on the Counter and in the Data Centre, to ensure that any attempted connection must use a valid certificate for that environment. Alerts and errors will be reported through the event management system.

The public key certificate for the appropriate Root CA and the SSL certificate signing sub-CA will be stored in the Counter certificate store. This technique means that it is easy to separate Live and Test environments as the SSL termination point and the Counter will be configured to only accept the appropriate certificate.

6.1.2.1 Key Management

Correct management of key material is of fundamental importance to HNG-X and there will be a number of subordinate HLDs, LLDs and policy documents to ensure these tasks are carried out properly. These documents are;

1) HNG-X Key Management HLD {DES/SEC/HLD/0003} covers the design of the key management system in greater detail.
2) HNG-X Strong Authentication HLD {DES/SEC/HLD/0001} covers the design of the strong two-factor authentication system.
3) HNG-X Crypto Services HLD {DES/SEC/HLD/0002} covers the design of the cryptographic API, (Crypto-API), and key management server, used by Banking authorisation agents, Debit and Credit Card authorisation agents, Audit workstations, Debit Card Management Server, Connect:Direct Gateway Server and the Key Management Workstations.

FUJ00088336

Through the implementation of a Crypto-API on all systems that require access to key material, an application can request the appropriate key for its purpose and will receive the key and passphrase/PIN value in a secure fashion.

The Crypto-API component communicates with a dedicated Key Server which supplies all of the relevant passphrase or PIN material. The Key Server retrieves the appropriate key from a table in the Network Persistent Store (NPS) database and returns both the key material and the passphrase. The NPS was chosen for this purpose as a result of it's high availability and security.

The detailed design for this mechanism is contained in the HNG-X Crypto Services HLD {DES/SEC/HLD/0002} and the HNG-X Key Management HLD {DES/SEC/HLD/0003}

6.1.2.2 Pin Pads

The PIN pad architecture is unchanged from Horizon and is described in detail in the following documents;

1. RS/MAN/017 User Guide for PIN Pad Initial Key Generation
2. RS/MAN/016 Post Office Account Usage of the SCT
3. RS/DES/010 Key Management High Level Design (Horizon)
4. TD/SOD/007 Outline Design for Remote Updating of Pinpads
5. DES/SEC/HLD/0003 Key Management High Level Design (HNG-X)

The following text is an architectural overview of how PIN Pads are managed, with particular reference to confidential material, in accordance with SEC-3216, which states "Once entered by a cardholder, plain text PINs shall be processed only in a physically secure device as defined in ISO 9564. At all other times, PINs shall be encrypted as defined in ISO 9564".

PIN Pad security relies on a combination of the PIN Encryption Device (PED) being physically secure and on key material on the PED being appropriately protected at all times during its lifetime.

The PIN Pad devices are supplied by Hypercom and are their HFT-117 model.

Fujitsu are responsible for generating a Base Derivation Key, (BDK), which is done using the SCA (SCT in Horizon) supplied with the Atalla HSM appliances. This ensures that the key is of the correct cryptographic strength with sufficient entropy. When unencrypted, the key is held as two (2) components (on paper) which are stored securely and separately by CS Security for back-up purposes.

A GKLK, (Global Key Loading Key), is also generated using the SCA (SCT in Horizon). This key is produced as three (3) components on paper, which are then manually communicated to Hypercom. The components are then used by Fujitsu for key generation and are stored securely when not in use.

The PIN Pad Key Generation Workstation is used to derive an Initial Key (IK) from the BDK in accordance with the Derived Unique Key Per Transaction (DUKPT) scheme specified in ANSI X9.24 : 2004

A number of files are received from Hypercom (known as Order Files) containing the serial numbers and other identifying information for each PIN Pad. These files are then used by the PIN Pad Key Generation Workstation to create, (in batches of 5000), the Initial Key (IK) for each PIN Pad listed in the Order File. A BKLK per PIN Pad is also generated at the workstation and is used to protect the IK during transit and loading into the PIN Pad at Hypercom. Files containing (IK)BKLK for each of the advised PIN Pads are sent to Hypercom on CD for PIN Pad building. This data is also used by Fujitsu for PIN Pad upgrading. All cryptographic operations performed at the PIN Pad Key Generation Workstation are in a tamper-detecting HSM.

Once a PIN Pad has been installed, the DUKPT scheme is used to ensure that every transaction containing a PIN block (the [R] message) is encrypted using a unique key. Prior to encryption the PINs are formatted to Format 0 in ISO 9564-1:2002.

These transaction messages are then processed by the agent servers, using the Atalla Hardware Security Modules (HSM) to securely translate the encrypted PIN Block from the DUKPT key to the Acquirer Working Key (AWK), for onward transfer to the relevant Financial Institution.

FUJ00088336

The PIN pad driver is modified for HNG-X but all other functionality, firmware, protection of PINs, PIN Blocks and transaction messages is as described in the documents listed at the start of this section.

6.1.3 Data Integrity

An unmanaged automatically generated key pair will be created on the Counter for each logon session. The public key portion of this key pair will be sent to the Data Centre during the logon process and will be digitally signed using the managed Branch Access Layer signing key. This is done to verify the integrity of the messages received from the Counter during each session.

Each transaction message, received from the Counter, will have its signature validated by the Branch Access Layer and by the appropriate authorisation agent. Any invalid signatures will result in the message being discarded and an alert raised.

This mechanism is described in HNG-X Architecture – Branch Access Layer {ARC/APP/ARC/0004}

6.1.4 Secure Communications

The use of IPSEC VPNs is restricted to communication over public networks either between Fujitsu locations or between a Fujitsu location and that of a third-party, (including Royal Mail). Cryptographic Key material for these connections is managed under the relevant policy or contract agreement depending on the connection in question.

CHAP secrets for the Branch Router configuration are stored in encrypted form in the Estate Management Database, (EMDB). EMDB also uses the Key Server to retrieve the appropriate key and passphrase to decrypt the CHAP secrets as they are required by the Boot Platform. The design of the EMDB database is contained in the Estate Management Database (EMDB) HLD {DES/SYM/HLD/0031}

SSL is used to protect the connection between the Counter Application and the Data Centre. This connection is terminated on a hardware SSL accelerator in the Data Centre. As there is, an 'in-clear gap' between the Branch Access Layer and the SSL termination point during which the network traffic is no longer encrypted, post-authorisation sensitive information between the Counter and the Data Centre, will have the relevant fields in each XML message encrypted or obfuscated independently of the network encryption.

SSH access is used to manage the Data Centre platforms, Counters and Network Devices. Access is only granted from specific restricted management platforms as defined in the appropriate design documents. Access is secured through the use of public/private key encryption and a locked down SSH configuration file.

This is defined in more detail in Section 5.1 Platform Support and in the HNG-X Cygwin/SSH High Level Design document {DEV/INF/LLD/0059}

6.1.4.1 Public networks

The HNG-X network infrastructure will be developed to protect Sensitive Authentication Data and Sensitive Cardholder Data in transit as described in ARC/NET/ARC/0001

- There will be no encryption over the X.25 network to Streamline for authorisation.
- The batch file network to Streamline will continue with the current encryption mechanism, which is implemented to Streamline specification. (This is an ISDN, MPPE, 128 bit, RC4 connection.)
- The Alliance and Leicester network connection already meets the requirements of the PCI-DSS and utilises a fixed IPSEC 256-bit AES connection.
- Connections to Link and CAPO are provided by themselves and are out of scope for this document.
- The interface for TESQA, which is used from the Royal Mail network, will be updated to use 128 bit SSL 3.0.

FUJ00088336

6.1.5 Data Confidentiality

The HNG-X Key Management HLD {DES/SEC/HLD/0003} contains a definitive list of the key material in use in HNG-X;

In addition to the key material defined in the above document, and previously in this section, the following key pairs and certificates are also managed under the key management regime;

1) Microsoft Encrypting File System, (used for temporary reconciliation file storage on the Debit Card Management Server and the Connect:Direct Gateway).
2) TES-QA application server SSL certificate.

6.1.6 PCI PAN Protection

In HNG-X, the Primary Account Number will be protected in one of three ways, depending on the location of the data.

1) The first 6 and the last 4 characters will be in clear. The remaining characters, (9 for a 19 digit PAN, 6 for a 16 digit PAN), will be overwritten using a character such as 'x' as a replacement for each character.
   a) For Example: *1234567890127890* will become *123456xxxxxxxx7890*
   b) For Counter receipts, this will be printed in the form *xxxxxxxxxxx7890* as per Visa and MasterCard requirements.
2) The first 6 and the last 4 characters will be in clear. The remaining characters, (9 for a 19 digit PAN, 6 for a 16 digit PAN), will be replaced with the equivalent number of characters from a base 64 hash of the PAN and a seed value. The first character of the hash characters will be a non-numeric character to facilitate the distinction between hashed and non-hashed PANs.
   a) e.g. *123456Yg20xAWIE7890*
3) The PAN will be encrypted.

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

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

The PAN will be replaced in all visible Data Centre displays and reports with a truncated secure SHA-1 hash of the PAN.

As described in option 2 above, this will display the first 6 characters and the last 4 characters of the PAN, (as permitted by PCI). The remaining 6 or 9 characters, (depending on the length of the PAN), will be based on a truncated hash of the PAN, using the Base 64 character set.

The effect of this is that the overall hashed PAN will be the same length as the original PAN and will have minimal impact on support staff who are used to using the PAN currently.

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

Hashed PANs will be created by the Counter Business Application, Connect:Direct Gateway and Debit Card Management Server, Audit Workstations and TES-QA application.

FUJ00088336

Encrypted PANs will be created by the Authorisation Agents using the network-attached Atalla Hardware Security Module devices.

Keys used by the Atalla HSM are in Atalla Key Block Format. This format contains a definition of the uses to which the key can be put. Therefore, encryption and/or decryption can be controlled through a combination of access to the HSMs and Key Server, network controls and the definition of the use(s) to which any particular key can be put.

This is defined in detail in the HNG-X Crypto Services HLD {DES/SEC/HLD/0002} and in the HNG-X Key Management HLD {DES/SEC/HLD/0003}

6.1.6.1 HNG-X Data Centre

HNG-X Data Centre systems will be developed to handle transactions whether they originate from HNG-X counters or from the revised Horizon counters. In addition the HNG-X Data Centre system will continue to support legacy Horizon counters as currently implemented.

Transactions from legacy Horizon counters will not be PCI compliant and the storage of data from these transactions will not be changed retrospectively. These transactions will continue to be stored in non-PCI compliant format until they reach the archive period for the database. (e.g. 90 days for DRS and 180 days for TES).

Historical Audit data will also continue to be stored in its original, non-PCI compliant, format and this will not be retrospectively changed. It will remain in the audit system in this format until its retention period has expired.

Where necessary, HNG-X Data Centre systems will automatically detect the appropriate type of transaction and handle accordingly.

6.1.6.2 HNG-X Counters

HNG-X Counters do not store either transaction data or any other data except in the form of diagnostic and event logs. In the event that transaction related information needs to be written to an event log on the Counter, it will be sanitised by either using the hashed version of the PAN, or by having the middle 6 or 9 characters overwritten depending on the point within the transaction sequence.

Counter receipt formats are already VISA compliant and only the final four numbers of the PAN are printed on the customer receipt. Therefore this format will not be changed.

The Counter Clerk dialogue will be changed so that cardholder data is only displayed when necessary. For example the fraud check screen displayed for swiped transactions where the Clerk is asked to verify the PAN displayed on screen against the number on the card.

6.1.6.3 Horizon Counters

See 9.17

6.1.6.4 PO Client workstations

TESQA will be developed with the capability to decrypt the PAN for an individual transaction. However normal result sets will show the hashed PAN rather than the clear-text PAN.

Other support and business functions that require access to, or the ability to search on, hashed PANs, will be provided with the functionality to do so.

6.1.6.5 Audit, TESQA and DRS

An encrypted version of the PAN will be stored in the Audit System, the Transaction Enquiry Service, the Network Persistent Store and the Branch Database.

A facility to decrypt an individual PAN will be available via the Audit team for Litigation Support.

FUJ00088336

TESQA will be enhanced to support queries based on either PAN or hashed PAN. Result sets will display hashed PAN only. Where a PAN is supplied, TESQA will derive the hashed PAN and use that for the query.

TESQA will have the capability to decrypt the PAN for an individual transaction, however normal result sets will show the hashed version of the PAN rather than the clear-text PAN.

For a Data Reconciliation Service workstation user to perform a query using the hashed PAN, they will first of all use the Transaction Enquiry Service to obtain the hashed PAN from the clear-text PAN. The DRS will still also support clear-text PAN based queries, but the returned results will show the hashed PAN value rather than the clear-text PAN.

Where this is insufficient, (e.g. for Debit / Credit card transactions), the audit interface described above would be used by Fujitsu staff to decrypt the PAN for individual transactions.

6.1.1.6 Debit and Credit Card

Batch files to and from Streamline, (Payment and EMIS files), which contain the PAN in clear, will be held on encrypted file store. The file store will be encrypted using the Microsoft Encrypting File System and is for temporary file storage only during file creation and transfer.

The process for creating the payment file will decrypt each encrypted PAN using the Atalla HSMs, as it writes it to the file on disk.

Processing of the EMIS file will result in PANs being hashed as they are written to the DRS.

The Audit version of these files will contain the hashed PAN.

To provide reversals for Streamline, the Application Interface Specification (AIS) has been updated to meet the requirements of v20 of Streamline's document *"TECHNICAL SPECIFICATION For the delivery of transaction data via DIRECT COMMUNICATION"* dated December 2005. This specification does not require Track 2 data. This change is documented in the HNG-X DCS Bulk File Agents HLD {DES/APP/HLD/0055}

Following this change and the expiry of the 180 day retention period for the DRS, (with the sole exception of legacy audit data), Track 2 data for debit and credit card will no longer be retained anywhere in the system.

6.1.1.7 Banking Specific

Banking reversals require Track 2 and can be performed up to 5 days after the transaction. Therefore there is a requirement to retain Track 2 for this purpose.

The encrypted Track 2 data will not go to the audit system, but will be held on the NPS database backup tapes before the tapes are recycled. However, the associated key is retained in the Atalla HSM appliances and therefore this is considered to be an acceptable risk.

Backup tapes will be securely erased at the end of their life in accordance with the requirements of the Information Security Policy {SVM/SEC/POL/0003}.

Encryption of Track 2 will be performed by the Banking Authorisation Agent and will use network attached Atalla HSM devices as described in HNG-X Key Management High Level Design {DES/SEC/HLD/0003} and HNG-X Crypto Services High Level Design {DES/SEC/HLD/0002}

Batch files to and from Alliance and Leicester, Link and CAPO, (REC and LREC files), which contain the PAN in clear, will be held on encrypted file store during file creation and transfer. The file store will be encrypted using the Microsoft Encrypting File System.

The Audit version of these files will contain the hashed PAN.

FUJ00088336

6.2 Identity and Access Management Service

6.2.1 Service Description

The identity and access management service provides facilities to create, modify and remove users, groups, roles and access permissions. The service controls access at an application and platform level including both local and remote access. This includes access to operational support, system support and data processing systems.

Management in the following list means provisioning, de-provisioning, authenticating and authorising;

1) Operational support users are managed using a directory service for access to platform instances and to network devices.
2) Branch business user access is managed using the Branch Database. This includes Global users such as Engineers on site visits and Branch Auditors.
3) Application accounts will be managed by the application concerned, except where the application designer has elected to utilise the Identity and Access Management Service.
4) Within the Data Centre, service accounts are managed using the directory service.
5) At the Counter, service accounts are local accounts.

The following facilities are supplied by the service;

- Provides identification
- Provides authentication
- Provides authorisation
- Provides accounting.
- Provides non-repudiation
- Provide role based access control.
- Provides network access control.
- Enables the addition, removal and change of users, groups and roles.
- Enables the addition, removal and change of network systems and devices.
- Enables segregation of duties.
- Controls and enables local and remote access for HNG-X.

6.2.2 Architectural Overview

The service is implemented using a number of different technologies and is split between business users and operational users.

Business users are defined as those users that utilise the functionality of the system from a Post Office or Royal Mail location or on behalf of the Post Office to perform a business function.

Operational users are defined as those users that provide operational support, management and testing of the HNG-X system itself such as SSC, ISD, SMG, MSS, SMC and ITU.

FUJ00088336

Other Business Users are the third-party support and remote business users of the system such as Royal Mail TES-QA users.

Branch users are defined as those users of the Counter Application such as the Sub-Postmaster and Counter Clerk or Global Users such as Engineers and Auditors. Branch user authentication and authorisation, including Engineering and Audit users, is a function of the Counter, Branch Access Layer and the Branch Database. This is to ensure that the line of business application is a closed functional group where the components of the group, (namely the Counter Application, the application server and the Branch Database), are not dependent on other components for their operation.

The management of users at an operational support or business user level is conducted in accordance with the HNG-X Information Security Policy {SVC/SVM/SEC/0003}. This policy and associated procedures ensure that the creation, modification and deletion of users are performed within a secure and audited environment.

In offline mode, when connectivity to the Data Centre is unavailable, the Counter will run a minimal engineering shell to provide basic diagnostic information to the Engineer.

Refer to the HNG-X Branch Access Layer Architecture {ARC/APP/ARC/0004} for the detailed design of the authentication / authorisation process.

6.2.2.1 Operational Support Authentication and Authorisation

Throughout the HNG-X infrastructure the same authoritative source of authentication and authorisation data is used to manage access control for all operational support users. The purpose of this approach is to:

1) Reduce the number of passwords required for support purposes
2) Ensure better audit and logging facilities for authentication and authorisation
3) Streamline the process for adding, changing and removing authentication and authorisation information
4) Provide a standard method of authentication and authorisation throughout the estate.

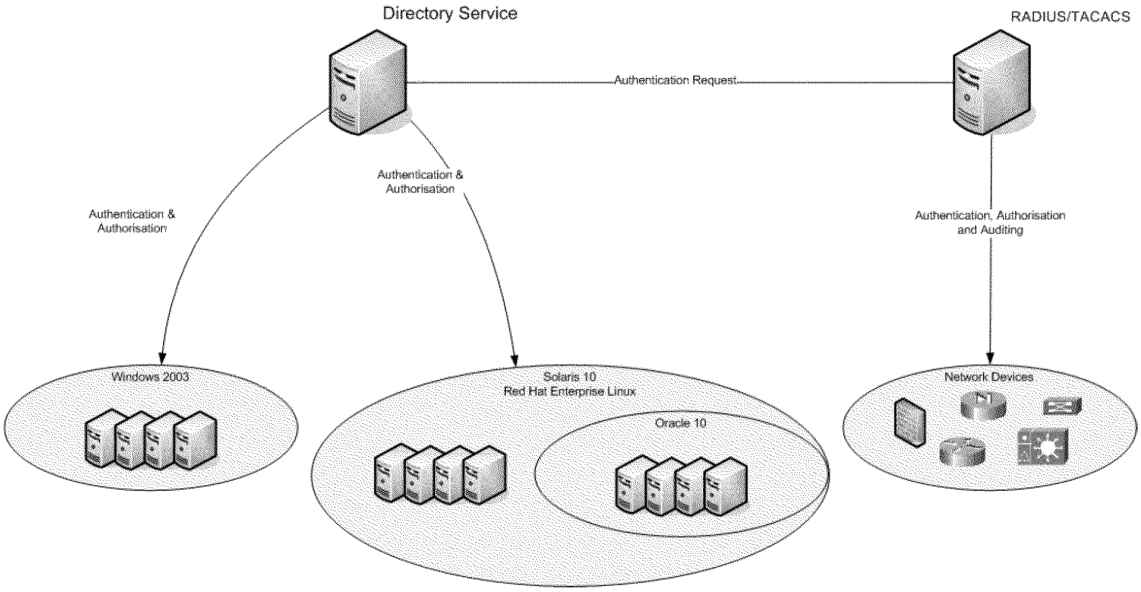


Figure 1 – Operational User Authentication and Authorisation

The Horizon-Online environment is managed using an Active Directory tree which controls access to resources through the Windows 2003 Kerberos and LDAP implementations.

FUJ00088336

UNIX and Linux systems are managed through the same Active Directory tree utilising a Pluggable Authentication Module (PAM) installed on each UNIX system.

Database access is managed through the implementation of scripts to create database users. This is no change from the current Horizon approach. This approach means that a role-based access control matrix will be created for each database using a standard set of roles across all databases.

Interactive access to a database will be controlled by the directory service in the following way. Access to a SQL Server database on a Microsoft platform instance will use native authentication and the user will therefore effectively have already been authenticated when the logged into the Active Directory domain. Access to an Oracle database will use the ops$_<username> concept which passes authentication of the user to the underlying operating system. This also means that the user needs a strong authentication token to logon to the Active Directory domain, prior to connecting to the database.

However, in each of these cases, the users username and access rights within the database will have been setup externally to Active Directory and will be managed using a script-driven manual process.

Access to a database over the network, (such as from an application or from a management tool), will be controlled through a combination of database access rights and network permissions. In all cases, over the network access to any database will still require that the user be setup within the database and access permissions provided accordingly. Users of any management tool will also have needed to authenticate themselves to Active Directory prior to using the tool.

All human access to any component of a platform will be controlled using strong authentication. The strong authentication solution uses the Vintella PAM module from Quest Software to enable UNIX and Linux systems to become objects in Active Directory. A hardware security token is also used, in conjunction with Active Directory, which uses a combination of the hardware token, public key cryptography and a user passphrase to provide secure authentication.

Before a user can access the system, they must have been provided with a security token, containing the appropriate credentials, by the security manager.

Initial provisioning of this token will be done by the CS Security Team using the functionality provided by the KMNg Workstation platform. Subsequent certificate renewal requests will occur automatically, but will require explicit approval by the Operational Security Manager before a new certificate is signed. This will be a manual step requiring the use of the KMNg Workstation.

When and if necessary, (for example, in the case of a lost or stolen token), certificate revocations will also be performed using the KMNg workstation.

This design is covered in detail in the Strong Authentication for HNG-X HLD {DES/SEC/HLD/0001}

Management domains using system management applications will also provide access and role control appropriate to the operational functions they offer. Where appropriate, this will utilise the capabilities of Active Directory. This is defined in the HNG-X System and Estate Management Overall Architecture {ARC/SYM/ARC/0001}

Platform event information detailing account logons & logoffs, object access, account management, privilege use and directory service access, (and their failures), are all logged using the Event Management service.

Network shares will also use the directory service for authentication and authorisation. This includes discrete, BladeFrame and NAS attached storage using native Microsoft Shares and those created using Samba.

6.2.2.2 Application and Business System Authentication and Authorisation

Authentication and authorisation for the Counter application is controlled through a combination of the Counter, Branch Access Layer and Branch Database.

Branch staff accounts are maintained in the Branch Database. This information includes the username, password and authorisation information relating to the user's role.

FUJ00088336

The communication between the Counter and the Data Centre is protected by an SSL session and the Utimaco VPN layer, but as an additional security measure the SRP protocol, (RFC 2945 The SRP Authentication and Key Exchange System), is implemented as a method of providing a secure logon facility.

A detailed design of this mechanism is described in HNG-X End-to-End Key Usage Overview High Level Design {DES/APP/HLD/0094}.

Database applications, (such as TES-QA), also control authentication and authorisation from within the database application itself. There are a limited number of functions that can be performed with these applications and they do not allow access to the underlying operating system. The users of these applications are located at Royal Mail or Fujitsu sites and therefore require physical as well as logical access to be able to use the application in question.

All such applications run in a user context that follows the principle of "least privilege".

6.3 Event Management Service

6.3.1 Service Description

The secure event management service is a component of the overall Tivoli event management solution, creating events and producing reports using the existing Tivoli event management database. Logs from network devices, intrusion prevention and detection appliances and firewalls are also aggregated by the Tivoli system either directly, or through the syslog server.

Logs will be aggregated and analyzed to provide security information and reports. Relevant information will be provided to the CS Security Team through the provision of regular reports.

The following facilities are supplied by the service;

- Provides log aggregation, correlation and analysis.
- Enables security event alerting and reporting.
- Enables compliance reporting with standards and regulation such as ISO 27001 and PCI.
- Enables trending and provides the ability to spot longer term security related events.

6.3.2 Event Management and Alerting

This service utilises the existing SYSMAN3 Tivoli event management infrastructure to forward all Data Centre security events in real-time, unfiltered.

Events from the existing Windows NT Counter will be reviewed as part of the design process and the relevant changes will be made for the Horizon-PCI and HNG-X application stages of the Counter development.

Each platform instance in the HNG-X infrastructure reports to the Tivoli Event Management system as defined in the HNG-X System and Estate Management Overall Architecture {ARC/SYM/ARC/0001}.

Standard operating system logs, network device logs and bespoke application logs are sent to the event management system using either a direct connection, controlled by the local Tivoli Agent, or through the use of the SYSLOG server. The latter route is designed for the use of appliances and networking devices.

Initially a set of standard alerts and reports will be configured, (based on operating system type and platform type), that will be refined as a result of observations made and lessons learned during the operation of Horizon-Online.

The CS Security team will be provided with a console onto the Tivoli Event Management system that will provide them with the ability to review alerts and reports, as well as generate Active Directory-hoc queries.

FUJ00088336

Security Event and Information Management, (SEIM), is a key detective control in the HNG-X security strategy, acting as a central aggregation point for logs from all business applications, network devices, security devices, platforms and Databases.

Event analysis and alerting take place in real-time and detailed event correlation reduces the number of events seen by the operator. The specific events to be logged will be established during the design phase and will be documented in the appropriate high and low-level design documents.

The original log files on each Data Centre platform type will be maintained for a period of time, before housekeeping tasks start to overwrite the file. This is to guarantee that a log file does not completely fill up a disk and cause a platform instance to halt. This period of time will be configurable and will be dependent on the platform type and on the volume of events expected. Typically, this housekeeping period will be set based on a period of time, rather than a file size. However it is considered more desirable that a platform instance has sufficient disk space rather than to mandate that a log file is allowed to grow for a set period of time

As the platform instance log files are read in real-time, (for those systems running a Tivoli agent), each entry to the file is read, converted into Tivoli Common Format and forwarded to the Tivoli collection layer as soon as it has been written.

The log files are then securely managed by the Tivoli event management system through a combination of user, file and database access control. This is in addition to the infrastructure access control provided by the Horizon-Online infrastructure such as segregated networking.

The Tivoli system has inbuilt role based access control facilities and these will be implemented to ensure that the users of the system, (administrative or otherwise), can only access the tools and functions that they need. The administrative users of the Tivoli system will use the Identity and Access Management service for access control and will require a token to be able to logon to the system. Non-administrative users, (such as Helpdesk staff), will have a set number of Tivoli tasks that can be executed on specific systems and will have very restricted command line access for obtaining specific diagnostic or log data.

The Event Management Service provides information and raises alerts through the Helpdesk, so that incidents in the Horizon-Online infrastructure can be responded to appropriately, in accordance with the incident response policy.

Reporting from the secure event management solution will be used to spot trends, carefully crafted attacks taking place over a long period of time and for reporting to provide compliance with regulation, legislation and standards. It is expected that these reports will change and be refined over time; therefore this section of the document will be updated as and when appropriate.

Initially, all events from Data Centre servers and network devices will be forwarded to the SYSMAN3 system.

Also refer to HNG-X System and Estate Management Monitoring Architecture {ARC/SYM/ARC/0003}

6.3.3 Audit

The audit subsystem is part of the support services solution and is responsible for collecting, sealing and securely storing transaction, application and system event logs.

Each application designer is responsible for defining the appropriate audit trail for their own system or application and providing the relevant information to the audit subsystem.

Housekeeping of audit files is performed by the Audit Server itself.

The resulting audit data can then be queried by the CS Security Prosecution Support Team to provide data in response to ARQs for Post Office investigations.

The audit subsystem is described in the HNG-X Support Services Architecture {ARC/SVS/ARC/0001}

FUJ00088336

6.4 Vulnerability Management Service

6.4.1 Service Description

The vulnerability management service ensures security patches and updates are maintained at the appropriate level. The service provides secure platform builds that have been hardened to reduce the vulnerability of the standard platform. The service provides protection against malware in the form of Viruses, Trojans, and Worms etc. and detects and prevents malicious code and malicious activity on the network. This service supplies the assurance that possible platform and application vulnerabilities have been reduced to a minimum.

The following facilities are supplied by the service;

- Provides system hardening.
- Provides vulnerability management.
- Provides patch management.
- Provides malware management.
- Controls vulnerabilities within HNG-X.

The vulnerability management service consists of a number of components that work together to identify and reduce vulnerabilities in HNG-X. This includes vulnerabilities caused by configuration errors as well as software bugs.

6.4.2 Architectural Overview

6.4.2.1 System Hardening

Platform foundation builds used for HNG-X have been hardened through the use of specialist scripts and build instructions. This hardening reduces the 'surface area' for attack and thereby reduces the level of vulnerability of each individual system.

The hardening is not intended to make each system as secure as a Bastion Host as the server platforms require a significant degree of functionality to be able to run applications. The hardening undertaken will remove unnecessary services and software as well as applying a base set of platform file permissions.

In situations where additional security is required, (such as for systems in the Internet DMZ), a HLD will be created to provide the necessary guidance.

This is covered in more detail in section 3.1.3 Operating Systems above.

6.4.2.2 Patch Management

To reduce vulnerability to exploitation and ensure that all systems within the HNG-X environment have the relevant and appropriate patches applied within a reasonable timeframe, there will be a patch management system designed as part of HNG-X. This system will provide mechanisms for;

1) Gathering patches and updates to major operating systems and applications,
2) Evaluating and filtering the patches and updates
3) Testing the patches and updates

FUJ00088336

4) Deploying the patches and updates.

A process will be established for the gathering, filtering and maintaining of patches.

The CS Security Team will then be responsible, along with platform owners, for establishing the relevance and priority of each patch or update.

The filtered patches will then go through LST testing and be distributed to the target platforms using the Tivoli software distribution mechanism. Data integrity of each patch or update, (and of software distribution in general), is assured using a file hashing mechanism. This does not give the same level of protection as a digital signature, but in conjunction with the other policy, procedure and technical security controls, it assures that the software installed is the software delivered by the configuration and release management system.

Due to the technical and management security controls in place throughout the Horizon-Online infrastructure, there is considered to be a greater threat from the installation of corrupted code than that from malicious code.

The software distribution mechanism is described in detail in HNG-X System and Estate Management Software Distribution and Asset Management {ARC/SYM/ARC/0002}

The design for the patch management system is described in DES/SEC/HLD/0006.

6.4.1.3 Anti-Virus

HNG-X uses the Sophos anti-virus product. This will be implemented on all Microsoft Windows 2003 Data Centre platforms and Microsoft Windows XP Support Workstations connected to a Data Centre network (i.e. from a remote site).

Updates of virus signatures and of the anti-virus engine will be obtained using the same process as for patch updates. The signatures and updates will also be put through LST testing to ensure their integrity and will be applied using the Tivoli software distribution system rather than the Sophos management tools.

This is to ensure consistency of delivery to system-managed platforms.

Anti-virus software will not be deployed onto either the existing Horizon Windows NT Counters or onto any HNG-X Counter.

Remote support workstations that are not under the control of the HNG-X Data Centre will be updated as required by the Fujitsu Corporate Security Policy document.

The design of the anti-virus system is also covered in DES/SEC/HLD/0006.

6.4.1.4 Vulnerability Scanning

The McAfee Foundstone vulnerability scanning appliance will be deployed into each Data Centre. This appliance will be configured to scan all systems, (including network devices), on a regular basis.

The scanner will always be configured to run non-destructive scans but will be configured with appropriate credentials, on the scanned platform, to enable in-depth OS scanning.

Reports will be produced from the vulnerability scanning server as input to the audit process and for analysis by the CS Security Team.

The vulnerability scanner will be used as a security testing tool during the development phases of the HNG-X project.

The design of the vulnerability scanning server is covered in the HNG-X Vulnerability Management HLD {DES/SEC/HLD/0008}

FUJ00088336

6.5 Payment Card Industry Solution – Debit/Credit Card System

6.5.1 Overview

This solution is intended to meet the requirements of Post Office CR-957, (CCN 1202), introduced as a result of the Payment Card Industry Data Security Standard.

All other architecture and subsequent design documents will also explicitly state the measures taken to meet the PCI requirements of this architecture.

The PCI definition of Sensitive Authentication Data and Cardholder Data is as below.

	Data Element	Storage Permitted	Protection Required	PCI DSS REQ. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

The Horizon-Online system has been designed to ensure that, for Horizon-Online transactions;

1) No Debit or Credit card full track information is stored anywhere in the system.
2) No Sensitive Authentication Data is stored post-authorisation for Debit and Credit card transactions.
3) Any PAN stored in the Horizon-Online system will either be in hashed format, encrypted along with the expiry data and issue number, or will otherwise be obfuscated by overwriting.

Legacy Horizon data will remain in its existing form and will not be modified. The following table identifies those data that are classed as legacy, their storage location and the current retention duration.

Data Type	Location	Duration

FUJ00088336

Reconciliation Data	Data Reconciliation Service	90 Days
Transaction Data	Counter Riposte Data Store	84 Days
Audit Data	Audit System	7 Years

The detailed solution design of how the Horizon-Online solution meets the requirements of CCN 1202 is in the following documents;

1) ARC/APP/ARC/0005- Online Services Architecture
2) DES/APP/HLD/0006- Generic Authorisation Services High Level Design
3) DES/APP/HLD/0007- DCS Authorisation Agent High Level Design

6.5.2 Cardholder Environment

The PCI Glossary defines the Cardholder Environment as, *"Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment"*

This architecture adopts the use of this definition and the HNG-X Cardholder Environment is defined in *PCI Cardholder Environment Definition* {ARC/SEC/SPE/0001}

6.5.3 PCI Data Flows - DCS

Appendix A – PCI Data Flows at the end of this document illustrates the detailed PCI Data Flows.

6.6 Payment Card Industry Solution – Network Banking System

6.6.1 Overview

This solution is intended to meet the requirements of Post Office CR-957, (CCN 1202), introduced as a result of the Payment Card Industry Data Security Standard.

All other architecture and subsequent design documents will also explicitly state the measures taken to meet the PCI requirements of this architecture.

The PCI definition of Sensitive Authentication Data and Cardholder Data is as below.

FUJ00088336

	Data Element	Storage Permitted	Protection Required	PCI DSS REQ. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

The Horizon-Online system has been designed to ensure that, for Horizon-Online transactions;

1) No card full track information is stored anywhere in the system.
   a) The Network Banking service (NBS) requires that the full track image is available for up to 5 days, post-authorisation, in the event that a reversal is required.
2) No Sensitive Authentication Data is stored post-authorisation for card transactions.
   a) As with 1a above, the NBS requires that the full track image is available for up to 5 days, post-authorisation, in the event that a reversal is required.
3) Any PAN stored in the Horizon-Online system will either be in hashed format, encrypted along with the expiry data and issue number, or will otherwise be obfuscated by overwriting.

Legacy Horizon data will remain in its existing form and will not be modified. The following table identifies those data that are classed as legacy, their storage location and the current retention duration.

Data Type	Location	Duration
NBS	Transaction Enquiry Service	180 Days
Reconciliation Data	Data Reconciliation Service	90 Days
Transaction Data	Counter Riposte Data Store	84 Days
Audit Data	Audit System	7 Years

The detailed solution design of how the Horizon-Online solution meets the requirements of CCN 1202 is in the following documents;

1) ARC/APP/ARC/0005- Online Services Architecture
2) DES/APP/HLD/0006- Generic Authorisation Services High Level Design
3) DES/APP/HLD/0009- NBS Authorisation Agents High Level Design

FUJ00088336

6.1.2 Cardholder Environment

The PCI Glossary defines the Cardholder Environment as, *"Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment"*

This architecture adopts the use of this definition and the HNG-X Cardholder Environment is defined in *PCI Cardholder Environment Definition* {ARC/SEC/SPE/0001}

6.1.3 PCI Data Flows - NBS

Appendix A – PCI Data Flows at the end of this document illustrates the detailed PCI Data Flows.

FUJ00088336

7 Recovery and resilience

The security architecture for HNG-X is as much a strategy as it is a simple technical solution. Therefore it is intrinsic to the solution and is embedded throughout all other architectures and designs. Therefore if the other architectures and designs in HNG-X follow this security architecture, whatever resilience measures are introduced by those designs will also be secure.

Where specific resilience measures are required, such as the Patch Management Server, the IPS and the Vulnerability Management Server, the High Level Designs will include resilience as part of the solution.

FUJ00088336

8 Performance

There are no specific performance requirements for the Security Architecture.

FUJ00088336

9 Migration

The migration strategy is defined in the HNG-X Migration Architecture {ARC/MIG/STG/0001}. This document describes the migration approach and defines each migration step, covering what is migrated, when it is migrated and how it is migrated?

The security implications of migration are considered in each appropriate architecture and design document. In this section this document refers out to these documents as they cover the migration steps, (including security), in more specific detail.

Due to the virtualisation of certain Horizon platforms, caused by the removal of the new Counter from the scope of HNG-X, there are certain security related systems that need to migrate. These are covered in the following sections.

Some of these will continue unchanged in the HNG-X environment, whereas some of them will be virtualised.

Additionally during Migration, appropriate risk assessments must be taken and controls implemented to ensure that the virtualisation process does not allow sensitive information to be distributed inappropriately.

9.1 PIN Pads

As the Horizon Counter is not being updated, following the removal of the new Counter from the scope of the HNG-X programme, the existing PIN Pads workstations will also be retained until such time as the Counter is upgraded.

These workstations are based in Bracknell and Lewes and are;

1) PIN Pad Proving Workstation
2) Training PIN Pad Loading Workstation
3) PIN Pad Key Generation Workstation
4) PIN Pad Test Workstation

There is no migration activity for these workstations as they are standalone

9.2 Horizon Access Control

The virtualisation of Horizon systems requires the Wigan and Bootle Windows NT support infrastructure also be virtualised and moved to Ireland. This support infrastructure is defined as;

1) Windows NT Domain Controllers
2) Windows NT SAS Servers (For Counter and SYSMAN2 management)
3) SYSMAN2 (For Counter software management)

During the design phase, this list will be verified and expanded if necessary.

The Horizon and HNG-X authentication mechanisms will be maintained as separate entities for the lifetime of any migrating Horizon system. The RSA SecurID strong authentication solution for Horizon will be retired, though the Horizon Windows NT SAS servers will be retained. This approach simplifies the design of the HNG-X authentication mechanism and reduces the complexity of the solution.

FUJ00088336

9.3 Utimaco VPN

The proposed retention of the Utimaco VPN Servers also requires the following platforms to be retained and virtualised.

1) VPN Servers
2) VPN Loopback Workstation
3) VPN Exception Server
4) VPN Policy Server
5) CAW

The VPN Servers will be virtualised onto discrete hardware as an additional layer of security protection. This will allow the servers to be placed in a DMZ that is secured between two separate firewalls. This reduces the likelihood of a single configuration error or compromise affecting the entire data centre or branch estate.

The CAW is a physical standalone platform located in BRA01 with a backup in LEW02. These will be used for the generation of new VPN keys, (known as xVPN keys), and for the provision of CRLs for the VPN keys.

9.4 HNG-X Migration Enabling Upgrades for Data Centres

No additional requirements from this architecture.

9.5 Data Centre Build

During the secure build of the Data Centre the following mechanisms will be deployed;

1) Active Directory (including Vintella Pluggable Authentication module for Red Hat Linux and Solaris)
2) Strong Authentication
3) Key Server and Key Management Workstation.
4) NPS for storage of key material
5) Firewall rules
6) VPN Servers
7) SSL Termination

In addition, between the completion of V&I testing and the start of live service, the Data Centre will be subject to a security penetration test to validate the configuration that has been deployed.

9.6 Move Wigan Network Management Servers

No additional requirements from this architecture.

9.7 Data Centre Preparation

As part of the final preparation of the Data Centre, the following activities will take place.

1) Data Centre penetration test.
2) Reset of user account passwords and refresh of two-factor authentication credentials.

FUJ00088336

3) Deployment of 'Live' key material where necessary.

9.8 Cutover Rehearsal

No additional requirements from this architecture.

9.9 Migration of POL FS

No additional requirements from this architecture.

9.10 Migration of Batch Services

Refer to the HNG-X Batch Services Architecture {ARC/APP/ARC/0007.}

9.11 HNG-X Specific Services

No additional requirements from this architecture.

9.12 Migration of Online Services

Refer to the HNG-X Online Services Architecture {ARC/APP/ARC/0005.}

9.13 Migration of Audit Services

The HNG-X Information Security policy must be followed to ensure the appropriate protection of Data in transit. This is defined in SVC/SEC/POL/0003.

No additional requirements from this architecture.

9.14 Migration of Branch Services

No additional requirements from this architecture.

9.15 Move Bootle Network Management Servers

No additional requirements from this architecture.

9.16 Decommission Wigan and Bootle

Refer to section 9.24 in this document.

9.17 Horizon Counter Changes for PCI Compliance

Horizon Counters will be modified to process, transmit and store data in a PCI compliant fashion. This modification will utilise an Online Service Router instance on the BAL, (instead of Riposte), for authorisation requests between a Counter and the Data Centre.

Recovery and Confirmation messages will still be passed through Riposte.

No additional requirements from this architecture.

FUJ00088336

9.18 HNG-X Migration Enabling Upgrades for Counters

No additional requirements from this architecture.

9.19 HNG-X Application Pilot and Rollout

Following the 'point of no return' in a Branch, the Counter secure filestore must be overwritten.

This will be done using the Microsoft Sysinternals ***sdelete*** tool, set to overwrite 3 times.

9.20 Branch Router Rollout

Refer to ARC/NET/ARC/0003

9.21 Counter Event Management Changes

The Tivoli system must be configured such that any security events and any required alerts created by the new Counter application are appropriately routed to the Data Centre and actioned.

Events that are no longer valid must be removed. For example where they relate to applications or functionality removed as part of the Counter upgrade.

9.22 Counter XP Upgrade

No additional requirements from this architecture.

Not in scope for HNG-X Release 1.

9.23 Post-Application ADSL Changes

Refer to ARC/NET/ARC/0003

9.24 Final Decommissioning

Upon final decommissioning of Wigan and Bootle it is critical to ensure that all hardware, (including but not restricted to, servers, workstations, network devices, backup tapes, CDs, DVDs and other portable media), are securely erased where necessary.

This activity will be run under the control of the CS Security Team and evidence of the process must be produced.

Every platform instance must be accounted for.

9.25 Estate Management Upgrade

No additional requirements from this architecture.

FUJ00088336

10 Testing and Validation

This section captures any architectural issues that affect the viability and cost effectiveness of validating the solution. For example an external service may need to be provisioned by the supplier with the capability to run in one of several modes (multiple test environments , production) and the enabling products must be engineered such that it can be configured to execute in any of these modes .

Security testing is a critical part of the HNG-X programme. It is vitally important to ensure that the security principles have been followed and that the subsequent security controls have been deployed correctly. In this sense, security testing takes the approach of, “How can I break it?”, rather than, “Does it work as expected?”

The security testing process will be an iterative one, beginning with stringent and exhaustive component testing of individual platform foundation builds and software, as they are released for system testing.

During each subsequent phase of testing, it is expected that the security testing load will change as the initial tests will not need to be repeated and the testing focus will move to cover integration features and the validation of firewall rules and access control lists.

The security testing process is covered, in detail, in a the following documents;

1) HNG-X Security Testing High Level Test Plan {TST/GEN/HTP/0004}
2) HNG-X System Test Security Testing High Level Test Plan {TST/SYT/HTP/0006}

FUJ00088336

11 Risk and Assumptions

The major security risks for HNG-X are identified in the programme information security risk register, maintained by the CS Security Team.

FUJ00088336

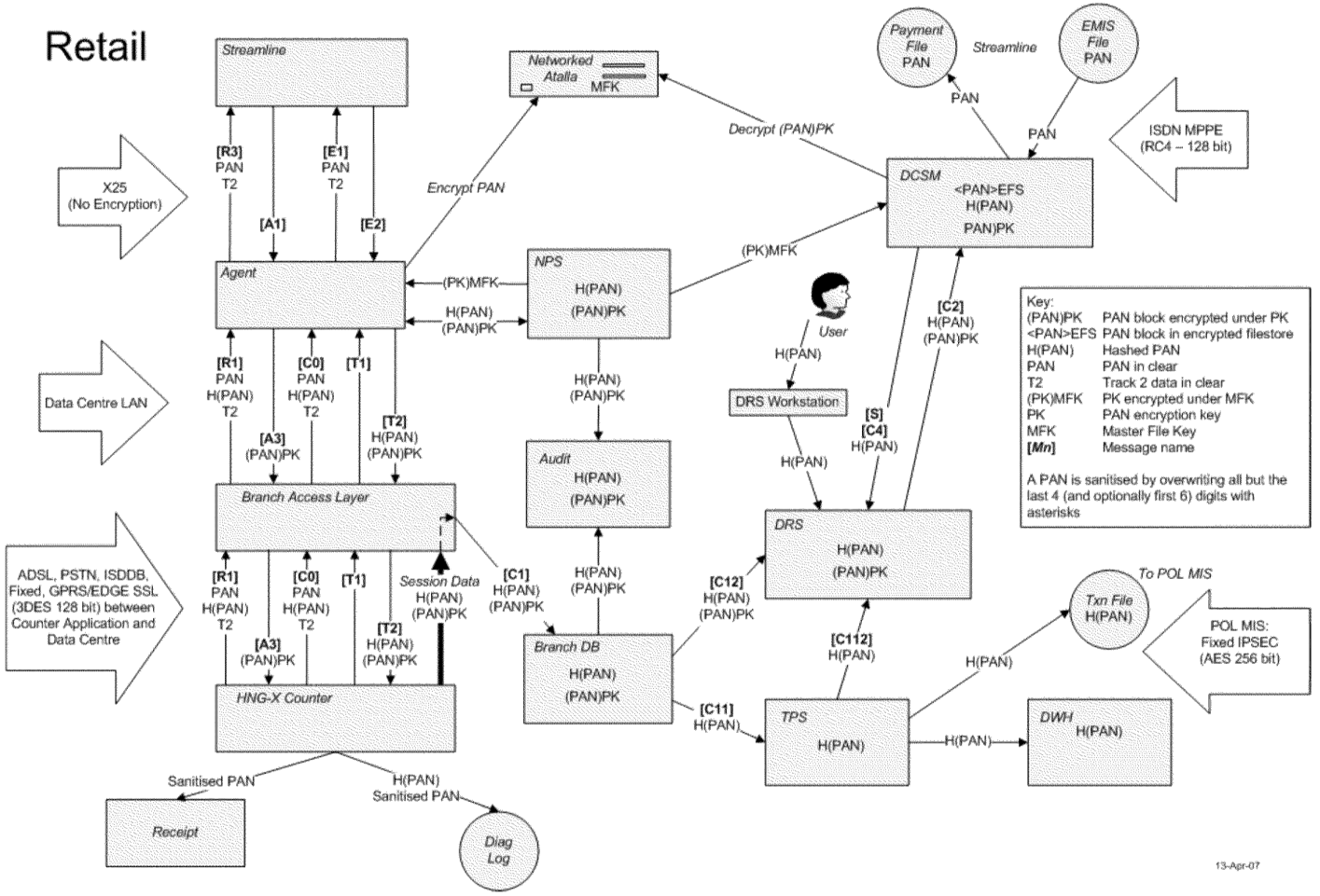
12 Requirements Traceability

Refer to the Requirements Traceability Matrix for Security {ARC/SEC/RTM/0001}

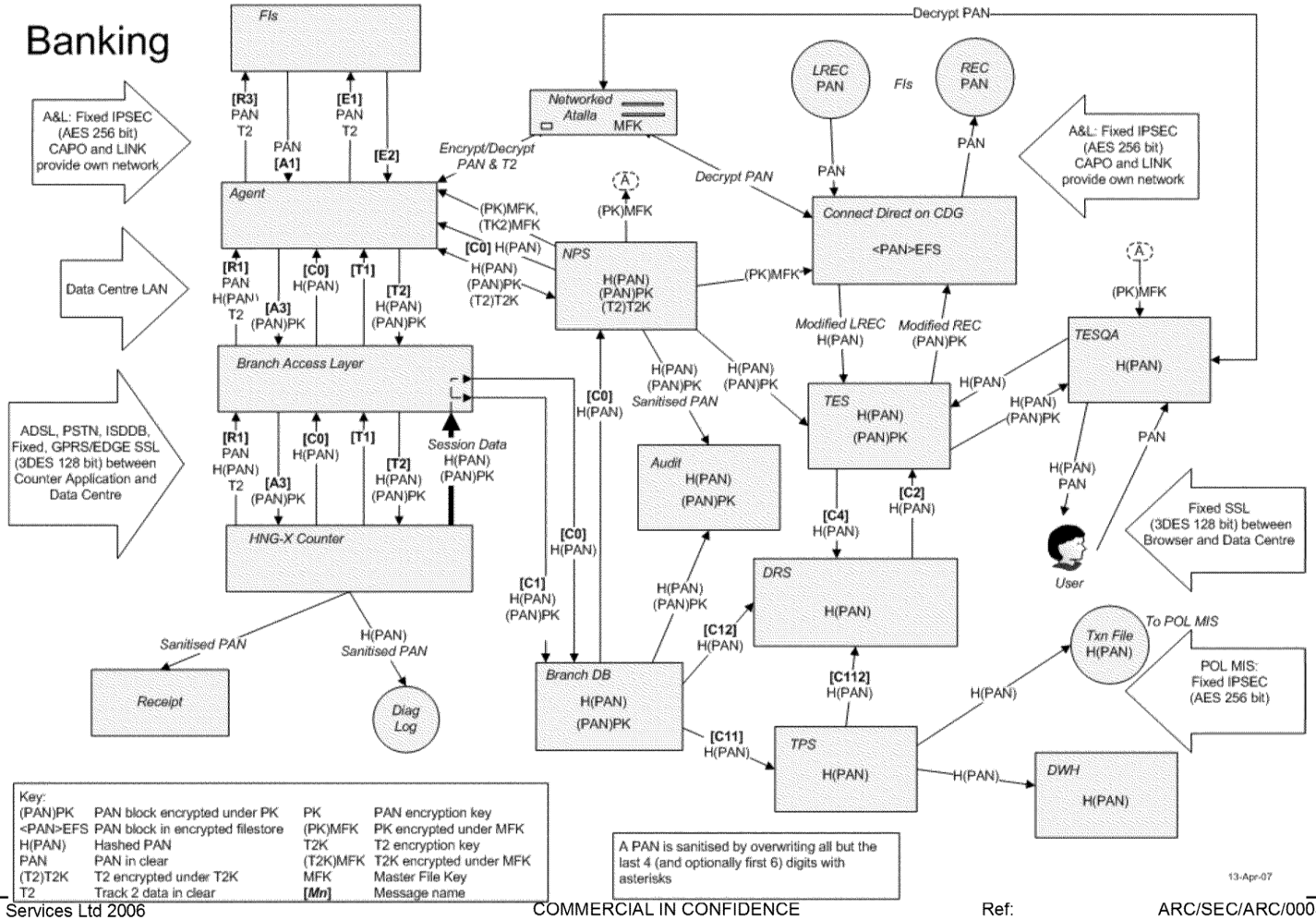
FUJ00088336

13 Appendix A – PCI Data Flows

FUJ00088336

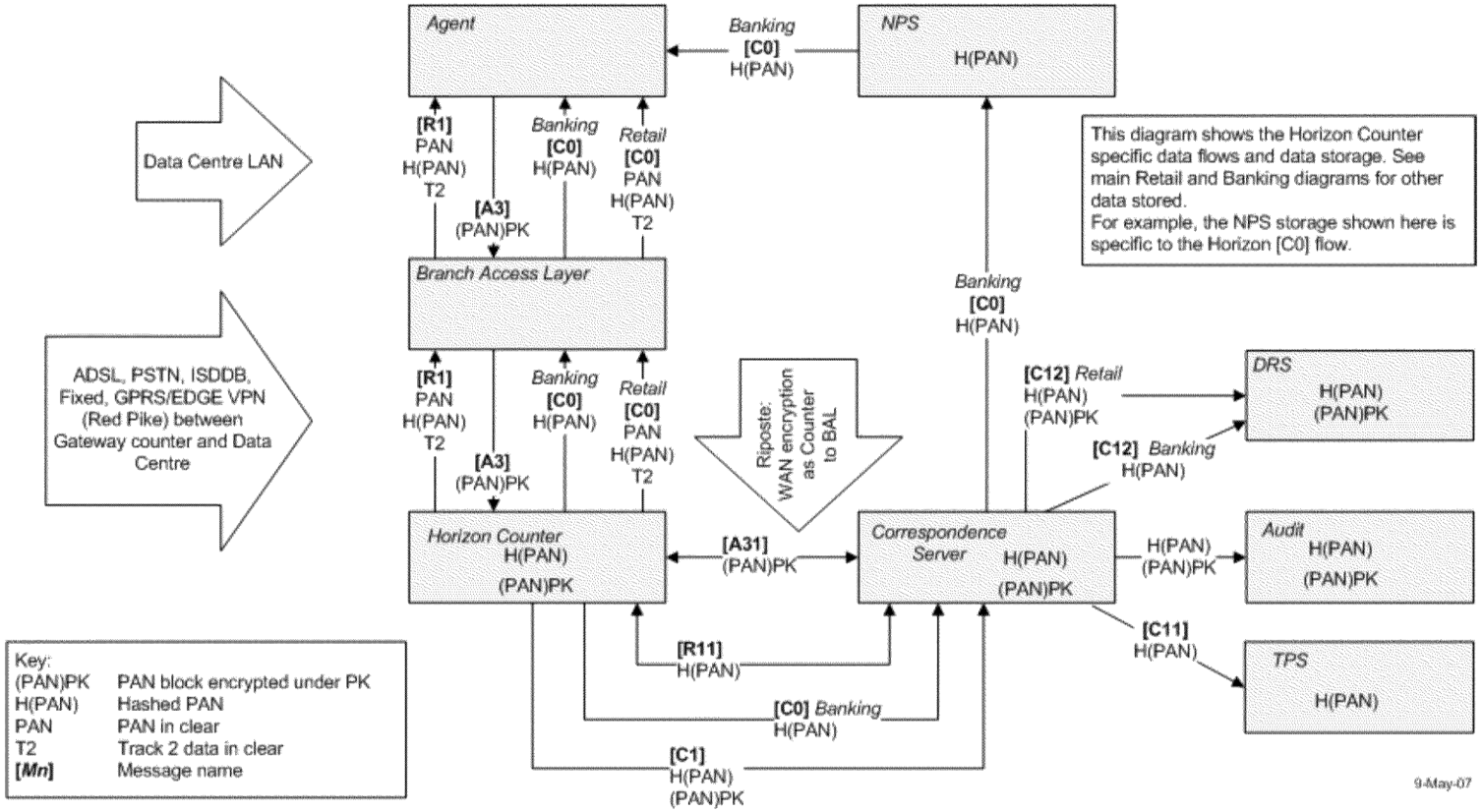


FUJ00088336



FUJ00088336

Horizon Counter



FUJ00088336

Audit