Document Title:	HNG-X Crypto Services High Level Design
Document Type:	High Level Design
Release:	Not Applicable
Abstract:	This document gives the High Level Design for bespoke application-level cryptographic services in HNG-X. This document contains sections that have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. These sections must not be changed without authority from the FS Acceptance Manager.
Document Status:	DRAFT
Author & Dept:	Rob Arthan, Sarah Selwyn
Internal Distribution:	(Specify those individuals who require approved version only. For Document Management to notify individuals via Weekly Approval notification)
External Distribution:	None

Approval Authorities:

Name	Role	Signature	Date
Adam Spurgeon	Solution Design		
Keith Tarran	Application Development Manager		
Tom Lillywhite	CISO		
Tim Jones	Solution Owner		

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.

0 Document Control

0.1 Table of Contents

0.2 Table of Figures

0.3 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	21-APR-2007	Initial Draft for review	N/A
0.2	10-MAY-2007	Changes in response to comments received and to reflect latest thinking.	N/A
0.3	30-MAY-2007	Further changes in response to comments received. The PAN Hash Seed Service has been renamed as "PAN Hash Seed Function" and is no longer implemented as a windows service.	N/A
0.4	21-DEC-2007	Further changes in response to comments. The description of the PAN Hash algorithm has been corrected. The passphrase for the Key Service key is now entered via a separate KS Workstation application.	N/A
1.0	11-APR-2008	Changes in response to comments. Section 3.2.4 changed to show that the function described has been implemented by the Counter team not the Crypto team. First approved version.	N/A
2.0	11-Jul-2008	Changes made for Acceptance by Review. Approved version.	N/A
2.1	17-Nov-2008	Changes made to the HSM deployment. The references to the PIN Pad Proving Workstations requiring an HSM have been removed since the PIN Pad is likely to be retained until 2010 and therefore an HNG-X PIN Pad proving workstation and HSM may not be required. Draft for review.	N/A
2.2.	04-Dec-2008	Changes made in response to review comments from Andy Williams: the number of active DEAs was changed from 2 to 1, PI was defined and corrected, EST confirmed not to use NB Crypto API, added LLD and KM Migration HLD refs and simplified implementation description. Section 3.1.1 added statement that raw PANS are always 16 to19 characters in length Section 3.1.1 Updated 2 CAPO servers to 4 CAPO servers. Draft version.	N/A
2.3	16-Dec-2008	Updated diagram 5.1 to show the Audit Workstation connected via the KSS in order to collect keys from NPS (using the standard Key Service Client functionality). The functionality to collect keys from CD-ROM by AUW was removed by CP4623). Updated Fig. 5.1 to remove PIN Pad Proving Rig and to add in EST, clients requiring SSL certificates, DCS Authorisation Server, and CDG. Draft version for approval.	N/A
3.0	17-Dec-2008	Updated to include comments from Stuart Honey to change fig 5.1 in order to show HSM shared between KMNGT workstation and Audit Workstation and to include reference to the C/C++ APIs.	N/A

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		Approved version.	
3.1	24-Feb-2009	Updated to change length of PAN from range 16 to 19 characters in length to range 13 to 19 characters in length. Removed reference to CXP (XP counter). Draft version for review.	N/A
3.2	12-Mar-2009	Updated section 3.1.2 HSM Access Service to remove 1 of the 2 instances of TWS since only one instance of TWS will be connected to the HSM Access Service during live or DR. Draft version.	N/A
4.0	22-Sept-2009	Updated to include comments from Andy Williams and Stuart Honey: • Included CDG in section 3.1.1 and 4.2 • Included MWS in section 5.1 Approved Version	
4.1	21-Feb-2014	Updated section 8 (System Management) to reflect the change in hardware capability of the new Atalla Ax160 HSMs being installed as part of the Belfast Refresh with respect to console output. Draft Version	CP1108(5665)

0.4 Review Details

Review Comments by :	10-Mar-2014
Review Comments to :	guy.standen GRO & RMGADocumentManagement GRO
Mandatory Review	
Role	Name
Security Architect	Dave Haywood
Development	Stuart Honey
SSC Manager	Steve Parker; sscdm GRO
SV&I Manager	Chris Maving
Testing Manager	Mark Ascott
Service Architect	Steve Godson
R&R Principal CSA	Tim Jones
Optional Review	
Role	Name
R&R Development Manager	Geof Slocombe
R&R Project Manager	Tim Salisbury
Project Manager	Anand Ashwani
Business Continuity	Sathish Ramalingam
Security Architect	Dave Haywood

CISO	Tom Lillywhite
Security & Risk Team	CSPOA.Security GRO
Programme Manager	Brian McCann
Programme Manager	Mark Andrews (AndrewsM2)
Business Architect	Gareth Jenkins
Infrastructure Architect	Jason Clark
Service Transition & Change	Tony Atkinson
Operational Change/Release Management	Alan Flack
Service Governance Manager	Adam Bowe
Application Lead SDM and Risk Manager	Yannis Symvoulidis
Network Operations Manager	Roger Stearn
Systems Mgt & Global Cloud	Catherine Obeng
Infrastructure Operations Manager	Andrew Hemingway
Senior Operations Manager	Alex Kemp
System Management Group	John Bradley (for SMG)
Lead SDM Problem & Major Incident	Steve Bansal
Operational Security	Kumudu Amaratunga
Release, Integration & InfRel	Vijesh Pandya
POL Test Manager	James Brett (POL, JTT)
POL R&R Project Manager	Bob Delataste (POL, via Post Office Account Document Management)
POL R&R Architect	Ghulam Hussain (POL, via Post Office Account Document Management)
Core Division	Ed Ashford
Core Division	Andrew Gibson
Application Development Manager	Keith Tarran
Development	Jon Hulme
Solution Design Architect	Sarah Selwyn

Reviewer list compiled from PGM/DCM/ION/0001 V84.
Please refer to the latest version of PGM/DCM/ION/0001 to check for changes.

(*) = Reviewers that returned comments

0.5 Acceptance by Document Review

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

POL NFR Acceptance Ref	Internal FS POL NFR Reference	Document Section Number	Document Section Heading
SEC-3216	SEC-3216	3.1	HSM Crypto Services

0.6 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
ARC/APP/ARC/0003			HNG-X Counter Architecture	Dimensions
ARC/APP/ARC/0005			HNG-X Architecture - Online Services	Dimensions
ARC/APP/ARC/0007			HNG-X Batch Applications Architecture	Dimensions
ARC/GEN/REP/0001			HNG-X Glossary	Dimensions
ARC/PER/ARC/0001			HNG-X System Qualities Architecture	Dimensions
ARC/SEC/ARC/0003			HNG-X Technical Security Architecture	Dimensions
ARC/SOL/ARC/0001			HNG-X Overall Solution Architecture	Dimensions
DES/SEC/HLD/0003			HNG-X Key Management High Level Design	Dimensions
CS/OLA/051			Operational Level Agreement for Network Banking between Fujitsu Services, Post Office Ltd. and LINK	PVCS
CS/OLA/052			Operational Level Agreement for Network Banking between Fujitsu Services, Post Office Ltd. and CAPO	PVCS
CS/OLA/053			Operational Level Agreement for Network Banking between Fujitsu Services, Post Office Ltd. and Alliance & Leicester	PVCS
NB/IFS/024			NBX – LINK Application Interface Specification	PVCS
NB/IFS/025			NBX – CAPO Application Interface Specification	PVCS
NB/IFS/026			NBX – A & L Application Interface Specification	PVCS
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
PGM/DCM/TEM/0002 (DO NOT REMOVE)			Fujitsu Services Post Office Account HNG-X Landscape Document Template	Dimensions
DES/SEC/IFS/0001			HNG-X Cryptographic Applications Programming Interface Specification	Dimensions
FIPS-140-2		25/5/2001	Security Requirements For Cryptograhic Modules	U.S. Dept. of Commerce
FIPS-180-1		17/5/1995	Secure Hash Standard	U.S. Dept. of Commerce
PCI	1.1	September 2006	Payment Card Industry (PCI) Data Security Standard	PCI Security Standards Council
RFC3548		July, 2003	The Base16, Base32, and Base64 Data Encodings	IETF
RS/REQ/007			Event Logging and Error Reporting for Crypto Code	PVCS

Reference	Version	Date	Title	Source
X9.19		1996	Financial Institution Retail Message Authentication	ANSI
DEV/APP/LLD/0125			HNG-X Network Banking Cryptography API LLD	Dimensions
DEV/APP/LLD/0120			HNG-X PAN Crypto API LLD	Dimensions
DEV/APP/LLD/0131			HSM Access Service LLD	Dimensions
DEV/APP/LLD/0148			HNG-X KM: PAN Hash API for PCI Compliant Data Centre LLD	Dimensions
TST/GEN/SPE/0024			HNG-X ITU TEST and LIVE RIG CONFIGURATION: HSMs	Dimensions

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

0.7 Abbreviations

See also [ARC/GEN/REP/0001].

Abbreviation	Definition
AKB	Atalla Key Block – the data format used to represent keys for use in the Atalla HSM.
ANSI	American National Standards Institute
AWK	Acquirer Working Key – the key that protects PIN blocks forwarded by NBS to the FIs.
AZMK	Acquirer Zone Master Key – the key that protects the AWK.
DCS	Debit Card Service
EFS	Encrypted File Store (specifically, the Microsoft product of that name)
FI	Financial Institution (the normal meaning of this term is extended to include LINK in the context of NBS)
HLD	High Level Design
HSM	Hardware Security Module (also known as NSP)
IETF	Internet Engineering Task Force
KCV	Key Check Value
KM,	Key Management
KMNG	Key Management Workstation Application
LLD	Low Level Design
NB	Network Banking
NBS	Network Banking Service
NBX	Network Banking Switch (a historical term, now synonymous with NBS)
NPS	Network Banking Persistent Store
NSP	Networked Security Processor (also known as an HSM unit)
PAN	Primary Account Number
PCI	Payment Card Industry Data Security Standard [PCI]
PI	Processing Interface. The connection point to an external FI.
PKI	Public Key Infrastructure
SCA	Secure Configuration Assistant: a handheld device supplied by Atalla used to load certain keys into the Atalla HSM.
SHA-1	Secure Hash Algorithm version 1: see [FIPS-180-1].

0.8 Glossary

See also [ARC/GEN/REP/0001].

Term	Definition
aka	Also Known As
Atalla	The subsidiary of Hewlett Packard that makes the HSMs used in Horizon and HNG-X

Term	Definition
Track 2	Block of data obtained from a payment card containing the PAN and other sensitive data.
NB Crypto API	See section 3.1.3.

0.9 Changes Expected

Changes
None.

0.10 Security Risk Assessment

Security risks have been assessed and it is considered that there are no security risks relating specifically to this document.

0.11 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.

1 INTRODUCTION

1.1 Summary

This document gives the High Level Design of the bespoke application-level Cryptographic Services infrastructure needed to support the HNG-X Retail and Banking applications and to address the new security requirements arising from the PCI standard.

1.2 Scope

This document is concerned with the bespoke, application-level Cryptographic Services required by the HNG-X Retail and Banking Applications (see section 2.1 for more detail on the functional requirements). The Cryptographic services include functions carried out using Atalla hardware and also the software hashing of PAN data.

This document does **not** cover:

- cryptographic services supplied by Java and C/C++ APIs
- OS-level cryptographic services such as filestore encryption (EFS etc.).
- Network security, such as firewalls and link encryption.
- Software associated with the PIN pads

Key Management is the subject of a separate HLD, but the automatic establishment of session keys is covered in this document where applicable.

Figure 1-1 shows the context of this document in the HNG-X architecture and design documentation.

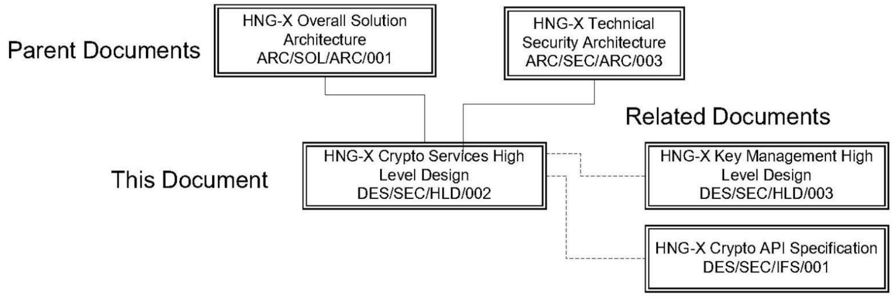
Parent Documents
HNG-X Overall Solution Architecture ARC/SOL/ARC/001
HNG-X Technical Security Architecture ARC/SEC/ARC/003
Related Documents
This Document
HNG-X Crypto Services High Level Design DES/SEC/HLD/002
HNG-X Key Management High Level Design DES/SEC/HLD/003
HNG-X Crypto API Specification DES/SEC/IFS/001

Figure 1-1. Document Relationships

1.3 Design Guidelines

The design approach adopted is to reuse the Horizon design wherever appropriate. In particular, the API offered to the Networking Banking applications is designed as an extension to the Horizon NBX Crypto API. The use in Horizon of the Riposte message store to deliver keys is replaced by the use of NPS for keys that are protected by an HSM master key.

Standard off-the-shelf mechanisms are to be used wherever possible, in particular, HSMs and standard cryptographic APIs. The following principles for protecting confidential cryptographic material are adopted:

- HSMs are used to give secure key handling for banking and PCI keys in transit and in storage

- Standard PKI techniques are used to protect private seed values in transit and in storage
- Standard PKI techniques are used to protect software encryption keys in transit and in storage

2 REQUIREMENTS

2.1 Functional Requirements

The facilities listed in the following table are required to support NBS:

Facility	Platform
PIN translate	NAA: A&L Banking Agent NAC: CAPO Banking Agent NAL: Link Banking Agent
Receive AWK	
Generate AWK	
Confirm AWK	
Check MAC	
Key Test Response	
Key Test Request	
Key Test Check	

To comply with the PCI requirements for DCS and NBS, the facilities listed in the following table are required:

Facility	Platform
Encrypt PAN	NAA: A&L Banking Agent NAC: CAPO Banking Agent NAL: Link Banking Agent CDG: Connect Direct Gateway TWS: TES Web Server DEA: DCS and ETS Agent Servers DCM: Debit Card Management Server AUW: Audit Workstation
Decrypt PAN	
Encrypt Data	
Decrypt Data	
PAN Hash	TWS: TES Web Server AUW: Audit Workstation CDG: Connect Direct Gateway CNH: Horizon Counter CNT: HNG-X Counter DCM: Debit Card Management Server

2.2 Non-Functional Requirements

2.2.1 Performance and Scalability

See [ARC/PER/ARC/0001] for overall system volumetrics.

2.2.2 Availability and Resilience

See [ARC/SOL/ARC/0001].

2.2.3 Usability

The Crypto Services are implemented as a set of APIs and do not have any user interface. The user interfaces to the Key Management System that supports the APIs are discussed in [DES/SEC/HLD/0003].

2.2.4 Security

The security requirements are derived from standards and from specific agreements with Post Office Ltd. and other parties, see [ARC/SEC/ARC/0003] for a complete list of security-related NFRs and see [CS/OLA/051], [CS/OLA/052], [CS/OLA/053], [NB/IFS/024], [NB/IFS/025] and [NB/IFS/026] for the specific agreements with CAPO, LINK & Alliance & Leicester relating to Network Banking Security.

2.2.5 Systems Management

See [ARC/SOL/ARC/0001].

3 Design Outline

3.1 HSM Crypto Services

3.1.1 Overview

HSMs are used to carry out the cryptographic functions to protect data that is transmitted from the HNG-X security domain to the security domains of the FIs by the Network Banking application and to protect data that is stored within the HNG-X domain both by Network Banking and Retail applications.

The HSM Crypto Services are split into two APIs: the NB Crypto API which performs the functions specific to the NB Agent functionality (PIN block encryption and MAC verification) and the PCI Crypto API which carries out encryption and decryption of data blocks, e.g., PANs.

The NB Crypto API and the PCI Crypto APIs are adapted from the Horizon NBX Crypto API. Internally, the implementations are adapted to use Atalla Networked Security Processors instead of internal HSM cards and to use keys obtained from the Key Server or from filestore (floppy disk) rather than the Riposte Message Store.

In addition to the HSMs used for business purposes, the KMNG workstation needs access to an HSM to carry out various functions relating to key management. The design of the KMNG Workstation is described in [DES/SEC/HLD/0003]. The Audit Workstation requires access to an HSM in order to process encrypted PANs in audit records.

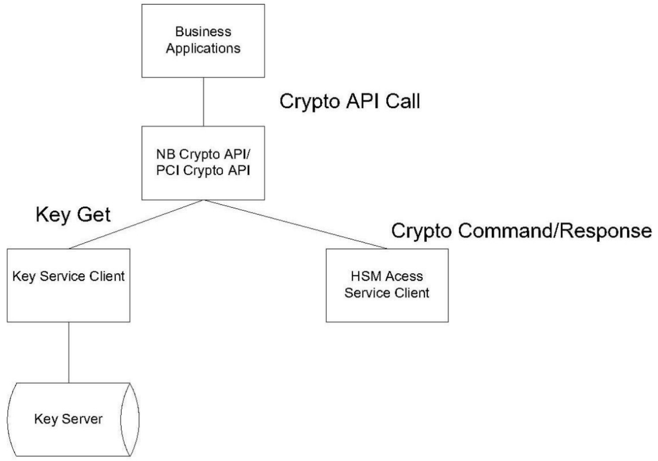

Figure 3-1. HSM Crypto Services Context

The Atalla HSM cards used in Horizon are obsolete. Their function was replaced in HNG-X by the current Atalla HSM technology which is packaged in rack-mounted tamper-proof modules that are accessed via TCP/IP over Ethernet. These are known as NSPs (Networked Security Processors) but are also referred to as HSMs.. HSMs in use in HNG-X come in two performance variants which shall be referred to as SPHSM (Standard Performance HSM) and HPHSM (High Performance HSM). The SPHSM maps on to the Atalla A8150 and A8160 models whereas HPHSM maps onto the Atalla A10150 and A10160 models. The Ax160 model HSMs are replacements for the older Ax150 model HSMs to be introduced as part of the Belfast refresh. The newer Ax160 models are like for like replacements for the older models with performance at least equal to their predecessors.

Each of these HSMs can support several simultaneous TCP/IP sessions (up to 64, but, this is for convenience rather than performance, since, in practice, processing time dominates communications time, so that full throughput can be obtained with say 2 simultaneous sessions).

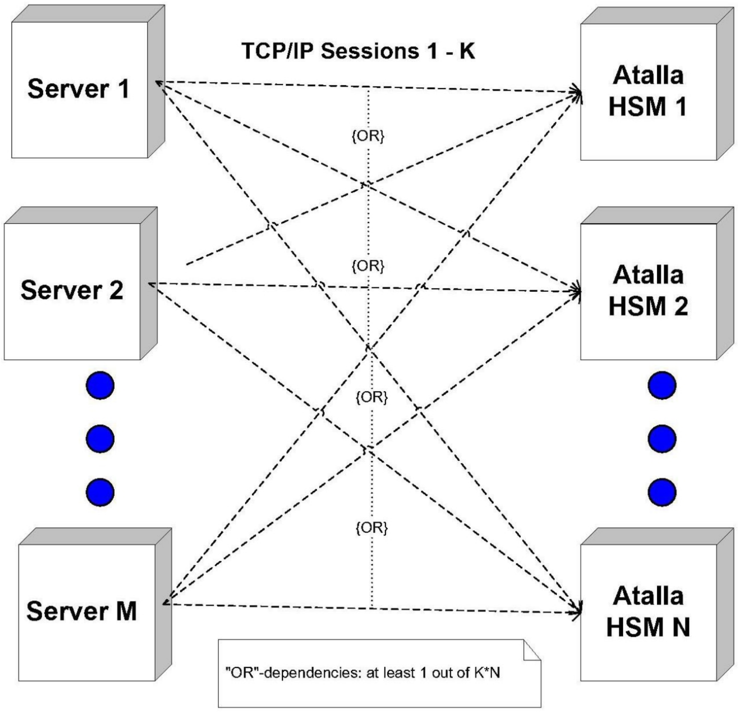

Figure 3-2. Server – Atalla HSM Connection Model

The networking connection model is shown in Figure 3-2, which depicts M servers each opening K connections on each of N Atalla HSMs. It is proposed that the implementation should support configurable values for M, N and K with K potentially varying from server to server up to a maximum of M = 20, N = 16 and K limited by the maximum of 64 connections per HSM.

The live configuration in the IRE11 data centre will have N = 3 HSMs, 3 HSMs being sufficient to handle peak required throughput (at 60% loading of the HSMs). IRE19 will have 2 live HSMs and one additional HSM available should IRE11 become unavailable. See TST/GEN/SPE/0024 for distribution of HSMs between live and DR sites. These figures are for the A10150 model HSM. See section 6.2 for more details of the volumetrics.

Performance information from Atalla indicates that near-optimal throughput will be achievable using between 2 and 4 simultaneous connections for the high-volume applications (running on the NBS and DCS Agent Servers and on the DCS Management Servers). There are M = 12 active servers altogether in each data centre as shown by platform type in the following table:

Server	Quantity	Comments
NAA, NAC, NAL: NBS Agent Servers	8	2 x A&L, 4 x CAPO, 2 x LINK
TWS: TES Web Server	1	Windows platform at HNG-X
DEA: DCS & ETS External Online Services	1	
DCM: Debit Card Management Server	1	
CDG: ConnectDirect Gateway	1	Windows 2003 platform. REC and LREC file

Server	Quantity	Comments
		processing.

The KMNG (KSN) and the Audit (AUW) workstations at BRA01 are to have a shared SPHSM on a private LAN. Similarly, the KSN and AUW at LEW02 will share an SPHSM. These systems do a very low volume of HSM cryptography. These two HSMs will be implemented as the special case of the model shown in Figure 3-2 in which M = N = K = 1.

3.1.2 HSM Access Service

The HSM Access Service allows application processes to share HSMs. From the application perspective, it provides similar functionality to the Atalla Load Balancer used in Horizon. When the service is started, it attempts to establish a small number of TCP/IP connections with each of the HSMs. Application threads make requests on the service via the NB Crypto API. The service dispatches these requests to the HSMs distributing the work randomly across the available sessions and returns the responses to the requesting application thread.

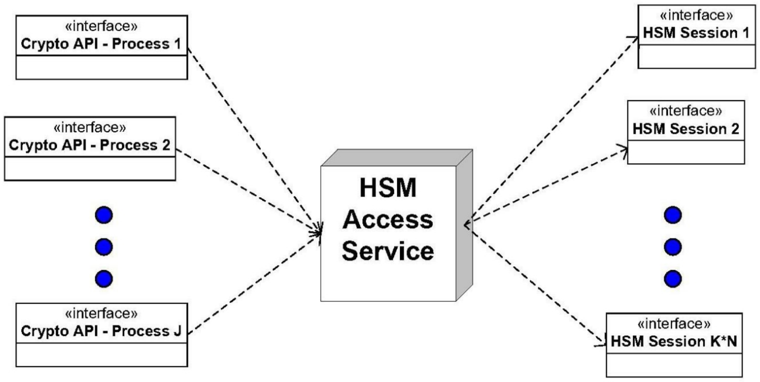

Figure 3-3. HSM Access Service

3.1.3 NB Crypto Functions

3.1.3.1 NB and PCI Crypto APIs

The NB Crypto API provides cryptographic functions that are specific to the NB Agent functionality (PIN block translation and MAC verification). The PCI Crypto API provides the PAN encryption and decryption functionality. The NB Crypto API is based on the Horizon NBX Crypto API. Both NB Crypto API and PCI Crypto API implement the notion of a "protection domain" identifying a cryptographic relationship and hence providing an abstract model for key access. The protection domains in use by the subsystems described in this document are listed in section 4.1.

The APIs provide a C++ language interface documented in [DES/SEC/IFS/0001]. This provides all the functions identified in section 2.1 apart from the PAN Hash function (for which see section 3.2).

3.1.3.2 Key Service Client

In Horizon, the cryptographic APIs obtained key material held in various kinds of repository via a component called the KM Client Agent. The Key Service Client replaces the functionality offered by the

KM Client Agent in Horizon obtaining key material via the Key Service. The high level design of the Key Service is given in [DES/SEC/HLD/0003].

3.2 PAN Hash Services

3.2.1 Overview

To meet PCI requirements, PANs are obfuscated using a hashing algorithm. The hashing algorithm replaces all but the first 6 and last 4 digits of the 13 to 19 digit PAN with a base 64-encoded hash value. To avoid various kinds of attack, the hashing algorithm uses a private seed value, i.e., it is a keyed one-way function. The seed comprises 10 bytes of binary data and the hash is computed by concatenating the seed and the PAN (as a string of ASCII digits) and then applying the SHA-1 algorithm to the resulting 26 to 29 bytes of data. The binary hash value returned by the SHA-1 algorithm is then base 64-encoded using the encoding of section 3 of [RFC3548], which uses the characters "/" and "+" to supplement the 62 alphanumeric characters. The base 64 encoding is then adjusted to give an alphanumeric string beginning with a letter as follows: if the first character is a decimal digit, it is converted into an upper case letter by mapping "0" to "A", "1" to "B", …, "9" to "J"; then any occurrence of a non-alphanumeric character is converted into a lower case letter by mapping "+" to "a" and "/" to "b" (The encoding also uses "=" for padding, but this is only at the end of the string and can be ignored.) The obfuscated PAN returned by the PAN Hash function has the same length as the original PAN and is the concatenation of: (1) the first 6 digits of the PAN, (2) the leading 3 to 9 characters of the adjusted base 64-encoded SHA-1 hash value and (3) the last 4 digits of the PAN.

For example,

PAN HASH SEED (hex):	123456789ABCDEF01234
PAN (ASCII digits):	1234567812345678
SHA-1 (hex):	d3f403f949cc9077df81ae63196ef353afccbd0a
SHA-1 (base 64)	0/QD+UnMkHffga5jGW7zU6/MvQo=
SHA-1 (base 64, adjusted)	AbQDaUnMkHffga5jGW7zU6/MvQo=
Truncated hash	AbQDaU
Obfuscated PAN:	123456AbQDaU5678

The PAN Hash seed value, PH, is managed like a cryptographic key and is distributed to the HNG-X platforms that use it via the Key Server (see [DES/SEC/HLD/0003]). See also section 11.2 for the delivery route to Horizon Counter PCs during migration. The PH is accompanied by a KCV comprising the first 4 hexadecimal digits of the SHA-1 digest of the (binary) PAN Hash Seed (PH) value.

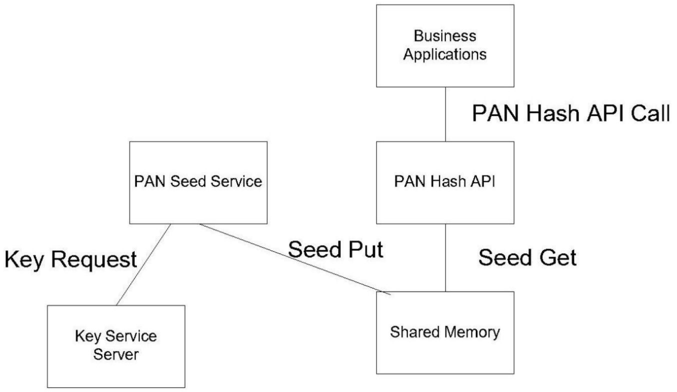

Figure 3-4. PAN Hash API Context

The PAN hash functionality has to be available on a variety of Windows platforms (including the Horizon counters) and on the HNG-X counters.

3.2.2 PAN Hash API

The PAN Hash API provides a C++ language interface documented in [DES/SEC/IFS/0001] that encapsulates the operation of obtaining the seed value and performing the seeded SHA-1 calculation described above. The seed is held in shared memory set up by the PAN Seed Function. This API is used on data centre Windows platforms and on Horizon counters. The version that runs on Horizon counters is a variant that obtains the seed value from filestore.

3.2.3 PAN Hash Seed Function

This function obtains the PAN Hash seed value (PH) and holds it in shared memory. This service runs on data centre Windows platforms only. The seed is obtained by a call to the Key Service Client.

3.2.4 Java PAN Hash Function

The Java PAN Hash function runs on HNG-X counters. The PAN Hash seed value (PH) is obtained from the Branch Access Layer during session logon and is then held as static data in the Java VM. An interface similar to the C++ interface documented in [DES/SEC/IFS/0001] was expected to be provided which calculates the PAN Hash value using PH and the algorithm described in section 3.2.1 above, but the Counter team have now implemented this.

4 Key Management Outline

4.1 Protection Domains

The following table lists the protection domains and keys used in the Crypto Services described in this document:

Protection Domain	Key(s)	Key Purpose	Where Created	Delivery Method	How Stored	Where Used	Number of Keys	Key Type and Length	Algorithm	Key Life	Key Compromise
ZA	AZMK	A key encryption key used to protect and authenticate working keys in messages between HNG_X and A&L	Fujitsu RMGA	3 parts on paper manually Combined using SCA and Key Loading W/S onto diskette (encrypted under MFK) Loaded into NPS via KMNG Workstation	Store under MFK for use by HSM in HNG-X	HSM & Agents	1	Key Encryption Key (KEK) Double Length	Triple DES	6 mthly, by agreement with POL/A&L	Generate & use new key
					A&L using a method agreed with POL	A&L					
NBPC_AL	AWK	PIN Encryption Key. Used to re-encrypt the PIN No during transfer from HNG-X to A&L	A&L	Delivered in messages from A&L processing interface (PI) to NBX Authorisation Agent under AZMK	Encrypted under MFK	HSM	1 per Agent session	Session Double Length	Triple DES	1 day	Generate & use new key
					A&L using a method agreed with POL	A&L					
ZC	AZMK	A key encryption key used to protect and authenticate working keys in messages between HNG-X and CAPO	CAPO	3 parts on paper manually Combined using SCA and Key Loading W/S onto diskette (encrypted under MFK) Loaded into NPS via KMNG Workstation	Store under MFK for use by HSM in HNG-X	HSM & Agents	1	Key Encryption Key (KEK) Double Length	Triple DES	6 mthly, by agreement with POL	Generate & use new key
					CAPO using a method agreed with POL	CAPO					

Protection Domain	Key(s)	Key Purpose	Where Created	Delivery Method	How Stored	Where Used	Number of Keys	Key Type and Length	Algorithm	Key Life	Key Compromise
NBPC_CAPO	AWK	PIN Encryption Key. Used to re-encrypt the PIN No during transfer from HNG-X to CAPO	Fujitsu RMGA (NBX Authorisation Agent server crypto co-processor.)	Delivered in messages to CAPO PI from NBX Authorisation Agent under AZMK	Encrypted under MFK CAPO using a method agreed with POL	HSM CAPO	1 per Agent Session	Session Double Length	Triple DES	1 day	Generate & use new key
ZL	AZMK	A key encryption key used to protect and authenticate working keys in messages between HNG-X and LINK	Fujitsu RMGA	3 parts on paper manually Combined using SCA and Key Loading W/S onto diskette (encrypted under MFK) Loaded into NPS via KMNG Workstation	Store under MFK for use by HSM in HNG-X LINK using a method agreed with POL	HSM & Agents LINK	1	Key Encryption Key (KEK) Double Length	Triple DES	6 mthly, by agreement with POL/LINK	Generate & use new key
NBPC_LINK	AWK	PIN Encryption Key. Used to re-encrypt the PIN No during transfer from HNG-X to LINK	LINK.	Delivered in messages from LINK PI to NBX Authorisation Agent under AZMK	Encrypted under MFK LINK using a method agreed with POL	HSM LINK	1 per Agent Session	Session Double Length	Triple DES	1 day	Generate & use new key
BK	BDK	Base Derivation Key. Used to derive the 'initial/start' value of the Pin encryption key (NBPO) for each PIN Pad	Fujitsu RMGA	Manual process using PIN Pad Key Generation Tool and PIN Pad Proving Tool.	Encrypted under MFK	NPS	1	DUKPT Double length	Triple DES	Indefinite	Change initial NBPO key (IK) of all PIN Pads, encrypt new BDK under MFK for HSM use
PAN	PK	PAN Encryption Key Used to encrypt and decrypt PANs stored in data centre	Fujitsu RMGA	Generated using SCA and Key Loading W/S onto diskette (encrypted under MFK) Loaded into NPS via KMNG Workstation	Encrypted under MFK	NPS	1	Data encryption key Double Length	Triple DES	6 months	Generate & use new key

Protection Domain	Key(s)	Key Purpose	Where Created	Delivery Method	How Stored	Where Used	Number of Keys	Key Type and Length	Algorithm	Key Life	Key Compromise
T2K	T2K	Track 2 Encryption Key Used to encrypt and decrypt Track 2 card data stored in data centre	Fujitsu RMGA	Generated using SCA and Key Loading W/S onto diskette (encrypted under MFK) Loaded into NPS via KMNG Workstation	Encrypted under MFK	NPS	1	Data encryption key Double Length	Triple DES	6 months	Generate & use new key
PAN_HASH	PH	Seed for the PAN hashing algorithm. 20 random hexadecimal digits.	Fujitsu RMGA	Generated by manual procedure and delivered into NPS encrypted under the Key Server Public Key.	NPS encrypted under the Key Server Public Key.	Counters Servers Various	1	Custom 20 bytes	Custom based on SHA-1	Indefinite	Requires software refresh see section 6.3

4.2 Key Route Maps

In the diagrams in the following section, the left of the dashed line represents the physically secure key management office. Where no source node is shown on the left, the key material is generated automatically using the SCA (and backed up via NPS).

4.2.1 AZMK_AL, AZMK_CAPO, AZMK_LINK

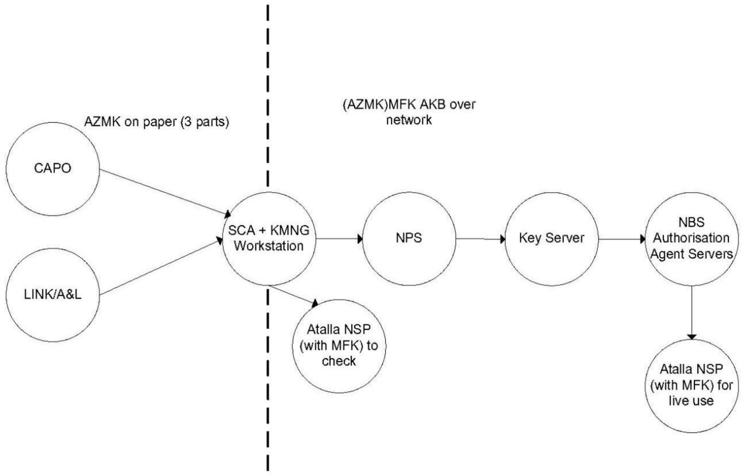
AZMK on paper (3 parts)
(AZMK)MFK AKB over network
CAPO
LINK/A&L
SCA + KMNG Workstation
NPS
Key Server
NBS Authorisation Agent Servers
Atalla NSP (with MFK) to check
Atalla NSP (with MFK) for live use

Figure 4-1. Key Management Routes: AZMK Domains

4.2.2 PAN

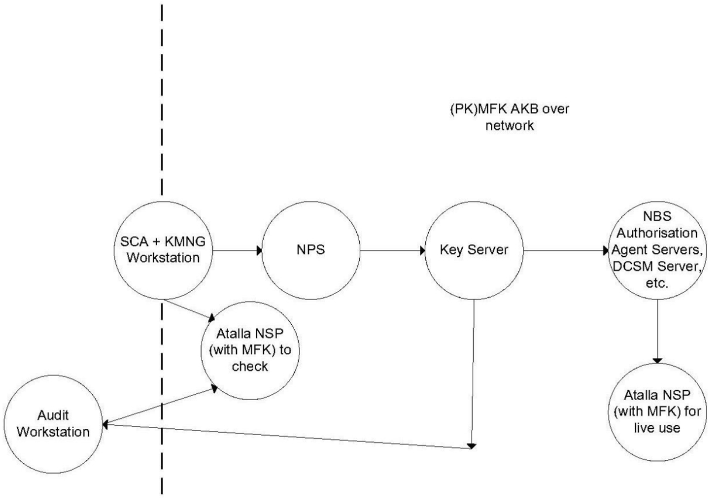
(PK)MFK AKB over network
SCA + KMNG Workstation
NPS
Key Server
NBS Authorisation Agent Servers, DCSM Server, etc.
Atalla NSP (with MFK) to check
Audit Workstation
Atalla NSP (with MFK) for live use

Figure 4-2. Key Management Routes: PAN

4.2.3 TRACK2

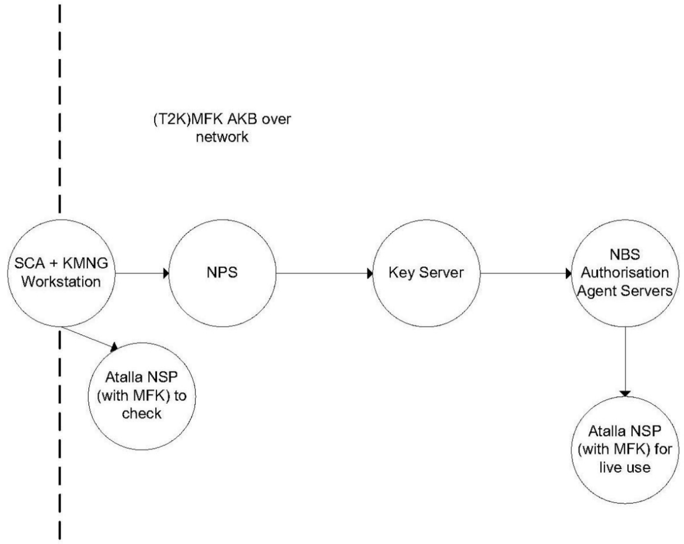
(T2K)MFK AKB over network
SCA + KMNG Workstation
NPS
Key Server
NBS Authorisation Agent Servers
Atalla NSP (with MFK) to check
Atalla NSP (with MFK) for live use

Figure 4-3. Key Management Routes: TRACK2

4.2.4 PAN_HASH

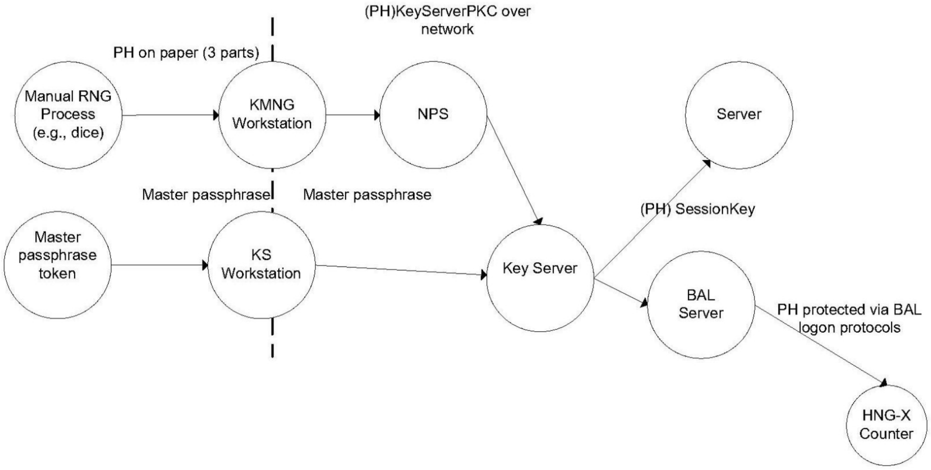

Figure 4-4. Key Management Routes: PAN_HASH (Server and Counter)

5 DEPLOYMENT

5.1 Overview

To show the system in context, Figure 5-1 shows the platforms that interact directly with the Key Management System subsystems described in this document.

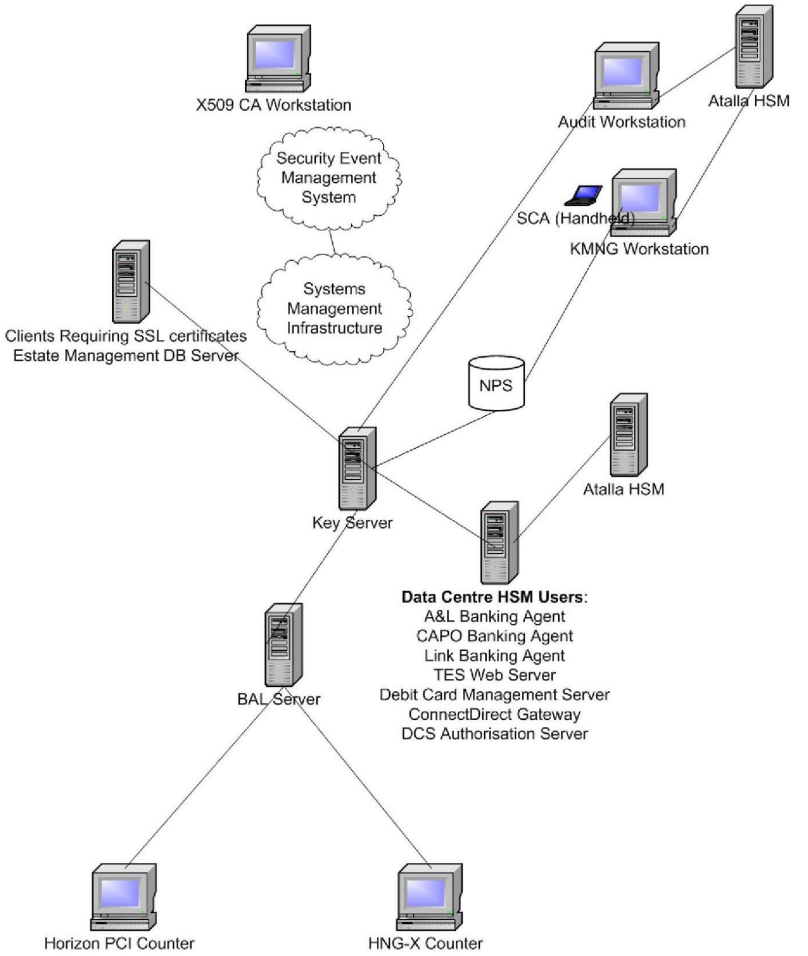

Figure 5-1. Crypto Landscape

Figure 5-2 shows the mapping of packages to platforms for the packages described in this document and the key service client package that supports some of them (the design of the Key Service is described in [DES/SEC/HLD/0003]).

	EST[1]	AUW	KSN	CDG	DCM	TWS	NBX	DEA	CNH	CNT
NB Crypto API							Y			
PCI Crypto API		Y		Y	Y	Y	Y	Y		
HSM Access Service		Y	Note 1	Y	Y	Y	Y	Y		
PAN Hash API		Y		Y	Y	Y			Note 2	Note 3
Application Key Retrieval API	Y									

Note 1 = KMNG workstation communicates with local HSM (e.g. BRA01) for key encryption and communicates with remote HSMs (IRE and e.g. LEW02) in order to check the HSM's status but neither communication involves the HSM Access Service.

Note 2 = Special Version of PAN Hash API for NT4 Horizon counter.

Note 3 = PAN Hash API developed in Java as an integral part of the PCI counter development.

Figure 5-2. Package/Platform Matrix

5.2 HSM Deployment

HSMs are to be provisioned for the data centres and support sites as shown in Figure 5-3 (see TST/GEN/SPE/0024 for further details).

	HPHSM	SPHSM	SCA	Notes
Development		2 (will reduce to 1 when all A8150 are end of life)	1	
Test: Other		2	1	
Live: BRA01		1	1	Used by Audit W/S and KMNG W/S
Live: Lewes DR		1	1	Used by Audit W/S and KMNG W/S
Test: IRE19	2 (1 on DR)			Covers full business volumes with 1 borrowed from live (LST has 2 available, 1 of which is moved to Live on DR)
Live: IRE11	3			Business Volumes + 1
Live DR: IRE19	2 (3 on DR)			Business Volumes (+ 1 on DR when an additional HSM is made available from LST)

Figure 5-3. HSM Deployment

[1] The 3 letter acronyms are the platform names for the services running on them as follows: EST = Estate Management Database Server, AUW = Audit Workstation, KSN = KMNG Workstation, CDG = ConnectDirect Gateway, DCM = Debit Card Management Server, TWS = TES Web Server, NBX = NAA, NAC, & NAL the Network Banking Authorisation Servers, DEA = DCS and ETS authorisation servers, CNH = Horizon Counter and CNT = HNG-X counter.

The HSMs offer two or three TCP/IP services. The default port numbers for these should be changed as shown in the following table to comply with the standards for allocating private port numbers:

Service	Default Port Number (DO NOT USE!)	HNG-X Port Number
Status Port	5000	55000
Command/Response	7000	57000
Management (Ax160 and newer model HSMs)	7005	57005

5.3 Implementation Notes

The interfaces for NB Crypto APIs, PCI Crypto APIs and the PAN Hash API are described in DES/SEC/IFS/0001 'HNG-X Cryptographic Applications Programming Interface Specification'.

5.3.1 NB and PCI Crypto APIs

The NB Crypto APIs are implemented as described in DEV/APP/LLD/0125 'HNG-X Network Banking Cryptography API LLD'.

The PCI Crypto APIs are implemented as described in DEV/APP/LLD/0120 'HNG-X PAN Crypto API LLD'.

These APIs are packaged as a Windows DLLs and both sets of APIs:

- replace the infrastructure that obtains keys from Riposte with call to the HNG-X Key Store Service that obtains the keys from the NPS database or filestore
- use the new HSM access service to access the networked HSMs, rather than use the local Atalla card access service to access platform resident Atalla cards.

The NB Crypto API is adapted from the Horizon NBX Crypto API to provide session base encryption translation functionality. The PCI Crypto API includes functions for PAN and Track 2 encryption.

5.3.2 HSM Access Service

This is a functional replacement for the local Atalla card access service used in Horizon. It has no external interface: applications access it indirectly via the NB Crypto API and PCI Crypto API. It is a Windows Service and is implemented in C++.

The HSM Access Service is implemented as described in DEV/APP/LLD/0131 'HSM Access Service LLD'.

5.3.3 PAN Hash API

5.3.3.1 Windows

The Windows PAN Hash API is implemented as described in DEV/APP/LLD/0148 'HNG-X KM: PAN Hash API for PCI Compliant Data Centre LLD'.

This is a new facility for PCI compliance. It is callable from C, VB, Java and PL-SQL on a range of platforms, all running Windows. It is packaged as a DLL offering a C interface and is implemented in C++. The PAN Hash Seed Function of section 3.2.3 is delivered as part of this package. There is a variant that runs on Horizon counters. It is written in C++.

5.3.3.2 Java

As described in section 3.2.4, a Java implementation of the PAN Hash API is deployed on the HNG-X counters.

6 SYSTEM QUALITIES

6.1 Resilience

6.1.1 HSM Crypto Services

The resilience requirements for the HSM Crypto Services derive from the resilience requirements of the applications they support, see [ARC/APP/ARC/0005], [ARC/APP/ARC/0007]. See section 3.1.1 for a discussion of the resilience characteristics of the HSM connection model. See [DES/SEC/HLD/0003] for information on the resilience of the Key Service on which the HSM Crypto Services depend for provision of keys.

6.1.2 PAN Hash Services

The resilience requirements for the PAN Hash Services derive from the resilience requirements of the applications they support, see [ARC/APP/ARC/0003], [ARC/APP/ARC/0005]. See [DES/SEC/HLD/0003] for information on the resilience of the Key Service on which the PAN Hash Services depend for provision of the PAN Hash Seed.

6.2 Performance and Scalability

6.2.1 HSM Usage in Network Banking and Retail

There is no requirement to scale for increasing business volumes, but the design of this document allows for some scaling for increased flexibility, e.g., if new requirements for HSM-based cryptography arise.

The volumetric calculations for the online use of the A10150 HSMs under peak loading are given in the following table showing that 2 HSMs are sufficient to meet peak **online** business volumes.

	Loading	**CAPO**	**LINK**	**A&L**	**Retail**	
PEAK PER SECOND		250	38	19	34	
SPT (Multisession)	40%	0.0127	0.0127	0.0127	0.0029	
SPT (Multisession)	60%	0.0084	0.0084	0.0084	0.0020	
SPT (Multisession)	80%	0.0063	0.0063	0.0063	0.0015	
SPT (Multisession)	100%	0.0051	0.0051	0.0051	0.0012	
						HSM Requirement
SPS (Multisession)	40%	3.17	0.48	0.24	0.10	**3.99**
SPS (Multisession)	60%	2.11	0.32	0.16	0.07	**2.66**
SPS (Multisession)	80%	1.58	0.24	0.12	0.05	**1.99**
SPS (Multisession)	100%	1.27	0.19	0.10	0.04	**1.60**

Legend

SPT = Seconds per transaction

SPS = Seconds per second, i.e., required concurrency

The volumetric calculations for the **offline** use of the A10150 HSMs for the NBX batch file processing (REC and LREC Bulk File Agents running on the CDG platform) are shown in the following table:

	#Records	Plus 50%	Decryption Time (2)	Decryption Time (2)	Decryption Time (2)
			1 HSM	3 HSMs	4 HSMs
A&L	80,418	120,627	00:03:35	00:01:12	00:00:54
CAPO	1,406,845	2,110,268	01:02:41	00:20:54	00:15:40
Link	152,169	228,254	00:06:46	00:02:15	00:01:42
Total	**1,639,432**	**2,459,148**	**01:13:02**	**00:24:21**	**00:18:15**

HSM Decrypts/sec (1)	561	(= 66% * 850)

Notes

(1) Based on figures from Atalla of 850 decrypts/second for multiple sessions at 66% loading.

(2) Assumes worst case of 1 PAN block decryption per record

DES/APP/HLD/0052 'NBS Bulk File Agents HLD' section 9.6 'Performance' supplies the maximum daily volumes (including number of records) of the REC and LREC files.

6.2.2 HSM Usage for Audit and Key Management

The A8150 HSMs are rated at 66 PIN block translations per second and the performance on the key management and decryption commands used on the KMNG and Audit Workstations (respectively) will be similar. This will be more than adequate for the very low volume interactive usage pattern of the HSMs on these platforms.

6.3 Security

See [ARC/SEC/ARC/0003] for a statement of the non-functional requirements relating to security and a cross-reference of those requirements against the ISO27001 control objectives. In particular, [ARC/SEC/ARC/0003] specifies the requirements for firewalls and other network security requirements.

Security Event Management conformant with [ARC/SEC/ARC/0003] is to be obtained via event logging following the policies of [RS/REQ/007]. The Systems Management Infrastructure monitors event logs and forwards security-relevant events to the Security Event Management System.

It is expected that the PAN hash seed value (PH) will last for the lifetime of the HNG-X system. In the event of it being compromised, replacing PH will involve updating applications software that does queries based on hashed PANs.

7 TESTING

Specification of test strategies for each component is to be defined in the relevant detailed design documents. Some general suggestions and constraints follow:

- A test schedule for each protection domain may be derived from the data flows shown in section 4.2 above.
- Test rigs to simulate application software will be required to allow testing of the clients.
- To test the key change protocols extensive accelerated life-cycle testing will be required during integration testing.
- Testing must not be carried out using live key material. Conversely, test key material should not be used in the live system. Procedures are required to enforce this separation at all stages of the development life cycle.
- It is a design constraint that adequate testing at all levels should be possible without using live key material (including secrets such as the PAN Hash Seed value).

8 SYSTEMS MANAGEMENT

With the exception of the Atalla HSM, systems management of the platforms mentioned in this design is outside the scope of this document.

The Atalla HSMs offer a status and error logging capability allowing messages to be monitored remotely.There is also a facility on early HSMs to view simple status messages on a console attached to the built in VGA port. On later HSM generations (Ax160s and beyond) the VGA port has been removed. On these later models the serial port will be configured to output the equivalent console messages (When configured this way the serial port can not be used for direct attachment of the SCA as a result the SCA can only be directly attached via USB) No other systems management facilities are provided.

The software infrastructure will implement event management to support the forwarding of security-relevant events by Tivoli to the Security Event Management Service as described in [ARC/SEC/ARC/0003].

9 DEPENDENCIES

The design is dependent on:

- the key management services described in [DES/SEC/HLD/0003]
- delivery of the PAN Hash Seed (PH) to the counter PCs via the Branch Access Layer logon protocol
- the TESQA platform running Windows rather than Solaris or Linux
- the KMNG workstation being able to read AKB diskettes in the format used by the Horizon KMA workstation

10 ASSUMPTIONS AND RISKS

10.1 Assumptions

Ref	Description
A1	The performance information supplied by Atalla is assumed to be representative.
A2	Following Horizon policies for event reporting will satisfy the security event management requirements.
A3	Appropriate event reporting mechanisms will be available on the HNG-X counter and on Red Hat Linux platforms to satisfy the security event management requirements.
A4	There will be a red LAN segment shared by the KMNG Workstation and the Audit Workstations giving them the necessary access to HSMs and the Key Service Server.

10.2 Risks

Ref	Description
R1	Failure to satisfy the dependencies listed in section 9.
R2	Errors in the assumptions listed in section 10.

11 MIGRATION

The HSM Crypto Services and PAN Hash Services are new functionality for the HNG-X platforms that use them (see section 2.1). The networked HSMs are new appliances for HNG-X and completely replace the Horizon Attalla Card HSMs. Reconciliation file processing is the first activity in the migration process which requires the new HSMs and the infrastructure that supports them.

Data Centre migration of key management is described in DES/SEC/HLD/0010 'Key Management Migration High Level Design'.

11.1 HSM Crypto Services

The HSM Crypto Services is effectively new infrastructure for HNG-X. Some keys will need to be transferred from the old system to the new. To facilitate this, the MFK (and PMFK) keys are to be carried over into the networked Atalla HSMs, so that the existing AKB files will work in the new system.

11.2 PAN Hash Services

For PCI-compliance, the Horizon counters will need access to the PAN Hash seed value (PH). This is to be supplied encrypted under the GDK Layer 7 key (managed by the Horizon KMA). The GDK will be changed before migration begins. A utility on the Offline Key Generation workstation is to be used to combine the three parts of PH and encrypt the result under GDK. (PH)GDK will then be distributed via the software distribution processes.

The PCI-compliant Horizon counter uses a variant of the PAN Hash API that offers the same calling interface but obtains (PH)GDK from filestore and decrypts it using Layer 7 and then holds it in global memory. (PH) GDK is delivered to the counters by the software distribution process as shown in Figure 11-1

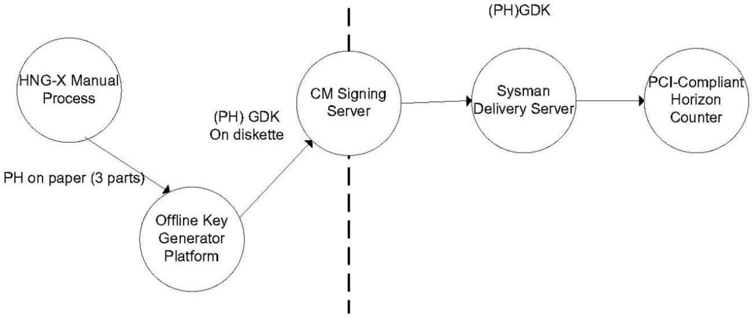

Figure 11-1. Key Management Routes: PAN_HASH (Horizon Counter)