POL00396892

Document Title:	Security Testing Inputs for PCI Audit.
Document Type:	Report (REP).
Release:	TST/GEN/REP/0011.
Abstract:	Collation of security testing inputs for PCI audit of Horizon and Horizon online.
Document Status:	DRAFT.
Author & Dept:	David Cohen.
Internal Distribution:	Dave King, Paul Halliden, Connie Penn, John Halfacre, Andrew Thompson, Lee Farmer, Becky Eynon, Brian Pinder.
External Distribution:	None.

Approval Authorities:

Name	Role	Signature	Date
Sue Lowther			

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

(*) = Reviewers that returned comments

POL00396892

0 Document Control

0.1 Table of Contents

[TOC \O "1-3" \H \Z \T "POA APPENDIX HEADING 1,1,POA APPENDIX HEADING 2,2"]

POL00396892

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	01 Aug 2008	Initial draft.	

0.3 Review Details

Review Comments by :	(date by which comments should be returned)
Review Comments to :	(authors name) & [HYPERLINK "mailto:PostOfficeAccountDocumentManagement GRO

Mandatory Review	
Role	Name
	Dave King
	Paul Halliden
	Connie Penn
	Andrew Thompson
	Jim Sweeting
	Becky Eynon
	Brian Pinder
	John Halfacre
	Nigel Taylor
Optional Review	
Role	Name
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001	N/A	N/A	Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
PGM/DCM/TEM/0002	N/A	N/A	Fujitsu Services Post Office Account HNG-X Landscape Document Template	Dimensions

POL00396892

Reference	Version	Date	Title	Source
ARC/SEC/ARC0001	2.0	18 June 2007	[TITLE * MERGEFORMAT]	Dimensions
ARC/SEC/ARC0003	1.4	11 June 2008	HNG-X Technical Security Architecture	Dimensions
DES/NET/HLD/0007	0.1	18 Jan 2007	[TITLE * MERGEFORMAT]	Dimensions
High Level Test Plan	0.3	19 August 2008	[TITLE * MERGEFORMAT]	Dimensions
CCN1202	7.0	20 June 2007	Handling PCI Sensitive Authentication Data and Cardholder Data	Dimensions
CCN1231	1.0	3 July 2008		Dimensions

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

0.5 Abbreviations

Abbreviation	Definition

0.6 Glossary

Term	Definition
CCN	Change Control Note
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard

0.7 Changes Expected

Changes

0.8 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.

POL00396892

0.9 Copyright

POL00396892

1 Introduction

1.1 Purpose of Document

This document has been drafted to provide clarification requested by Connie Penn on a number of testing issues related to HNG-X PCI compliance.

1.2 Introduction

The following is drawn from a paper on the scope of PCI work for POL produced by Rebecca Eynon, Fujitsu Services:

RMGA are not implementing a solution to provide PCI compliance – instead putting in place a number of measures as explicitly agreed with POL. These measures address individual aspects of the PCI requirements from VISA and Mastercard.

The main changes are:

- CCN 1202: Handling of Track 2 (to avoid it being stored even when encrypted, and PAN) and network protocol (encryption algorithms use of SSL etc.)
- CCN 1231: File integrity monitoring

These changes are made to lots of systems within the data centres, which become capable of handling both old and new style transactions. The changes also use some of the new HNG-X components such as BAL and HSM (Atalla hardware security modules).

However the actual business change is only achieved as the counter software update is applied to the estate. This is the main reason for the retro-fitting of the changes to the Horizon branch estate.

Due to network design (routing from Horizon counters to the BAL) It is only after weekend D that we can actually start to roll out the Horizon branch changes. Hence we achieve the PCI required protection on Track 2 and Card holder data (PAN etc.) gradually and can only claim conformance when we have completed the Horizon counter roll-out.

1.2.1 CCN 1202

CCN 1202 describes Fujitsu's proposed response to CR-957. This CR requested certain modifications to the HNG-X system, namely;

1. The Solution Architecture and proposal for HNG-X is updated to ensure that PCI "Sensitive Authentication Data" (including PIN blocks) is not stored in any file or database including log, audit or diagnostic files after a transaction has been authorised even if the data is encrypted. Such data must also be deleted after use. Exceptionally, any data element required to be submitted in the settlement or reconciliation files may be retained for a configurable number of days after the file is successfully submitted. For the avoidance of doubt, it can be assumed that reference data will not be set to collect Track 2 data from payment cards for the loyalty card program. Apply from the start of the pilot phase.

POL00396892

2. The Solution Architecture and proposal for HNG-X is updated to ensure that PCI "Sensitive Cardholder Data" (i.e. PAN) is rendered unreadable anywhere it is stored (including data on portable media, backup media, and in logs) by using any of the approaches approved by PCI. For the avoidance of doubt, this requirement does not apply to the notification of scanned account numbers passed via AP to POCA to record the issue of cards. After the final Horizon Counter has moved to the HNG X application.

3. The Solution Architecture and proposal for HNG-X is updated to ensure that all PCI Sensitive Authentication Data and PCI Sensitive Cardholder Data is encrypted using approved algorithms and encryption protocols whilst in transit over any public network unless specifically agreed in writing by the client. [Approved algorithms are 128-bit 3DES (as per ANSI X9.52) and 256-bit AES (FIPS 197). Approved encryption protocols are SSL v3 / TLS, SSH, IPSec, and PPTP v2]. Apply from the start of the pilot phase.

4. The Fujitsu CCD "Service Description for the Security Management Service" (Ref: CS/SER/016) is updated to cover support for the annual Level 1 PCI audit of HNG-X. Should be assumed to occur within a year of HNG-X going into Pilot.

The Horizon PCI Counter update is dependant on the availability of the Branch Access Layer and the Branch Database. It is NOT dependant on the Data Centre migration; this is simply a consequence of the current plan which requires the BAL and the Branch Database to be implemented into the new Data Centres.

PCI Compliance will NOT be achieved when the Data Centre migration has happened. As stated above, PCI compliant transactions are produced as a result of;

a) Horizon PCI Counter update or,

b) HNG-X Application rollout.

Therefore, until the entire estate has been updated, (to either one of the Horizon PCI Counter or the HNG-X Counter), Track 2 data will still be created and sent by the Counters, and will be processed and stored by the core Data Centre systems.

1.2.2 CCN 1231

This change only applies to HNG-X and is in support of POL's business requirement to conform to the PCI Data Security Standard. It is issued in response to POL CR 01119 which requests;

1. Identify File Integrity Monitoring software to implement in the cardholder environment within HNGX.

2. Identify the boundaries of the cardholder environment within HNGX.

3. Propose costs for implementing and supporting File Integrity Monitoring within HNGX for agreement by POL.

4. Propose acceptance criteria for implementing File Integrity Monitoring within HNGX for agreement by POL.

The agreed scope of the requirement is to implement File Integrity Monitoring software into the HNG-X Data Centre environment to protect the Cardholder Environment. (This is defined in the attached Solution Outline).

To meet the requirements of CR01119, it is proposed that the Tripwire File Integrity Monitoring product be installed on all systems within the Cardholder Environment. This software works by creating a signature for each file it is monitoring, storing this in a secured location and re-evaluating the files on a periodic basis. The file signature is compared to the original on each re-evaluation and an event is raised if there are any changes.

In Release One of HNG-X, this is an installation of;

- The file integrity monitoring software
- The appropriate template for that operating system

POL00396892

- Specific changes based on the Platform Type

Compliance Reports can be produced as required to show that files have not been changed since there installation or last approved update.

A process will need to be developed such that when a new release of software is applied to a monitored system, the events raised are expected and can be dealt with correctly.

Documentation will be provided from Jim Sweeting to show that the HNG-X architecture meets the requirements of these CCNs.

POL00396892

2 Royal Mail group policies S17/S18 compliance

2.1 S17 - Security Architecture

The Royal Mail Group Security Architecture provides systems and application developers with a methodology for selecting technical security controls that are commensurate with the criticality of the system or application, or with the sensitivity of the information processed by the system or application.

The architecture defines a methodology for deploying appropriate levels of security and technical solutions for information systems. It provides a common approach that meets the needs of all parties in the field of Access Control and data security provides a flexible methodology to meet the Access Control and Data Security requirements of Royal Mail during a period of organisational and architectural transition.

It also identifies a set of future technologies that can be addressed in the longer term.

C:\Documents and Settings\david.cohen

S17 Policy Document

C:\Documents and Settings\david.cohen

Architecture/HLTP/HLD mapping matrix

2.2 S18 - IT Security Design & Testing Policy

The IT Security Design & Testing Policy defines the controls required to reduce the risks associated with the development of IT Systems and Applications.

The policy requires that all systems and applications under development must undergo formal testing before entering production to ensure that they perform to the required specification.

This requirement is being met by:

a) Testing against DOORS requirements.
b) The Security HLTP.
c) Specific tests loaded into JQC.

POL00396892

C:\Documents and Settings\david.cohen

S18 Policy Document

Jim Sweeting has confirmed that the security design of HNG-X as documented in ARC/SEC/ARC/0003 meets all aspects of policies S17 and S18, with the exception of code reviews (see section 5 for more details).

Reviews will be conducted to ensure that all policy requirements continue to be met.

2.3 PCI requirements v HLTP v Security Architecture

The following matrix maps the high level PCI requirements to the High Level Test Plan and Security Architecture document ARCSECSARC0003 (see section 10 for document).

C:\Documents and Settings\david.cohen

PCI v HLTP v ARC/SEC/ARC/0003

POL00396892

3 CCN 1202

An indication of which tests are being carried out to test that the development meets the requirements set out in CCN 1202 has been requested.

3.1 Definition of CCN 1202

CCN1202 exists to amend the agreement for the introduction of new and/or modified applications and operational services.

Specific requirements are as per the embedded spreadsheet:

C:\Documents and Settings\david.cohen

CCN 1202 requirements

3.2 POL Responsibilities

The following POL responsibilities are defined in CCN 1202:

(a) Provision of a PCI external assessment of the proposed design early in the development cycle and raising Change Requests for any further changes that it becomes apparent are required as a result of that assessment;

(b) Provision of support from Streamline during HNG-X testing;

(c) Providing confirmation that the existing HNG-X Streamline accreditation testing will include all necessary Streamline accreditation testing for PCI changes;

(d) Confirming that Version 20 of the Streamline document entitled "For the delivery of transaction data via DIRECT COMMUNICATION" dated December 2005 constitutes the full documentation from Streamline of the revised Payment and EMIS file specifications and providing a formal copy of this document to Fujitsu RMGA Document Management;

(e) Providing confirmation from Streamline that the batch interface to Streamline will continue as at present based on MPPE / RC4;

(f) Providing confirmation that LINK and CAPO networks are PCI compliant;

(g) Providing confirmation that no changes are required to the LINK interface specification;

(h) Implementing the roll out of the updates to the Client workstations for TESQA users;

(i) Providing confirmation of the list of authorised TESQA users prior to the Data Centre move and distribute their new Authentication tokens (note that this will be implemented in release 2);

POL00396892

(j) Confirming that Streamline will makes changes to their systems that enable Fujitsu Services to introduce the change to the new payment file format at the point of the move to the new Data Centres.

These responsibilities are addressed in the ARC/SEC/ARC001 security architecture document; Jim Sweeting has confirmed that these requirements have all been met in the security architecture.

Reviews will be conducted to ensure that all policy requirements continue to be met.

POL00396892

4 Vulnerability testing in both datacentres

A high level security test plan has been drafted and circulated for formal review (document reference TSTGENHTP0004).

Brian Pinder has overall responsibility for vulnerability and penetration testing in both data centres, a low level test plan is being created and implemented.

Mark Havard is available for a two week period from 8th September 2008 and will assist in the creation of the low level test plan.

David Cohen and Nigel Taylor are permanent security testing resources and will assist with security testing as directed.

Brian Pinder has confirmed that initial vulnerability/penetration testing will be conducted in the first instance by Fujitsu prior to formal external testing by an approved scanning vendor (ASV) in Q1 2009 prior to go live.

POL00396892

5 Custom code review plans

At present it is believed that as there is no external facing web code there will be no need for any code review for PCI compliance purposes.

It is not clear whether any server or client side Java or JavaScript will be subject to review for PCI compliance, clarification is requested if this is in fact a requirement.

POL00396892

6 Penetration testing

FJS will provide resources independent from the HNG-X project to plan and carry out vulnerability assessments and penetration tests. A draft Vulnerability and Penetration Test plan will be produced in September 2008.

Vulnerability and Penetration testing will subsequently be added to the overall HNG-X Programme Plan.

The interface between the Security Testing HLTP and the penetration test/vulnerability assessment test plans will be considered to ensure that no duplication of work occurs and to ensure that sample testing of relevant tests in the HLTP exists.

Test scripts will be entered in Joint Quality Centre, with detailed test outputs and documentation held in Dimensions to allow for audit and repeatability of test results.

It has been established that PCI Penetration testing is a very small subset of the overall penetration testing to be carried out, but penetration testing is not something the joint test team will be doing as this is being handled by Fujitsu Services under the direction of Brian Pinder.

POL00396892

7 Firewall testing

Testing of both the firewalls themselves and the subnets they protect will be covered by penetration testing, firewall testing, and firewall configuration/rulebase reviews.

Jim Sweeting has confirmed that a milestone plan which shows that tests are performed at the various stages of migration from the test environment(s) to the fully operational state will be produced by the customer service security team.

Brian Pinder has overall responsibility for testing in the data centres, all testing will be documented.

POL00396892

8 Segmentation between test and production environments.

The network architecture stipulates that the SANs use separate disks for test and production systems to ensure that drive segmentation exists not only logically but also physically.

Network segmentation has been built in to the security architecture as per the ARC/SEC/ARC/0003 security architecture and SAN HLD documents (document reference DES/NET/HLD/0007).

A review of segmentation between test and production environments will take place, this testing will be conducted by Fujitsu and will commence on 19th January 2009. A three week testing window has been scheduled.

During this period a network review and data cleanup will be undertaken before the BC weekend migration (the weekend of the migration of the batch and online systems to the IRE11 and IRE19 data centres).

An external penetration test that includes tests in this scope has been scheduled for 16-23 March 2009. These tests will be conducted in the first instance by Fujitsu.

Connie Penn is to advise of any specific concerns identified to data with data leakage.

Jim Sweeting is to verify how segmentation can be verified and/or demonstrated.

POL00396892

9 Personnel

Assurance has been requested that any external company/consultant/testers used to test the cardholder environment have PCI DSS knowledge and experience.

PCI ASV and QSA contractors will obviously have the relevant PCI experience and knowledge.

It has been established that most joint test team testers will need a thirty minute intranet based CBT course.

It is expected that security specialists will need to complete more in-depth training.

POL00396892

10 External documents and/or references

10.1 High Level Test Plan Document

C:\Documents and Settings\david.cohen

High Level Test Plan

10.2 ARC/SEC/ARC/0003 HNG-X Technical Security Architecture Document

C:\Documents and Settings\david.cohen

ARC/SEC/ARC/0003

10.3 ARC/SEC/ARC/0001

C:\Documents and Settings\david.cohen

ARC/SEC/ARC/0001

10.4 CCN 1202 Documents

CCN1202	CCN TITLE: Handling PCI Sensitive Authentication Data and Cardholder Data
CCN1202att1	Attachment 1 to CCN 1202
CCN1202att2	Attachment 2 to CCN 1202
CCN1202att3	Attachment 3 to CCN 1202
CCN1202att4	Attachment 4 to CCN 1202

POL00396892

10.5 CCN 1231 Documents

CCN1231	CCN TITLE: Introduction of File Integrity Monitoring for HNG-X
CCN1232 Att1	Attachment 1 to CCN1231

10.6 SAN High Level Design Document

DES/NET/HLD/0007	SAN High Level Design

POL00396892

11 HNG-X High Level Test Plan

11.1 Current version

The current version of the High Level Test Plan is version 0.3, see section 10 for document.

POL00396892