FUJ00156114

Document Title: Audit Trail Sanitisation for PCI

Document Reference: REQCUSFSR0001

Document Type: Proposal

Release: N/A

Abstract:

Document Status: DRAFT

Author & Dept: Jim Sweeting

Internal Distribution:

External Distribution: N/A

Approval Authorities:

Name	Role	Signature	Date

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

FUJ00156114

FUJ00156114

0 Document Control

0.1 Table of Contents

FUJ00156114

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	13/05/2009	Initial Draft	
0.2	02/07/2009	Revised version	
0.3	12/10/2009	Final Draft	

0.3 Review Details

Review Comments by :	N/A
Review Comments to :	N/A
Mandatory Review	
Role	Name
N/A	N/A
Optional Review	
Role	Name
N/A	N/A
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	3.0	16-May-08	RMGA HNG-X Generic Master Document Template	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

FUJ00156114

0.6 Glossary

Term	Definition
PAN	Primary Account Number – The 16 to 19 digit number embossed on a bank card that identifies the cardholders account.
PCI	Payment Card Industry
DSS	Data Security Standard

0.7 Changes Expected

Changes
None.

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.

0.9 Copyright

FUJ00156114

1 Introduction

As a consequence of the introduction of the PCI Data Security Standard (PCI DSS) Post Office have a requirement to sanitise the existing legacy audit trail data. This will include all data stored in the audit system from the beginning until the last Horizon non-PCI transaction is generated.

Sanitisation in this sense means the removal or obfuscation of the following in the Riposte messages held by the audit system;

Data	Treatment
Encrypted Track 2 data	Removed or Overwritten
Encrypted PIN Block	Removed or Overwritten
PAN	Obfuscated and Encrypted

This paper is the initial solution overview and scoping document for the work.

FUJ00156114

2 Audit System Overview

The Horizon audit system currently (May 2009) contains approximately 80TB of Data. This data is stored on two Centera disk arrays in separate Data Centres. The audit system collects data from platforms as audit trails and tracks, seals them using a hashing algorithm and writes them to each Centera in turn. The data as to the hash value and the location of the data in each Centera is recorded in a database on the Audit Server itself. This approach results in the data on each Centera being the same, but it is not a mirror image. (ie. The same records can be stored in different locations on different Centeras).

Individual audit files written to the Centeras vary in size up to approximately 60MB.

The Prosecution Support Service uses an audit query application to support Post Office with investigations.

The Audit system will operate in a similar fashion for HNG-X and a detailed overview of the audit system is contained within the ARC/SVS/ARC/0001 Support Services Architecture document. However, for HNG-X the transaction data collected by the audit system, are already sanitised in accordance with PCI requirements. This is achieved through the use of data encryption, overwriting and the use of a hashing algorithm.

Where necessary, the encrypted PANs can be decrypted on an individual basis (there is no bulk decryption facility available to users) to validate the number.

FUJ00156114

3 Proposed Sanitisation Solution

There are a number of possible alternatives for dealing with the legacy audit data. It has been decided by Post Office that deleting the legacy data is not a practical option and is therefore out of scope for this paper.

The solution outlined below will need to be investigated further as part of the design exercise. A final recommendation will then be produced, agreed with Post Office and the solution developed.

An example of an audit trail record is;


```
<Message:<GroupId:901777><Id:1><Num:69622><Date:14-May-2008><Time:07:43:32><User:MIG
R01><Expiry:34><Application:DCA><Data:<RACMess:<Id:<HTxnNum:44-901777-1-69621-3><Lcl
Dte:20080514><LclTme:084324><TransNum:010031><BdC:0>><Txn:<TranType:71><PAN:40000000
00000002><ReqAmt:69><CurrCd:GBP><EtyMde:3><IssSchId:0000000055><LangCd:1><ClientId:2
4283><RtngGwy:24239><RsnOnLnCd:09>><ICCData:<82:5C00><9F36:0002><9F26:F628E33AB83913
05><9F06:A0000000031010><9F27:80><9F34:410302><9F10:06050A03A40000><9F33:E0B8C8><9F3
5:22><95:4080008000><9F37:434E03FF><9F1A:0826><5F2A:0826><9C:00><9A:080514><9F08:008
3><9F09:0084><5F34:01><9F0F:F070FCD870><9F39:32>><Sec:<Encrypt:AAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA>
>><DSig:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA><SigType:RAG><Ctrl:<Msg
Type:R1><AgtHash:0><AgtTmOut:18000><FnclTxn:1><Omode:SC>><Recov:<ProductNo:9363><Con
tainer:MJC>><MsgVersion:<Major:4><Minor:NBRequestReply 1.0>>><CRC:8B64077D>>
```


3.1 Requirements

A thorough requirements exercise will be required as part of the design work. The following is an initial list.

1. Development of sanitisation application code will be under securely controlled conditions.
2. The application will be compiled and digitally signed.
3. Detailed record of changes made by the sanitisation program.
4. Key management.
5. Sanitised Horizon audit records will be accessible from HNG-X audit workstations in the same way as HNG-X audit trail records.
6. Existing HNG-X code will be reused as far as practical.
7. The original Transaction Record length will remain the same.
8. Obfuscation of all <Encrypt:....> fields by overwriting.
9. Obfuscation of all <DSig:....> elements by overwriting.
10. Obfuscation of all <PIN:.....> fields by overwriting.
11. Encryption of all PANs and the addition of an <EPAN:...> field to the transaction record.
12. Obfuscation of all but the first 6 and last 4 characters of the <PAN:..> field.

3.2 Per Transaction Sanitisation

This section is an outline of how the sanitisation process will actually work. It will be confirmed as part of the design process. This process will be followed for every transaction record in an Audit Track. A 'dummy' run will execute initially to detect any problems with the proposed sanitisation. Assuming none are found, the sanitisation will proceed.

1. Validate the CRC check for each transaction message prior to sanitising it.

FUJ00156114

2. Strip all data from <DSig:...>, <PAN:..>, <encrypt:..> and <PIN:..> tags for every relevant transaction record in the file and create a SHA-1 hash value over the remaining data. Record the hash to the sanitisation audit trail. This will be verified in step 4. below to prove that no other data have been changed.
3. Overwrite all data from <DSig:...>, <encrypt:..> and <PIN:..> tags for every transaction record in the file. Replace data with an equivalent number of "X" characters (for example), to maintain the original record length.
   - e.g. <encrypt:g2DHa32nBSDkNDkc> becomes <encrypt:XXXXXXXXXXXXXXXX>)
4. Strip all data from <DSig:...>, <PAN:..>, <encrypt:..> and <PIN:..> tags for every transaction record in the file and verify that the SHA-1 hash value is the same as 1. above. This indicates that nothing else has changed.
5. Encrypt the PAN using a dedicated key per calendar year. Store the encrypted PAN at the end of each transaction record as <EPAN:..>.
6. Using the HNG-X hashing code and PAN Hash Seed value, create a hashed PAN and replace the existing plaintext PAN.
7. For each sanitised file, create a digital signature over entire file. Store the Public Key inside the audit file so that the digital signature covers the Public key.
8. Write the sanitised file back to Centeras. The original file will be maintained on the Centera for a short period until the Audit retrieval process has verified that the newly sanitised file is accessible and usable.

FUJ00156114

4 Risks, Issues, Assumptions and Constraints

4.1 Risks

- The sanitised audit trail will not be admissible as evidence in criminal or civil proceedings. This risk will be mitigated by the design.
- Data loss may occur during the sanitisation process. This risk will be mitigated through the implementation of the 'dummy' run cycle.
- Unexpected data modification may occur during the sanitisation process. This risk will be mitigated through the implementation of the 'dummy' run cycle.

4.2 Issues

- None Identified

4.3 Assumptions

- Design of the solution will begin subject to resource availability and HNG-X programme timescales.
- Development of this solution will not start until HNG-X Weekends B/C and D have been completed. It is recommended that the sanitisation exercise does not begin until the completion of Horizon-Online Branch rollout.
- A full risk assessment will be completed as part of the design and development of this solution

4.4 Constraints

- Live audit data will be needed for component testing.

FUJ00156114

5 Design and Development

The following is a list of activities required to design, develop, test and implement the solution.

Governance and Policy		
General Governance		x days
Project Management		x days
Audit Trail		x days
Architecture		
General	Requirements Specification	x days
Infrastructure	Platforms	x days
	Network	x days
	Monitoring	x days
Application	Data Extraction	x days
	Data Validation	x days
	Data Sanitisation	x days
	Application Audit Trail	x days
	Query Clients	x days
	Key Management	x days
Design		
Infrastructure		x days
Systems Mgmt & Scheduling		x days
Application		x days
Key Management		x days
Sanitisation Application Audit Trail		x days
Functional Test Design		x days
Non-Functional Test Design		x days
Development		
Infrastructure		x days
Application		x days
Key Management		x days

FUJ00156114

Sanitisation Application Audit Trail		x days
Testing		
Development Functional Testing		x days
Functional Testing		x days
Non-Functional Testing		x days
Development		
Infrastructure		x days
Application		x days
Key Management		x days
Sanitisation Application Audit Trail		x days

The outputs from this process will be;

- Requirements specification document
- Solution overview document
- High Level Design document
- Working prototype

Following agreement with Post Office as to the validity of the approach, a Low Level Design will be produced and the final solution will be developed.

FUJ00156114

6 Sanitisation Process

1. Using the existing key management process and key management infrastructure a set of unique cryptographic keys shall be created for encryption and digital signing purposes.

   1.1. A set of unique key pairs shall be created for each Calendar year or part thereof (running from January to December). This key pair will be used for providing digital signatures of the audit data for that year. The public key portion of this key pair shall be signed using the existing Certificate Authority.

   1.2. A set of unique encryption keys shall be created for each Calendar year or part thereof. Keys shall be created following best practice for the generation of cryptographic key material. (Creation of random material using Dice etc) {Specific reference needed here}

   1.3. A unique PAN Hash seed value shall be generated for each Calendar year or part thereof.

   1.4. Keys shall be loaded into the system following the guidance in the existing HNG-X key management process {Specific reference needed here}.

2. The sanitisation application shall use the existing key client software to obtain the keys required as each record or set of records is sanitised.

3. An audit trail will be kept of each sanitisation pass

4. A named individual will be responsible for initiating each sanitisation pass. This must not be the same individual responsible for generating and loading cryptographic keys (including the PAN Hash seed value).

   4.1. Once initiated, the application will run as a background process on the sanitisation server. This process and its output will be monitored by the Tivoli system to ensure that any errors are quickly identified and managed.

5. The sanitisation application will start with the most recent un-sanitised data and work backwards towards the oldest. This is to prevent a situation whereby the oldest data is sanitised first, then is immediately deleted from the Audit system as its retention data expires. (Testing is likely to use a sample of the oldest data)

6. Following completion of each sanitisation pass, the same {Should this be the same individual or someone different?} named individual will check the audit trail reports for errors.

7. It is recommended that the sanitisation exercise starts on completion of the Horizon-Online Application Branch rollout. Exact dates will be agreed on acceptance of the CT relating to CR01762