FUJ00117495

Requirements for KMS at CSR+

Scope

This paper addresses the requirements for the KMS to be implemented at CSR+. It takes account of the Treasury Review outcome whereby BPS has been withdrawn for the Pathway system. It also recognises that contractually, Pathway are only bound to develop and implement services contained within the POCL Agreement and that the BA Agreement and Authorities Agreement are nullified as a consequence of the Treasury Review. As such, any requirements relevant to the implementation of the KMS contained within the SFS have been reviewed to ensure that they are supporting POCL services.

It has been recognised that Pathway's ability to meet the forecast date of 17 April 2000 for CSR+ is critical to the business success of both Pathway and ICL and issues with regard to Pathway's ability to introduce KMS by that date are considered in a working paper entitled 'Option for de-risking 17th April 2000 with KMS'.

Overview

It should be noted from the outset that KMS is being developed to support the crypto solution implemented by Pathway to protect applications and data. The requirement as such is to have a secure method for the management of the crypto Keys employed, notably the ability to securely change these Keys every two years and the ability to deal with Key compromise. The management of Keys can be effected by automated and manual methods, each equally valid given that the correct controls, processes and procedures are in place. However, it is recognised in Pathway that with 20,000 remote outlets and a forecast of 300 potential AP client sites, that an automated key management service is the only cost effective mechanism for the management of crypto Keys.

'Crypto Keys' are the primary security enforcing component of any cryptographic solution. It is the 'Keys' that allow any given implementation to be unique and therefore allow the business to trust data protected by the solution. The strength and validity of the Keys are all important and as such, each Key has a shelf life before it can be reasonably expected that any sustained attack would eventually lead to the 'secret' being broken. Equally, it is important that such Keys are protected, both in situ and in transit, to ensure that any potential attacker does not get hold of the secret and thus the ability to extract or inject data or items from/into the system.

Requirements for KMS

To establish the requirement for the KMS, it is important to establish the requirement for cryptography within the Pathway solution. Where there is an instance of Private Keys at the remote end of the link (e.g. post office outlets, AP Client sites), the KMS will be required. This is due to the fact that each instance of a Private Key is unique (i.e. each Private Key held at a post office outlet will result in 20,000 individual Keys to be managed). The requirements for cryptography are the result of a risk analyses being carried out by Tom Parker and Peter Harrison [Pathway Security Report 8th July 1996] and subsequent contractual with the customer negotiations, resulting in entries in the SFS, to agree security measures to mitigate against such risk. It is recommended that the Pathway Security Report be reviewed in light of the Treasury Review.

VPN

Documented requirement references:

FUJ00117495

POCL Agreement; Schedule A16 (reference no. 479)
SFS Section 8.6

Purpose:

VPN is being introduced to protect the links from the POCL Central Services Domain to the post office outlets.

Number Keys to be managed:

20,000 - each outlet having a private Key.

Notes:

On initial roll out of VPN, there will be one global Key used. However, this is for migration purposes and accepted as non compliant to the Security requirement

AP Signing

Documented requirement references:

POCL Agreement; Schedule G01 - '4.2.3.4 Where POCL requires the origin of data to be authenticated, the CONTRACTOR shall apply a digital signature to the data prior to transmission and shall then check it upon receipt. Digital signature techniques and the data to which they are applied shall be described in the Security Functional Specification" referenced in Schedule B3 [S467]'

Requirement 952; and Pathway's response.

SFS Section 8.5

Purpose:

The assurance that AP messages received in the datacentre came from an authorise source.

Number Keys to be managed:

20,000 - each outlet having a private Key.
AP client secret key; 1 (at 300 locations)
See also Siemens Metering requirement for the acknowledgement AP Key

Notes

POCL have, in the past, vehemently defended the requirement for applying digital signatures to AP messages at the outlet. This was reviewed as part of the VPN implementation, but again the PDA refused to negotiate the removal of this requirement unless VPN was to be implemented on the LAN at post office outlets.

Protection of Siemens (formally Landis and Gyr) code and data

Documented requirement references:

FUJ00117495

SFS Section 9.5.4
Statements on Security Objectives and Methods for the Protection of Siemens Metering Code and Data [contractually controlled document]

Purpose:

Pathway have agreed the use of strong cryptographic protection of the Siemens Metering code and data which, if compromised, could lead to the fraudulent 'charging up' of electricity and water metering keys.

Number Keys to be managed:

20,000 - each outlet having a private Key.
Additional private Key at each campus for AP acknowledgements.

Notes:

It took 9 months of negotiation with Siemens Metering (and previously Landis and Gyr) to agree suitable security controls for their code and data. Their implementation of cryptography involves the use of a global key, normally contained within secure hardware, with no Key management. Should this be compromised, Siemens metering would have to replace all hardware devices currently in use throughout the country.

Filestore Encryption

Documented requirement references:

SFS Section 10

Purpose:

Nominated files on Post office workstations and gateway machines will be automatically encrypted at disk access level to preserve data confidentiality in the event of the workstation being stolen [note: Siemens metering code/data and elements of the Key material are protected in the filestore]

Number Keys to be managed:

20,000 - each outlet having a private Key (manufactured using a hardware random number generator - SFS 8.12.1.2).

Notes:

There currently a crude Key management system in place which has an onerous overhead on the SMC helpdesk. Until KMS is introduced, Keys are not generated using a hardware random number generator.

Software Issue Signing

Documented requirement references:

SFS Section 9.5

FUJ00117495

Purpose:

All messages initiated by the Tivoli management mechanism will be digitally signed, for protection in transmission.

Number Keys to be managed:

1 (at 20,000 locations)

Notes:

Also referenced in 'Statements on Security Objectives and Methods for the Protection of Siemens Metering Code and Data'.

Certification Authority

Documented requirement references:

SFS Sections : 8.3.1.2; 8.5.1.1; 9.2

Purpose:

Under public Key technology, protected messages are digitally signed by a private Key and validated using the private Key's matching public Key. Working public Keys are distributed either at roll out or by a KMS in public Key certificates signed by a private key from a Certification Authority.

Notes:

The use of Public/Private Key technology requires the use of a Certification Authority to give the required strength of protection afforded by the Key algorithm used. KMS is central to the implementation of the Certification Authority.

Other

A number of FTMS services utilise crypto protection, typically 1 Secret Key per link. In addition to this, there are further protection domains to support KMS.

Conclusion

The requirement for the KMS is a result for the Crypto solution agreed between Pathway and POCL. As new requirements appeared for cryptographic protection, the solution was designed around existing components. A good example of this is the Siemens Metering protection, which utilises VPN, Filestore encryption, SI Signing and AP Signing to minimise the need for additional code.

To de-scope the requirement for the KMS at CSR+, Pathway will either have to:

a) negotiate 'lets' on the crypto protection for the majority of services itemised above, or

b) to introduce alternative mechanisms to manage the crypto estate.

Option a) would be high risk, as POCL would argue that the risk to their business could be considerable, should fraud be evident on the system due to lack of robust protection. This could compromise their ability to market their system as a secure network for potential E-commerce and Government Gateway business.

FUJ00117495

Option b) is considered in more detail in the paper 'Options for de-risking 17th April 2000 with KMS'.