Table of Contents

1 Management Summary

1.1 Introduction

Customer ZZZ is in the process of building a new Public Key Infrastructure (PKI) to a highly assured standard, which will support smartcard authentication to local and national systems. Customer ZZZ currently has smartcards issued to their estate but the certificates on the cards aren't trusted for access to the local or national systems. Due to this they are undertaking a project to migrate the current Smartcard Management System (SCMS) onto the new highly assured infrastructure. This includes the migration of the symmetric encryption keys used for Global Platform smartcards and the unique symmetric encryption key used by *their* SCMS to create a "secure channel" to their issued smartcards.

It is imperative that the symmetric encryption keys used by the SCMS when migrated are still functional; if this process fails it could impose a huge risk to the ZZZ estate as they will be unable to manage their existing (8000) smartcards. The process of the key migration also needs to be done in a secure manner to ensure that assurance can be put in the newly created SCMS infrastructure and the existing cards in their estate.

1.2 Objective

This document articulates the overview of the SCMS key migration process for Customer ZZZ.

1.3 Scope

The following elements are within the scope of this document:

- CMS key migration strategy overview.

The following elements are outside the scope of this document:

- Design and build of the new highly assured PKI – Reference [01];
- Re-issuance process for existing smartcards – Reference [02].

1.4 Pre-Requisites

When this procedure is performed it **will** break certain existing infrastructure. It is imperative that any services reliant on the existing netHSM and Security World are decommissioned before this procedure is performed. The following are pre-requisites for this procedure:

- 802.1X network authentication has been switched off;
- IPSec is either switched off or is using Kerberos for authentication;
- All existing offline CA's have been powered on and new CRL's published;
- The existing CA certificates are available in case they need adding to any Root CA stores;
- The existing user CA has been taken *offline*;
- The ZZZ Transient CA is *online* – this CA does not use the HSM;
- The existing device CA's have fresh CRL's published;
- All CRL's are available online on the existing HTTP CDP and within AD;
    - The Device CA CRL's should be valid for 7 days which will give us 7 days to perform this procedure;
- A current *good* backup of the existing SCMS database – ready to be restored if necessary;
- A current *good* backup of the existing SCMS servers, including backups of the following:
    - PIV configuration;
    - CMS keys – the nCipher Security World files;

The ACS cards and the current SCMS operator cards, with their passphrases should be available.

1.5 Assumed Knowledge

As assumption is made in this document that the reader has knowledge of the following:

- What an HSM is;
- What a Security World is;
- What an ACS is;
- What an OCS is;
- What an SCMS is;
- What a CA is;
- The reasoning behind doing this procedure and the historical knowledge of the ZZZ National PKI and SCMS infrastructure and project.

2 CMS Key Migration Overview

2.1 High Level Steps

The following list provides high level steps for the migration of the CMS keys:

- CMS key migration;
  - Prepare old SCMS infrastructure;
  - Copy scripts and files;
  - Creation of an "intermediate world";
  - Add module files to "intermediate world";
  - Transfer of keys between world (key migration);
- Movement of existing infrastructure to CONFIDENTIAL network;
  - Re-commission old netHSM (format and rebuild);
  - Add old netHSM to new high assurance security world;
  - Final netHSM configuration;
  - Migrate SCMS database to CONFIDENTIAL;
- Install new SCMS server;
  - Prepare new server;
  - Enrol SCMS server to netHSM;
  - Enrol for new SCMS certificates (RA, web and operator) from new PKI;
  - Install SCMS;
  - Install and configure PIV toolkit;
- SCMS configuration;
  - Validate existing SCMS configuration;
  - Validate existing security settings;
  - Validate MDIDC configuration;
  - Configure new SCMS operator roles;
  - Declare new CA's;
  - Validate LDAP group configuration;
  - Create new SCMS card policies;
  - Create new card policy assignments;
  - Enrol new SCMS operators to system;
  - Enrol new Domain and Enterprise Administrators.

The above infrastructure is illustrated in Figure 1:

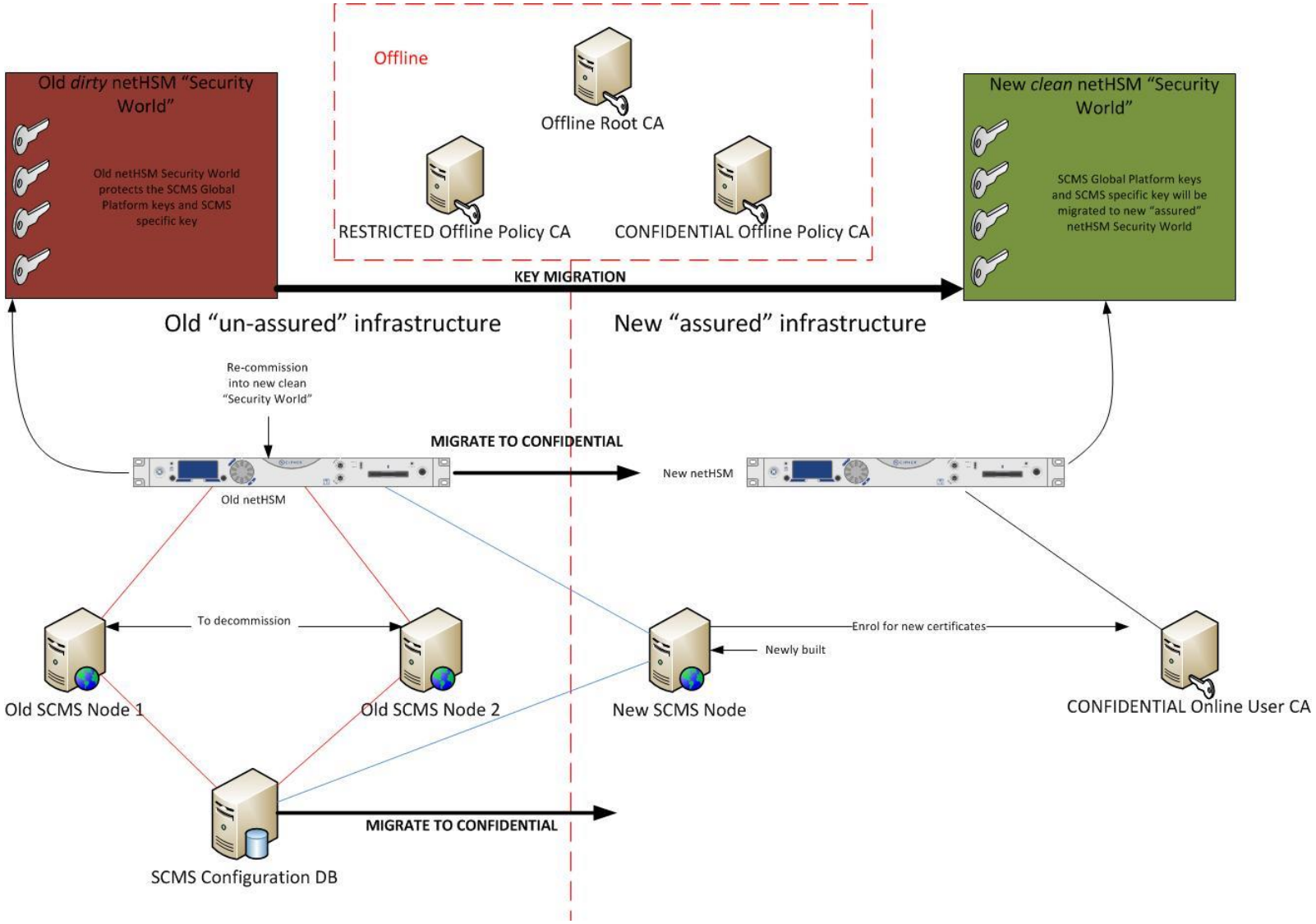

Figure 1: CMS Key Migration Overview

3 CMS Key Migration

The initial procedure for the overall key migration process will involve several steps. After this procedure has been performed the SCMS keys will have been migrated to the new Security World ready for the new SCMS to be built.

The migration steps for this procedure comprise of the following actions detailed in the subsections below.

3.1 Prepare infrastructure, copy files and scripts

This step involves ensuring the SCMS server is in the correct state ready for migration. Before we start the secondary CMS server will be shut down and we will be working on the primary SCMS server *only.*

The preparatory tasks will involve making sure that only the relevant keys are included in the migration and some legacy configuration is deleted.

After the servers are ready the relevant files for the migration scripts will also be copied.

3.2 Create Intermediate Security World

Due to the HSM Security World's conforming to strict FIPS 140-2 Level 3 compliance the key migration cannot be done straight between the new and old Security World. An "Intermediate" Security World needs to be instantiated to act as a transitory location for the keys.

The instantiation of the intermediate security world is done from the *existing* SCMS server using the *existing* netHSM. Due to the flexibility of the nCipher Security World model the old Security World can be backed up by taking a copy of the following folder:

- C:\ProgramData\nCipher\Key Management Data\local (%NFAST_KMDATA%\local)

As long as the original ACS can be reconstituted and the above data files restored a back out plan exists for this procedure.

The instantiation of the new world is done from the command line and creates a new Security World *without* FIPS 140-2 level 3 compliance. The new world must have the ACS 1 /1. During the instantiation of the intermediate world the CMS key data is still encrypted by the old CMS OCS and Security World ACS, therefore still protected. However the existing netHSM can longer load the encrypted keys due to the HSM being loaded with the new intermediate world. The association of the HSM and keys therefore does not exist any longer.

The following command creates the intermediate Security World:

- new-world -i -Q 1/1 -k aes

When the new intermediate world has been created it creates a new %NFAST_KMDATA%\local folder and renames the old local folder to %NFAST_KMDATA%\local_0. We then rename this folder to %NFAST_KMDATA%\local_old.

3.3 Add World Files to Module

When the intermediate world has been instantiated we are ready to prepare this for its transitory role. Firstly the new *clean* Security World needs to be copied to the server; this involves copying the %NFAST_KMDATA%\local\world file and the relevant CMS OCS card files from the new infrastructure. This will be available on a DVD once the new PKI has been built. The files will need to be copied to the existing server to %NFAST_KMDATA%\local_new. Once this has been done we will have three sets of Security World data files on the server:

- %NFAST_KMDATA%\local_old – old Security World with existing SCMS keys encrypted with old SCMS OCS and Security World key (not loaded to current netHSM);
- %NFAST_KMDATA%\local – intermediate Security World currently loaded to the existing netHSM;
- %NFAST_KMDATA%\local_new – new *clean* Security World with new Security World key and new SCMS OCS card files (not loaded to current netHSM);

Now we have file access to all Security Worlds from the SCMS server with a connection to the existing netHSM. The netHSM can only be a member of one Security World at a time but nCipher provide a tool to load multiple Security World keys into the HSM – this isn't the same as the HSM being a member of multiple Security Worlds but does give the HSM access to different Security World master keys. The intermediate Security World key is already loaded to the HSM so we only need to load the old and the new world master key.

The following command is run from the server to load the old Security World key:

- mk-reprogram --owner %NFAST_KMDATA%\local" add "%NFAST_KMDATA%\local_old"

During this process a quorum of the ACS card from the intermediate world first needs to be loaded to authorise this operation. Once loaded a quorum of cards from the *old* ACS needs to be loaded to decrypt the old Security World master key. Please note that the Security World key is only ever in the *clear* within the actual HSM hardware, it only ever exists on the file system in an encrypted form and the ACS cards are effectively the decryption keys for the master key.

The following command is run from the server to load the new Security World key:

- mk-reprogram --owner %NFAST_KMDATA%\local" add "%NFAST_KMDATA%\local_new"

Again, during this process the ACS card for the intermediate Security World needs to be presented to the HSM to authorise the operation. After this a quorum of ACS cards from the new Security World needs to be presented to decrypt the new Security World master key. As stated earlier this key is only ever in the clear within the confines of the HSM.

3.4 Transfer Keys between Security Worlds

When all previous steps have been completed the encrypted keys are ready to be migrated between the old and new Security Worlds. To perform this procedure nCipher provide a command line tool. During this procedure the old encrypted keys are decrypted in the HSM using the key recovery features and the old Security World master key. The keys are subsequently re-encrypted with the new Security World master key and double encrypted with the new SCMS OCS. Once this process has been performed the SCMS encrypted keys can be fully managed from any HSM within the new "assured "Security World.

To transfer the keys the following command is run from the server:

- key-xfer-im "%NFAST_KMDATA%\local_old" "%NFAST_KMDATA%\local_new" --cardset *OCSHASHFORNEWOCS* "%NFAST_KMDATA%\local_old*KEYIDENTIFIER*"

This command can be run so each key is transferred one at a time by re-running the command and presenting a different keyid or by passing multiple keyid's separated by a comma to the same command line. During the procedure a quorum of ACS cards from the old Security World will need to be presented to the HSM, this is so the OCS encrypted keys can be *recovered* and decrypted inside the HSM. A quorum of new SCMS OCS cards is then presented to the HSM so the decrypted keys are re-encrypted with the new Security World master key and the new OCS.

Once the encrypted keys have been migrated they will exist in the %NFAST_KMDATA%\local_new folder. The files in this folder can then be copied off and when ready copied to the new SCMS server. When the netHSM has been re-commissioned and the server enrolled at the HSM it will be able to access the encrypted keys.

4 Movement of Existing Infrastructure to CONFIDENTIAL

This procedure involves moving the old netHSM and SCMS database server to the new CONFIDENTIAL network. The netHSM will be re-commissioned to join to the new Security World and the SCMS DB server will be transitioned over to CONFIDENTIAL. The SCMS DB server cannot be rebuilt as it holds the entire SCMS configuration and references to existing cards. If the database is lost the new SCMS will n to be able to manage any of the existing cards.

4.1 Re-Commission Old netHSM into New Security World

The re-commissioning process for the old netHSM involves physically moving the HSM onto the CONFIDENTIAL environment, resetting the module to factory defaults and reconfiguring it from scratch. This will ensure the HSM is *clean* before it is added to the new Security World.

Once the netHSM has its base configuration it will be added to the new Security World. To perform this procedure a quorum of ACS cards is needed from the new world.

Once the netHSM has been added to the new world the final configuration steps will be performed.

4.2 Migrate SCMS database to CONFIDENTIAL

To migrate the SCMS database into the new CONFIDENTIAL network a new server will exist already built and configured. This server will be installed on the Server 2008 SP2 platform and will have SQL 2005 installed. To migrate the database we will restore an existing database backup to the new server. It will also need to be assured that the correct permissions exist for the SCMS service accounts.

5 Install New SCMS Server

This procedure involves building a totally new SCMS server within the CONFIDENTIAL network. This server will connect to the old netHSM which has been re-commissioned and attach to the existing database.

5.1 Prepare Server and Enrol to netHSM

Before SCMS can be installed on the new server some preparatory steps need to be performed on the server, this will be standard configuration items. The server will then be enrolled as a client of the old netHSM which has just been built into the new Security World.

5.2 Enrol for SCMS Certificates

SCMS needs several certificates for its installation; these certificates will need to be enrolled for from the new "assured" PKI. The following certificates will be needed:

- SCMS SSL certificate;
- SCMS operator certificate;
- Enrolment Agent certificate for new CA.

5.3 Install SCMS

Once all prep work has been done the new SCMS server can be installed. During the installation we will select to use an existing database and attach the server to the recently moved SCMS DB server. Also, during the installation we will provide the relevant certificates which have been enrolled for, this will mean the new SCMS server has its certificates issued from a trusted authority.

The SCMS will be installed on the Windows Server 2008 R2 platform with CMS 4.2. Before CMS 4.2 can be installed the SQL database will need to be patched using the ActivIdentity tools.

5.4 Configure PIV Toolkit

After SCMS has been installed the PIV toolkit will need to be configured.

6 Configure SCMS

This procedure will validate all existing configuration on the SCMS server and make amendments where necessary. When the SCMS configuration has been performed SCMS operators and administrators can be enrolled into the system and have smartcards issued to them.

6.1 Validate Existing Configuration

All existing configuration will be validated. The SCMS server should already have configuration information from the old system as this is stored in the SCMS database. To ensure all configurations are as required for the new SCMS each menu item will be checked and any amendments made, where necessary. The following are items which will be checked:

- SCMS configuration including directories;
- Security Settings;
- My Digital ID Card;
- LDAP groups.

6.2 Configure new SCMS Operator Roles

New SCMS operator roles will be configured to match up with the ZZZ workflow requirements.

6.3 Declare CA's

The new CONFIDENTIAL user CA will be configured at the SCMS. This is so the SCMS can enrol for certificates against this CA.

6.4 Create New Card Policies

New card policies will be created to match up with the ZZZ workflow requirements.

6.5 Create Card Policy Assignments

The newly created card policies will be assigned to the existing LDAP groups.

6.6 Enrol new SCMS Operators to System

All SCMS operators will have a new smartcard issued to them. The certificate on this card will issued from the new PKI. Once the operators have cards issued to them they can be assigned the correct operator role within SCMS.

As well as issuing smartcards to the SCMS operators the administrators of the new CONFIDENTIAL network will have cards issued to them. This will ensure that administrators in sensitive areas are using two-factor authentication.