Document Control	
Title	ABC Primary CA - HSM Key Protection Migration
Description	Deployment of ABC CAs
Version	0.99
Issue Status	Draft
Author	David Wozny
Customer Organisation	ABC

Table of Contents

1. Introduction

1.1. Purpose

This document provides instructions for the migration of the ABC Primary CA's private key protection from HSM OCS protection to HSM 'module only' protection.

1.2. Scope

This document presents technical instructions for the following:

- Migrating the CA's private key protection to *module only*
- Erasure of the *now redundant* OCS

1.3. Applicability and Circumstances

This procedure is applicable to the following systems:

- *Virtual server console* used to connect to *Mascara server guests*
- Primary nShield Connect HSM in the *primary datacentre*
- Secondary nShield Connect HSM in the *primary datacentre*
- Virtual server guest hosting the ABC Class 2 Primary CA

This procedure is NOT applicable to any other system.

1.4. Role Abbreviations

Below is a list of the role abbreviations used in this document:

- Key Ceremony Director [KCD]
- CA Administrator [CAO]
- Key Component Holder [KCH]

1.5. Reading Note

The screenshots contained in this document are intended to represent an example of the screen you should expect to see at a particular point in the procedure. The text accompanying the screenshot is the authoritative instruction to follow and should be the only source of information for configuring the system.

Where reference is made to opening a "PowerShell prompt as administrator" – this means in the context of User Access Control (UAC). Where reference is made to executing a PowerShell script, it is implied that the qualified path is specified, i.e. "`.\`" precedes the script name to be executed.

2. Prior to Key Migration

2.1. Copy Diagnostics File

Begin Procedure – Performed at the Class 2 Primary CA Guest
01. [CAO] **DMW: This entire section could be eliminated if we know the PowerShell script is present** Verify if the following file exists (using Windows Explorer) • `D:\Commissioning\HSM\03.HSM-Diagnostics.ps1` If the file exists, go straight to Section 2.2
02. [CAO] Insert the USB memory stick containing the following file: • `03.HSM-Diagnostics.ps1`
03. [CAO] Copy the file into the following location on the Class 2 Primary CA Server: • `D:\Commissioning\HSM`
End Procedure

2.2. Backup Key Management Data

Begin Procedure – Performed at the Class 2 Primary CA Guest
01. [CAO] Open the **Certification Authority** MMC snap-in Stop the **Active Directory Certificate Services** service
02. [CAO] Remove and secure (temporarily) the OCS cards in the primary and secondary network HSMs
03. [CAO] Start Windows Explorer and create the following folder: • `D:\Emergency-Recovery-Material\PKIData\nCipher\YYYY-MM-DD` *Note: YYYY-MM-DD is the reference date for when this operation is being performed*

04. [CAO] Copy the contents of following folder: • `D:\PKIData\nCipher\Key Management Data` Into the following folder: • `D:\Emergency-Recovery-Material\PKIData\nCipher\YYYY-MM-DD` *Note: If prompted to provide Administrator permission, click the **Continue** button*
End Procedure

2.3. Confirm OCS Key Protection in Use

Begin Procedure – Performed at the Class 2 Primary CA Guest

01. [CAO]

Start a PowerShell session (as Administrator) and change directory to:

- `D:\Commissioning\HSM`

Run the command shown below:

- `rocs`

02. [CAO]

Run the command shown below:

- `list keys`

Verify the command output is as shown below:

```
No. Name                       App      Protected by
1   ABC Class 2 Prima   caping   PROD-CCA-OCS-1
```

03. [CAO]

Run the commands shown below:

- `set changeprot`
- `module 1`

04. [CAO]

Run the command shown below:

- `list cardsets`

Verify the command output is as shown below:

```
No. Name                     Keys (recov) Sharing
    module                   0 (0)        ---
1   PROD-CCA-OCS-1           1 (1)        1 of 2; persistent
```

End Procedure

3. Perform Key Migration

3.1. Perform the Key Protection Migration

Begin Procedure – Performed at the Class 2 Primary CA Guest

01. [CAO]

In the PowerShell session, run the command shown below:

- `target module`

02. [CAO]

Run the command shown below:

- `mark 1`

03. [CAO]

Run the command shown below:

- `recover`

04. [KCH]

The actions in this section must be performed at the primary network HSM in the datacentre. A quorum of ACS card holders are required to insert their ACS cards into the network HSM and enter the relevant pass phrase at the console used to initiate the command

Insert the first ACS card into the network HSM

Verify the command output is *similar* to shown below (the names and card numbers may vary):

```
Authorising OCS replacement:
 Module 1: 0 cards of 1 read
 Module 1 slot 0: empty
 Module 1 slot 0: Admin Card #1
 Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.
```

05. [CAO]

Run the command shown below:

- `save`

06. [KCH]

Remove the last ACS card from the HSM

End Procedure

3.2. Validate Migration

Begin Procedure – Performed at the Class 2 Primary CA Guest

01. [CAO]

In the PowerShell session, run the command shown below:

- `list keys`

Verify the command output is as shown below:

```
No. Name                       App      Protected by
1   ABC Class 2 Prima   caping   module
```

02. [CAO]

Run the command shown below:

- `exit`

End Procedure

4. Post Key Migration

4.1. Start ADCS and Publish a Fresh CRL

Begin Procedure – Performed at the Class 2 Primary CA Guest
01. [CAO] Open the **Certification Authority** MMC snap-in Start the **Active Directory Certificate Services** service
02. [CAO] In the **Certification Authority** MMC snap-in: Select the **Revoked Certificates** container Choose **All Tasks | Publish** from the context menu Click **OK** when prompted (it may take up to sixty seconds)
03. [CAO] Start Windows Explorer and select the following folder: • `D:\PKIData\IDP` Validate that the time stamp on the following file reflects the *current time*: • `ABC Class 2 Primary CA.crl`
End Procedure

4.2. Generate Diagnostic Output

Begin Procedure – Performed at the Class 2 Primary CA Guest
01. [CAO] In the PowerShell prompt run the following command: • `03.HSM-Diagnostics.ps1` In the log file that is automatically opened in Notepad, verify both Module 1 and Module 2 return no errors - see Appendix B for indicative diagnostic output
End Procedure

4.3. Erase Redundant OCS Cards

Begin Procedure – Performed at the Class 2 Primary CA Guest
01. [CAO] KCH inserts their OCS card into the network HSM
02. [CAO] In the PowerShell prompt, run the following command: • `createocs --module 1 –erase` Press the Enter key when prompted
03. [KCH] When the command has completed, KCH removes the OCS card
04. [KCH] Repeat the first three steps for the entire set of OCS cards
End Procedure

4.4. Purge Redundant OCS Files from the File System

Begin Procedure – Performed at the Class 2 Primary CA Guest

01. [CAO]

Start Windows Explorer and change to the following folder:

- `D:\PKIData\nCipher\Key Management Data\local`

02. [CAO]

Delete all files prefixed with either of the following two names:

- `card`
- `cards`

End Procedure

4.5. Change ADCS to Start Automatically

Begin Procedure – Performed at the Class 2 Primary CA Guest

01. [CAO]

Open the Services MMC snap-in

02. [CAO]

Change the start-up type for Active Directory Certificate Services to:

- Automatic (Delayed Start)

End Procedure

4.6. Restart the Server and Publish a Fresh CRL

Begin Procedure – Performed at the Class 2 Primary CA Guest
01. [CAO] Restart the server
02. [CAO] Open the **Certification Authority** MMC snap-in and confirm that ADCS is started Select the **Revoked Certificates** container Choose **All Tasks | Publish** from the context menu Click **OK** when prompted (it may take up to sixty seconds)
03. [CAO] Start Windows Explorer and select the following folder: • `D:\PKIData\IDP` Validate that the time stamp on the following file reflects the *current time*: • `ABC Class 2 Primary CA.crl`
End Procedure

Appendices

Appendix A: Bring Along Items

The following items are required to perform the procedure described in this document:

- A quorum of **ABC Class 2 PKI** ACS cards
- The complete set of **PROD-CCA-OCS-1** OCS cards (for erasure)
- The `03.HSM-Diagnostics.ps1` commissioning file on a USB stick

Appendix B: Diagnostic Output

```
enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        6D05-0BE0-D947 2C05-0250-D947
 mode                 operational
 version              2.103.13
 speed index          956
 rec. queue           218..366
 level one flags      Hardware HasTokens
 version string       2.103.13cam19, 3.3pla21 Built on Feb  2 2017 10:10:03, Bootloader:
1.1.28, Security Processor: 2.1.18 , 3.63.3cam1, 3.3pla21 Built on Feb  2 2017 10:10:03,
Bootloader: 1.1.28, Security Processor: 2.1.18 , 3.63.3cam1
 checked in           00000000487debd5 Wed Jul 16 12:38:45 2008
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasPollCmds
FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp HasLongJobs
ServerHasLongJobs AESModuleKeys NTokenCmds JobFragmentation LongJobsPreferred Type2Smartcard
ServerHasCreateClient HasInitialiseUnitEx Type3Smartcard HasKLF2
 module type code     0
 product name         nFast server
 device name
 EnquirySix version   4
 impath kx groups
 feature ctrl flags   none
 features enabled     none
 version serial       0
 remote server port   9004

Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        6D45-02E0-D937
 mode                 operational
 version              3.3.21
 speed index          478
 rec. queue           22..50
 level one flags      Hardware HasTokens
 version string       3.3pla21 Built on Feb  2 2017 10:10:03, Bootloader: 1.1.28, Security
Processor: 2.1.18 , 3.63.3cam1
 checked in           0000000058934bca Thu Feb 02 15:10:02 2017
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasPollCmds
FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp HasLongJobs
ServerHasLongJobs AESModuleKeys NTokenCmds JobFragmentation LongJobsPreferred Type2Smartcard
ServerHasCreateClient HasInitialiseUnitEx Type3Smartcard HasKLF2
 module type code     12
 product name         nC3025E/nC4035E/nC4035N
 device name          Rt1
 EnquirySix version   6
 impath kx groups     DHPrime1024 DHPrime3072
 feature ctrl flags   LongTerm
 features enabled     StandardKM HSMBaseSpeed LoadObjBaseCap
 version serial       36
 connection status    OK
 connection info      esn = 6D05-02E0-D747; addr = INET/173.16.29.3/9004; ku hash =
94af7a7dc042681586e908719ce273f96f34116a, mech = Any; time-limit = 24h; data-limit = 8MB
 image version        12.42.14cam3
 max exported modules 3
 rec. LongJobs queue  21
 SEE machine type     PowerPCELF
 supported KML types  DSAp1024s160 DSAp3072s256
 using impath kx grp  DHPrime3072
 hardware status      OK

Module #2:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        2C45-02E0-c947
 mode                 operational
 version              3.3.21
 speed index          478
 rec. queue           22..50
 level one flags      Hardware HasTokens
 version string       3.3pla21 Built on Feb  2 2017 10:10:03, Bootloader: 1.1.28, Security
Processor: 2.1.18 , 3.63.3cam1
 checked in           0000000058934bca Thu Feb 02 15:10:02 2017
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasPollCmds
FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp HasLongJobs
ServerHasLongJobs AESModuleKeys NTokenCmds JobFragmentation LongJobsPreferred Type2Smartcard
ServerHasCreateClient HasInitialiseUnitEx Type3Smartcard HasKLF2
 module type code     12
 product name         nC3025E/nC4035E/nC4035N
 device name          Rt2
 EnquirySix version   6
 impath kx groups     DHPrime1024 DHPrime3072
 feature ctrl flags   LongTerm
 features enabled     StandardKM HSMBaseSpeed LoadObjBaseCap
 version serial       36
 connection status    OK
 connection info      esn = 2C05-05E0-D947; addr = INET/173.16.29.5/9004; ku hash =
410c5a9c7f632612e10ad2acc32289e09d3d3b08, mech = Any; time-limit = 24h; data-limit = 8MB
 image version        12.42.14cam3
 max exported modules 3
 rec. LongJobs queue  21
 SEE machine type     PowerPCELF
 supported KML types  DSAp1024s160 DSAp3072s256
 using impath kx grp  DHPrime3072
 hardware status      OK
=================================
nfkminfo
World
 generation  2
 state       0x7270000 Initialised Usable Recovery !PINRecovery !ExistingClient RTC NVRAM !FTO
!AlwaysUseStrongPrimes !DisablePKCS1Padding !PpStrengthCheck SEEDebug
 n_modules   2
 hknso       72adaa197a4d0e92c9f40e1c11c5541759ae5c28
 hkm         7d482037785020eb8b99b9cab1b5b1b497c19967 (type Rijndael)
 hkmwk       1d572201be533ebc89f30fdd8f3fac6ca3395bf0
 hkre        ee1be204e8a1dcf334376dd4e0c02ed775c4be70
 hkra        3bd706c4a4649ec484caf4f5f40adc147d84b0cb
 hkmc        d96c82d0d775d17df459fa845de0b24d23d9c603
 hkrtc       f5e4023829674db3d5d9f675e32bbd43362c757b
 hknv        d98452a6a4017f51b858aa204583cfe56c1a7474
 hkdsee      305b0ce50dd6307fd8080dcac59cb29a85e02e88
 hkmnull     0100000000000000000000000000000000000000
 ex.client   none
 k-out-of-n  1/2
 other quora m=1 r=1 nv=1 rtc=1 dsee=1
 createtime  2017-07-24 15:52:18
 nso timeout 10 min
 ciphersuite DLf3072s256mRijndael
 min pp      0 chars

Module #1
 generation 2
 state      0x2 Usable
 flags      0x0 !ShareTarget
 n_slots    2
 esn        6D05-02E0-D947
 hkml       35e1c360d681d8573688afa4ade7afc5e5f80b43

Module #1 Slot #0 IC 0
 generation    1
 phystype      SmartCard
 slotlistflags 0x2 SupportsAuthentication
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
No Cardset

Module #1 Slot #1 IC 0
 generation    1
 phystype      SoftToken
 slotlistflags 0x0
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
No Cardset

Module #2
 generation 2
 state      0x2 Usable
 flags      0x0 !ShareTarget
 n_slots    2
 esn        2C05-02E0-D947
 hkml       455c14c743bfc1ecb97bff377775ef7c6d71cd70

Module #2 Slot #0 IC 0
 generation    1
 phystype      SmartCard
 slotlistflags 0x2 SupportsAuthentication
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
No Cardset

Module #2 Slot #1 IC 0
 generation    1
 phystype      SoftToken
 slotlistflags 0x0
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
No Cardset

No Pre-Loaded Objects
=================================
nfkmverify

** [Security world] **
    Ciphersuite: DLf3072s256mRijndael
    128-bit security level
    2 Administrator Card(s)
    (NOT IN ANY SLOT of an attached module)
    HKNSO 72adaa197a4d0e92c9f40e1c11c5541759ae5c28
    Cardset recovery ENABLED
    Passphrase recovery disabled
    Strict FIPS 140-2 level 3 (does not improve security) disabled
    SEE application non-volatile storage ENABLED
    real time clock setting ENABLED
    SEE debugging ENABLED
    SEE debugging restricted
    Foreign Token Open authorization disabled
    Generating module ESN 6D05-02E0-D947 currently #1 (in same incarnation)

Verification successful, confirm details above.  0 keys verified.

=================================
nfkmcheck
nfkmcheck: information: Module #1 Slot #0 Empty
nfkmcheck: information: Module #2 Slot #0 Empty
nfkmcheck: everything seems to be in order
```