Document Control	
Title	Root CA CRL Publication Procedure
Description	Procedure for Publishing the Root CA CRL and Backup of the Root CA
Version	0.99
Issue Status	Issued
Author	
Customer Organisation	MSP

Change Record

Issue No.	Date	Issued By	Reason for Issue
1.0	31/12/1999	D. Wozny	First issue

Distribution List

Copy	Issued To	Position
1	AN Other	ABC Head of Compliance, tPKI PMA Chair

Table of Contents

1. Introduction

1.1. Background

The publication of a time valid (fresh) CRL by the Root CA is essential in maintaining the operational availability of the tPKI. The Root CA CRL is valid for a period of 190 days, it is therefore necessary to publish a fresh CRL prior to the existing CRL expiring (going stale).

1.2. Purpose

This document describes the operational processes for starting up the Root CA and publishing a fresh CRL and subsequent transferral thereof to removable media in readiness for promulgation.

1.3. Scope

1.3.1. In Scope

- Start-up of the “Root CA laptop host” and the VMWare based Root CA server “guest”
- Authorisation and activation of Root CA key material protected by an HSM - by presenting a quorum of ROOTCA OCS cards
- Logon to the Certification Authority MMC application and publication of a fresh CRL
- Transfer of the Root CA CRL to removable media
- Backups of the Root CA both to a local folder on the laptop host and removable media

1.3.2. Out of Scope

- Promulgation of the freshly created CRL

1.4. Role Abbreviations

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

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

1.5. Pre-Requisites / Bring Along

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

- “Root CA laptop host” (in tamper evident bag)
- nShield Edge unit and USB cable (in tamper evident bag)
- Laptop Administrator (Windows Server 2008 R2) password record form (in tamper evident bag)
- Root CA server (guest) Sysmanager password record form (in tamper evident bag)
- Suitable new tamper evident bags
- A quorum (three) of ROOTCA OCS cards (and corresponding pass phrases)
- USB memory stick for promulgation of the CRL
- Two USB memory sticks for backups of the Root CA server (VMWare guest)

2. Initial Tasks

2.1. Preparation

Performed at the Root CA Host Laptop
01. CAO Remove the laptop from the tamper evident bag and connect its power supply Power on the laptop
02. CAO Remove the “laptop host” TROOT-HOST\Administrator password record form from the tamper evident bag Note: Referenced as “Root CA Lenovo Laptop Host 2008 R2” Log on as Administrator
03. CAO Inspect the time on the laptop and ensure that it is within two minutes accuracy
04. CAO Open the Windows Event Logs and inspect them for any irregular events

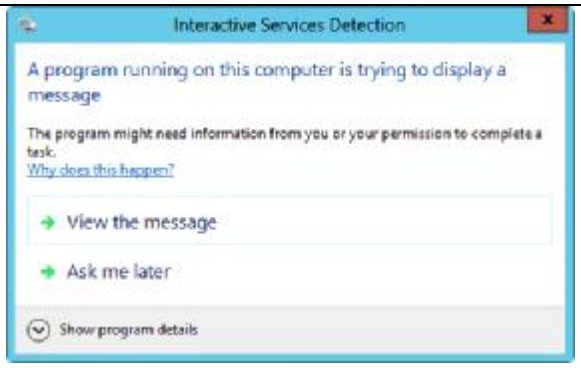
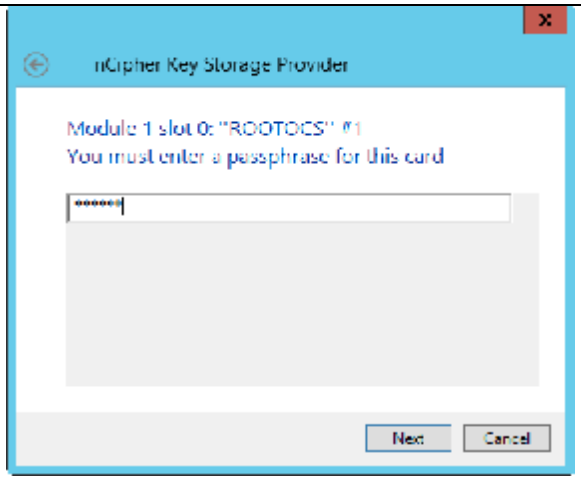
2.2. Start Guest

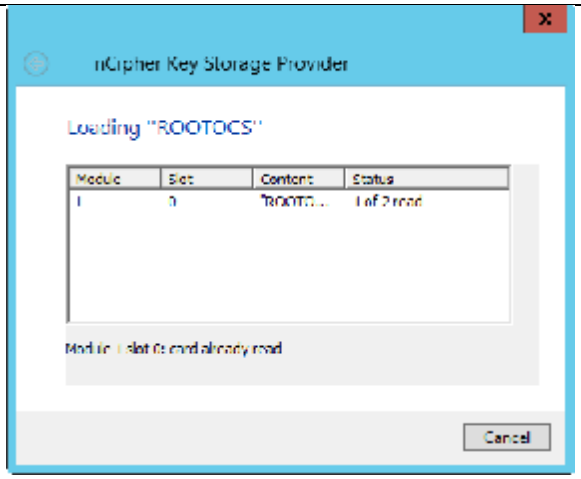
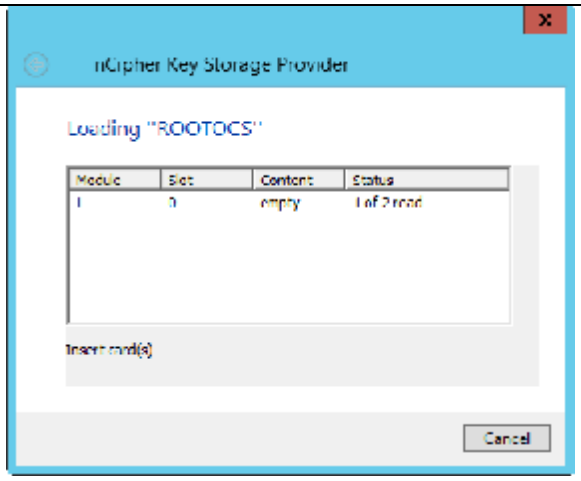
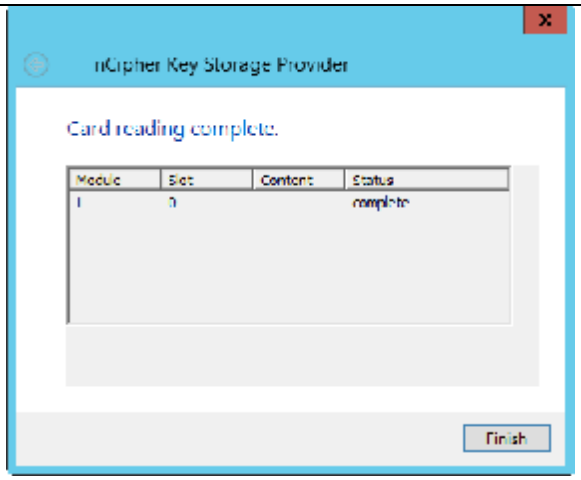
Performed at the Root CA Host Laptop
01. CAO Start **VMWare Workstation**
02. CAO Select the **ABC Root CA** server (guest) and click the **Start** button
03. CAO Retrieve the **RCA01\Sysmanager** password for the ABC Root CA server (guest) When the ABC Root CA server (guest) starts up, log on as Sysmanager

04. CAO Inspect the time in the ABC Root CA guest and ensure that it is within two minutes accuracy
05. CAO Open the Windows Event Logs in the ABC Root CA guest and inspect them for any irregular events
06. CAO Whilst the VMWare Workstation ABC Root CA guest is “in focus”, attach the nShield Edge to the USB port on the laptop Note: The correct port is marked using white masking tape

3. Publish Fresh CRL

3.1. Start ADCS Service

Performed at the Root CA Host Laptop (on the ABC Root CA Guest)	
01. CAO Open the **Certification Authority** console Select **Start this service** from the toolbar	**<Image Removed>**
02. CAO Click on the **Interactive Services Detection** icon on the Taskbar Click **View the message**	
03. CAO Click the **Finish** button	**<Image Removed>**
04. KCH1 The KCD instructs KCH1 to retrieve their Root CA OCS card from their temporary storage contain and insert it into the USB HSM smart card reader KCH1 enters the PIN code then click the **Next** button	

05. KCH1 When the dialogue box indicates the OCS card is *already read*, the KCH1 removes it from the smart card reader and places it back into their temporary storage container	
06. KCD Observe panel indicating prompting for insertion of further OCS cards *Note: At this stage the status will show 1 of 3 cards read*	
07. KCD The previous three actions are repeated for KCH2 and KCH3 until such time that the status indicates "complete"	
08. KCH3 When the dialogue box indicates card reading is complete, KCH3 removes their card from the smart card reader and places it back into their temporary storage container Click the **Finish** button	

09. CAO Click the **Return now** button	
10. CAO Select the **Issued Certificates** node *If ADCS isn't working an error will be displayed*	**<Image Removed>**

3.2. Publish CRL and Verify

Performed at the Root CA Host Laptop (on the ABC Root CA Guest)	
01. CAO Open a PowerShell prompt (as administrator) Run the following command: • `certutil -crl`	
02. CAO Open the following folder in Windows Explorer: • `D:\PKIData\IDP`	
03. CAO Double-click the following file to open it: • `ABC Root CA.crl` Verify that the Effective date is *today*	**<Image Removed>**

3.3. Transfer CRL to USB Memory Stick

Performed at the Root CA Host Laptop (on the ABC Root CA Guest)
01. CAO Insert the USB memory stick assigned to ABCPKI promulgation

02. CAO

Copy the following file:

- `D:\PKIData\IDP\ABC Root CA.crl`

To the root of the USB memory stick

03. CAO

Disconnect the USB memory stick assigned to ABCPKI promulgation