PKI Support Guide

Author: David Wozny
Department: Enterprise Architecture (via IT Security Solutions)

Version: 1.0
Last update: 31st December, 1999
Project: 70EETRC10151 – PKI Implementation

CONTENTS

1. DOCUMENT CONTROL

1.1. Document History

Version	Date	Reason for Change
1.0	31/12/1999	First issue

1.2. Document Owners

Name	Position	Organisation
No Name	Enterprise Architecture Manager	ABC

1.3. Document Distribution

Name	Position	Organisation
No Name 2	Project Manager	ABC

1.4. Document Scope

The scope of the OurABC PKI support document encompasses the following platforms:

- OurABC Root CA (ROOTCA)
- OurABC Issuing CA1 (ENNIS.OurABC.cccusers.com)
- HTTP CDP1 (PILAR01.OurABC.cccusres.com)
- HTTP CDP2 (PILAR02.OurABC.cccusres.com)

2. ROUTINE MONITORING TASKS (DAILY)

2.1. Event Log Monitoring of Ennis Issuing CA

01.

Log onto the Issuing CA and start the event viewer

02.

Review Active Directory Certificate Services Server Role Event Log

Select the following node:

- Event Viewer | Custom Views | Server Roles | Active Directory Certificate Services

Review the list of events for anything extraordinary

03.

Review PKI Related Security events

Select the following node:

- Event Viewer | Windows Logs | Security

Select the Create Custom View action

In the Include/Exclude Event IDs, set the following range:

- 4868-4900 (see Appendix E)

Note: These are ADCS specific events

Save the view as PKI Security Events

Review the list of events for anything extraordinary

04.

Review General (non-PKI) Related Security events

Select the following node:

- Event Viewer | Windows Logs | Security

Select the Create Custom View action

In the Include/Exclude Event IDs, set the following range:

- -4656,-5447,-5152,-5156,-5158

Note: This is to filter out "noise"

Save the view as non-PKI Security Events

Review the list of events for anything extraordinary

05.

Review PKI Related Application Events

Select the following node:

- Event Viewer | Windows Logs | Application

Select the Create Custom View action

Select by Source, then choose the following sources:

- CertificationAuthority
- CertificationAuthority-EnterprisePolicy
- CertPolEng

Save the view as PKI Application Events

Review the list of events for anything extraordinary

06.

Review PKI CAMonitor Generated Events

Select the following node:

- Event Viewer | Windows Logs | Application

Select the Create Custom View action

Select by Source, then choose the following sources:

- CA Operations

In the Include/Exclude Event IDs, set the following range:

- -911

Note: These events are related to the monitoring task which is triggered by a scheduled task

Note: There may be a preference to not exclude event 911, such that there is confidence that the scheduled task is actually running

Save the view as PKI CA Monitor Events

Review the list of events for anything extraordinary

2.2. Manually Run CA Monitor at Ennis Issuing CA

01.

Note: This only needs to be run if the CA Monitor scheduled tasks generate errors – which then need further investigation

Open a DOS command prompt (with Administrator privileges) and change directory to:

- `D:\Commissioning\Tasks`

Run the following command:

- `02.CA-Monitoring-Program.cmd`

To get interactive feedback on the health of the PKI; any problems will be reported into the Application Event log of the console where the command is executed.

```
29/11/2010 11:21:35      eventcreate /T SUCCESS /SO "CA Operations" /ID 911 /D "
Info: CAMonitor.vbs starting" /L Application:OK
29/11/2010 11:21:36      certutil -ping:OK
29/11/2010 11:21:36      certutil -pingadmin:OK
29/11/2010 11:21:37      checking validity of CN=OurABC Issuing CA1, O=Ches
hire Shared Services, C=GB Serial Number:61B9298C000000000002
29/11/2010 11:21:37      CA Cert OK
29/11/2010 11:21:37      checking validity of CN=OurABC Root CA, O=Cheshire
 Shared Services, C=GB Serial Number:149DAEED1A5ACF844A01E908972FEA1F
29/11/2010 11:21:37      CA Cert OK
29/11/2010 11:21:37      Retrieve environment variable 'COMPUTERNAME':OK
29/11/2010 11:21:37      CDPs from:CN=OurABC Issuing CA1-Xchg, O=Cheshire S
hared Services, C=GB
29/11/2010 11:21:37      HTTP CDP: http://pki.OurABC.cccusers.com/idp/OurCh
eshire%20Issuing%20CA1.crl
29/11/2010 11:21:37      LDAP CDP: ldap://CN=OurABC Issuing CA1,CN=ENNIS,CN
=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cccusers,DC=com
29/11/2010 11:21:37
29/11/2010 11:21:37      Checking: http://pki.OurABC.cccusers.com/idp/OurCh
eshire%20Issuing%20CA1.crl
29/11/2010 11:21:37      Retrieve environment variable 'temp':OK
29/11/2010 11:21:38      HTTP CRL successfully written to file
29/11/2010 11:21:39      CRL Checked - CRL Status: 0
29/11/2010 11:21:39      Checking: ldap://CN=OurABC Issuing CA1,CN=ENNIS,CN
=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cccusers,DC=com
29/11/2010 11:21:39      Retrieve environment variable 'temp':OK
29/11/2010 11:21:39      LDAP CRL successfully written to file
29/11/2010 11:21:39      CRL Checked - CRL Status: 0
29/11/2010 11:21:39      CDPs from:CN=OurABC Issuing CA1, O=Cheshire Shared
 Services, C=GB
29/11/2010 11:21:39      HTTP CDP: http://pki.OurABC.cccusers.com/idp/OurCh
eshire%20Root%20CA.crl
29/11/2010 11:21:39      LDAP CDP: ldap://CN=OurABC Root CA,CN=RootCA,CN=CD
P,CN=Public Key Services,CN=Services,CN=Configuration,dc=cccusers,dc=com
29/11/2010 11:21:39
29/11/2010 11:21:39      Checking: http://pki.OurABC.cccusers.com/idp/OurCh
eshire%20Root%20CA.crl
29/11/2010 11:21:39      Retrieve environment variable 'temp':OK
29/11/2010 11:21:39      HTTP CRL successfully written to file
29/11/2010 11:21:39      CRL Checked - CRL Status: 0
29/11/2010 11:21:39      Checking: ldap://CN=OurABC Root CA,CN=RootCA,CN=CD
P,CN=Public Key Services,CN=Services,CN=Configuration,dc=cccusers,dc=com
29/11/2010 11:21:39      Retrieve environment variable 'temp':OK
29/11/2010 11:21:39      LDAP CRL successfully written to file
29/11/2010 11:21:39      CRL Checked - CRL Status: 0
29/11/2010 11:21:39      Root CA Cert - no CDP present, skipping check
29/11/2010 11:21:39      No KRAs
29/11/2010 11:21:39      eventcreate /T SUCCESS /SO "CA Operations" /ID 911 /D "
Info: CAMonitor.vbs completed" /L Application:OK
```

2.3. Enterprise PKI Viewer

01. Open the Enterprise PKI Viewer by running PKIView.msc
02. Select the OurABC Issuing CA1 node **<PKI view image removed>** *Observe that all entries in the centre pane show "OK"*
03. Select the OurABC Root CA node **<PKI view image removed>** *Observe that all entries in the centre pane show "OK"*

3. PUBLISH A FRESH ROOT CA CRL (ANNUALLY)

3.1. Startup Root CA and Attach Floppy Disk

01. Open VMWare console and select the following node: Ø Valon | Minerva Avenue | HACluster5 | RootCA Start up the Root CA Server
02. Open a VMWare console session on the Root CA Logon to the Root CA
03. Attach the Virtual Floppy disk[1] to the Root CA Ø Open the VMWare tools applet Ø Select the Devices tab Ø Check (select) “Floppy 1” Ø Click Apply

3.2. Perform CA Database Backup and Publish CRL (at the Root CA)

[1] Datastore reference: slow23\rootca\Rootca.flp

01.

Note: Executing the CA backup program triggers a fresh CRL to be published

Open a command prompt and change the directory to:

- `D:\Commissioning\PKI`

Run the following command:

- `B.03a.Root-CA-BackupDB.cmd <yyyy.mm.dd>`

The parameter <yyyy.mm.dd> should be entered without the angled brackets and the letters replaced by year, month and day values

Observe output similar to that shown below:

```
Enter Date in Following Format  -YYYY-MM-DD: 2010.11.21
CertUtil: -CRL command completed successfully.
Full database backup for RootCA\OurABC Root CA.
Backing up Database files: 100%
Backing up Log files: 100%
Truncating Logs: 100%
Backed up database to D:\CA-Backup\2010.11.21
Database logs successfully truncated.
CertUtil: -backupDB command completed successfully.
```

02.

Verify that the following data structure is created on the D-Drive:

```
D:\
  \---CA-Backup
    |---2010.11.21
        \---DataBase
                certbkxp.dat
                OurABC Root CA.edb
                edb00002.log
```

03.

Copy the following file on the Root CA to the root of the virtual floppy disk drive:

- `D:\IDP\OurABC Root CA.crl`

04.

Select the following folder on the Root CA:

- `D:\CA-Backup\YYYY-MM-DD`

Simultaneously select the following files:

- `D:\CA-Backup\ca-registry.txt`
- `D:\CA-Backup\OurABC Root CA.p12`

From the context menu, select: Send to | Compressed (zipped) folder; then name the backup:

- `D:\CA-Backup\ROOTCA-Backup-YYYY-MM-DD.zip`

05.

Copy the compressed backup file **(**`D:\CA-Backup\RootCA-Backup-YYYY-MM-DD.zip`**)** to the root of the virtual floppy disk

Once the zipped file has been successfully transferred to the virtual floppy disk, delete the zipped file **(**`D:\CA-Backup\ROOTCA-Backup-YYYY-MM-DD.zip`**)**

06.

Disconnect the Virtual Floppy disk drive from the Root CA

- Ø Open the VMWare tools applet
- Ø Select the Devices tab
- Ø Uncheck (deselect) “Floppy 1”
- Ø Click Apply

07.

Shut down the Root CA server

3.3. Publish Root CA CRL to Active Directory

01.

Attach the Virtual Floppy Disk to ENNIS

- Ø Open the VMWare tools applet
- Ø Select the Devices tab
- Ø Check (select) “Floppy 1”
- Ø Click Apply

02.

Copy the following file on the Virtual Floppy disk:

- Ø `OurABC Root CA.crl`

To the following location on ENNIS:

- Ø `D:\IDP\OurABC Root CA.crl`

03.

Open a command prompt and change the directory to:

- Ø `D:\Commissioning\PKI`

Run the following command:

- Ø `R.01.Publish-Fresh-Root-CA-CRL-to-AD.cmd`

The following output is expected:

```
Base CRL added to DS store.
Certutil: -dsPublish command completed successfully
```

3.4. Confirm Fresh CRL is Correctly Published in Active Directory

01.

Open the Enterprise PKI MMC snap-in by running the following command:

- Ø `pkiview.msc`

02.

Select the OurABC Root CA node

The status for all entries should be: OK

<PKI view image removed>

3.5. Transfer Root CA Database to Persistent Storage

01.

Attach the Virtual Floppy Disk to ENNIS

- Ø Open the VMWare tools applet
- Ø Select the Devices tab
- Ø Check (select) “Floppy 1”
- Ø Click Apply

02.

Copy the following file on the Virtual Floppy disk drive:

- `ROOTCA-Backup-YYYY-MM-DD.zip`

To the following folder on the DELICIA server:

- `E:\CA-Backup\Root-CA\ROOTCA-Backup-YY-MM-DD.zip`[2]

Delete the contents of the virtual floppy disk

Disconnect the Virtual Floppy disk drive from ENNIS

- Open the VMWare tools applet
- Select the Devices tab
- Uncheck (deselect) "Floppy 1"
- Click Apply

3.6. Transfer Root CA VMWare Files to Persistent Storage

01.

Use the VSphere data store browser to take a copy of all VM files associated with the Root CA to the APPOLLO server

- Valon | Minerva Avenue | HACluster5
- Select Configuration Tab
- Select slow23 datastore
- Browse the datastore and select the RootCA folder
- Copy all files into the buffer

Paste the files into the following folder on APPOLLO:

- `H:\RootCA-Backups`

[2] This is via a UNC (\\DELECIA\E$\CA-Backup\Root-CA) to DELECIA