Document Control	
Title	PKI Detailed Engineering
Description	ABC PKI Detailed Engineering
Version	0.99
Issue Status	Draft
Author	David Wozny
Customer Organisation	ABC

Table of Contents

1. Management Summary

1.1. Background

TBC

1.2. Objective

TBC

1.3. Scope

1.3.1. In Scope

1.3.2. Out of Scope

2. Active Directory Preparation

2.1. OID Registration

2.1.1. Script

```
..\Commissioning\ADPrep\OID-Registration.ps1
```

2.1.2. Content

```
Register-ObjectIdentifier -FriendlyName "ABC Org Class 3 Primary CA Certificate Policy" -Value
"1.2.826.0.9999.509.11.31" -OidGroup IssuancePolicy -CPSLocation
"http://www.ABC.Org.uk/pki/rpac3p.pdf" -UseActiveDirectory
```

2.1.3. Explanation

This command uses the PSPKI PowerShell module to register a “friendly label” against the Certificate Policy OIDs that are utilised in the pki – both ABC and “NPIA” OIDs are registered.

The “friendly label” is displayed when using Windows tools to inspect a certificate.

The command is repeated for each certificate policy to be registered.

2.2. Active Directory Population

2.2.1. Script

```
..\Commissioning\ADPrep\PKI-Delegation-Population.ps1
```

2.2.2. Content

```
# Domain
$CONFLDAP="DC=Confund,DC=ABC,DC=Org,DC=uk"
$CONFAD="Confund.ABC.Org.uk"
$RESTAD="Fund.ABC.Org.uk"
# Organisation Units
$TopPKIou="ou=PKI"
# Groups
$CAAdminGroupcn="cn=RGG-PKI-CA-Admin"
$CAAdminGroup="RGG-PKI-CA-Admin"
$CertManagerGroupcn="cn=RGG-PKI-Cert-Mgr"
$CertManagerGroup="RGG-PKI-Cert-Mgr"
$LocalAdminGroupcn="cn=RGG-PKI-Local-Admin"
$LocalAdminGroup="RGG-PKI-Local-Admin"
#Users
$eCENotificationUsercn="cn=eCE-Notify"
$eCENotificationUser="eCE-Notify"
$CAAdminUsercn="cn=CA-Admin-Op"
$CAAdminUser="CA-Admin-Op"
$LocalAdminUsercn="cn=Local-Admin-Op"
$LocalAdminUser="Local-Admin-Op"
$CertManagerUsercn="cn=Cert-Manager-Op"
$CertManagerUser="Cert-Manager-Op"
# Create OUs
dsadd.exe ou $TopPKIOU`,$CONFLDAP

& dsadd.exe group $CAAdminGroupcn`,$TopPKIOU`,$CONFLDAP -samid $CAAdminGroup
```

```
& dsadd.exe group $CertManagerGroupcn`,$TopPKIOU`,$CONFLDAP -samid $CertManagerGroup
& dsadd.exe group $LocalAdminGroupcn`,$TopPKIOU`,$CONFLDAP  -samid $LocalAdminGroup
# Create PKI Operator Accounts
& dsadd.exe user $eCENotificationUsercn`,$TopPKIOU`,$CONFLDAP   -samid $eCENotificationUser -
upn $eCENotificationUser@$CONFAD -display $eCENotificationUser -email
$eCENotificationUser@$CONFAD -pwd Passw0rd   -disabled no
& dsadd.exe user $CAAdminUsercn`,$TopPKIOU`,$CONFLDAP   -samid $CAAdminUser -upn
$CAAdminUser@$CONFAD -display $CAAdminUser -email $CAAdminUser@$CONFAD -pwd Passw0rd      -
disabled no
& dsadd.exe user $CertManagerUsercn`,$TopPKIOU`,$CONFLDAP   -samid $CertManagerUser -upn
$CertManagerUser@$CONFAD -display $CertManagerUser -email $CertManagerUser@$CONFAD -pwd
Passw0rd       -disabled no
& dsadd.exe user $LocalAdminUsercn`,$TopPKIOU`,$CONFLDAP    -samid $LocalAdminUser  -upn
$LocalAdminUser@$CONFAD  -display $LocalAdminUser  -email $LocalAdminUser@$CONFAD  -pwd
Passw0rd       -disabled no
#Populate PKI Admin Security Groups
& dsmod.exe group $CAAdminGroupcn`,$TopPKIOU`,$CONFLDAP -addmbr
"cn=$CAAdminUser`,$TopPKIOU`,$CONFLDAP"
& dsmod.exe group $CertManagerGroupcn`,$TopPKIOU`,$CONFLDAP -addmbr
"cn=$CertManagerUser`,$TopPKIOU`,$CONFLDAP"
& dsmod.exe group $LocalAdminGroupcn`,$TopPKIOU`,$CONFLDAP  -addmbr
"cn=$LocalAdminUser`,$TopPKIOU`,$CONFLDAP"
#Add PKI Groups to Local Administrators Group on CA
& net localgroup administrators $CONFAD\$CAAdminGroup /add
& net localgroup administrators $CONFAD\$LocalAdminGroup /add
```

2.2.3. Explanation

The script uses dsadd and dsmod directory services administration tools to create sample security groups and user accounts.

This script should only be used in an “informal” test environment and should not be used in Ref / PP / Production.

The script uses legacy commands and should be updated to leverage PowerShell cmdlets.

2.3. Publishing Root CA Material to Active Directory

2.3.1. Command

```
..\Commissioning\ADPrep\Publish-Root-CA-Material-to-AD.ps1
```

2.3.2. Content

```
$RootCACert="D:\PKIData\ABC Org Root CA.crt"
certutil -dspublish -f $RootCACert RootCA
certutil -pulse
```

2.3.3. Explanation

The script publishes the ABC Org Root CA certificates into the relevant Active Directory (IL3 or IL4) from where it is propagated to the Trusted Root Certification Authority Store of all domain joined computers.

Note: A batch file that provides the same functionality is provided to utilise in situations where PowerShell is not available.

Note: This command is for use out-of-band of the key ceremony – there is a command in the flow of the key ceremony which achieves this same objective

2.4. Publishing Class 3 CA Material to Active Directory

2.4.1. Command

```
..\Commissioning\ADPrep\Publish-Class3-CA-Material-to-AD.ps1
```

2.4.2. Content

```
$Class3PrimaryCACert="D:\PKIData\ABC Org Class 3 Primary CA.crt"
$Class3SecondaryCACert="D:\PKIData\ABC Org Class 3 Secondary CA.crt"
certutil -dspublish -f $Class3PrimaryCACert SubCA
certutil -dspublish -f $Class3PrimaryCACert NTAuthCA
certutil -dspublish -f $Class3SecondaryCACert SubCA
certutil -pulse
```

2.4.3. Explanation

The script publishes the Class 3 CA certificates into the relevant Active Directory (IL3 or IL4). Both Class 3 CA certificates are published into the SubCA container, from where they are propagated to the Trusted Root Certification Authority Store of all domain joined computers.

The Class 3 Secondary CA certificate is not published to the NTAuthCA container, hence eliminating its certificates from being candidates for use in smart card logon to Windows.

3. HSM Scripts

3.1. Enable Logging

3.1.1. Command

```
..\Commissioning\HSM\01.Enable-CNG-Logging.ps1
```

3.1.2. Content

```
new-Item -Name "Cryptography"  -Path "HK1M:\SOFTWARE\nCipher\"  -type Directory -Force
New-ItemProperty -Path HK1M:\SOFTWARE\nCipher\Cryptography -Name LogLevel -PropertyType dword
-Value "2" -Force
Some-Content
```

3.1.3. Explanation

The commands create a new registry sub-key, then two keys which are used to create a log path for both CAPI and CAPI2 logging from nCipher (Thales) software.

3.2. Enable Interactive Services

3.2.1. Command

```
..\Commissioning\HSM\01.Enable-UI0-Service.ps1
```

3.2.2. Content

```
Some-Content
```

3.2.3. Explanation

The command enables the use of Interactive Services capability, which is leveraged by nCipher software.

3.3. Diagnostics

3.3.1. Command

```
..\Commissioning\HSM\HSM-Diagnostics.ps1
```

3.3.2. Content

```
Some-Content
```

3.3.3. Explanation

The commands generate a set of diagnostic outputs validating HSM connectivity.

3.4. Licences

3.4.1. Command

```
..\Commissioning\HSM\Licences\CDE-C104-C9D7-2F9E.txt
```

3.4.2. Explanation

There are two files in the Licences sub-folder – these are placeholders for when client licences are procured from Thales for uploading into the HSM; the client licences will be shipped as “(signed) text files”.

4. PKI

4.1. Remote Server Admin Tools

4.1.1. Command

```
..\Commissioning\PKI\01.Add-ADDS-RSAT-Binaries.ps1
```

4.1.2. Content

```
Some-Content
```

4.1.3. Explanation

The command installs the AD Directory Services remote server administration tools; which are useful to have available for troubleshooting purposes on the AD Certificate Services server.

4.2. Remote Server Admin Tools

4.2.1. Command

```
..\Commissioning\PKI\02.Add-ADCS-CA-Binaries.ps1
```

4.2.2. Content

```
Some-Content
```

4.2.3. Explanation

The command installs the Certification Authority component of the AD CS role.

5. Root CA

5.1. CAPolicy

5.1.1. Command

```
..\Commissioning\PKI\RootCA\A.00.Root-CA-CAPolicy.inf
```

5.1.2. Content

```
Some-Content
```

5.1.3. Explanation

The script specifies the following:

- Empty CRL and AIA extensions in the Root CA certificate
- Renewal key length and validity periods
- keyUsage of certificate and CRL signing (specified in Base64 encoding)
- keyUsage marked as critical

5.2. Set TCP Address

5.2.1. Command

```
..\Commissioning\PKI\RootCA\A.01.Set-TCPIP-Address.ps1
```

5.2.2. Content

```
Some-Content
```

5.2.3. Explanation

The command assigns a static IP address to the loopback interface of the Root CA guest.

5.3. Report TCP Address

5.3.1. Command

```
..\Commissioning\PKI\RootCA\A.02.Report-TCPIP-Address.ps1
```

5.3.2. Content

```
Some-Content
```

5.3.3. Explanation

The command reports the TCP/IP address set in the previous step.

5.4. Implement Root CA (Validation Only)

5.4.1. Command

```
..\Commissioning\PKI\RootCA\B.01a.Root-CA-Implement-ADCS-CA-WhatIf.ps1
```

5.4.2. Content

```
Some-Content
```

5.4.3. Explanation

The command executes a dry-run installation of the Root CA configuration – validating pre-requisites such as HSM connectivity (the –WhatIf paraABCer prevents the command from making state changes).

5.5. Implement Root CA (For Real)

5.5.1. Command

```
..\Commissioning\PKI\RootCA\B.01b.Root-CA-Implement-ADCS-CA.ps1
```

5.5.2. Content

```
Some-Content
```

5.5.3. Explanation

The command executes the installation of the Root CA; it specifies the following:

- Enabling administrator interaction (top enter pass phrases for OCS cards)
- CA type: Standalone
- Subject naming information
- RSA key length of 4,096 bits
- Hash algorithm of SHA256
- KSP: nCipher
- Validity period of twenty years

5.6. Set AIA and CDP Extensions

5.6.1. Command

```
..\Commissioning\PKI\RootCA\B.02.Root-CA-Set-IDP.ps1
```

5.6.2. Content

```
Some-Content
```

5.6.3. Explanation

The command specifies the following:

- Removes default AIA and CDP extensions
- Specifies (two) CRL publication locations (not added to CDP extensions)
- Specifies the four mandated CDP extensions to be included in issued certificates
- Specifies the four mandated AIA extensions to be included in issued certificates

5.7. General Configuration

5.7.1. Command

```
..\Commissioning\PKI\RootCA\B.03.Root-CA-Configure.ps1
```

5.7.2. Content

```
Some-Content
```

5.7.3. Explanation

The command specifies the following:

- CRL validity period (190 days)
- CRL overlap, CRL clock skew (zero)
- Disables delta CRL publication
- Certificate validity period (10 years)
- CA audit filtering (enable all CA audit categories)
- Windows Server audit filtering (enable all certificate services audit categories)
- Disable automatic cross-certificate generation (when performing a re-key)
- Disable CRL deletion after a re-key
- Set lowest level of certificate serial number *complexity*
- Specify default hash algorithm
- Enable specification of critical key usage (to facilitate ABC specification of keyUsage in subordinate CA certificates)
- Enable CAPI2 logging
- Create a dependency on the ADCS service of the nFast server service
- Enable automatic start of “Interactive Services”
- Set ADCS to start manually – to allow OCS submission

5.8. Diagnostics

5.8.1. Command

```
..\Commissioning\PKI\RootCA\C.01.Root-CA-Diagnostics.ps1
```

5.8.2. Content

```
Some-Content
```

5.8.3. Explanation

The command performs the following:

- Generates a set of “certutil” diagnostic duABC
- Exports the ADCS registry key
- Performs HSM diagnostic duABC

5.9. Backup

5.9.1. Command

```
..\Commissioning\PKI\RootCA\D.01.Root-CA-Backup.ps1
```

5.9.2. Content

```
Some-Content
```

5.9.3. Explanation

The script performs the following:

- Creates a backup destination folder with the current date / time
- Publishes a fresh CRL, then waits five seconds
- Performs an AD CS database backup to the previously created destination path
- Exports the AD CS registry key

6. Class 3 Primary CA

6.1. CAPolicy

6.1.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\A.00.Class3-Primary-CA-CAPolicy.inf
```

6.1.2. Content

```
Some-Content
```

6.1.3. Explanation

The script specifies the following:

- Renewal key length and validity periods
- Disable loading of default certificate templates
- Set Basic Constraints extension values (critical with a zero path length)
- Specify certificate policies asserted in the CA certificate
- keyUsage of certificate and CRL signing and digital signature (specified in Base64 encoding)
- keyUsage marked as critical

6.2. Implement Class 3 Primary CA (Validation Only)

6.2.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\A.01a.Class3-Primary-CA-Implement-ADCS-CA-WhatIf.ps1
```

6.2.2. Content

```
Some-Content
```

6.2.3. Explanation

The command executes a dry-run installation of the Class 3 Primary CA configuration – validating pre-requisites such as HSM connectivity (the –WhatIf paraABCer prevents the command from making state changes).

6.3. Implement Class 3 Primary CA (For Real)

6.3.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\A.01b.Class3-Primary-CA-Implement-ADCS-CA.ps1
```

6.3.2. Content

```
Some-Content
```

6.3.3. Explanation

The command executes the installation of the Root CA; it specifies the following:

- Enabling administrator interaction (top enter pass phrases for OCS cards)
- CA type: Enterprise subordinate
- Subject naming information
- RSA key length of 2,048 bits
- Hash algorithm of SHA256
- KSP: nCipher
- Validity period of ten years
- CSR file name

6.4. Set AIA and CDP Extensions

6.4.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\A.02.Class3-Primary-CA-Set-IDP.ps1
```

6.4.2. Content

```
Some-Content
```

6.4.3. Explanation

The command specifies the following:

- Removes default AIA and CDP extensions
- Specifies (three) CRL publication locations (not added to CDP extensions) – the LDAP location is used for CRL expiry validation
- Specifies the four mandated CDP extensions to be included in issued certificates
- Specifies the four mandated AIA extensions to be included in issued certificates

6.5. General Configuration

6.5.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\A.03.Class3-Primary-CA-Configure.ps1
```

6.5.2. Content

```
Some-Content
```

6.5.3. Explanation

The command specifies the following:

- Creates CRL publication folder
- CRL validity period (48 hours)
- CRL overlap (48 hours)
- CRL clock skew (zero)
- Disables delta CRL publication
- Certificate validity period (3 years)
- CA audit filtering (enable all CA audit categories)
- Windows Server audit filtering (enable all certificate services audit categories)
- Enable auditing of certificate template objects
- Disable automatic cross-certificate generation (when performing a re-key)
- Disable CRL deletion after a re-key
- Set lowest level of certificate serial number *complexity*
- Allow subject alternative name (SAN) to be included in scripted certificate requests
- Enable down-level certificate enrolment (support for Windows Server 2003)
- Suppress certificate template OIDs from issued certificates
- Specify default hash algorithm
- Enable specification of critical key usage (to facilitate ABC specification of keyUsage in subordinate CA certificates)
- Specify CA Exchange CSP – to prevent bug whereby the CA CSP (nCipher) would otherwise be used
- Enable CAPI2 logging
- Create a dependency on the ADCS service of the nFast server service
- Enable automatic start of “Interactive Services”
- Set ADCS to start manually – to allow OCS submission

6.6. Capicom

6.6.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\A.04.Register-CAPIcom.ps1
```

6.6.2. Content

```
Some-Content
```

6.6.3. Explanation

Register the CAPIcom DLL which is used in the monitoring capability.

6.7. Submit CSR to Root CA

6.7.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\B.02.Subordination-Submit-CSR-to-Root-CA.ps1
```

6.7.2. Content

```
Some-Content
```

6.7.3. Explanation

Submits the Class 3 Primary CA CSR to the Root CA.

6.8. Approve CSR at Root CA

6.8.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\B.03.Subordination-Approve-CSR-to-Root-CA.ps1
```

6.8.2. Content

```
Some-Content
```

6.8.3. Explanation

Approves the Class 3 Primary CA CSR at the Root CA.

6.9. Retrieve Certificate from Root CA

6.9.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\B.04.Subordination-Retrieve-Certificate-from-Root-CA.ps1
```

6.9.2. Content

```
Some-Content
```

6.9.3. Explanation

Retrieves (exports) the Class 3 Primary CA certificate from the Root CA

6.10. Publish Root CA Certificate to Local

This step is redundant as certificate publication to AD has been performed out-of-band (after the Root CA was commissioned).

6.11. Publish Root CA Certificate to Active Directory

This step is redundant as it has been performed out-of-band (after the Root CA was commissioned).

6.12.Install CA Certificate

6.12.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\D.01.Class3-Primary-CA-Install-Certificate.ps1
```

6.12.2. Content

```
Some-Content
```

6.12.3. Explanation

Installs the Class 3 Primary CA certificate into AD CS – triggering an OCS submission to enable matching to be made with the corresponding private key.

6.13.Configure SMTP Settings

6.13.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\D.02.Class3-Primary-CA-SMTP.ps1
```

6.13.2. Content

```
Some-Content
```

6.13.3. Explanation

Configures the categories of CA events which will trigger the SMTP exit module to send an email; specifies the email server and mail account information to be used.

6.14.Publish Certificate Templates

6.14.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\E.01.Class3-Primary-CA-Publish-Certificate-Templates.ps1
```

6.14.2. Content

```
Some-Content
```

6.14.3. Explanation

Publishes the relevant ABC Class 3 and National certificate templates at the CA.

6.15.Diagnostics

6.15.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\F.01.Class3-Primary-CA-Diagnostics.ps1
```

6.15.2. Content

```
Some-Content
```

6.15.3. Explanation

The command performs the following:

- Generates a set of “certutil” diagnostic duABC
- Exports the ADCS registry key
- Performs HSM diagnostic duABC

6.16.Create Promulgation Scheduled Task (1)

6.16.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\G.01a.Create-ADCS-CRL-Promulgation-1-Task.ps1
```

6.16.2. Content

```
Some-Content
```

6.16.3. Explanation

The command performs the following:

- Creates a scheduled task to run the CRL promulgation (1) script
- Sets the task to run in the context of the local system on Startup

6.17.Create Promulgation Scheduled Task (2)

Identical to the first promulgation task with the exception of specifying a second CRL promulgation script

6.18.Create CRL Monitor Scheduled Task

6.18.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\G.02.Create-ADCS-CRL-Monitor-Task.ps1
```

6.18.2. Content

```
Some-Content
```

6.18.3. Explanation

The command performs the following:

- Creates a scheduled task to run the CRL monitoring (VBS) script
- Specifies arguments to be passed to the monitoring script – namely the CA server hostname and IL4 CDP server hostnames
- Sets the task to run in the context of the local system on every six hours

6.19. Create Database Backup Scheduled Task

6.19.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\G.03.Create-ADCS-Database-Backup-Task.ps1
```

6.19.2. Content

```
Some-Content
```

6.19.3. Explanation

The command performs the following:

- Creates a scheduled task to run the AD CS database backup script
- Sets the task to run in the context of the local system at 11pm every day

6.20. Create Backup Purge Scheduled Task

6.20.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\G.04.Create-ADCS-Backup-File-Purge-Task.ps1
```

6.20.2. Content

```
Some-Content
```

6.20.3. Explanation

The command performs the following:

- Creates a scheduled task to run the database backup folder purge script
- Sets the task to run in the context of the local system at 10pm once per week on a Sunday
- Specifies paraABCers for sending email confirmation
- Specifies purge paraABCer of thirty days

6.21. Run Scheduled Tasks (Ad Hoc)

6.21.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\G.05.Start-Scheduled-Tasks-on-Demand.ps1
```

6.21.2. Content

```
Some-Content
```

6.21.3. Explanation

The command executes each of the scheduled tasks in turn – rather than waiting for the prescribed schedules.

6.22.CRL Promulgation Run Script (1)

6.22.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\H.01a.Run-ADCS-CRL-Promulgation-1.ps1
```

6.22.2. Content

```
Some-Content
```

6.22.3. Explanation

The script performs the following:

- Specifies the folders to monitored by the RoboCopy command and the destination share folder
- Specifies the monitoring threshold (1 file change)

6.23.CRL Promulgation Run Script (2)

Identical to the first promulgation run script with the exception of specifying a second CRL destination share folder.

6.24.CRL Monitor Run Script

6.24.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\H.02.Run-ADCS-CRL-Monitor.vbs
```

6.24.2. Content

See specific script (too long to paste here).

6.24.3. Explanation

The script performs the following:

- Checks that CRLS for a given set of CA Servers are no more than 25 hours old, in AD & on a given set of IIS servers.
- Specifies custom even log entries to record successful and unsuccessful CRL monitoring results

6.25. CRL Monitoring Run Script (Ad Hoc)

6.25.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\H.02.Run-ADCS-CRL-Monitor-AdHoc.ps1
```

6.25.2. Content

```
Some-Content
```

6.25.3. Explanation

Development file used for tweaking and testing of CRL monitoring script in the event of problems.

6.26. AD CS Database Backup Run Script

6.26.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\H.03.Run-ADCS-Database-Backup.ps1
```

6.26.2. Content

```
Some-Content
```

6.26.3. Explanation

The script performs the following:

- Creates a backup destination folder with the current date / time
- Publishes a fresh CRL, then waits five seconds
- Performs an AD CS database backup to the previously created destination path
- Exports the AD CS registry key
- Mails the backup results to the target email account

6.27. Database Backup Purge Run Script

6.27.1. Command

```
..\Commissioning\PKI\Class3PrimaryCA\H.04.Run-ADCS-Backup-File-Purge.ps1
```

6.27.2. Content

See specific script (too long to paste here).

6.27.3. Explanation

The script provides the following description:

- Script to delete files older than x-days. The script is built to be used as a scheduled task, it automatically generates a logfile name based on the copy location and the current date/time.
- There are two main routines, one to delete the files and a second routine that checks if there are any empty folders left that could be deleted.

7. Certificate Templates

7.1. Export Certificate Templates from AD

7.1.1. Command

```
..\Commissioning\PKI\Templates\00a.Certificate-Template-Export-from-IL4-AD.inf
```

7.1.2. Content

```
Some-Content
```

7.1.3. Explanation

Script used for development only – exports specified certificate templates from Active Directory into LDIF files.

7.2. Import Certificate Templates to AD

7.2.1. Command

```
..\Commissioning\PKI\Templates\A.01a.Certificate-Template-Import-to-IL4-AD.ps1
```

7.2.2. Content

```
Some-Content
```

Note: List of repeated commands is truncated

7.2.3. Explanation

Use DSACLS command to specify the access control lists for the default certificate templates in Active Directory.

7.3. Set ACLs on Custom (Imported) Certificate Templates

7.3.1. Command

```
..\Commissioning\PKI\Templates\A.03a.Certificate-Template-Delegation-Custom-IL4.ps1
```

7.3.2. Content

```
Some-Content
```

7.3.3. Explanation

Use DSACLS command to specify the access control lists for the custom (imported) certificate templates in Active Directory.

7.4. Report Certificate Templates ACLs

7.4.1. Command

```
..\Commissioning\PKI\Templates\ A.04a.Certificate-Template-Reports-IL4.ps1
```

7.4.2. Content

```
Some-Content
```

7.4.3. Explanation

Use DSACLS command to specify the access control lists for the custom (imported) certificate templates in Active Directory.

7.5. Certificate Template Development

ExportCertificateTemplates.ps1, Get-TemplateEffectivePermission.ps1 and ImportCertificateTemplates.ps1 are currently not in use.

8. Development

8.1. Tools

The `..\Commissioning\Tools` folder contains executables and DLLs used AD CS commissioning.

8.2. Cross Certification

The `..\Commissioning\Tools` folder contains scripts that are awaiting verification of cross-certification exercise with PID.

8.3. Manual Enrolment Scripts

The `..\Commissioning\ZEnroll` folder contains a collection of scripts that can be customised and leveraged for ad hoc (manual) certificate enrolment.