securosys

SWISS SECURITY TECHNOLOGIES
FOR COMMUNICATIONS SYSTEMS

Securing Microsoft Web Server (IIS)

Internet Information Services
Using Primus Hardware Security Module
Application Note

Primus HSM Integration Guide for
Microsoft Windows Server 2016/2012R2

Securosys SA, Förrlibuckstrasse 70
CH-8005 Zürich, Switzerland
Tel. +41 44 552 31 00 • www.securosys.ch
info@securosys.ch

Microsoft Partner

securosys

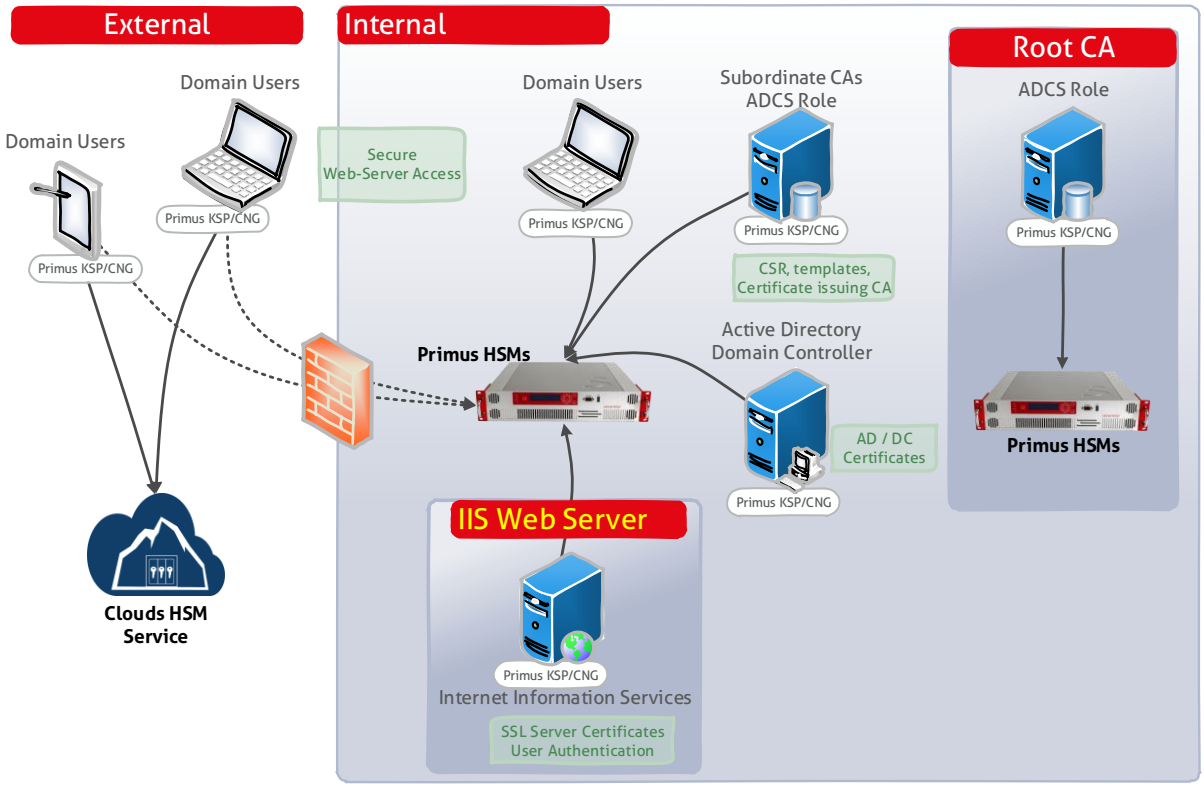
Table of Contents

1 Introduction

This document describes how to secure the private keys used for the Microsoft Internet Information Services (IIS) by using the Securosys Primus HSM or Clouds HSM service.

Internet Information Services (IIS) for Windows Server is a flexible, secure and manageable Web server for hosting anything on the Web. IIS can communicate with MS SharePoint, Visual Studio .NET, ASP.NET and Web Distributed Authoring and Versioning (WebDAV).

The MS Cryptography Next Generation (CNG) API supports Cryptographic Algorithm Providers and Key Storage Providers (KSP) in software and hardware. This allows the Internet Information Services to create and handle private keys and related cryptographic functions on Hardware Security Modules, thereby fulfilling new compliance requirements (e.g. GDPR).



The Primus Hardware Security Modules (HSMs) from Securosys improve drastically the security of Microsoft Internet Information Services, and all applications based on Microsoft CNG API.

The Primus HSMs are built to securely generate and store true random cryptographic keys, providing a central, certified secure storage. They also control and regulate access to the keys and the related cryptographic functionality. The Primus HSM combined with IIS meets or exceeds the best practice security requirements and is one step ahead of fulfilling your compliance demands by providing:

- Hardware-based secure generation of true random cryptographic keys
- Central and highly secure storage of cryptographic keys

- Load balancing and fail-over by clustering the HSMs
- Controlled and regulated access to the keys
- Hardware acceleration of cryptographic operations such as encryption, authentication, and digital signatures, relieving the host server of processor intensive computations
- Scalable performance at manageable cost

All certificate issuance and validation processes occur within the protected confines of the HSM. Private keys are never accessible outside the HSM.

The Primus HSM can easily be integrated in a Microsoft Windows system by installing the Primus CNG Provider. This enables all Windows servers and clients to generate and store their private keys and certificates securely in the HSMs, and perform all related cryptographic functionality, like signing or certificate validation, hardware accelerated on the Primus HSM.

1.1 Requirements

- Windows Server 2008R2, Windows 7 or higher
- Internet Information Services 7.5 or higher
- Primus HSM V2.6 or higher
- Securosys Primus HSM or Clouds HSM with CNG/KSP Provider V1.21.4 or higher, installed and configured

1.1.1 Software and Hardware Used for this Setup

- Virtualization Software (VMWare Workstation 14.1.2)
- Windows Server 2016/x64 (1607) and Internet Information Services 10.0.14393, with latest patches installed
- Securosys KSP Provider V1.21.4
- Securosys Primus-X HSM V2.6.x

1.2 References and More Information

- For more information about OS support, contact your Microsoft sales representative or integration partner.
- For more information about HSM administration, refer to the Primus HSM User Guide or contact Securosys support.
- The official Microsoft IIS Site: https://www.iis.net/

2 Procedures

This procedure provides a straightforward integration process, which has been tested. Please take notice that there may be other ways to achieve interoperability. This guide assumes that you are familiar with the Primus HSM, the Microsoft Internet Information Services and certificates. For the sake of simplicity only the domain administrator role is used instead of the IIS management roles defined by Microsoft.

Note: Throughout this guide, the term HSM refers to Securosys Primus HSM products.

2.1 Securosys Primus HSM Setup

Setting-up the Securosys Primus HSM hardware or your Clouds HSM partition is not part of this application note. Please refer to the corresponding Quick Start Guides and User Manuals.

2.1.1 Installing the Primus HSM CNG/KSP Provider

Download and install the latest CNG/KSP Provider from the Securosys support portal. Configure and test the Primus or Clouds HSM connections using the Securosys Key Storage Provider Configuration application.

For details regarding installation and configuration of the CNG/KSP Provider consult the application note "PrimusHSM_CNGInstallation_AN", downloadable at the Securosys support portal.

2.2 Internet Information Service, Generating and Installing the Certificate

As the IIS 10 Manager does not yet support creation of certificates protected by CNG keys on the graphical user interface, these keys and certificates need to be created using the command line utility certreq.exe.

There are slightly different approaches depending on the used certification authority (e.g. MS ADCS) and the validity range of the certificates (internal/public). The section below differentiates between the following two scenarios:

- using an internal Microsoft PKI infrastructure (ADCS, requires template definitions)
- using a public certificate, signed by an official public certification authority (CA)

2.2.1 Preparing the Certificate Signing Request Input File

To generate a request for an SSL certificate linked to the appropriate private key stored on the Primus HSM, create and prepare the input file for the certreq.exe tool.
The sample file *iis-certrequest.inf* below is intended to issue a certificate for a secure web server serving *https://test.demo-iss.hsmdemo.test* using the MS ADCS template WebServerHSM3:

```
[Version]
Signature= "$Windows NT$"
[NewRequest]
```

```
Subject = "CN=test.demo-iis.hsmdemo.test,O=hsmdemo,OU=IT,L=Zuerich,S=ZH,C=CH"
FriendlyName = "IIS Demo Certificate on Primus HSM"
MachineKeySet = True
Exportable = FALSE
HashAlgorithm = SHA256
KeyAlgorithm = RSA
KeyLength = 4096
KeyUsage = 0xa0
ProviderName = "Securosys Primus HSM Key Storage Provider"
KeyContainer = "iisdemokey"
;RequestType = PKCS10
;ValidityPeriod = Years
;ValidityPeriodUnits = 1
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
[RequestAttributes]
CertificateTemplateName = WebServerHSM3
```

Update the following values:

- **Subject**, replace with your real data
- **KeyContainer** – define your key container ID (visible key name on the HSM) or remove the line for default values
- Adapt the algorithms according to your requirements
- **RequestType** – comment-out if you want to use a public signed certificate (PKCS10)
- Define additional extensions if required
- **CertificateTemplateName** –required if using MS ADCS

2.2.2 Generating the Certificate Signing Request using Internal Microsoft PKI (ADCS)

This step applies only in case using MS Active Directory Certificate Services (ADCS) to sign the CSR.

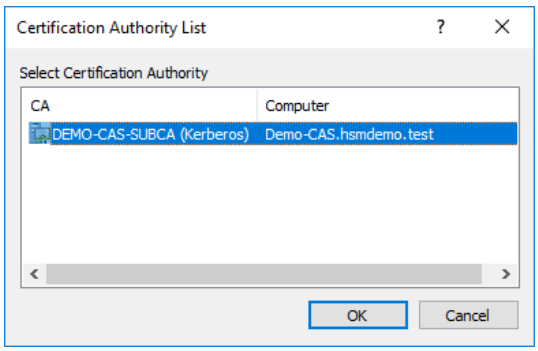
- Adapt the iis-certrequest.inf file
  - comment-out or delete the line with "`;RequestType = PKCS10`"
  - add the section "`[RequestAttributes]`" and the line "`CertificateTemplateName = <yourADCSTemplate>`" (in our example WebServerHSM3, see chapter 3.2)
- Generate the Certificate Signing Request (CSR) to be signed by the MS ADCS SubCA:

```
certreq.exe -new iis-certrequest.inf iis-certrequest.req
CertReq: Request Created
```

- Submit the certificate signing request to the MS SubCA with the following command:

```
certreq.exe -submit -attrib "CertificateTemplate:<yourADCSTemplate>" iis-certrequest.req
Active Directory Enrollment Policy
  {5DA464A9-C243-4515-BA8D-7137CFEC7B17}
  ldap:
RequestId: 77
```

- You are prompted to select the issuing CA



- Depending on the certificate template settings, the certificate is issued immediately or has to be confirmed by a CA administrator.
  - If issued immediately you get the file save dialog to store the issued certificate.
  - Otherwise note the certificate RequestId: Retrieve the certificate from the SubCA with the following command:

```
certreq -retrieve <number> <certificateFilename.cer>
```

where `<number>` is the next sequential certificate request to the issuing SubCA.

2.2.3 Generating the Certificate Signing Request (CSR) using Public CA

This step applies only when using a public certification authority to sign the CSR.

- Adapt the iis-certrequest.inf file
  - uncomment/add the line "`RequestType = PKCS10`"
  - comment-out/delete the line with "`CertificateTemplateName = <yourADCSTemplate>`"
- Generate the Certificate Signing Request (CSR) to be signed by a public certification authority:

```
certreq -new iis-certrequest.inf iis-certrequest.csr
```

- Sign the resulting CSR file by your certification authority

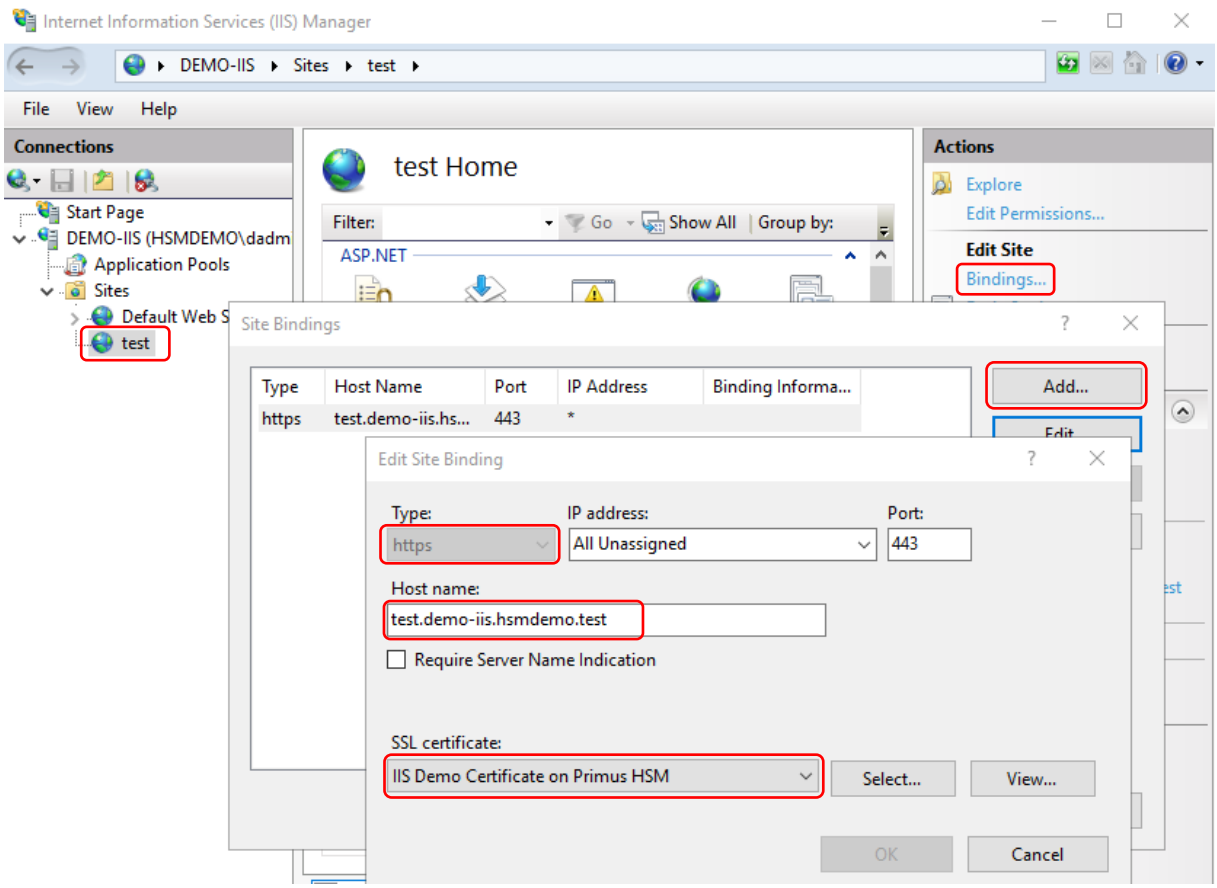
2.2.4 Installing the CA Signed Web Server Certificate

Make the certificate, signed by the certification authority, available for use in IIS:

```
certreq.exe -accept -machine <certificateFilename.cer>
```

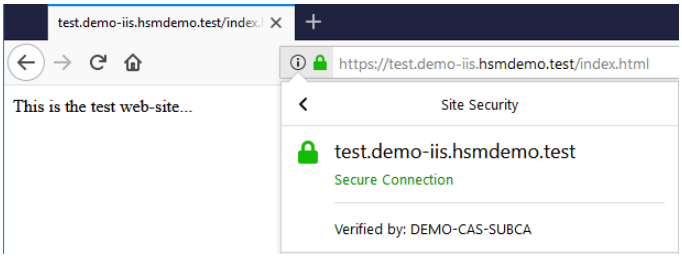
Where `<certificateFilename.cer>` is the binary signed certificate received from the CA/SubCA.

2.2.5 Binding the Certificate with a Secure IIS Web Server



To bind the certificate with a secure IIS Web Server:

- Open the IIS Manager from Start > Administrative Tools > Internet Information Services (IIS) Manager.
- Under Sites on the left-hand side of the IIS Manager Window, select the desired Web site (test).
- On the right-hand side of the IIS Manager, click **Bindings**.
- In the Site **Bindings** window, click **Add**.
- Select the protocol Type as **https**.
- Select IP address of the machine running IIS from the IP Address drop-down list.
- Select the certificate from the drop-down list (using Certificate Friendly Name).
- To complete the certificate binding for SSL connection, click **OK**.
- Open a browser and type the URL e.g. https://test.demo-iss.hsmdemo.test.



If a certificate error is shown, check the certificate details, if the corresponding root certificate is installed and the CRL chain can be verified.

3 Appendix

3.1 IIS Installation with PowerShell

On Windows Server 2016 the IIS can be installed via GUI or PowerShell.

Open the PowerShell with administrative privileges and run the cmdlet as shown below:

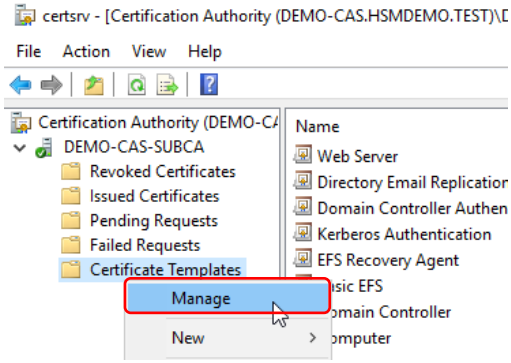
```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

3.2 MS ADCS Certificate Templates

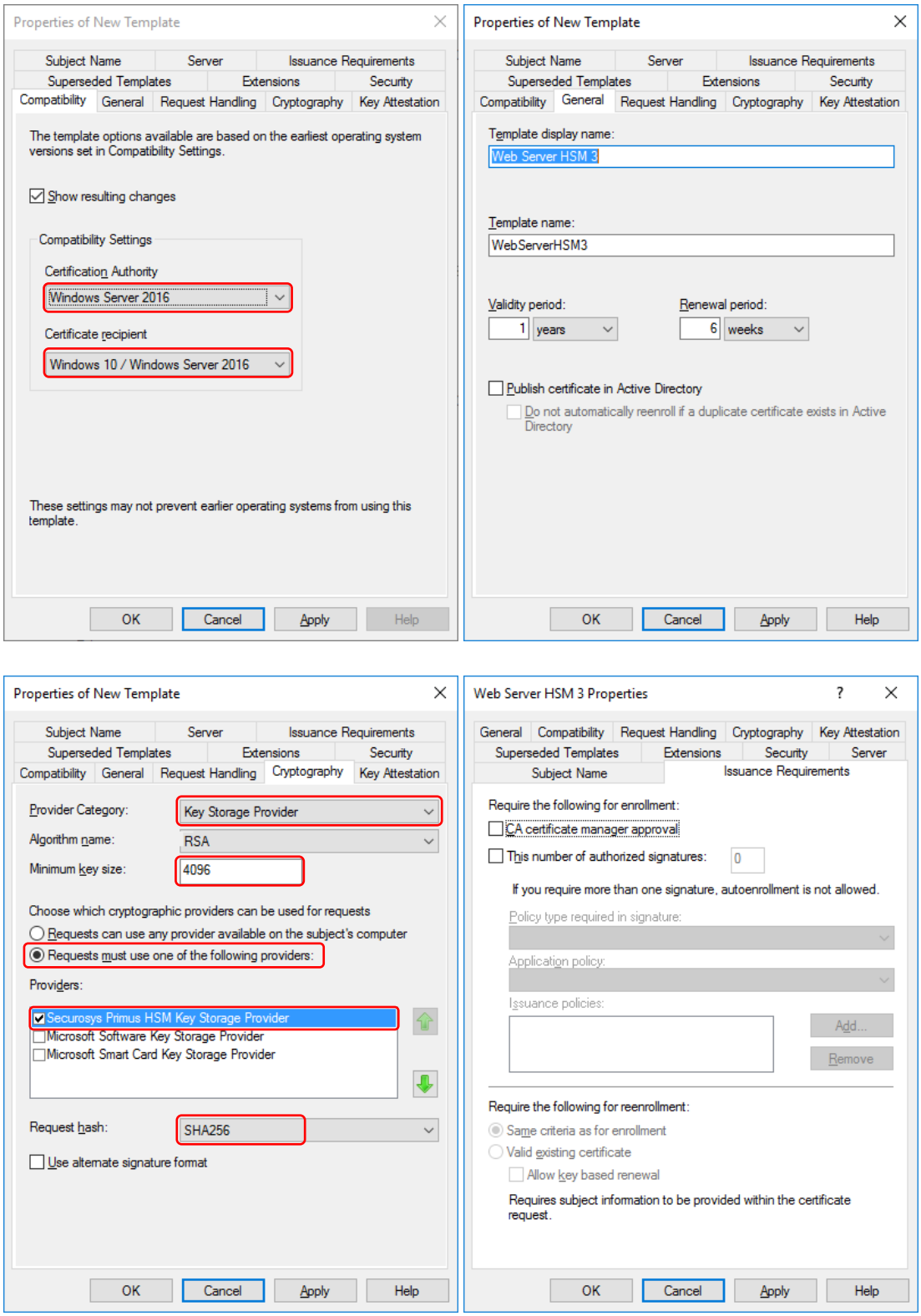
Microsoft ADCS (Enterprise CA) provides several certificate templates, stored in Active Directory, to use as a starting point (see also Application Note PrimusHSM_MS-PKI-ADCS_AN). These templates predefine common properties to apply (e.g. CNG provider, key length, validity, auto-enrollment, etc.) and are also used to define the enrollment policy on the CA. An Enterprise CA can only issue certificates based upon the templates it is configured to use. When requesting a certificate, a client can just specify the template name in the request and the CA will build the certificate based upon the requestor's information in Active Directory and the properties defined in the template. Version 3 templates are required to support the CNG (HSM).

3.2.1 Modifying and Deploying the Certificate Request Templates

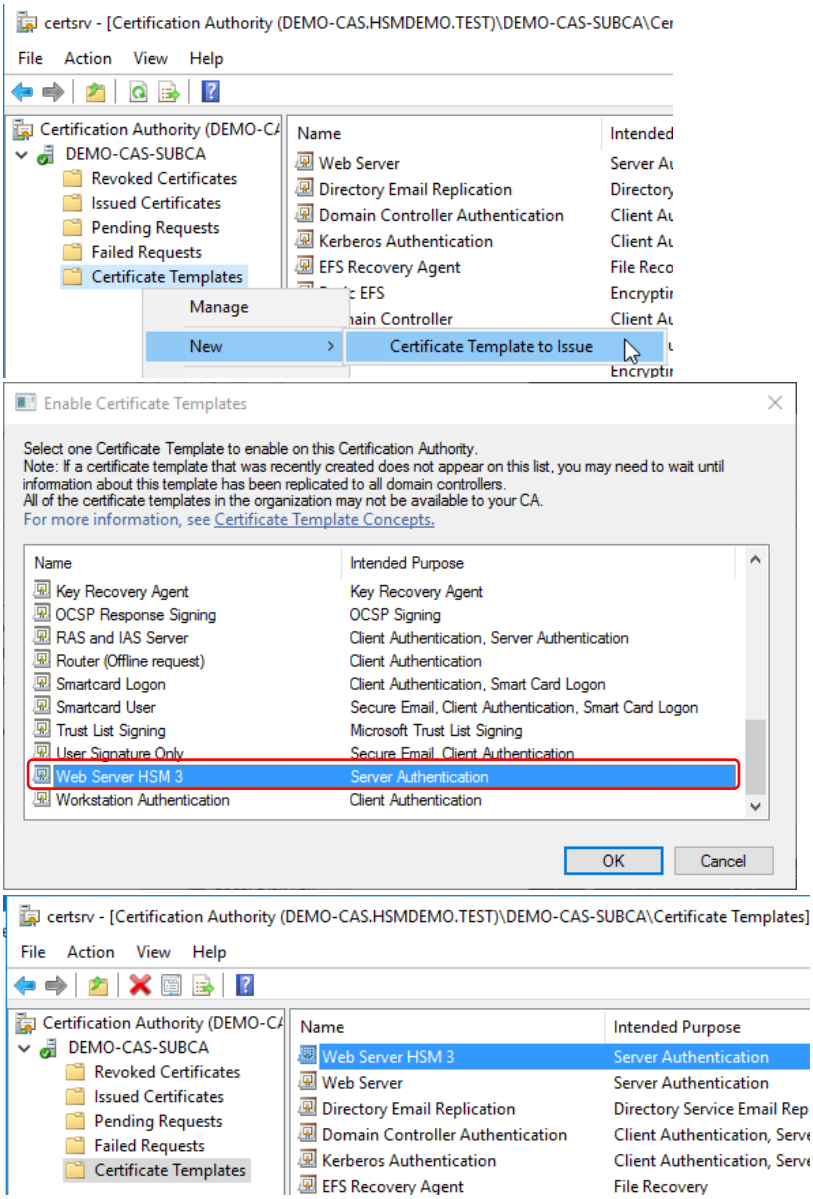
- On the subordinate CA server, open the CA console (certsrv), right-click **Certificate Templates** and select **Manage**.



- Choose your target template (e.g. Web Server), right-click and select **Duplicate Template**. Modify the definitions according your needs (Compatibility, General settings, Cryptography). The following is a sample template definition, using Securosys HSM as Key Storage Provider.
  Note: CNG requires compatibility settings for at least Windows Server 2008R2 or higher.



- Then publish the modified templates for issuing certificates. This is done from Certificate Templates folder of CA console. Right-click **Certificate Templates**, click **Certificate Template to Issue** and select the templates to publish, then click **OK**. The steps are depicted below:

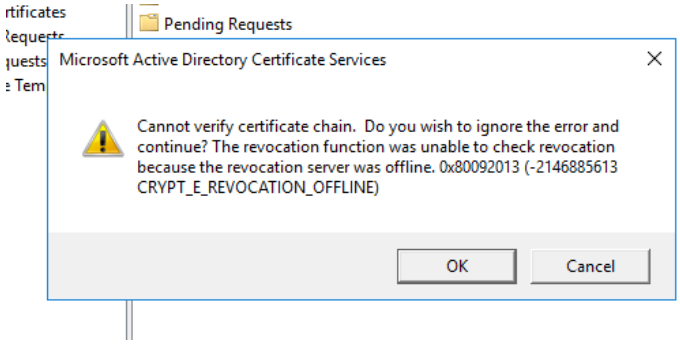

certsrv - [Certification Authority (DEMO-CAS.HSMDEMO.TEST)\DEMO-CAS-SUBCA\Cer
File Action View Help
Certification Authority (DEMO-CA
DEMO-CAS-SUBCA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended
Web Server
Directory Email Replication
Domain Controller Authentication
Kerberos Authentication
EFS Recovery Agent
Manage
New
Certificate Template to Issue
Enable Certificate Templates
Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.
Name
Intended Purpose
Key Recovery Agent
Key Recovery Agent
OCSP Response Signing
OCSP Signing
RAS and IAS Server
Client Authentication, Server Authentication
Router (Offline request)
Client Authentication
Smartcard Logon
Client Authentication, Smart Card Logon
Smartcard User
Secure Email, Client Authentication, Smart Card Logon
Trust List Signing
Microsoft Trust List Signing
Web Server HSM 3
Server Authentication
Workstation Authentication
Client Authentication
OK
Cancel
certsrv - [Certification Authority (DEMO-CAS.HSMDEMO.TEST)\DEMO-CAS-SUBCA\Certificate Templates]
File Action View Help
Certification Authority (DEMO-CA
DEMO-CAS-SUBCA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended Purpose
Web Server HSM 3
Server Authentication
Web Server
Server Authentication
Directory Email Replication
Directory Service Email Rep
Domain Controller Authentication
Client Authentication, Serve
Kerberos Authentication
Client Authentication, Serve
EFS Recovery Agent
File Recovery

3.3 Troubleshooting

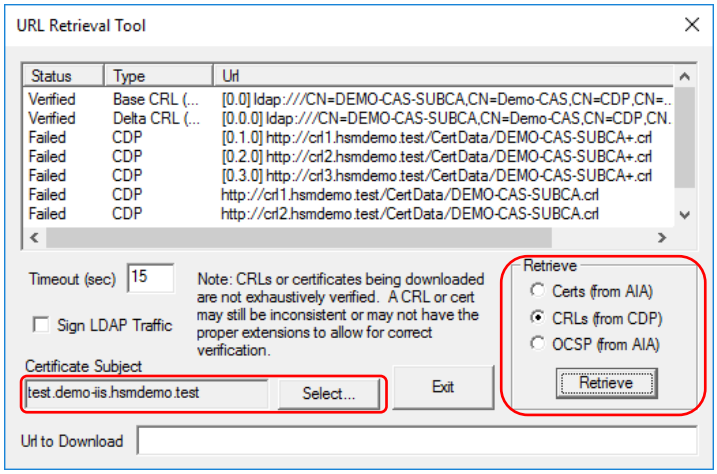
3.3.1 Verify Certificate Revocation List (CRL) Chain

A certificate is by default invalid if the CRL (Delta-CRL) verification fails. This can happen due to

- CRL not retrievable (e.g. wrong configuration or CRL server not reachable)
- CRL or Delta-CRL not renewed/updated within the defined time frame



- In case you get the above message, check if you can retrieve the certificate revocation lists from the known URL or the certificate itself with
  `certutil -URL C:\issdemokey.cer` (filename of the IIS certificate) or
  `certutil -URL http://crlserver.hsmdemo.test/folder/caname.crl`



3.3.2 Helpful Tools

Below is a list of helpful Windows tools:

Tool	Usage, Comment
`certlm.msc`	Certificate manager (local computer/machine)
`certmgr.msc`	Certificate manager (current user)
`certreq.exe`	Certreq can be used to request certificates from a certification authority (CA), to retrieve a response to a previous request from a CA, to create a new request from an .inf file, to accept and install a response to a request, to construct a cross-certification or qualified subordination request from an existing CA certificate or request, and to sign a cross-certification or qualified subordination request.
`certsrv.msc`	Microsoft ADCS (Certification Authority)

`certutil.exe`	Certutil.exe is a command-line program that is installed as part of Certificate Services. You can use Certutil.exe to dump and display certification authority (CA) configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains.
	E.g. to verify CRL, certificates:
	`certutil -URL "http://crl1.hsmdemo.test/certenroll/DEMO-CAR-CA.crl"`
	`certutil -URL C:\issdemokey.cer`
	To dump requests and certificates:
	certutil -dump <certificate.req/cer>
	certutil -repairstore my *

`gpmp.msc`	Change group policy management (e.g. password policy, ...)
`gpupdate.exe`	Refreshes the local computers policy and any Active Directory-based Group policies (e.g. gpupdate /force)
`hsmcons.exe`	KSP/CNG test tool for the Primus HSM (within the Debug Build Folder ... \SecurosysPrimusKsp_v1.xx.y\bin\Debug\x86\)
`pkiview.msc`	Enterprise PKI MMC snap-in allows to assess and manage the health of a Windows **Enterprise CA** hierarchy
`Rsop.msc`	Resultant Set of Policy utility, to check group policy
`sc query <svcname>`	Service Control query