Peter Brügger, 15.10.2019

Manuelles Enrollment Zertifikate Klasse E System Templates

Anleitung

Version: vom 02.03.2020

Status	in Arbeit	in Prüfung	genehmigt zur Nutzung
	☐	☐	☒

Beteiligter Personenkreis	
Autoren:	Peter Brügger
Genehmigung:	
Benützer/Anwender:	
zur Information/Kenntnis:	

Änderungskontrolle, Prüfung, Genehmigung			
Wann	Version	Wer	Beschreibung
5.03.2014	X.0.5	Juergen Weber	Prozess und Prüfungskriterien in Kapitel 3 Manuelles Enrollment Zertifikate nach Methode 2 der ManApp Templates vom Security Officer anhand des Dokumentes „Enrollment SCOMClient Zertifikate“, eingearbeitet, bewilligt und freigegeben.
13.042015	X0.8	Peter Brügger	Zusammenfügen der Dokumente „Enrollment SCOMClient Zertifikate“, „manuelles Enrollment von KlasseCCE Zertifikaten“ Manuelles Enrollment Zertifikate von ManApp TemplatesX0.9“ zum Dokument Manuelles Enrollment Zertifikate von Klasse E Templates“
30.04.2015	X0.83	Peter Brügger	Input von Pascal Joye eingearbeitet
26.05.2015	X0.84	Peter Brügger	Kapitel 3.1.1 und 4.2.4 Befehl 2 Templatenamen korrigiert, Prozesse von Bullets auf Nummern angepasst
2.06.2015	X0.85	Peter Brügger	Input von Nicolas Monney eingearbeitet
11.06.2015	X0.86	Peter Brügger	Kapitel „Gruppenmanagement für Benutzerobjekte, zum manuellen Enrollment von ManApp Templates“ Erstellt, dazu im Prozess 1-2 Tasks entfernt. Kapitel Voraussetzungen erweitert
16.06.2015	X0.88	Peter Brügger	Input von Mario Muster eingefügt

24.06.2015	V1.0	Beatrice Metaij	CD Bund und PDF-Version
07.07.2015	V1.01	Peter Brügger	Schritt 7 im Prozess Kapitel ”Der Prozess für ManApp Templates nach Methode 2“ eingefügt

\08.07.2015	V1.05	Peter Brügger	Kapitel „Vereinbarung für ManApp und noManApp Templates“ eingefügt Kapitel „Gruppenmanagement für Benutzerobjekte, zum manuellen Enrollment von ManApp Templates“ enfernt.
09.07.2015	V1.10	Peter Brügger	Input von Mario Muster von Version 1.05 eingefügt Enleitung angepasst von ManApp zu noManApp Kapitel „Manuelles Enrollment Zertifikate nach Methode 3 (noManApp Templates)“ eingefügt
13.07.2015	V1.11	Peter Brügger	Certreq Befehl für noManApp Template angepasst
20.07.2015	V1.12	Peter Brügger	Schreibfehler korrigiert und kleine Korrekturen eingefügt
21.07.2015	V1.13	Peter Brügger	Erster Untertitel in Kapitel Methode 2 u 4 umbenannt
30.07.2015	V 1.14	Peter Brügger	Übersicht verbessert
29.10.2015	V 1.15	Peter Brügger	Ablauf nach Methode 3 korrigiert.
14.01.2015	V1.16	Peter Brügger	Kapitel über Wildcard Zertifikate eingefügt
18.04.2017	V1.17	Peter Brügger	Befehl psexec –s –i cmd angepasst auf psexec cmd –s –i Voraussetzungen für manuelles Enrollment nach Methode 3 präzisiert.
12.09.2017	V1.18	Peter Brügger	Wildcard Zertifikat nicht mehr erlaubt, Sachverhalt unter Kap. 1 eingetragen Befehl Certreq -submit -attrib "CertificateTemplate: BVerwE-System-ClientServerAuth-noManApp" config in Methode 4 korrigiert auf Certreq -submit -attrib "CertificateTemplate: BVerwE-System-ClientServerAuth-noManApp" -config
15.10.2019		Peter Brügger	DNS und CA Namen der neuen Issuing CA in Intra ab 20. Nov.2019 in Kapitel 3 u. 5 eingetragen
02.03.2020	V1.2	René Röthlisberger	CA Namen angepasst
23.03.2020	V1.3	René Röthlisberger	Versionsnummer korrigiert
24.03.2020	V1.4	René Röthlisberger	Beispiel-Befehle korrigiert

Inhaltsverzeichnis

1 Einleitung

Die bevorzugte Enrollment Methode von Zertifikaten der produktiven Microsoft Enterprise CA ist autoenrollment.

Manuelles Enrollment wird benötigt, wenn Subject oder SAN im Zertifikat nicht dem Computernamen oder DNS des Systems in Active Directory entsprechen.

Manuelles Enrollment wird ebenfalls benötigt, wenn Windows Systeme nicht Mitglied des Forest Intra oder ADR sind, für UNIX-Server und Workgroup-Server Zertifikate, welche Zertifikate einer Windows Enterprise CA beziehen wollen

Das Verfahren mit autoenrollment wird nicht weiter beschrieben

Diese Anleitung beschreibt das manuelle Enrollment von System-Zertifikaten, welche durch einen CA Certificate Manager approved werden, kurz ManApp Templates genannt oder ohne(no) CA Manager Approval, kurz noManApp Templates ausgegeben werden.

1.1 System-Zertifikate

Für System Zertifikate mit Extended Key Usage: Client Authentication, Server Authentication und Client/Server Authentication werden je 3 Zertifikatstemplates zur Verfügung gestellt

- auto: Templates mit autoenrollment von Zertifikaten
- ManAPP:Templates für manuelles Enrollment von Zertifikaten mit Manager Approval
- noManAPP: Templates für manuelles Enrollment von Zertifikaten ohne (no) Manager Approval

1.1.1 Übersicht: manuelles Enrollment von System-ManApp Templates

Zertifikate von ManApp-Templates werden ausgerollt sofern Prüfkriterien vorhanden sind
Sind keine Prüfkriterien vorhanden, werden Zertifikate von noManApp Templates eingesetzt.

Für das manuelle Enrollment von Zertifikaten der ManApp Templates stehen zwei Methoden zur Verfügung

- Manuelles Enrollment nach Methode 1. In Kapitel 2 beschrieben für Windows-Server welche Member im Forest Intra oder ADR sind.
  Hier wird der Computer-Account auf dem Template über eine universale Gruppe berechtigt.
  Enrollment mit Snap-IN Certificates Computer Account
- Manuelles Enrollment nach Methode 2. In Kapitel 3 beschrieben
  Für Systeme ausserhalb der Forest Intra oder ADR, Workgroup Server oder UNIX Maschinen
  Hier wird der Benutzer-Account auf dem Template über eine universale Gruppe berechtigt
  Enrollment mit Tool wie certreq.exe unter Windows

1.1.2 Übersicht: manuelles Enrollment von System-noManApp Templates

Für das manuelle Enrollment von Zertifikaten der noManApp Templates stehen auch zwei Methoden zur Verfügung.

- Manuelles Enrollment nach Methode 3. In Kapitel 4 beschrieben für Windows-Server welche Member im Forest Intra oder ADR sind.
  Hier wird der Computer-Account auf dem Template über eine universale Gruppe berechtigt.
  Enrollment mit Snap-IN Certificates Computer Account
- Bei dieser Methode meldet der Verantwortliche frühzeitig den Computeraccount (z.B. adb\sb007 für die Berechtigung mit dem erforderlichen Template bei pki-info.admin.ch an.
- Manuelles Enrollment nach Methode 4. In Kapitel 5 beschrieben
  Für Systeme ausserhalb der Forest Intra oder ADR, Workgroup Server oder UNIX Maschinen
  Hier wird der Benutzer-Account auf dem Template über eine universale Gruppe berechtigt
  Enrollment mit Tool wie certreq.exe unter Windows

1.1.3 Vereinbarung für ManApp und noManApp Templates

Ein Enrollment von ManApp oder noManApp Templates erfordert eine unterschriebene Vereinbarung.
In dieser Vereinbarung, werden die Benutzeraccounts und Zertifikatstemplates aufgelistet.
Die Benutzer-Accounts werden über Gruppen auf den definierten Templates berechtigt ein Enrollment auszuführen.
Einer der aufgeführten Benutzer ist der Verantwortliche, um neue Benutzer für das Enrollment hinzuzufügen oder zu löschen. Änderungen werden über pki-info@bit.admin.ch abgewickelt.
Alle Jahre wird die Gruppenmitgliedschaft überprüft und wenn nötig korrigiert.

1.1.4 Wildcard Zertifikate von Templates der Klasse E

Wildcard Zertifikate sind nicht erlaubt!

1.2 Die System Templates (Stand Aug. 2016)

Eine Übersicht der Templates zeigt das Dokument auf
https://www.bit.admin.ch/adminpki/00240/04614/index.html?lang=de

in der rechten Spalte unter “Ausprägungen der Klasse E System Zertifikate“

2 Manuelles Enrollment Zertifikate nach Methode 1 (ManApp Templates)

2.1 Vorgehen Windows Server 2008/2012 oder Windows 7 Member von INTRA\ADR

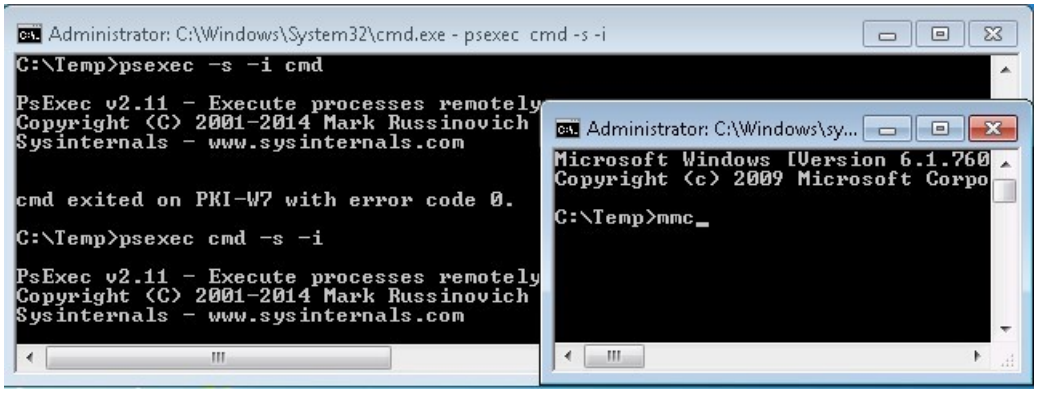
Das Vorgehen dieser Methode wird anhand eines manuellen Enrollments eines Zertifikats für einen Web Server beschrieben.
Dieser Web Server muss Member des Forest Intra oder ADR sein. Je nach Forest ändern die CA-Namen und die DNS-Namen der CA!

2.1.1 Voraussetzungen

- Der Zielserver ist Member des Forest Intra oder ADR
- lokale Admin Rechte
- Der Zielserver benötigt Read / Enroll Rechte auf dem entsprechenden Zertifikatstemplates.
- FQDN und Zertifikatstemplate müssen in der Bestellung angegeben werden
- Das SNAP-In Certificates Computer Account muss im Maschinenkontext ausgeführt werden, dazu

  Command Prompt mit administrator Rechten starten

Psexec cmd –s –i ausführen (ein sysinternals Tool auf Microsoft Homepage)
Im Maschinenkontext Comand Prompt mmc ausführen
Das SNAP-In Certificates Computer Account hinzufügen



- autoenrollment für Maschinen muss auf dem Zielserver aktiviert sein. Feststellen ob autoenrollment über GPO aktiviert ist.
  Zeigt der Registry Key HLM\Software\Policies\Microsoft\Cryptography\AutoEnrollment\AEPolicy, den Wert 7 ist die GPO gesetzt und aktiv.
  Als Übergangslösung kann Autoenrollment auf dem lokalen Server über den Registry Key: HLM\Software\Microsoft\Cryptography\AutoEnrollment\AEPolicy mit Wert 7 temporär aktiviert werden. Nach Abschluss des Enrollments kann der Registry Key wieder zurückgesetzt werden.

2.1.2 Der Prozess für W2008/W2012 Member in den Forest INTRA und ADR

1. Der Antragsteller meldet sein Anliegen mittels einem signierten E-Mail an pkiinfo@bit.admin.ch.
   Folgende Angaben werden im Bestellungsmail erwartet:
   Der Computer Account inkl. Domäne z.B adb\SB90003A auf welchem schlussendlich das manuelle Enrollment durchgeführt wird und Berechtigungen auf dem Template erhält. Diese Maschine muss Member des Forest Intra oder ADR sein Der Namen des Templates, von dem ein Zertifikat bezogen werden soll.
2. pki-info@bit.admin.ch gibt den Auftrag an die CA-Betreiber weiter
3. CA-Betrieb fügt den angegebenen Computer-Account zur entsprechenden universalen Gruppe hinzu, welche Enrollment Berechtigungen für das entsprechende Template vergibt
4. CA-Betrieb schickt dem Antragsteller die Anleitung oder den Link auf die Anleitung auf www.pki.admin.ch mit dem o.k. zu
5. Der Antragsteller führt den Request im MMC-SNAP-IN aus. (siehe unten Kapitel 2.1.2.1) und meldet dies dem CA-Betreiber.
   ACHTUNG:
   Das SNAP-In Certificates Computer Account muss im Maschinenkontext ausgeführt werden
6. CA-Betrieb genehmigt den hängigen Request und informiert den Antragsteller
7. Der Antragsteller führt über das MMC-SNAP-in ein „Automatically Enroll and Retrieve Certificates“ aus (siehe unten Kapitel 2.1.2.2), damit wird das Zertifikat in den Certificate Store des Servers eingefügt.

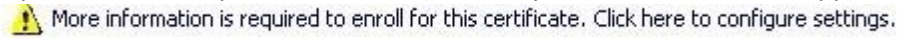
ACHTUNG: damit Schritt 8 erfolgreich ist, müssen folgende 2 Punkte eingehalten werden

- Das SNAP-In Certificates Computer Account muss im Maschinenkontext ausgeführt werden
- Autoenrollment für Maschinen muss aktiviert sein.

8. Mittels E-Mail meldet der Antragsteller an pki-info@bit.admin.ch.den erfolgreichen Abschluss des Enrollment. pki-info@bit.admin.ch orientiert CA-Betrieb
9. pki-info@bit.admin.ch. legt das Bestellungsmail Mail des Antragstellers in einem definierten Folder ab.

2.1.2.1 Beschreibung zum Punkt 5 des Prozesses: MMC-SNAP-IN

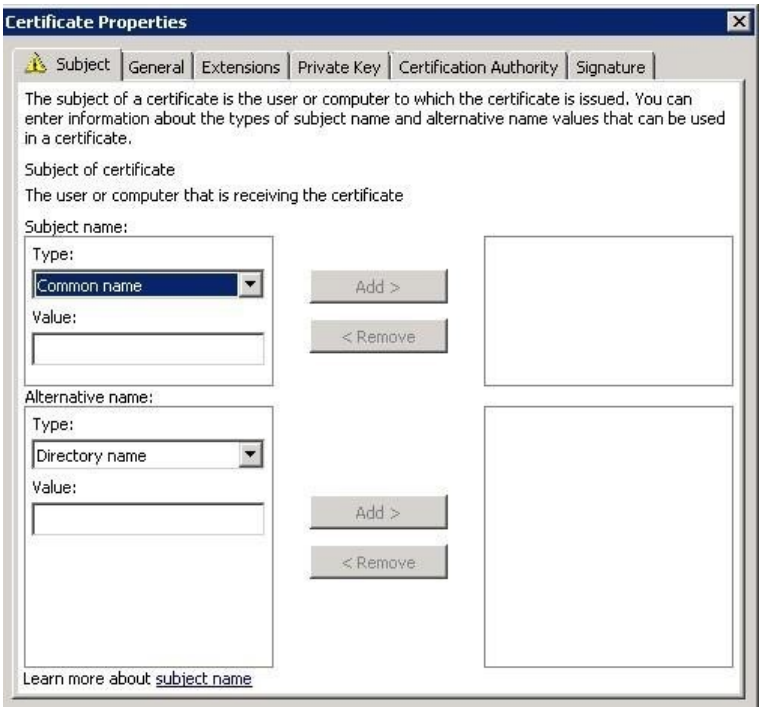
Mit dem MMC-SNAP-IN mmc --> Add/Remove Snap-in --> Certificates --> Computer Account --> Local Computer unter Certificates (Local Computer)--> Personal -> All Tasks --> Request New Certificate entsprechendes Template auswählen (BVerw-System-ServerAuthManApp) und mit Klick auf



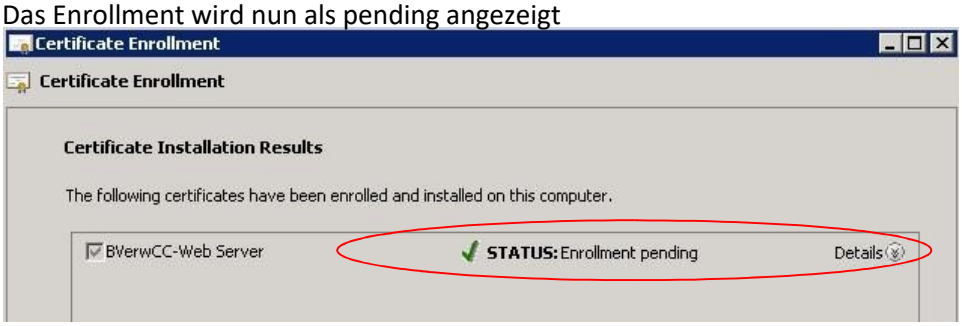
weiterfahren.

ACHTUNG:
Das SNAP-In Certificates Computer Account muss im Maschinenkontext ausgeführt werden.

Unter Subject name: Type: Common name auswählen und in Value die URL des Web-Servers eingeben, mit Add ausführen. Mit Enroll den Request beenden.



Das Enrollment wird nun als pending angezeigt

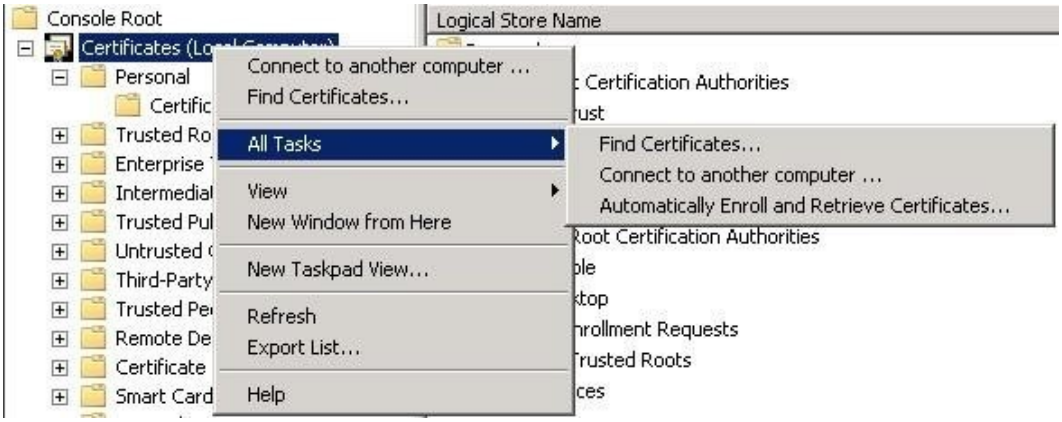


2.1.2.2 *Beschreibung zum Punkt 7 des Prozesses Ausführen von „Automatically Enroll and Retrieve Certificates“*

Der Antragsteller lässt das Zertifikat mit dem MMC-SNAP-IN unter Certificates (Computer Account) -> All Tasks --> Automatically Enroll and Retrieve Certificates in den Certificate Computer Store des Servers einfügen.

ACHTUNG:
Das SNAP-In Certificates Computer Account muss im Maschinenkontext ausgeführt werden.

Damit dieser Schritt erfolgreich durchgeführt werden kann, muss autoenrollment für Maschinen Zertifikate aktiviert sein.



Nach einem <NEXT> wird das unter Punkt 5 ausgewählte Template bereits als markiert angezeigt,

<Enroll> und <FINISH> drücken, das Zertifikat und der private Key befinden sich jetzt im Certificate Computer Store des Servers.

2.1.3 Lifecycle

ACHTUNG: Zertifikat Ablauf nicht verpassen! Das Zertifikat ist 3 Jahre gültig und wird nicht automatisch erneuert!

Der Server-Betreiber ist für den Lifecycle des Zertifikats zuständig.

3 Manuelles Enrollment Zertifikate nach Methode 2 (ManApp Templates)

Das Vorgehen des manuellen Enrollments nach Methode 2 von einem ManApp Template wird anhand eines Beispiels für das Enrollment von SCOM Zertifikate beschrieben. Bei SCOM Servern handelt es sich um Windows Maschinen, darum wird auf das Tool certreq.exe verwiesen.

3.1 Vorgehen Windows Server nicht Intra/ADR Member, UNIX, Workgroup-Server

3.1.1 Voraussetzungen für das Enrollment

Das Vorgehen nach Methode 2 setzt zwei Maschinen voraus:

1. Der Zielserver, dieser Server wird mit einem Zertifikat ausgerüstet und erstellt den Zertifikatrequest und damit den private Key.
    - Auf dem Zielserver muss sich das Root Zertifikat SwissGovernment-E-Root01 im „Trusted Root Certification Authorities“ Store befinden und das Issuing CA Zertifikat SwissGovernment-E-Intra01 im “Intermediate Certification Authorities” Store befinden
2. Ein „Server im Forest Intra“, dieser Server übermittelt den Request zur CA und fordert das signierte Zertifikat von der CA.
    - Anstelle eines Servers kann für diese Tasks auch eine Workstation mit Windows 7 oder höher eingesetzt werden. Mit dieser Maschine werden die Befehle certreq -submit und -retrieve ausgeführt.
    - Der „Server im Forest Intra“ muss fähig sein über autoenrollment Zertifikate von der CA SwissGovernment-E-Intra01 zu beziehen. Damit wird sichergestellt, dass die benötigten Netzwerkprotokolle zur CA offen sind.

3.1.2 Der Prozess für ManApp Templates nach Methode 2

1. Der Antragsteller, der Kunde (der Betreiber des Servers) meldet sein Anliegen mittels einem signierten E-Mail an pki-info@bit.admin.ch.
   Folgende Angaben werden im Bestellungsmail erwartet:
   Der Namen des Templates, von dem ein Zertifikat bezogen werden soll.
2. pki-info@bit.admin.ch gibt den Auftrag an die CA-Betreiber weiter
3. CA-Betrieb schickt dem Antragsteller die Anleitung oder den Link auf die Anleitung auf www.pki.admin.ch mit dem o.k. zu
4. Der Antragssteller Kunde erstellt ein Zertifikatsrequest auf seinem Zielserver. z..B mit certreq -new
5. Der Kunde kopiert den Zertifikatsrequest vom Zielserver auf den „Server im Forest Intra“
6. Der Kunde schickt mittels certreq submit das Requestfile an die CA SwissGovernment-E-Intra01, unter dem im Punkt 1 angegebenen Account. Dieser Task wird auf einem „Server im Forest Intra“ ausgeführt.
7. Der Antragsteller informiert pki-info@bit.admin.ch, wenn der Request erstellt wurde 8.
   CA-Betrieb stellt das Zertifikat aus und benachrichtigt den Antragsteller mit E-Mail
9. Der Kunde holt auf dem Server im Forest Intra, das ausgestellte Zertifikat mit certreq retrieve, mit dem unter Punkt 1 angegebenen Account, von der CA ab.
10. Der Kunde kopiert das Zertifikat vom Server im Forest Intra auf den Zielserver.
11. Der Kunde installiert das Zertifikat auf dem Zielserver, mittels „certreq –acceptS.“ Mittels e-mail meldet der Antragsteller an pki-info@bit.admin.ch den erfolgreichen Abschluss des Enrollment

12. PKI Operation legt das Mail des Antragsteller in einem definierten Folder ab

3.1.3 Templates Konfiguration (als Information)

Template Namen: BVerwE-System-ClientServer-ManApp

US-intraCA-System-ClientServerAuth-ManApp read / enroll

Berechtigungen: über universale Gruppe, welche die Maschinen Objekte enhält

Subject Name Supply in the request “aktiviert”

Issuance Requirements: CA Certificate Manager approval „aktiviert“ Laufzeit

des Zertifikates: 3 Jahre

3.1.4 So könnten die Certreq Befehle aussehen

Befehl 1:
Auf dem Zielserver Request-File erstellen certreq –new SCOM.inf
(vorbereitete INF-Datei) SCOM.req

Befehl 2:
Auf dem Server in Forest Intra Request-file zur CA senden
Certreq -submit -attrib "CertificateTemplate:BVerwE-System-ClientServerAuth-ManApp" -config sf01097a.intra.admin.ch\SwissGovernment-E-Intra01 SCOM.req SCOM.cer

When the certificate is issued, you see RequestId: <number> displayed, where <number> is the next sequential certificate request to the issuing CA. Make a note of this number.

Do not close the command prompt.

Ausstellen des SCOM Zertifikats auf der CA; durch den CA-Admin

Befehl 3:
Auf dem „Server im Forest Intra“wird das das SCOM Server Zertifikat von der CA heruntergeladen.
certreq –retrieve <number> SCOM.cer
For example, if the request number previously displayed was 12, type: certreq –retrieve 12 SCOM.cer
You are prompted to select the issuing CA SwissGovernment-E-Intra01 in the Select Certification Authority dialog box. Select the CA, and then click OK. Click OK to overwrite the existing file.

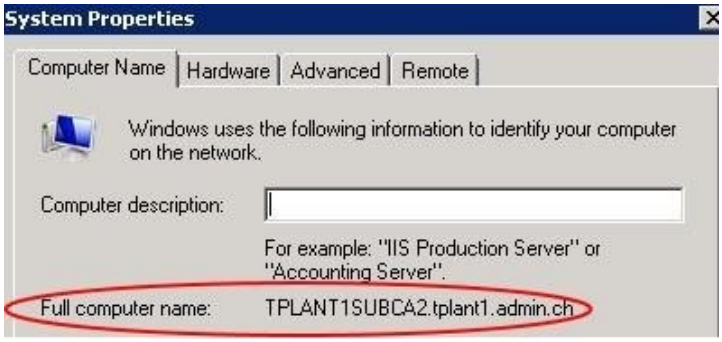
Befehl 4:
Auf dem Zielserver, Installation des Zertifikates certreq –accept
-machine SCOM.cer
Im lokalen Computer Store des Servers ist jetzt ein SCOM Zertifikat bereitgestellt. Dieses Zertifikat muss noch mit der Anwendung verlinkt werden.

3.1.5 Eine INF-Datei als Beispiel für SCOM Zertifikate

[NewRequest]
Subject = "CN=FQDN eintragen [1)]"
MachineKeySet = True
KeyLength=2048
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
FriendlyName="zB.den FQDN oder einen passenden Namen eintragen wie My SCOM Zertifikat" KeySpec=1
[RequestAttributes]

[1)] Grundsätzlich muss unter Subject

- für SCOM-Zertifikate der „Full Computer name“ des Windows Systems angegeben werden, sichtbar unter „System Properties“,“ Computer Name“



- Für Web–Server Zertifikate die URl des Web-Servers z.B. www.pki.admin.ch

3.1.6 Vorhandene Einschränkungen

Es steht nur ein gültiger CDP Path vom Zertifikat zur Verfügung.
Der 1. CDP Pfad ist www.pki.admin.ch/crl und ist überall auflösbar
Der 2. CDP Pfad zeigt auf das Active Directory intra.admin.ch und ist für Server die sich nicht im Forest INTRA befinden nicht auflösbar.

3.1.7 Lifecycle

ACHTUNG: Zertifikat Ablauf nicht verpassen! Das Zertifikat ist 3 Jahre gültig und wird nicht automatisch erneuert! Der Server-Betreiber ist für den Lifecycle des Zertifikats zuständig.

4 Manuelles Enrollment Zertifikate nach Methode 3 (noManApp Templates)

4.1 Vorgehen: Windows Maschinen W2008/W2012/W7 Member von INTRA\ADR

Das Vorgehen dieser Methode wird anhand eines manuellen Enrollments eines Zertifikats für einen Web Server beschrieben.
Dieser Web Server muss Member des Forest Intra oder ADR sein. Je nach Forest ändert der CA-Name und der DNS-Name der CA.

4.1.1 Voraussetzungen

- Die Vereinbarung ist unterschrieben
- Der Zielserver ist Member des Forest Intra oder ADR
- lokale Admin Rechte
- Der Zielserver benötigt Read / Enroll Rechte auf dem entsprechenden Zertifikatstemplates.
- Das SNAP-In Certificates Computer Account muss im Maschinenkontext ausgeführt werden,

- Die entsprechenden Computer-Accounts muss auf dem Template read und enroll Rechte haben.
- Ein „Subject name“ wie im Kapitel 4.1.2.1 beschrieben, muss für ein erfolgreiches enrollment angegeben werden.

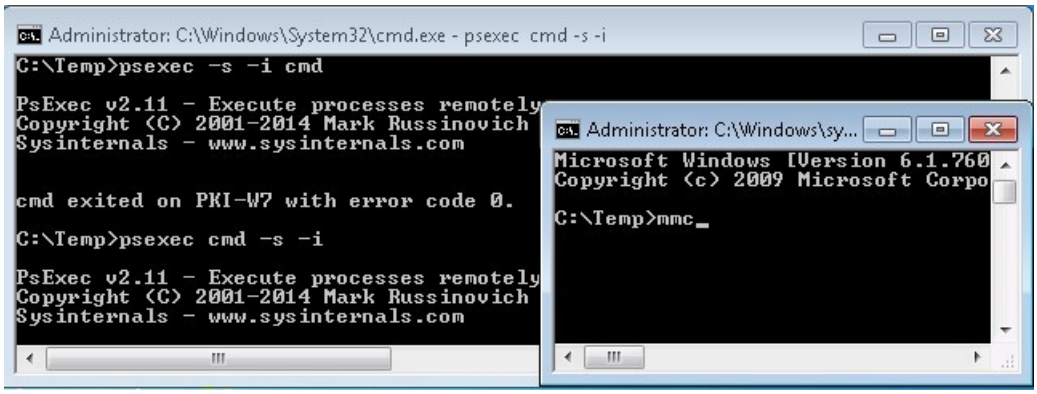
4.1.2 Der Prozess für W2008/W2012 Member in den Forest INTRA und ADR

1. Der Antragsteller führt den Request im MMC-SNAP-IN aus.

   Das SNAP-In Certificates Computer Account muss im Maschinenkontext ausgeführt werden, dazu

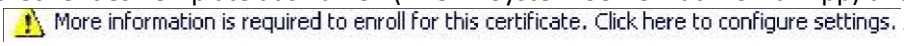
   - Command Prompt mit administrator Rechten starten

   Psexec cmd –s –i ausführen (ein sysinternals Tool auf Microsoft Homepage)
   Im Maschinenkontext Comand Prompt mmc ausführen Das
   SNAP-In Certificates Computer Account hinzufügen



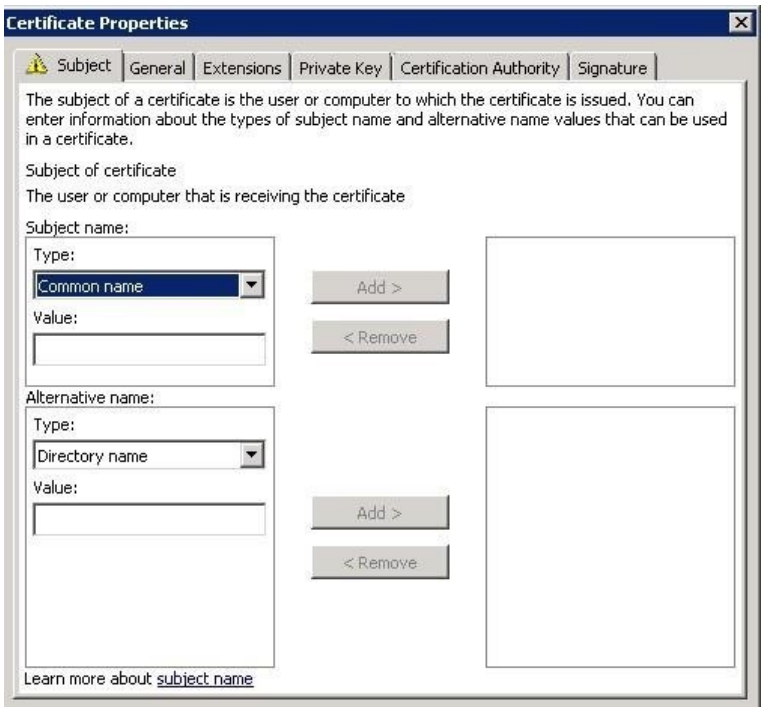
4.1.2.1 Beschreibung zum Punkt 1 des Prozesses: MMC-SNAP-IN

Mit dem MMC-SNAP-IN mmc --> Add/Remove Snap-in --> Certificates --> Computer Account --> Local Computer unter Certificates (Local Computer)--> Personal -> All Tasks --> Request New Certificate entsprechendes Template auswählen (BVerw-System-ServerAuthnoManApp) und mit Klick auf

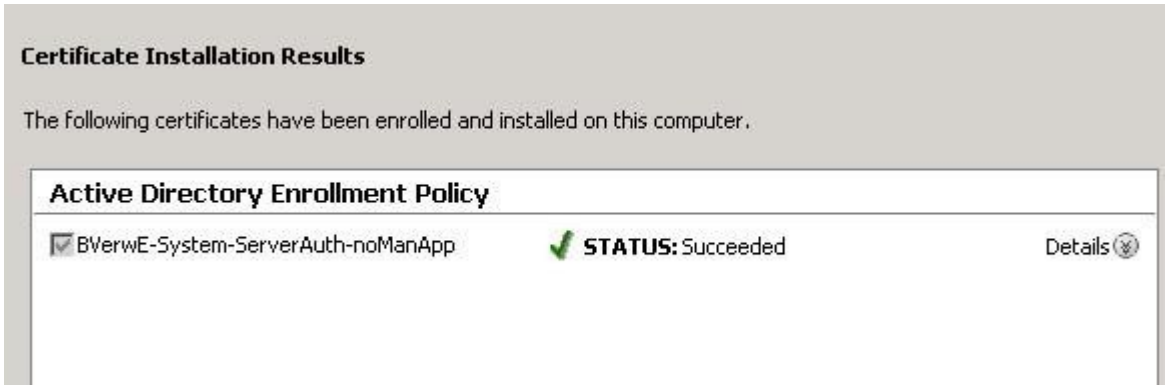


weiterfahren.

Unter Subject name: Type: Common name auswählen und in Value die URL des Web-Servers eingeben, mit Add ausführen. Mit Enroll den Request beenden.



Mit Enroll weiterfahren.



Mit Finish Task beenden

4.1.3 Templates Konfiguration (als Information)

Template Namen: BVerwE-System-Server-noManApp

US-intraCA-System-ServerAuth-ManApp read / enroll

Berechtigungen: über universale Gruppe, welche die Maschinen Objekte enhält

Subject Name Supply in the request “aktiviert”

Issuance Requirements: CA Certificate Manager approval nicht „aktiviert“

Laufzeit des Zertifikates: 3 Jahre

4.1.4 Lifecycle

ACHTUNG: Zertifikat Ablauf nicht verpassen! Das Zertifikat ist 3 Jahre gültig und wird nicht automatisch erneuert!

Der Server-Betreiber ist für den Lifecycle des Zertifikats zuständig.

5 Manuelles Enrollment Zertifikate Methode 4 (no-ManApp Templates)

5.1 Vorgehen

Das Vorgehen des manuellen Enrollments wird anhand eines Beispiels eines Zertifikats für SCOM beschrieben. Bei SCOM Servern handelt es sich um Windows Maschinen, darum wird auf das Tool certreq.exe verwiesen.

5.2 Vorgehen Windows Server nicht Intra/ADR Member, UNIX, Workgroup-Server

5.2.1 Voraussetzungen für das Enrollment

Das Vorgehen nach Methode 2 setzt zwei Maschinen voraus:

3. Der Zielserver, dieser Server wird mit einem Zertifikat ausgerüstet und erstellt den Zertifikatrequest und damit den private Key.
   - Auf dem Zielserver muss sich das Root Zertifikat SwissGovernment-E-Root01 im „Trusted Root Certification Authorities“ Store befinden und das Issuing CA Zertifikat SwissGovernment-E-Intra01 im “Intermediate Certification Authorities” Store befinden
4. Ein „Server im Forest Intra“, dieser Server übermittelt den Request zur CA und fordert das signierte Zertifikat von der CA.
   - Anstelle eines Servers kann für diese Tasks auch eine Workstation mit Windows 7 oder höher eingesetzt werden. Mit dieser Maschine werden die Befehle certreq -submit und -retrieve ausgeführt.
   - Der „Server im Forest Intra“ muss fähig sein über autoenrollment Zertifikate von der CA SwissGovernment-E-Intra01 zu beziehen. Damit wird sichergestellt, dass die benötigten Netzwerkprotokolle zur CA offen sind. Eine Vereinbarung muss unterschrieben sein.

Die in der Vereinbarung angegebenen Service-Accounts müssen read /enroll Rechte auf dem entsprechenden noManApp Template haben.

5.2.2 Der Prozess

1. Der Kunde erstellt ein Zertifikatsrequest auf seinem Zielserver. Für Windowsmaschinen kann das Tool certreq benutzt werden. Der Zertfikatsrequest darf den Template Einstellungen nicht widersprechen
2. Der Kunde kopiert den Zertifikatsrequest vom Zielserver auf den “Server im Forest Intra“
3. Der Kunde schickt mittels certreq submit das Requestfile an die CA SwissGovernment-E-Intra01, dazu muss einer der Benutzer-Accounts oder der Service–Accounts benutzen welche in der Vereinbarung aufgeführt sind. Dieser Task wird auf „dem Server im Forest Intra“ ausgeführt.
4. Die CA erstellt und signiert das Zertifikat und schickt dieses an den „Server im Forest Intra“ zurück, sofern die CA den Request als gültig und nicht fehlerhaft betrachtet.

WICHTIG: Die CA signiert nur bestimmte, dafür vorgesehene Templates, diese Templates sind in der Vereinbarung aufgeführt, diese aber ohne weitere Prüfung.

5. Der Kunde kopiert das Zertifikat auf seinen Zielserver
6. Der Kunde installiert das Zertifikat auf dem Zielserver, mittels „certreq –acceptS.“, falls es sich beim Zielserver und einen Windows Server handelt

5.2.3 Templates Konfiguration (als Information)

Template Namen: BVerwE-System-ClientServer-noManApp

US-intraCA-System-ClientServerAuth-ManApp read / enroll

Berechtigungen: über universale Gruppe, welche die Maschinen Objekte enhält Subject Name

Supply in the request “aktiviert”

Issuance Requirements: CA Certificate Manager approval nicht „aktiviert“ Laufzeit des Zertifikates:

3 Jahre

5.2.4 So könnten die Certreq Befehle aussehen

Befehl 1 Auf dem Zielserver Request-File erstellen certreq –new
SCOM.inf (vorbereitete INF-Datei) SCOM.req

Befehl 2 Auf dem Server in Forest Intra Request-file zur CA senden
Certreq -submit -attrib "CertificateTemplate:BVerwE-System-ClientServerAuth-noManApp" -config sf01097a.intra.admin.ch\SwissGovernment-E-Intra01 SCOM.req SCOM.cer

Befehl 3 Auf dem Zielserver, Installation des Zertifikates certreq –accept machine SCOM.cer

Im lokalen Computer Store des Servers ist jetzt ein SCOM Zertifikat bereitgestellt. Dieses Zertifikat muss noch mit der Anwendung verlinkt werden.

ACHTUNG: Zertifikat Ablauf nicht verpassen! Das Zertifikat ist 3 Jahre gültig und wird nicht automatisch erneuert!

Der Server-Betreiber ist für den Lifecycle des Zertifikats zuständig.

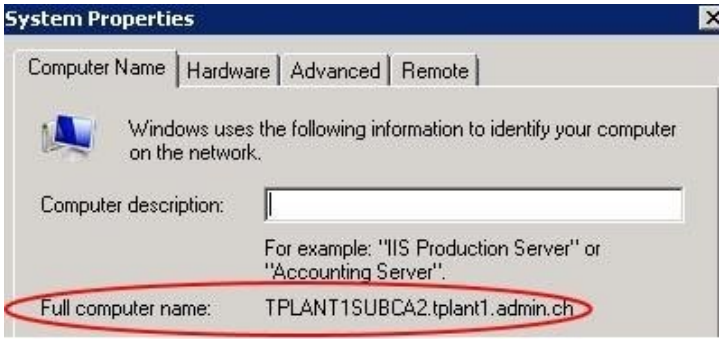
5.2.5 Eine INF-Datei als Beispiel für SCOM-Zertifikate

[NewRequest]

Subject = "CN=FQDN eintragen [1)]"
MachineKeySet = True
KeyLength=2048
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
FriendlyName="zB.den FQDN oder einen passenden Namen eintragen wie My SCOM Zertifikat" KeySpec=1
[RequestAttributes]

[1)] Grundsätzlich muss unter Subject

- für SCOM-Zertifikate der „Full Computer name“ des Windows Systems angegeben werden, sichtbar unter „System Properties“,“Computer Name“



- Für Web–Server Zertifikate die URl des Web-Servers z.B. www.pki.admin.ch

5.2.6 Vorhandene Einschränkungen

Der 1. CDP Pfad ist www.pki.admin.ch/crl und ist überall auflösbar
Der 2. CDP Pfad zeigt auf das Active Directory intra.admin.ch und ist für Server die sich nicht im Forest INTRA befinden nicht auflösbar.
Es steht also nur ein gültiger CDP Path zur Verfügung.

5.2.7 Lifecycle

ACHTUNG: Zertifikat Ablauf nicht verpassen! Das Zertifikat ist 3 Jahre gültig und wird nicht automatisch erneuert!
Der Server-Betreiber ist für den Lifecycle des Zertifikats zuständig.