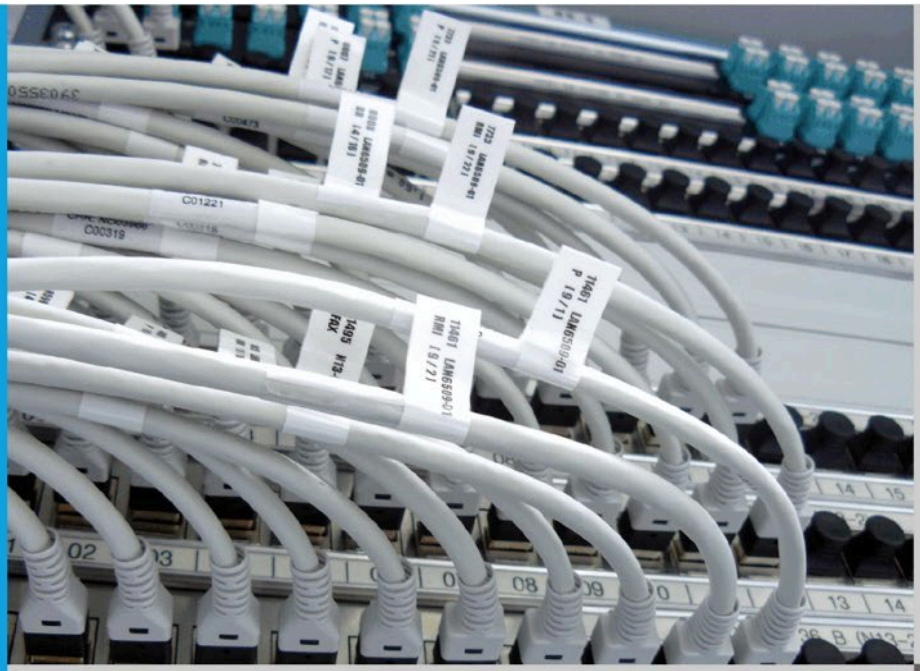
Landesamt für Digitalisierung,
Breitband und Vermessung



IT-Dienstleistungszentrum des Freistaats Bayern

WinEP

Benutzerhandbuch

Bearbeitung:
Ulrich Kronenberg, Veronika Metz, Kerstin Ehrhardt, Bernhard Vogl

München, den 27.02.2023

Dokumententwicklung

Version	Datum	Bearbeiter	Beschreibung, QS-Maßnahme	Status *s. u.
1.0	18.05.2016	Kronenberg, Metz	Erstellung	freigegeben
1.1	29.09.2016	Metz	Ergänzung bei den Punkten 7 (WinEP Officer) und 10.2-10.5 (Cryptography)	freigegeben
1.2	10.10.2016	Metz	Anpassung 10.2 (Template Name)	freigegeben
1.3	28.11.2016	Metz	Ergänzung bei 3.1 und 3.2	freigegeben
1.4	09.07.2019	Ehrhardt	Änderungen aufgrund Umstellung auf neue CA-Hierarchie eingearbeitet (Kapitel 2)	
1.5	03.05.2021	Böhm	Anpassungen aufgrund Umstellung der ausstellenden CA für Client Zertifikate bei 1 und 2	
1.6	17.06.2021	Ehrhardt	Anpassungen bei 10.x	freigegeben
1.7	03.08.2021	Vogl	Anpassungen bei 8 und 10.4	freigegeben
1.8	19.10.2021	Ehrhardt	Anpassungen bei 8	freigegeben
1.9	07.02.2022	Vogl	Anpassung 1.2	freigegeben
1.10	19.07.2022	Ehrhardt	Anpassungen bei 10.x	freigegeben
1.11	27.02.2023	Ehrhardt	Neues Kapitel 12	freigegeben

* zu verwenden sind: in Bearbeitung, vorgelegt, freigegeben

München, den 27.02.2023

1 Übersicht

Bei dem neXus Windows Enrollment Proxy (kurz: WinEP) handelt es sich um einen Service, der es ermöglicht, dass Clients per Windows Autoenrollment Nutzer-Zertifikate und Maschinenzertifikate der Bayern-PKI beantragen können.
Diese Zertifikate werden automatisch am Client installiert. Die Clients müssen hierfür in Prime registriert sein, Nutzer müssen zudem ihr Initialpasswort geändert haben.
Bei Nutzer-Zertifikaten ist während der Beantragung eine PIN-Vergabe notwendig. Diese PIN wird auch bei der Nutzung der Zertifikate benötigt.
Der private Schlüssel des persönlichen Verschlüsselungszertifikats wird für ein späteres Key Recovery bei der Beantragung verschlüsselt an das Zertifikatsverwaltungssystem Prime übertragen und dort archiviert.
Alle mittels WinEP beantragten Zertifikate sind in Prime ersichtlich und können auch dort gesperrt werden.

1.1 Anforderungen

Für die Installation von WinEP benötigen Sie einen AD-integrierten Server.
Die winep.msi installiert sowohl das WinEP Configuration Tool, als auch den WinEP Service.
Der WinEP Service läuft unter einem Service Account.

Folgende Systeme werden unterstützt:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Stellen Sie bitte sicher, dass die beigefügten Root- und Sub-CA-Zertifikate in Ihrer Domäne entsprechend verteilt sind (siehe Punkt 3.3).

Für die Konfiguration von WinEP benötigen Sie ein WinEP-Officer Zertifikat.
Bitte fordern Sie dieses per E-Mail bei uns an: pki-support@ldbv.bayern.de

1.2 Anlagen

- Root-CA-Zertifikate
  - Bayern-PKI: Bayern-Root-CA-2019.cer
- Sub-CA-Zertifikate
  - Issuing CA: Bayern-Softtoken-Issuing-CA-2019.cer
- KRA Zertifikat
- Ldif-Dateien für Enrollment Services
  - Für pers. Zertifikate: es_Bayern-PKI-IssuingCA-2019.ldf
- WinEP.msi
- WinEP Officer Zertifikat (P12 mit PIN, siehe 1.1)
- System-CA Zertifikat (Wurzelzertifikat des WinEP Officers): System-CA-2022.cer

2 Importieren der AD-Einträge

Für die nachfolgenden Importe der verschiedenen Zertifikate in die entsprechenden AD-Container sind Enterprise-Admin-Rechte erforderlich.

Stellen Sie bitte sicher, dass die beigefügten Root- und Issuing-Zertifikate in Ihrer Domäne entsprechend verteilt sind.

2.1 Certification Authorities Container

Der „Certification Authorities“-Container (Zertifizierungsstellen) beinhaltet alle Wurzel-CA-Zertifikate des AD-Forests.

Die beiden Root-CA Zeritifkate müssen in diesen Container (CN= Certification Authorities, CN=Public Key Services, CN=Services, CN=Configuration, DC=<domain>, DC=<local>) geladen werden.

Dazu cmd-Konsole als Administrator starten und folgenden Befehl eingeben:

certutil -f -dspublish Bayern-Root-CA-2019.cer RootCA

Zertifikate können aus diesem Container mittels pkiview.msc gelöscht werden. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf Enterprise PKI (Unternehmens-PKI) und dann auf „Manage AD Containers“.

2.2 Enrollment Services Container

Der „Enrollment Services“-Container (Registrierungsdienste) enthält die Zertifizierungsstellen (CA), die Zertifikate für Benutzer, Computer oder Dienste des Forests ausstellen können.
Die „Bayern-Softtoken-Issuing-CA-2019“ wird für die Erstellung von Benutzer Zertifikaten und Maschinen Zertifikate (Client Zertifikate) verwendet.
Um das entsprechende CA-Zertifikat in den Container (CN=Enrollment Services, CN=Public Key Services, CN=Services, CN=Configuration, DC=<domain>, DC=<local>) importieren zu können, benötigen Sie die mitgelieferte ldf-Datei.

Zuerst müssen folgende Werte an Ihre Domäne angepasst werden:

- dn
- distinguishedName
- dNSHostName (<FQDN_des_WinEP_Servers>)
- objectCategory

Anschließend können die angepassten Dateien auf dem Domain Controller importiert werden:

ldifde -i -f es_Bayern-PKI-IssuingCA-2019.ldf -s <FQDN des DC>

Zertifikate können aus diesem Container mittels pkiview.msc gelöscht werden. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf Enterprise PKI (Unternehmens-PKI) und dann auf „Manage AD Containers“.

2.3 KRA Container

Der „KRA“-Container enthält die Zertifikate für die Key Recovery Agents des Forests.
Das mitgelieferte Zertifikat wird für die Schlüsselarchivierung der privaten Verschlüsselungs-Schlüssel in Prime benötigt.

Importieren Sie das Zertifikat in den Container (CN= KRA, CN=Public Key Services, CN=Services, CN=Configuration, DC=<domain>, DC=<local>) mittels:

certutil -f -dspublish system_KEK_2019_winep.cer KRA

Zertifikate können aus diesem Container mittels pkiview.msc gelöscht werden. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf Enterprise PKI (Unternehmens-PKI) und dann auf „Manage AD Containers“.

2.4 NTAuth Container

Der „NTAuth“-Container enthält alle Zertifizierungsstellenzertifikate des Forest.
Das Sub-CA-Zertifikat muss in diesen Container importiert werden.

Dazu cmd-Konsole als Administrator starten und folgenden Befehl eingeben:

certutil -dspublish -f Bayern-Softtoken-Issuing-CA-2019.cer NTAuthCA

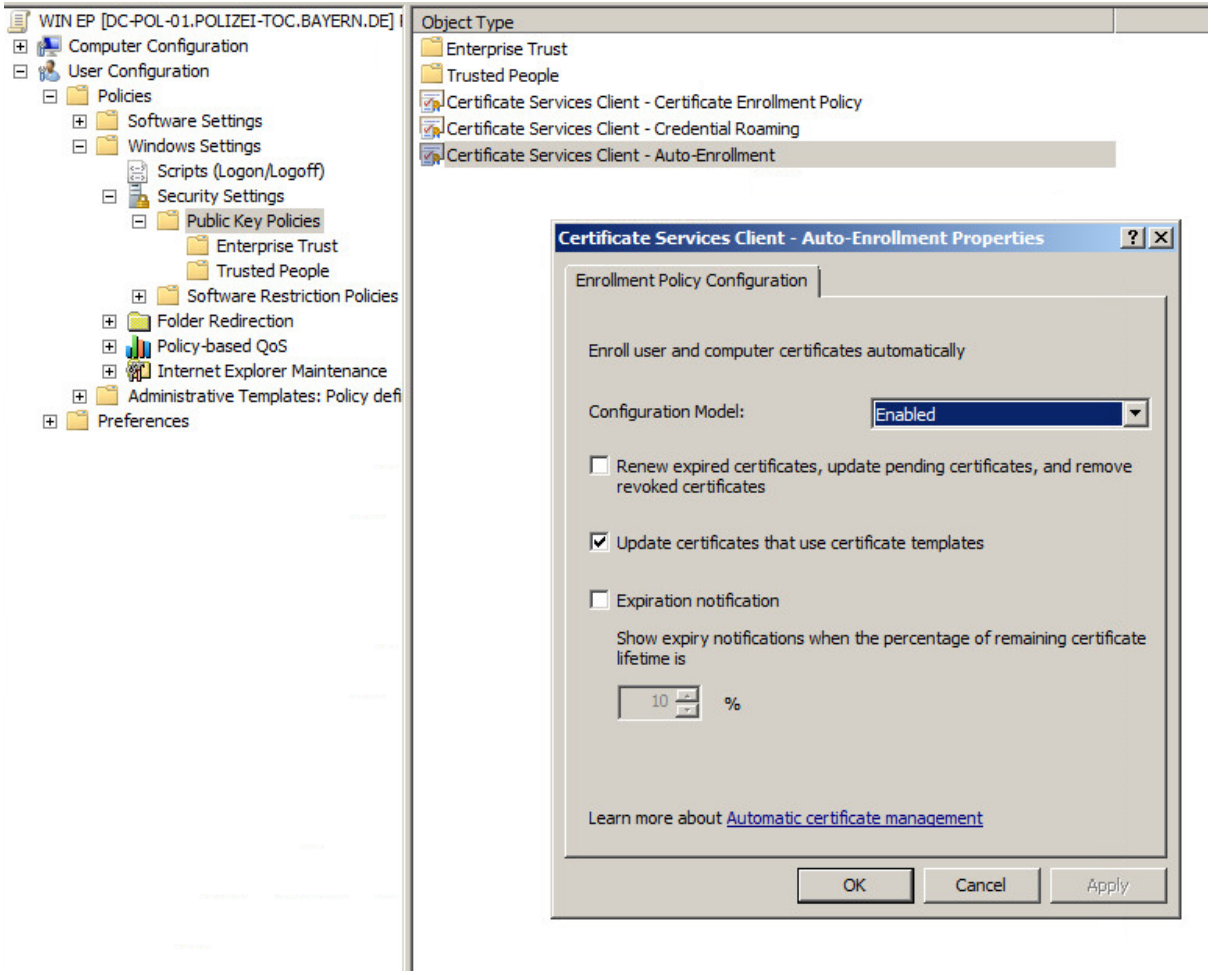
Oder Zertifikate mit pkiview.msc importieren:
Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf Enterprise PKI (Unternehmens-PKI) und dann auf „Manage AD Containers“.
Wählen Sie den Container NTAuthCertificates. Dort können Sie das Zertifikat mit „Add…“ hinzufügen.
Hier können die Zertifikate auch aus dem Container gelöscht werden.

3 GPO für Autoenrollment der Zertifikate

Informationen zum Einrichten von Gruppenrichtlinien für die automatische Zertifikatsverteilung finden Sie auch hier:
https://technet.microsoft.com/en-us/library/cc771025

3.1 GPO für Nutzerzertifikate

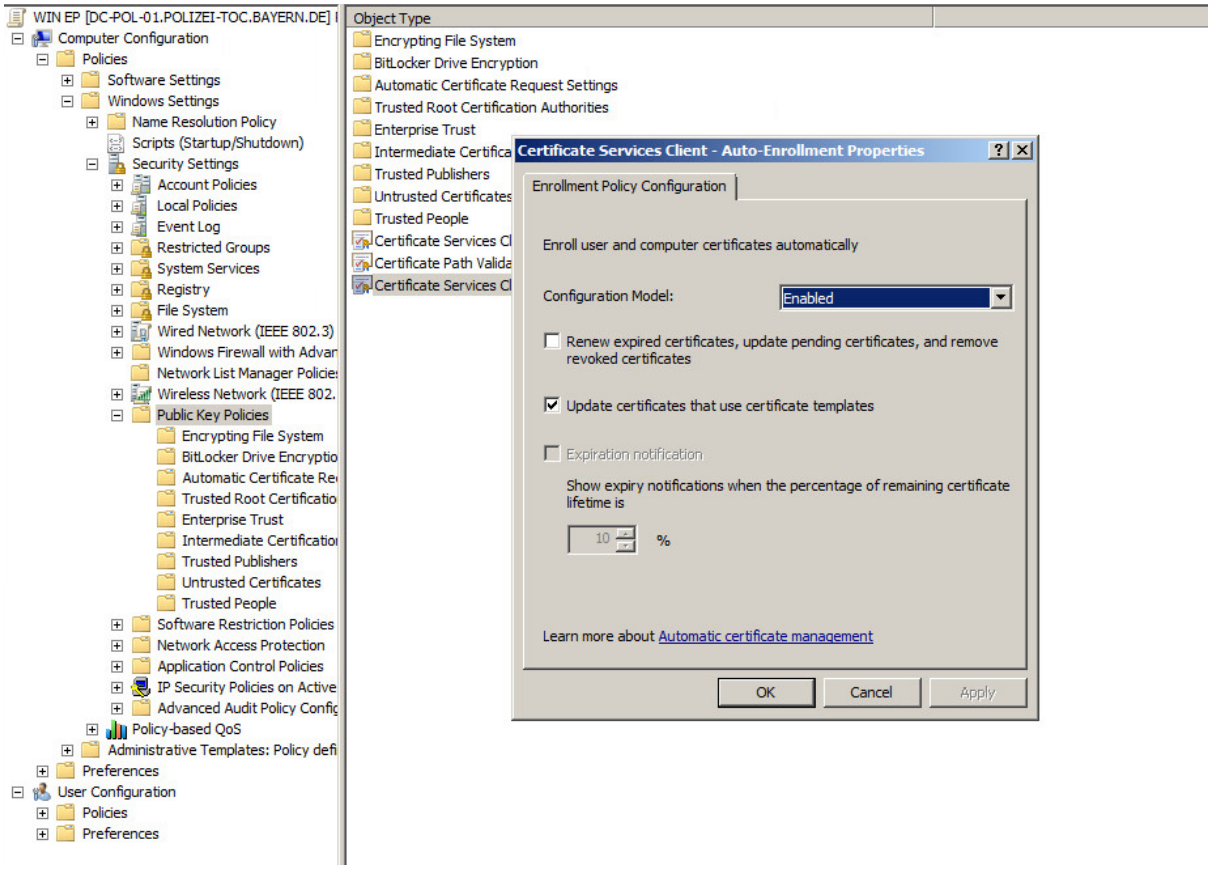
Um die automatische Beantragung von Nutzerzertifikaten zu aktivieren, benötigen Sie eine Gruppenrichtlinie welche unter „User Configuration, Policies, Windows Settings, Security Settings, Public Key Policies“ das *Certificate Services Client – Autoenrollment* aktiviert. Stellen Sie dazu unter Eigenschaften das „Configuration Model“ auf *enabled* und setzten Sie bei „Update certificates that use certificate templates“ eine Haken:



Wenn Sie „Renew expired certificates, …“ aktivieren, werden alle abgelaufenen oder gesperrten Zertifikate (egal woher diese kommen) aus dem Zertifikatsspeicher gelöscht.

3.2 GPO für Maschinenzertifikate

Um die automatische Beantragung von Maschinenzertifikaten zu aktivieren, benötigen Sie eine Gruppenrichtlinie welche unter „Computer Configuration, Policies, Windows Settings, Security Settings, Public Key Policies“ das *Certificate Services Client – Autoenrollment* aktiviert.
Stellen Sie dazu unter Eigenschaften das „Configuration Model“ auf *enabled* und setzten Sie bei „Update certificates that use certificate templates“ eine Haken:



Wenn Sie „Renew expired certificates, …“ aktivieren, werden alle abgelaufenen oder gesperrten Zertifikate (egal woher diese kommen) aus dem Zertifikatsspeicher gelöscht.

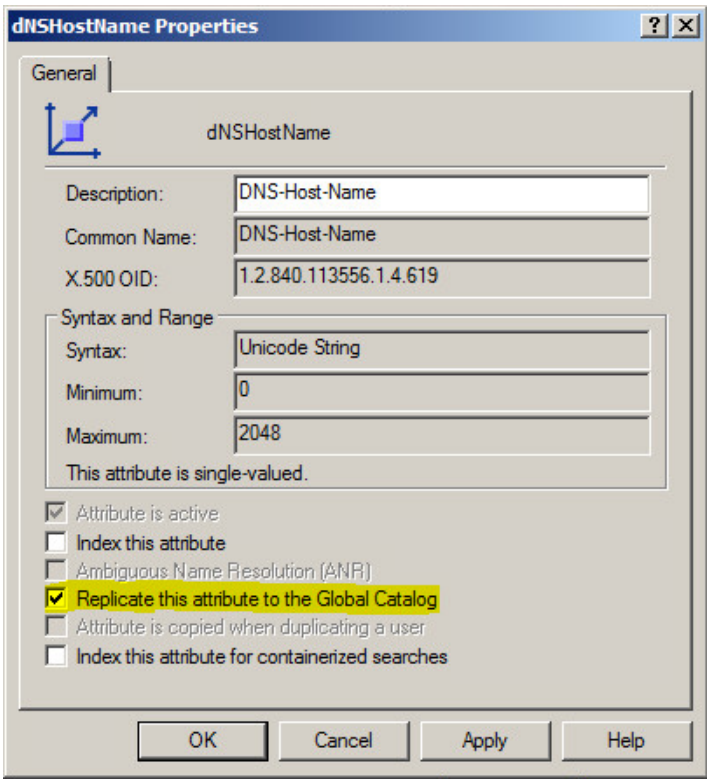
3.3 GPO für Wurzel- und Sub-CA-Zertifikate

Damit die automatische Beantragung der Zertifikate funktioniert müssen die mitgelieferten Wurzel- und Sub-CA-Zertifikate in Ihrer Domäne bekannt sein. Dies kann auch mittels einer Gruppenrichtlinie erfolgen.
Fügen Sie hierzu die Wurzel-Zertifikate unter “*Computer Configuration, Policies, Windows Settings, Security Settings, Public Key Policies, Trusted Root Certification Authorities*” hinzu.
Die Sub-CA-Zertifikate müssen entsprechend in den *Intermediate Certification Authorities* Ordner importiert werden.
Informationen dazu finden Sie auch auf unserer Webseite:
https://www.pki.bayern.de/index.php?option=com_content&view=article&id=14&Itemid=16

4 Global Catalog

Im Global Catalog muss das Attribute *dnsHostName* für das Active Directory Schema konfiguriert werden. Dieses Attribute wird zum Nachschlagen und Überprüfen der Antragstellerdaten benötigt.

Falls nicht vorhanden, kann das *Active Directory Schema* Snap-In wie folgt auf dem Domain Controller nachgeladen werden: cmd-Konsole öffnen und Befehl ***regsvr32 schmmgmt.dll*** eingeben
Snap-In in der *mmc.exe* hinzufügen→ links ausklappen und auf *Attributes* klicken → Rechtsklick auf *dnsHostName* und prüfen, dass die Option *„Replicate this attribute to the Global Catalog“* gewählt ist



5 WinEP-Serviceaccount

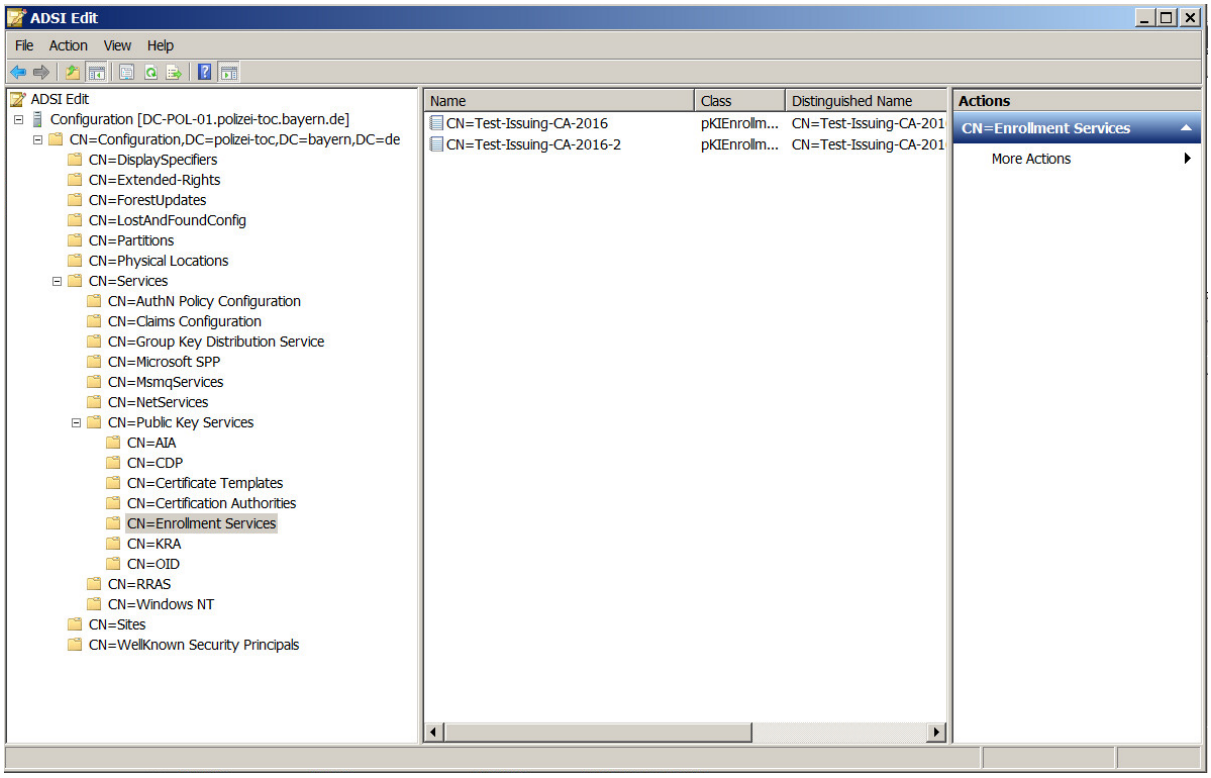
1. Anlegen eines neuen Domänenbenutzers: WinEP-User (Service Account)

2. Hinzufügen des Nutzers in die Gruppe der lokalen Administratoren auf dem WinEP Server

3. ADSI Edit öffnen und im *Configuration* Context zu “CN=Enrollment Services, CN=Public Key Services, CN=Services, CN=Configuration, DC=<*domain*>, DC=<*local*>” navigieren

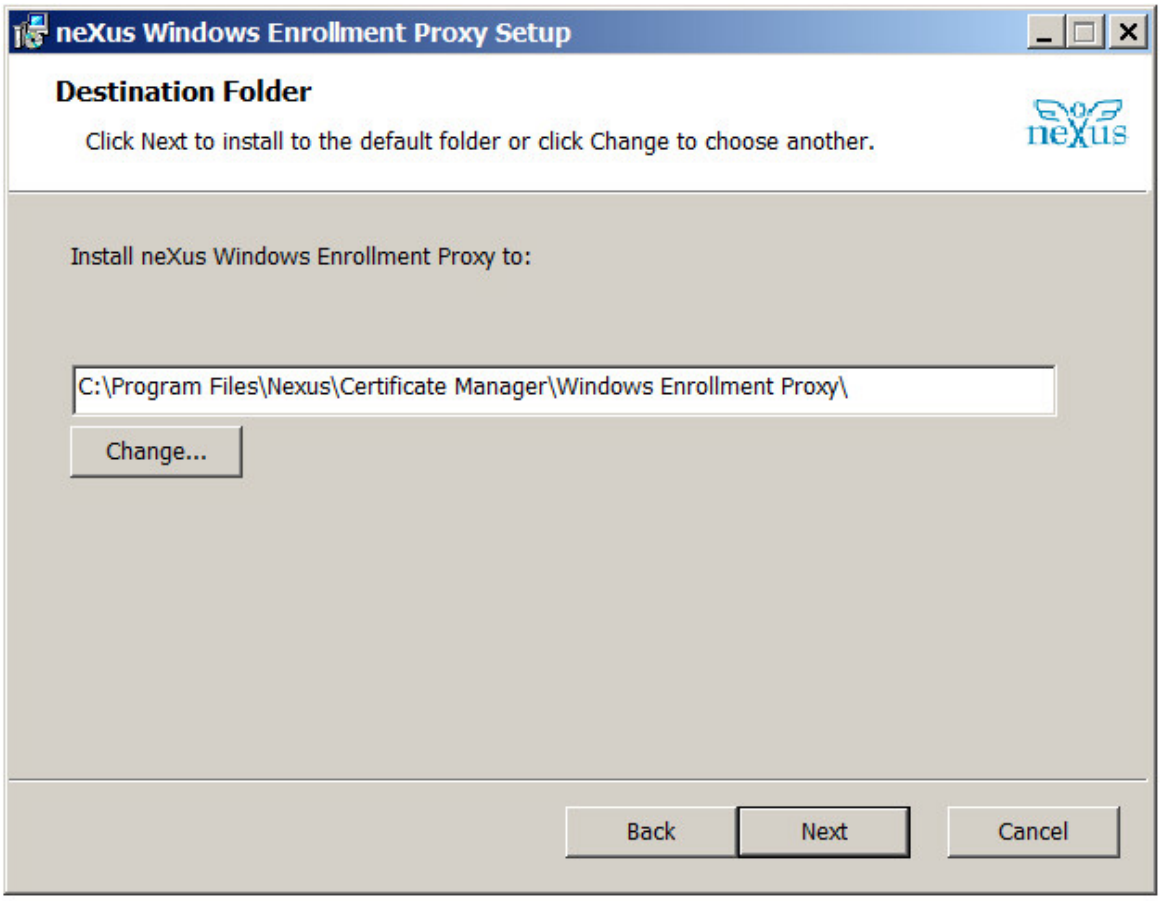
4. Rechtsklick auf die importierte CA und *Properties* wählen. Unter *Security* den WinEP-User hinzufügen und „Read“ und „Write“ Rechte zuweisen.
Diese Rechte werden benötigt um die WinEP Certificate Templates der entsprechenden ausstellenden CA zuzuordnen (siehe Schritt 10).

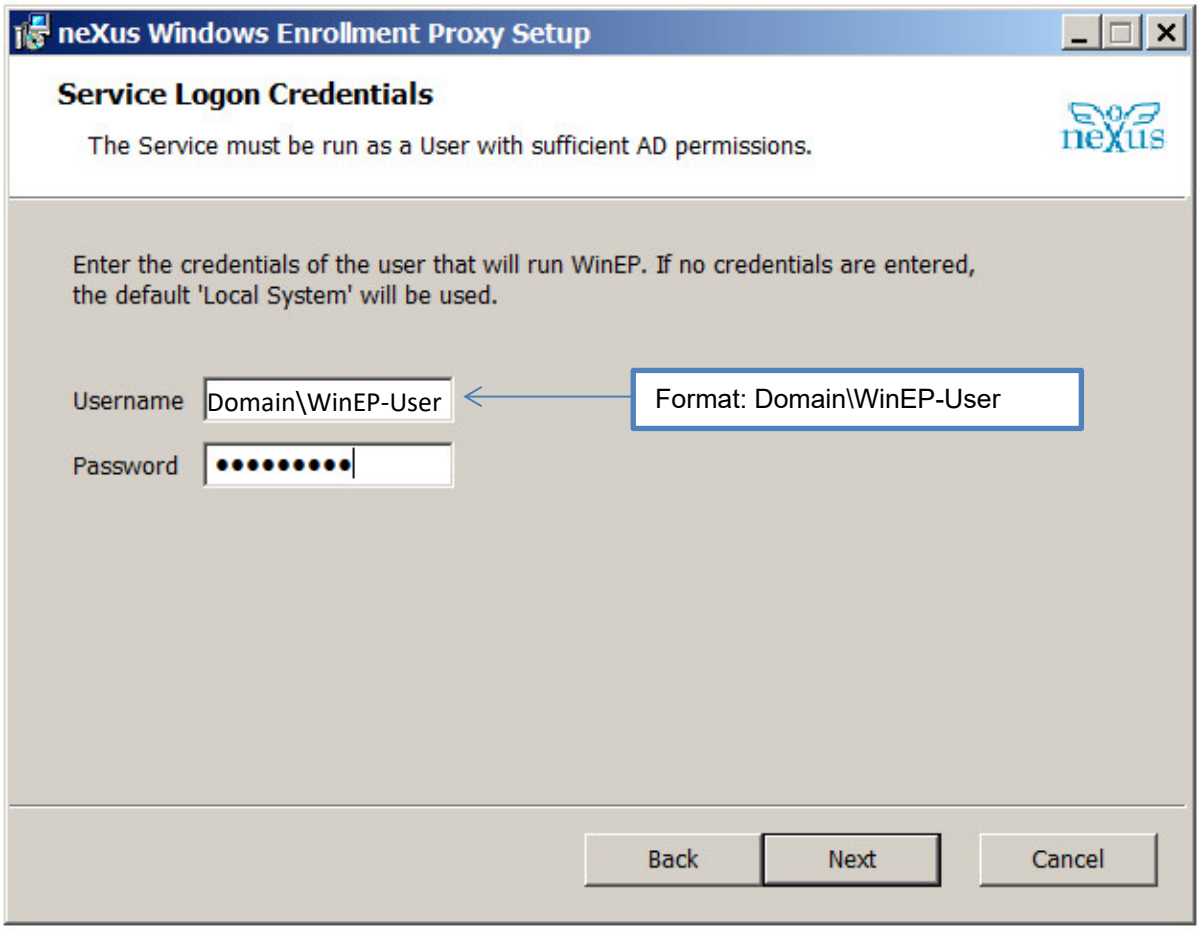
Für alle, unter Punkt 2.2 importierten, CAs durchführen.

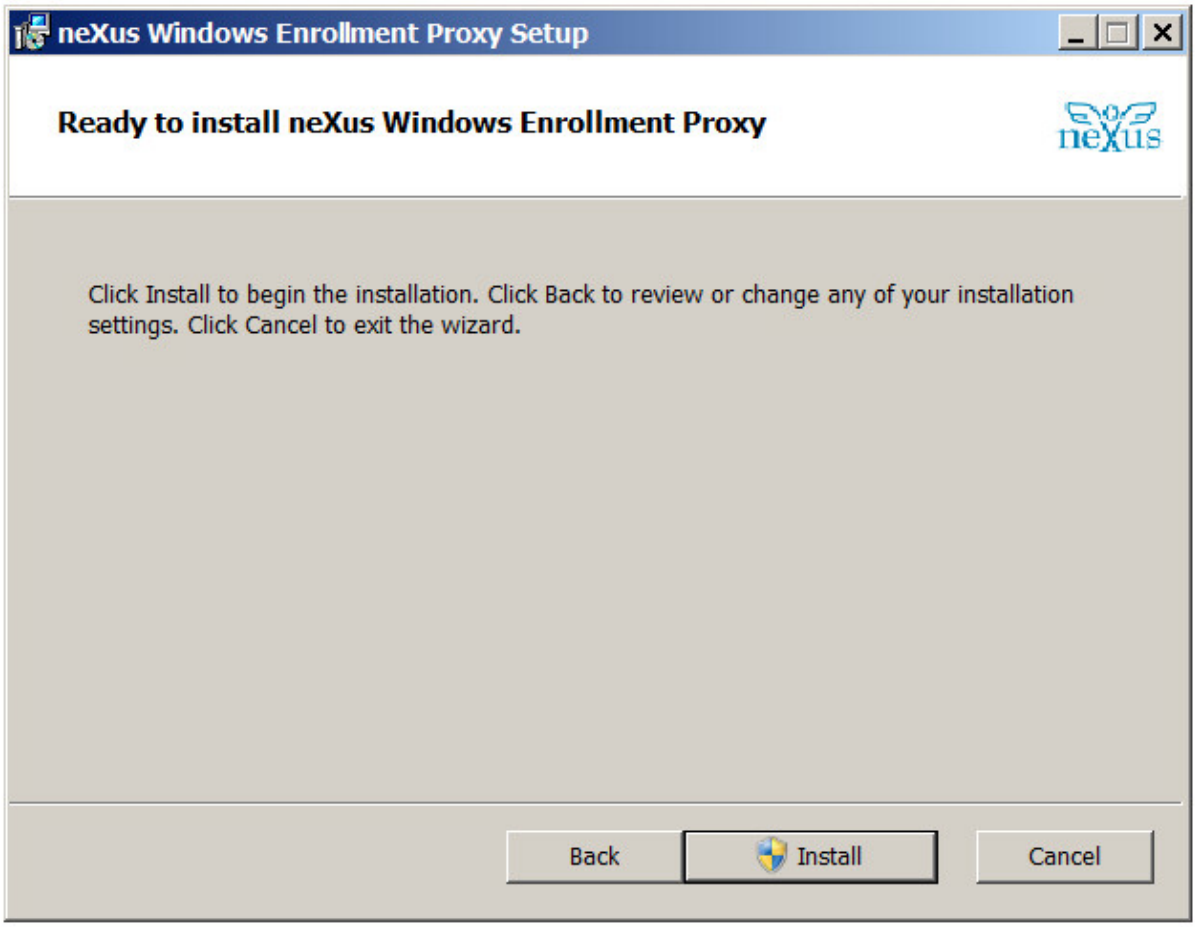


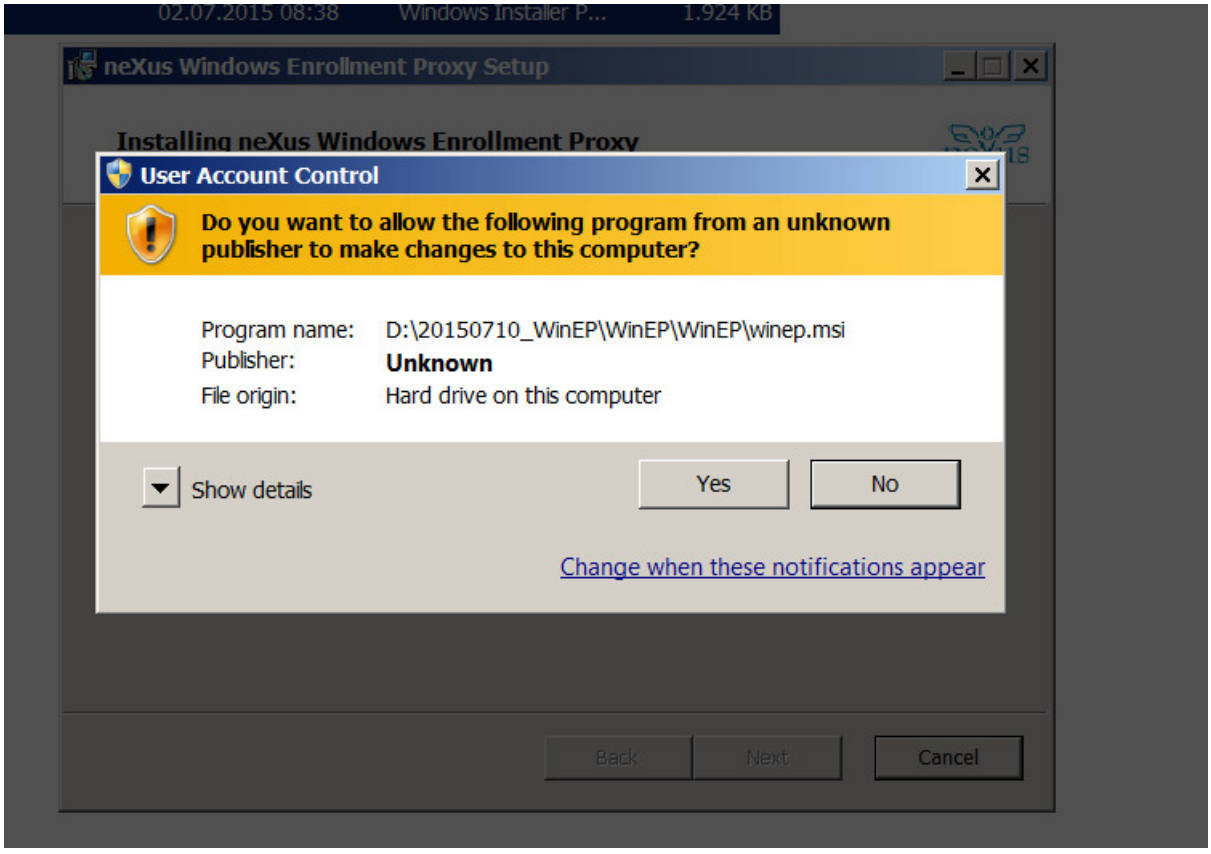
6 Installation WinEP

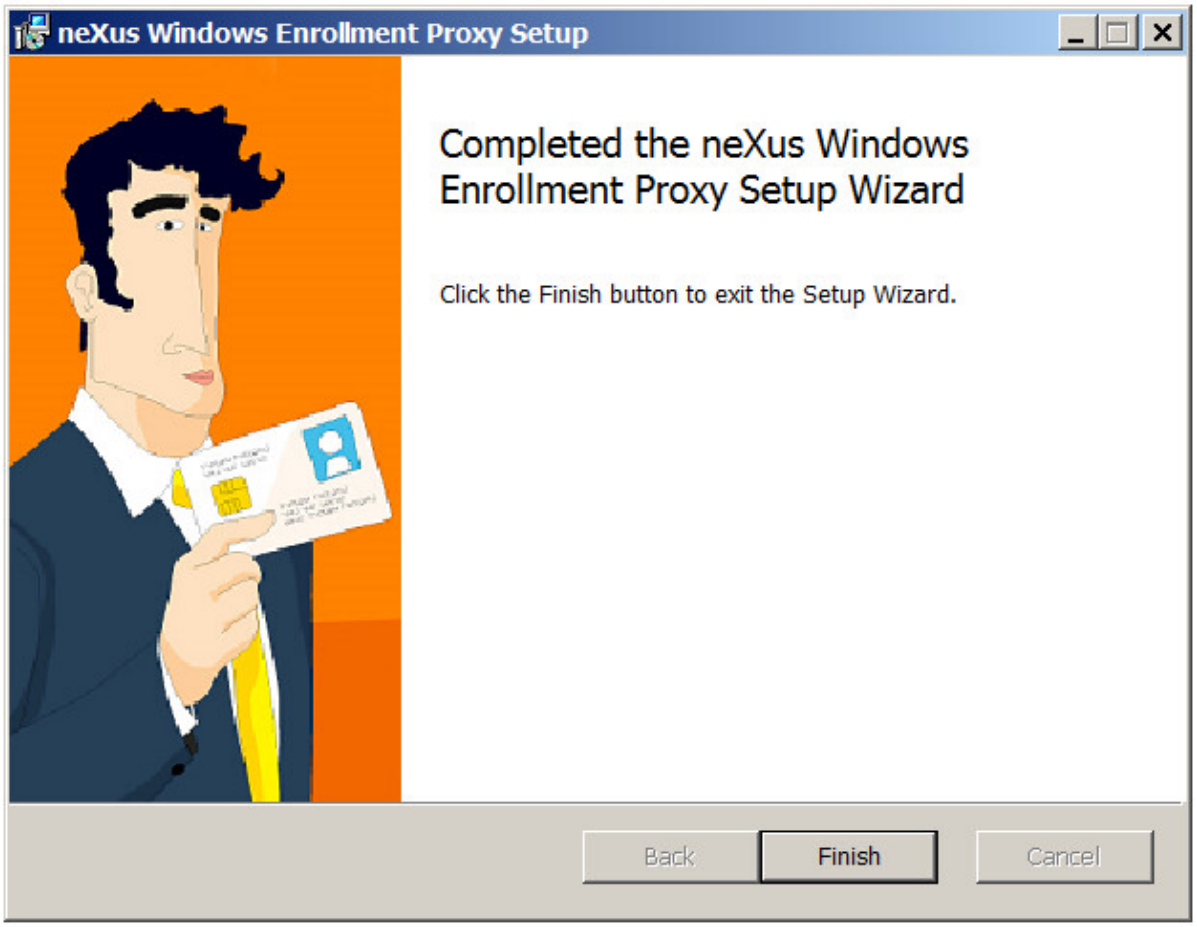
Ausführen der winep.msi auf dem WinEP Server (als WinEP-User):


neXus Windows Enrollment Proxy Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
neXus
Install neXus Windows Enrollment Proxy to:
C:\Program Files\Nexus\Certificate Manager\Windows Enrollment Proxy\
Change...
Back
Next
Cancel


neXus Windows Enrollment Proxy Setup
Service Logon Credentials
The Service must be run as a User with sufficient AD permissions.
neXus
Enter the credentials of the user that will run WinEP. If no credentials are entered,
the default 'Local System' will be used.
Username
Domain\WinEP-User
Format: Domain\WinEP-User
Password
Back
Next
Cancel


neXus Windows Enrollment Proxy Setup
Ready to install neXus Windows Enrollment Proxy
neXus
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel


02.07.2015 08:38
Windows Installer P...
1.924 KB
neXus Windows Enrollment Proxy Setup
Installing neXus Windows Enrollment Proxy
User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: D:\20150710_WinEP\WinEP\WinEP\winep.msi
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear
Back
Next
Cancel


neXus Windows Enrollment Proxy Setup
Completed the neXus Windows Enrollment Proxy Setup Wizard
Click the Finish button to exit the Setup Wizard.
Back
Finish
Cancel

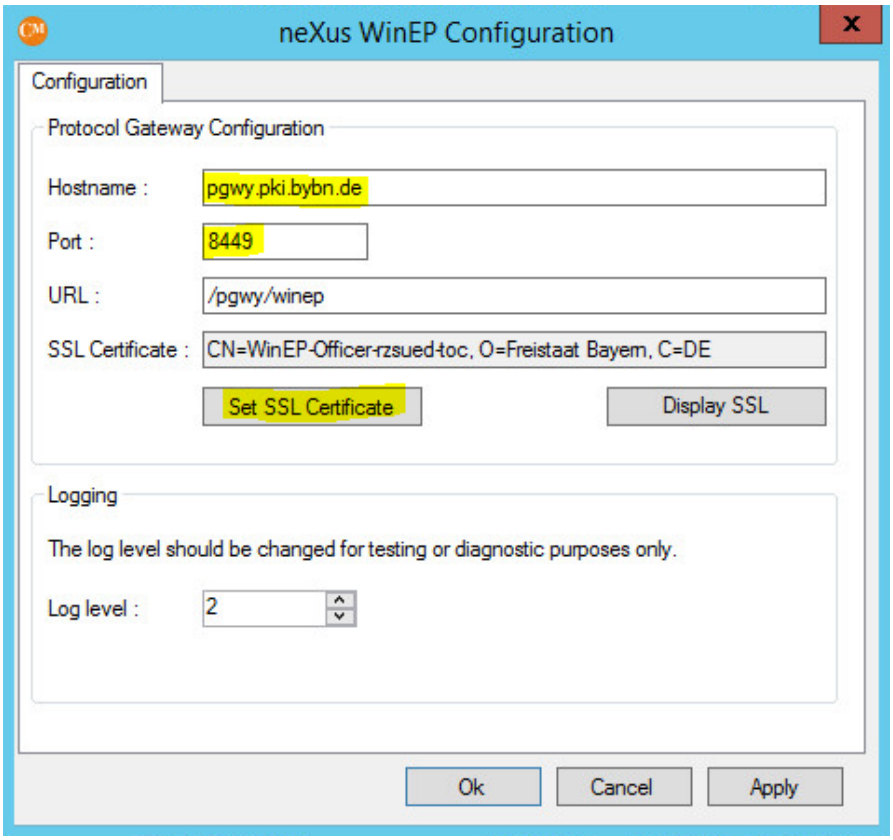
7 Konfiguration WinEP

Installieren Sie auf dem WinEP Server das System-CA Zertifikat (als Certificate Store: *Trusted Root Certification Authorities* wählen) mittels Doppelklick auf die Zertifikatsdatei.
Zur Installation des WinEP Officer Zertifikats gehen Sie bitte wie folgt vor:
mmc.exe (als WinEP User) öffnen, Add/Remove Snap-in „Certificates“ → „My User Account“ wählen: Certificates - Current User → Personal → Rechtsklick „All Tasks → Import…“ → WinEP Officer P12-Datei auswählen und importieren

Als WinEP-User das *neXus WinEP Configuration Tool* ausführen:

1. Hostname: pgwy.pki.bybn.de
2. Port: 8449
3. Setzen des *WinEP Officer Zertifikates (P12)*.
   Dieses muss zuvor Installiert werden (s.o.)
4. Log level:
   Folgende Log Levels können gewählt werden:
   - 0 – kein Logging
   - 2 – Nur Fehler und Warnungen – wir empfehlen dieses Log-Level
   - 5 – Fehler, Warnungen und Info-Meldungen
   - 10 – Debug Logging

   Die protokollierten Meldungen sind im Event Viewer unter *Windows Logs → Application* zu finden.
5. Auf *Ok* klicken → Service wird neugestartet
   Falls der Service nicht startet (Logon Failure), die WinEP Service Kennung über *Services → neXus WinEP → Rechtsklick: Properties → Log On* neu berechtigen



8 Firewall Freischaltung

8.1 WinEP Server

8.1.1 Zugriff Protocol Gateway

Der Zugriff vom WinEP Server auf das Protocol Gateway (pgwy.pki.bybn.de, IP-Adresse: 10.173.224.39) Port 8449 muss freigeschaltet werden.

8.1.2 RPC-Ports (nur AD intern)

Folgende RPC-Ports werden für die Windows-Zertifikatsbeantragung benötigt:

- Inbound
  - TCP Port 135 (RPC)
  - TCP Ports 49152 – 65535 (RPC dynamische Ports)
  - UDP Port 135 (RPC)
  - UDP Ports 49152 – 65535 (RPC dynamische Ports)
- Outbound
  - TCP Port 135 (RPC)
  - UDP Port 135 (RPC)

Informationen zu den dynamischen Ports finden Sie auch hier:
https://support.microsoft.com/de-de/kb/832017

8.2 Clients (nur AD intern)

Alle Clients benötigen für die Windows-Zertifikatsbeantragung folgende Freischaltungen:

- Outbound
  - TCP Port 135 (RPC)
  - TCP Ports 49152 – 65535 (RPC dynamische Ports)
  - UDP Port 135 (RPC)
  - UDP Ports 49152 – 65535 (RPC dynamische Ports)

9 DCOM Konfiguration

Der WinEP-Service wird mittels DCOM von den Clients angesprochen. Dafür sind folgende Einstellungen erforderlich:

1. dcomcnfg.exe starten
2. Component Services→ Computers→ *My Computer:*
   Rechtsklick und *Properties* wählen
3. *COM Security* Tab
   a. *Access Permissions* → *Edit Limits: Authenticated Users* hinzufügen und alle Berechtigungen auf *Allow* setzen
   b. *Launch and Activation Permissions* → *Edit Limits: Authenticated Users* hinzufügen und alle Berechtigungen auf *Allow* setzen
4. Component Services→ Computers→ DCOM Config→*neXus WinEP:*
   Rechtsklick und *Properties* wählen
5. *Security* Tab → *Launch and Activation Permissions: Customize* → *Edit*
   a. WinEP-User (Serviceaccount) hinzufügen und alle Berechtigungen auf *Allow* setzen
   b. *Everyone* hinzufügen und alle Berechtigungen auf *Allow* setzen
6. *Security* Tab → *Configuration Permission: Customize* → *Edit*
   a. WinEP-User (Serviceaccount) hinzufügen und *Full Control* und *Read*-Rechte vergeben
   b. *Authenticated Users* hinzufügen und *Read*-Rechte zuweisen
7. *Identity* Tab → WinEP-User (Serviceaccount) als ausführenden Account der Applikation hinterlegen

10 Windows Zertifikats Templates für WinEP

Die Zertifikatsvorlagen können in der *mmc.exe* konfiguriert und angepasst werden. Hierzu muss das Snap-In *Certificate Templates* hinzugefügt werden.

Informationen zu diesem Snap-In finden Sie z.B. hier:
https://technet.microsoft.com/en-us/library/cc732445.aspx
Dort steht auch beschrieben, wie das *Certificate Templates* Snap-In nachgeladen werden kann.

Die Templates müssen exakt wie vorgegeben benannt werden, damit die Kommunikation mit dem Protocol Gateway funktioniert.

Bei persönlichen Zertifikaten muss für alle Vorlagen die Option *„Prompt the user during enrollment and require user input when the private key is used“* aktiviert werden, damit die Verwendung der Zertifikate policykonform stattfindet.

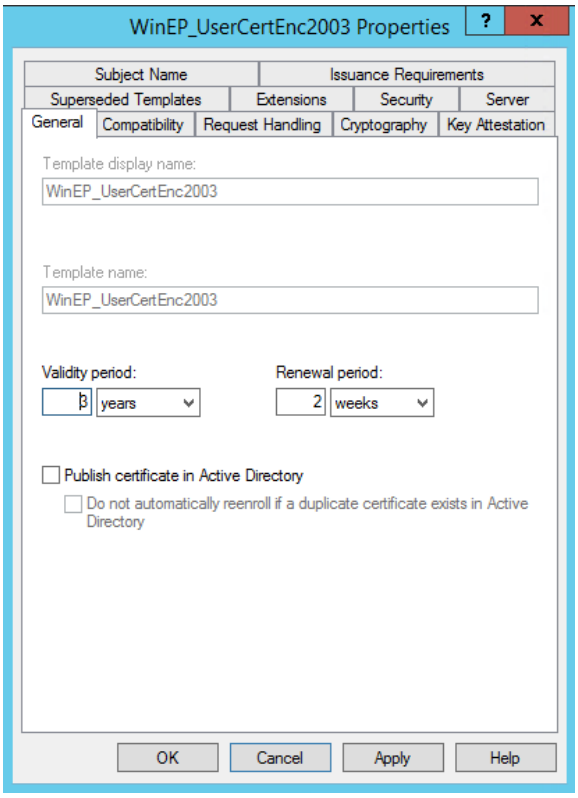
Nach Änderungen an den Templates muss der WinEP Service neu gestartet werden:
Als WinEP-User das *neXus WinEP Configuration Tool* ausführen und Service mit Klick auf *Ok* neustarten.
Hierbei sollten die Templates im „Enrollment Services“-Container bei dem entsprechenden CA-Zertifikat unter *Properties → certificate Templates* ergänzt werden (siehe auch Schritt 5).

10.1 Nutzer Verschlüsselungszertifikat - WinEP_UserCertEnc2003

Für das Template des pers. Verschlüsselungszertifikat „WinEP_UserCertEnc2003“ kann das vorhandene „User“-Template dupliziert werden. Damit das Backup des privaten Schlüssels funktioniert, ist jedoch darauf zu achten, dass die Kompatibilität auf höchstens auf *„Windows Server 2008 R2*“ (nachfolgender Screenshot 2) und bei Cryptography der Provider *„Legacy Cryptography Service Provider“* (nachfolgender Screenshot 4) ausgewählt wird.

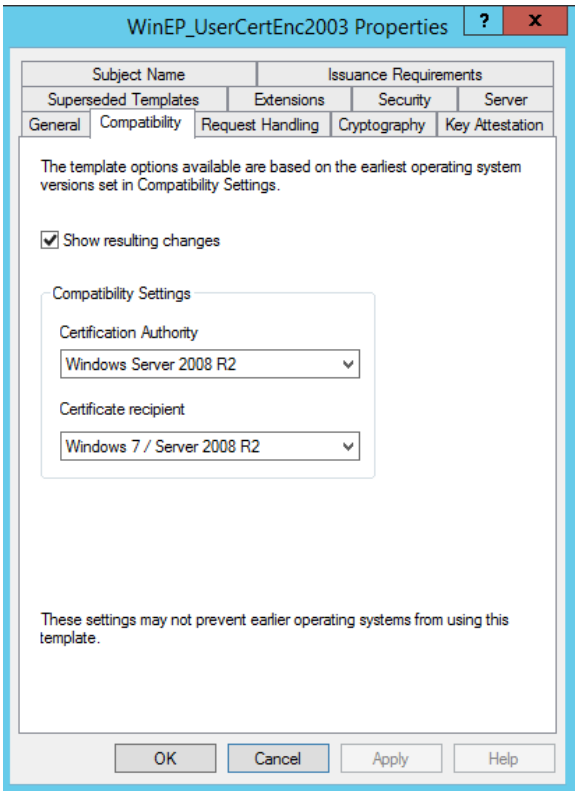
In den einzelnen Tabs müssen folgende Einstellungen getroffen werden, nicht genannte Einstellungen bitte standardmäßig belassen:

1. General:
   - Einstellung der Zertifikatsgültigkeitsdauer: *3 Jahre*
   - Renewal period: *2 Wochen*

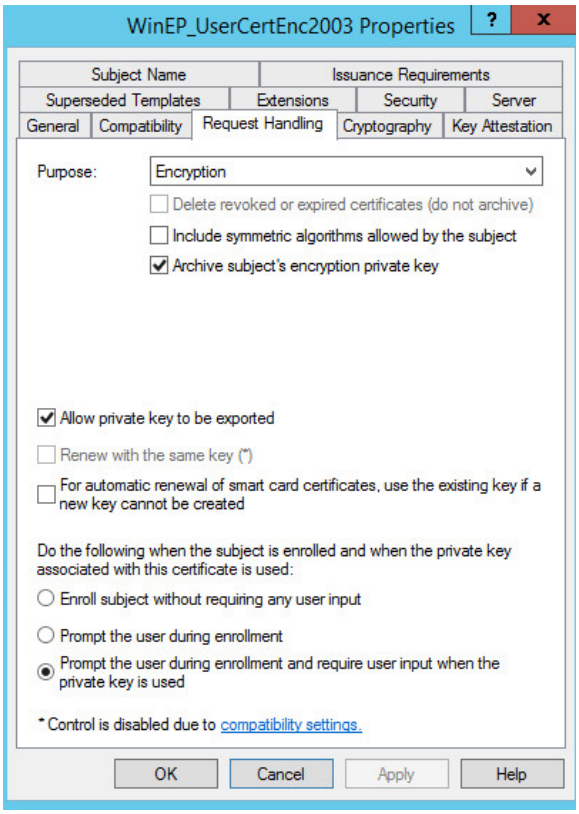


2. Compatibility:

Es darf höchstens „Windows Server 2008 R2“ und „Windows 7 / Server 2008 R2“ konfiguriert werden.

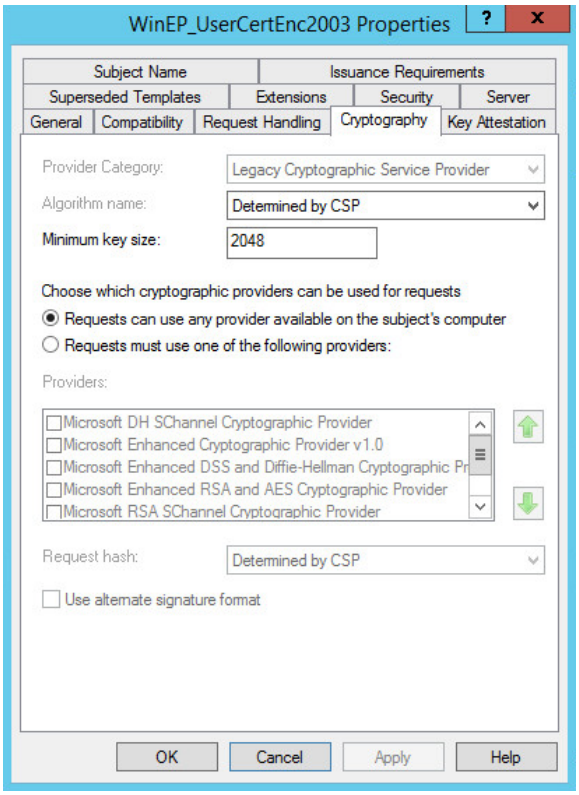


3. Request Handling:
   - Purpose: *Encryption*
   - Haken bei *„Archive subject's encryption private key“*
   - Haken bei *„Allow private key to be exported“*
   - *“Prompt the user during enrollment and require user input when the private key is used”* aktivieren

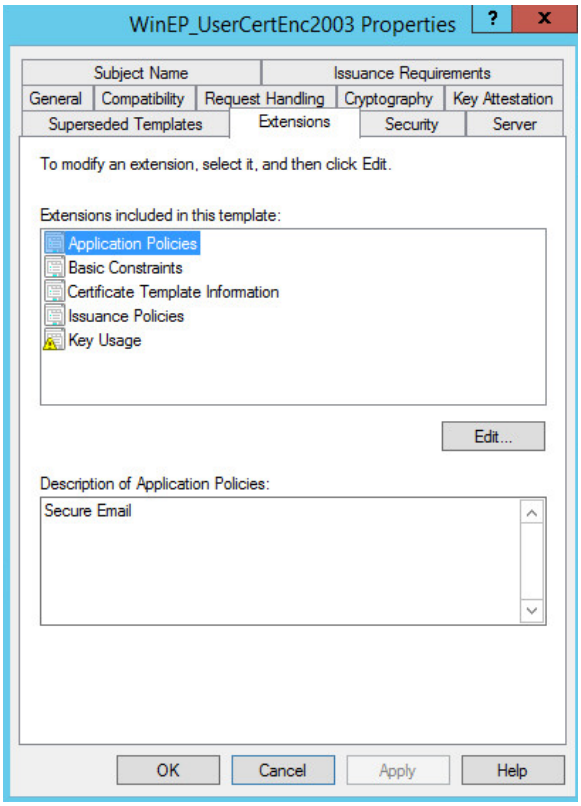


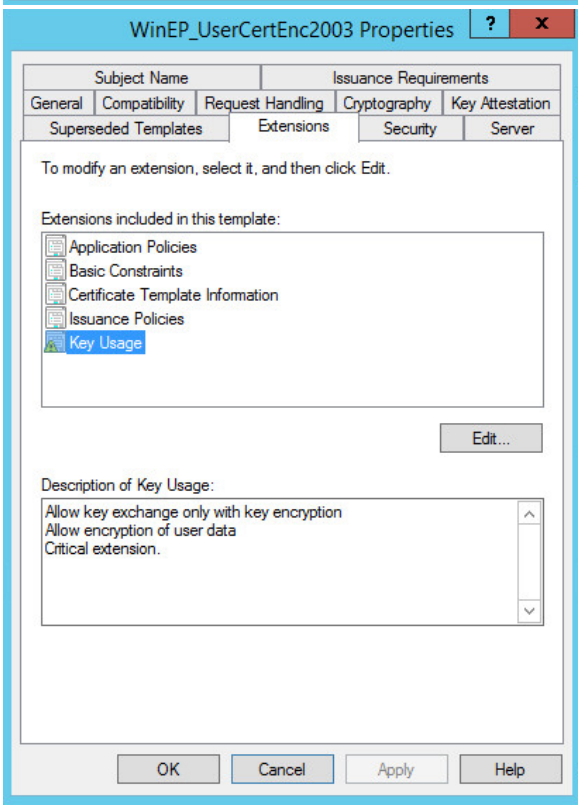
4. Cryptography:
   - Minimum key size: 2048

Es muss der Provider „Legacy Cryptography Service Provider“ eingestellt werden, da sonst die Schlüsselarchivierung fehlschlägt.

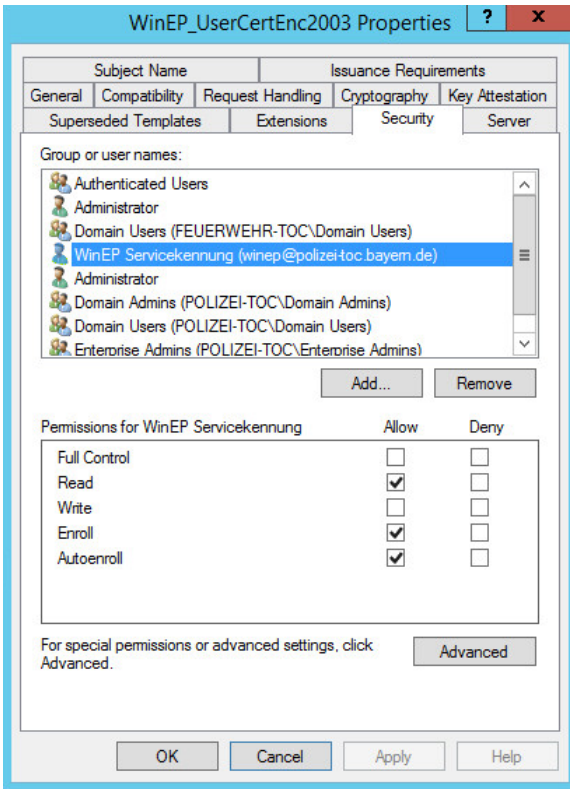


5. Extensions:
   - Application Policies: *Secure Email*
   - Key Usage:
     - Allow key exchange only with key encryption
     - Allow encryption of user data
     - Critical extension

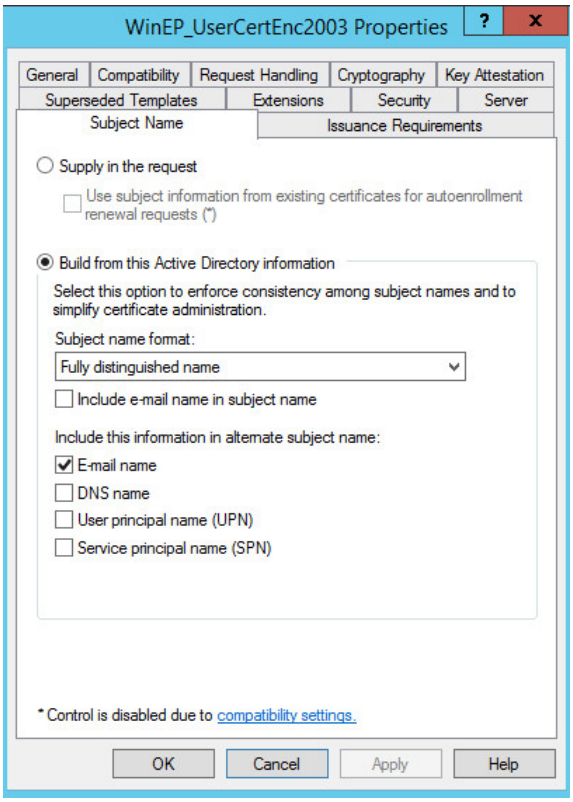




6. Security:
   - Die zuvor eingerichtete WinEP Servicekennung hinzufügen und die Rechte *Read, Enroll* und *Autoenroll* vergeben
   - Alle Nutzerobjekte, die Zertifikate beantragen können sollen, hinzufügen und die Rechte *Read*, *Enroll* und *Autoenroll* vergeben



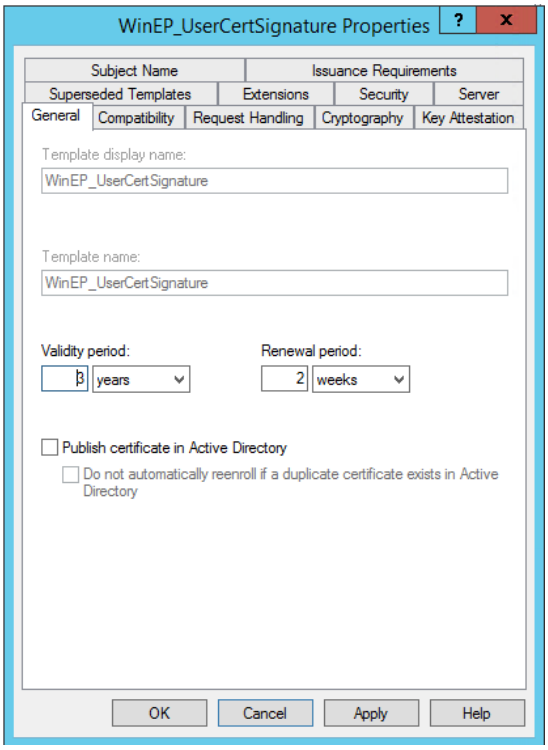
7. Subject Name:
   - *Fully distinguished name* auswählen und Haken bei *E-Mail name* setzen



10.2 Nutzer Signaturzertifikat - WinEP_UserCertSignature

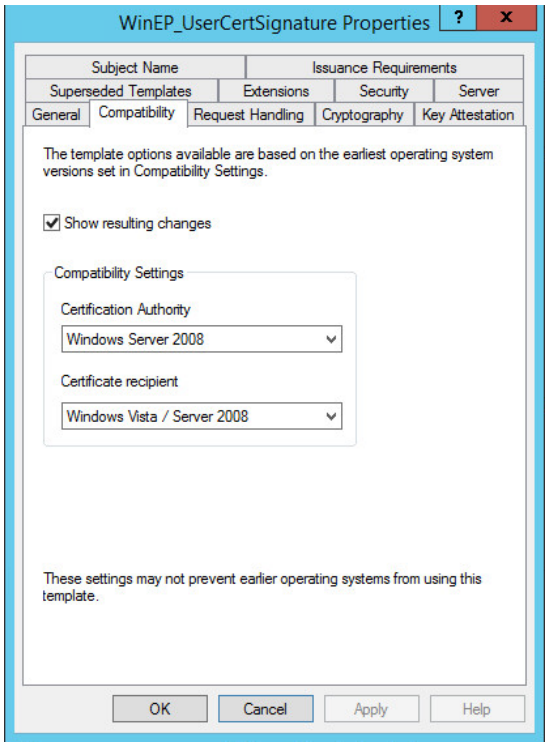
Für das Template des pers. Signaturzertifikat „WinEP_UserCertSignature“ kann das vorhandene „User“-Template, oder auch das oben angelegte Template dupliziert werden.

1. General:
   - Einstellung der Zertifikatsgültigkeitsdauer: *3 Jahre*
   - Renewal period: *2 Wochen*

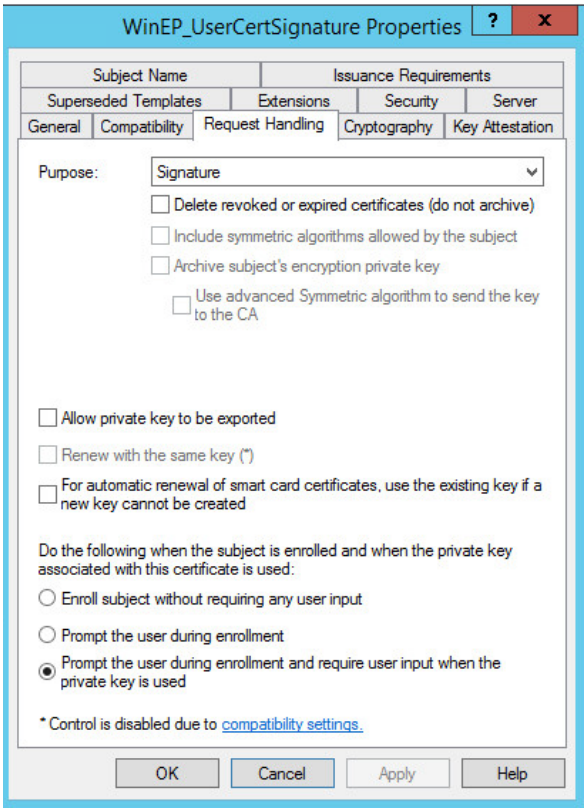


2. Compatibility:

Falls vorhanden (ab Active Directory Version 2008) gemäß Ihrer Umgebung anpassen.

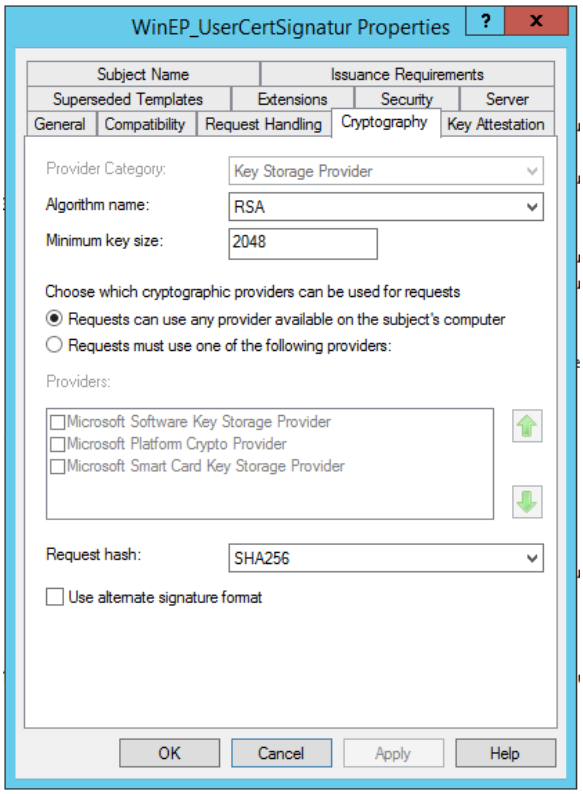


3. Request Handling:
   - Purpose: *Signature*
   - Haken bei *„Allow private key to be exported“ (optional)*
   - *“Prompt the user during enrollment and require user input when the private key is used”* aktivieren

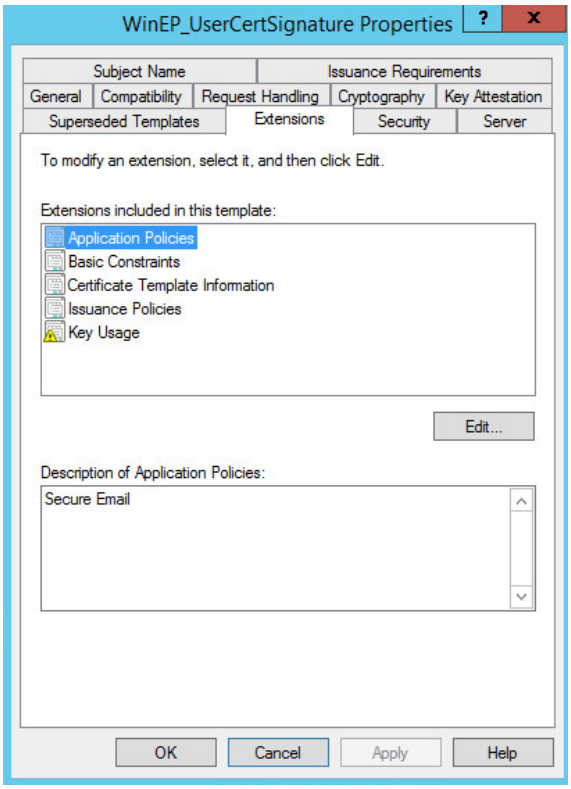


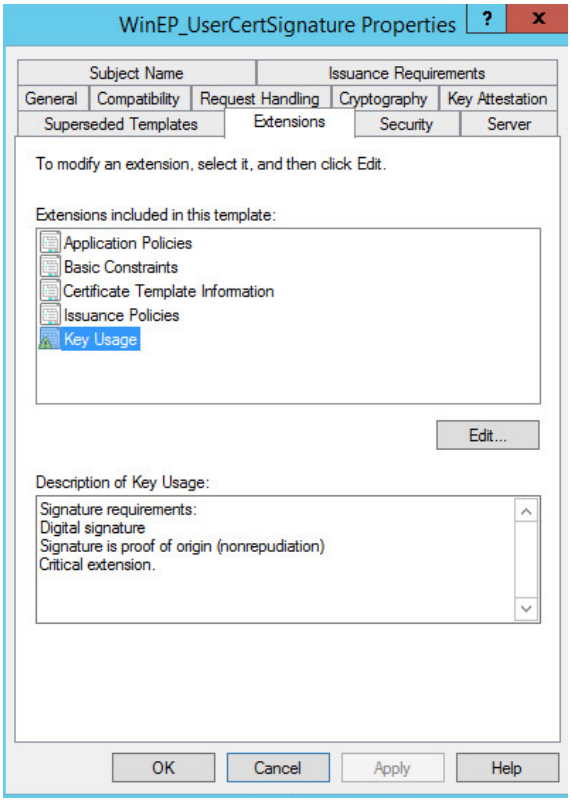
4. Cryptography:
   - Algorithm name: RSA
   - Minimum key size: 2048
   - Request hash: SHA 256

Es darf der Provider „Key Storage Privider“ oder „Legacy Cryptography Service Provider“ eingestellt werden, wobei die Empfehlung bei „KSP“ liegt.
Für „KSP“ muss für die Kompatibilität mind. Windows Server 2008 ausgewählt sein.

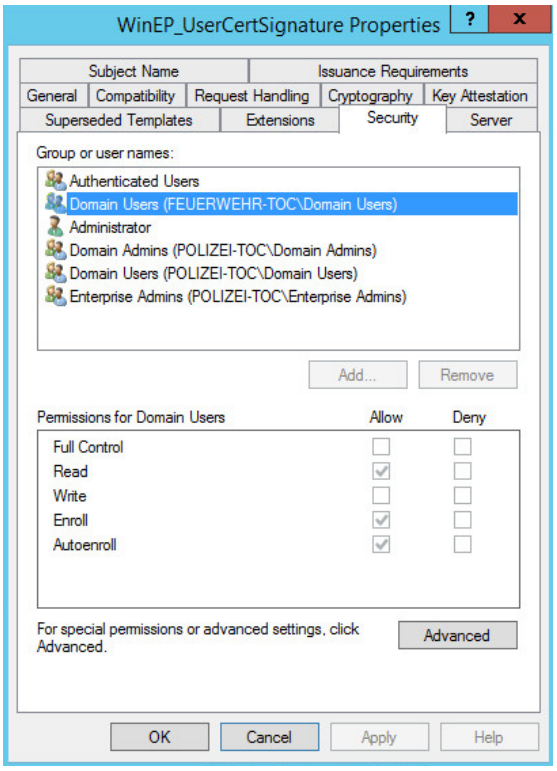


5. Extensions:
   - Application Policies: *Secure Email*
   - Key Usage:
     - Digital signature
     - Signature is proof of origin (nonrepudiation)
     - Critical extension

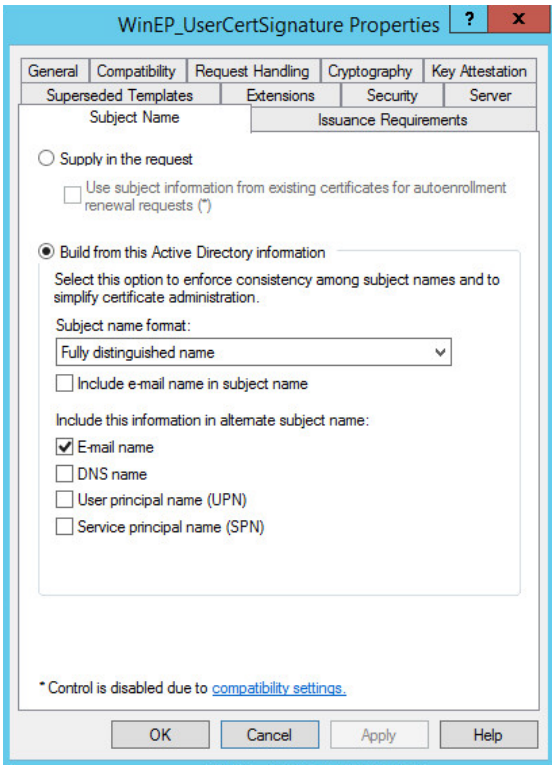




6. Security:
   Alle Nutzerobjekte, die Zertifikate beantragen können sollen, hinzufügen und die Rechte *Read*, *Enroll* und *Autoenroll* vergeben



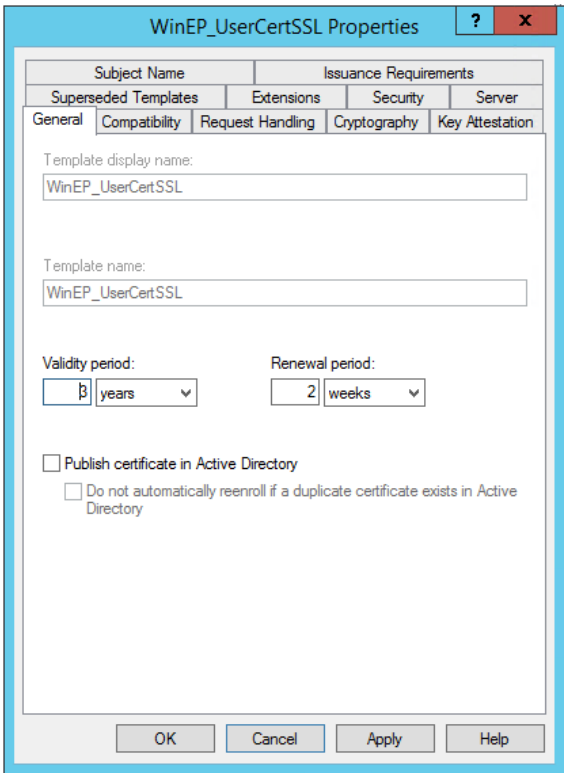
7. Subject Name:
   - *Fully distinguished name* auswählen und Haken bei *E-Mail name* setzen



10.3 Nutzer Authentifizierungszertifikat - WinEP_UserCertSSL

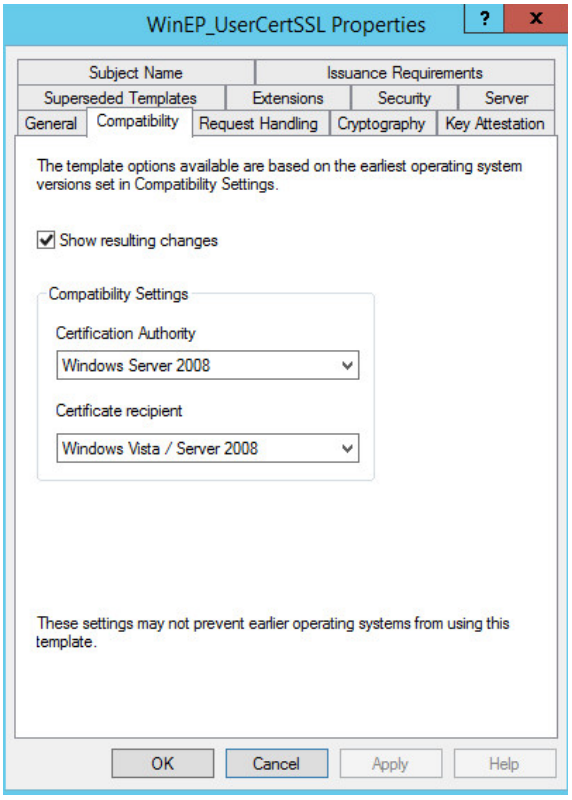
Für das Template des pers. Authentifizierungszertifikat „WinEP_UserCertSSL“ kann das vorhandene „User“-Template, oder auch das oben angelegte Template dupliziert werden.

1. General:
   - Einstellung der Zertifikatsgültigkeitsdauer: *3 Jahre*
   - Renewal period: *2 Wochen*

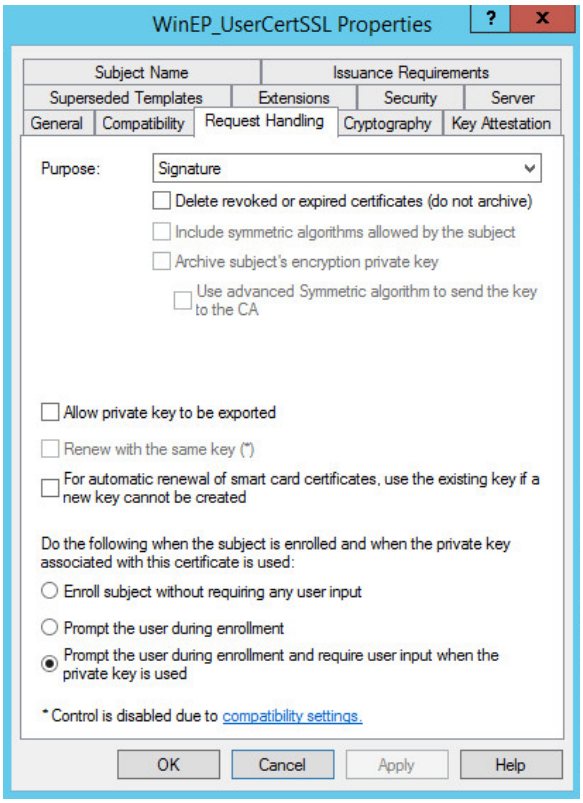


2. Compatibility:

Falls vorhanden (ab Active Directory Version 2008) gemäß Ihrer Umgebung anpassen.

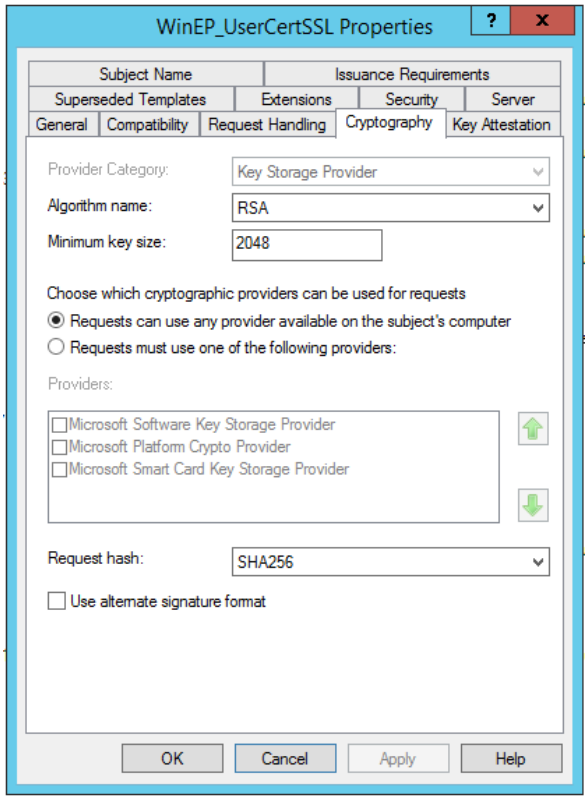


3. Request Handling:
   - Purpose: *Signature*
   - Haken bei *„Allow private key to be exported“ (optional)*
   - *“Prompt the user during enrollment and require user input when the private key is used”* aktivieren

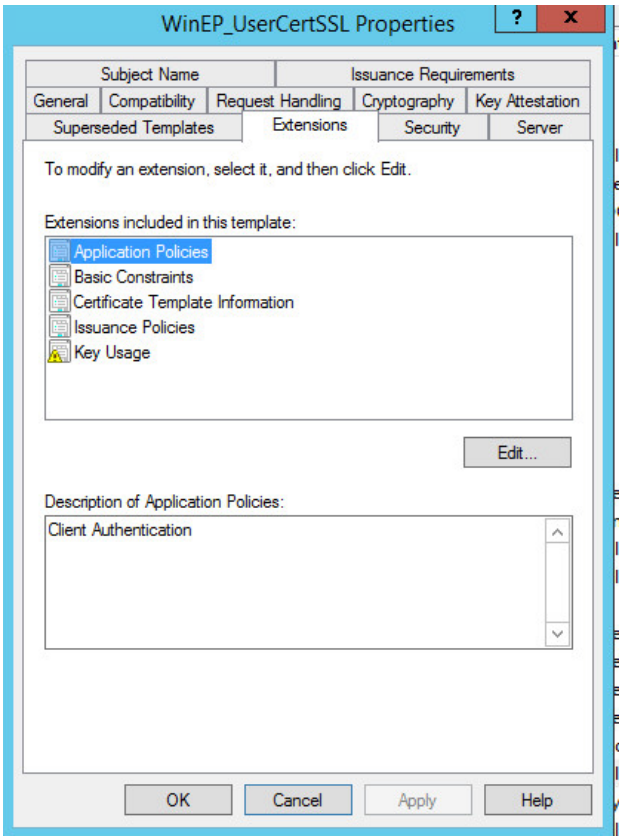


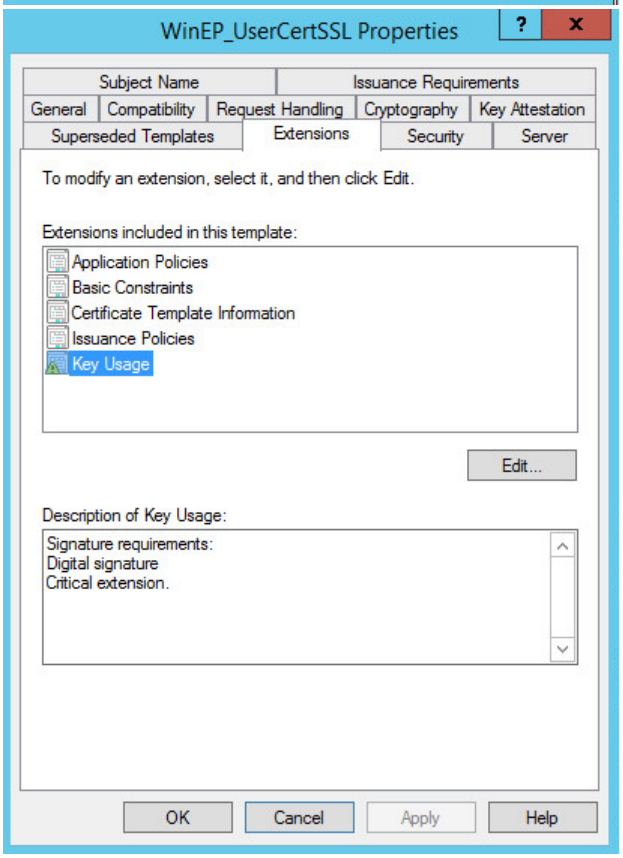
4. Cryptography:
   - Algorithm name: RSA
   - Minimum key size: 2048
   - Request hash: SHA 256

Es darf der Provider „Key Storage Privider“ oder „Legacy Cryptography Service Provider“ eingestellt werden, wobei die Empfehlung bei „KSP“ liegt.
Für „KSP“ muss für die Kompatibilität mind. Windows Server 2008 ausgewählt sein.

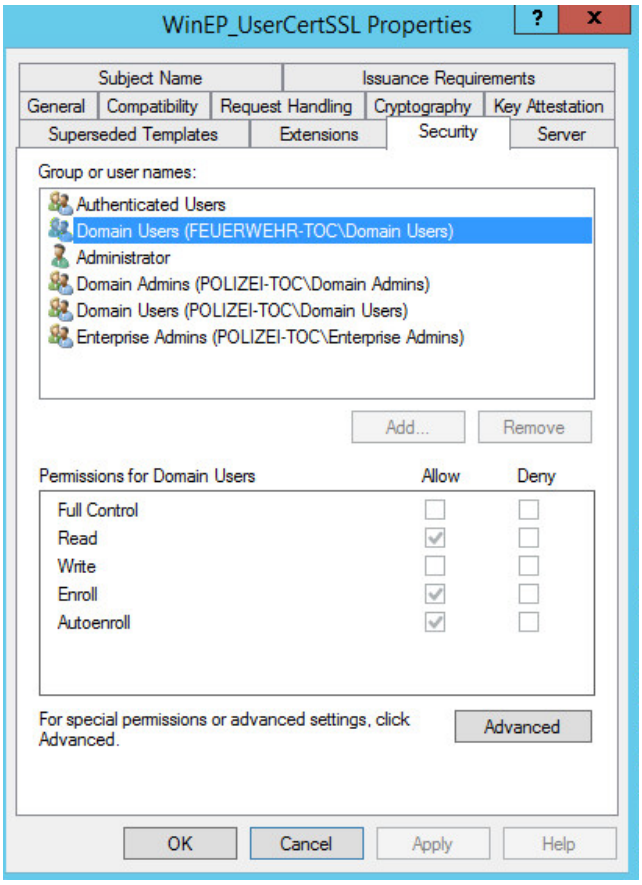


5. Extensions:
   - Application Policies: *Client Authentication*
   - Key Usage:
     - Digital signature
     - Critical extension

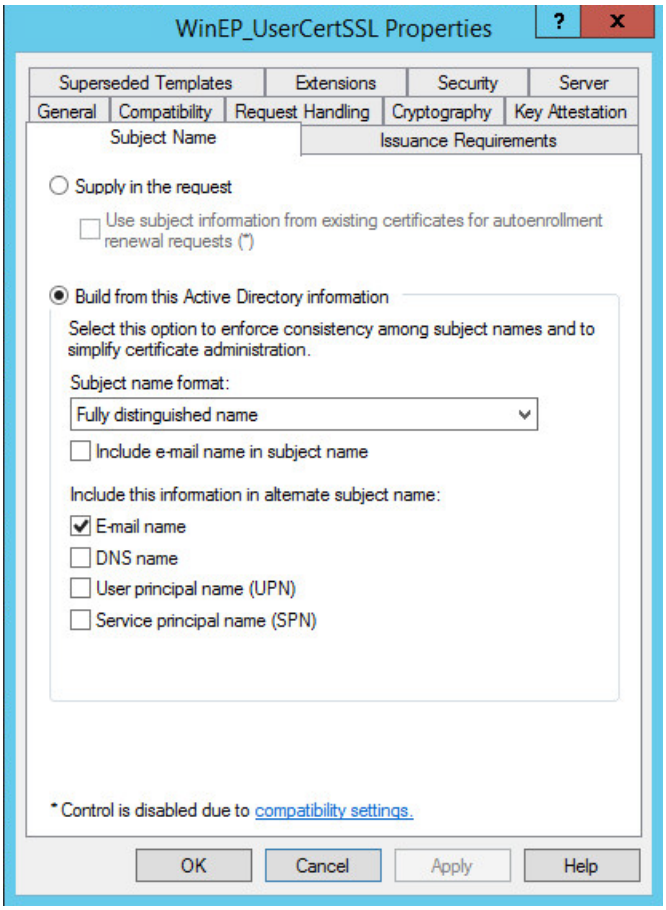




6. Security:
   Alle Nutzerobjekte, die Zertifikate beantragen können sollen, hinzufügen und die Rechte *Read*, *Enroll* und *Autoenroll* vergeben



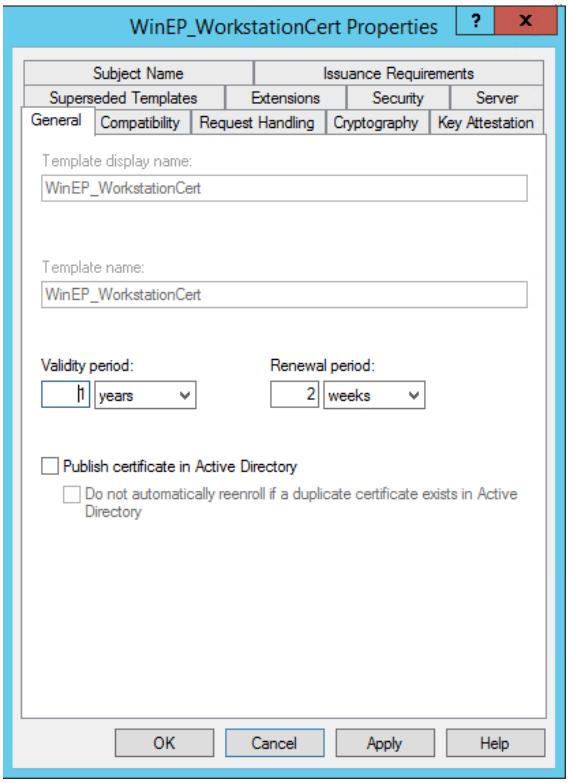
7. Subject Name:
   - *Fully distinguished name* auswählen und Haken bei *E-Mail name* setzen



10.4 Maschinen-Zertifikat - WinEP_WorkstationCert

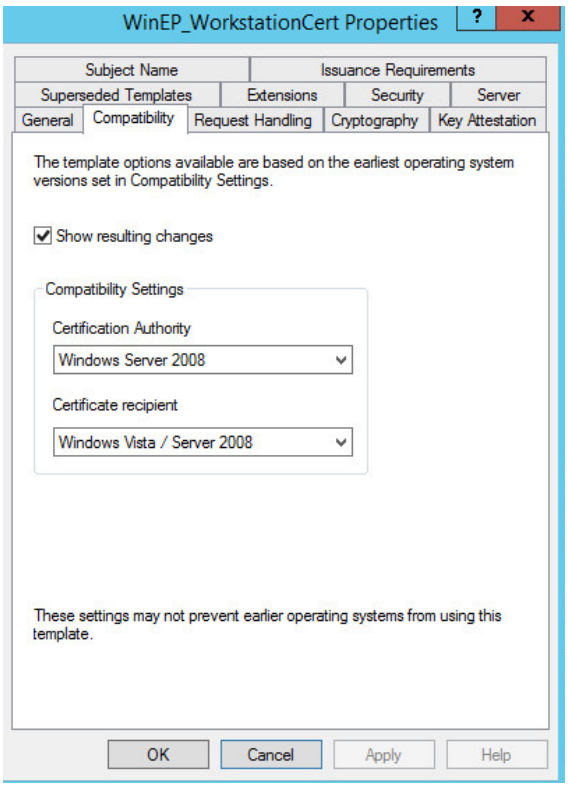
Für das Template des Maschinen-Zertifikats „WinEP_WorkstationCert“ kann das vorhandene „Workstation Cert“-Template dupliziert werden.

1. General:
   - Einstellung der Zertifikatsgültigkeitsdauer: *1 Jahr*
   - Renewal period: *2 Wochen*

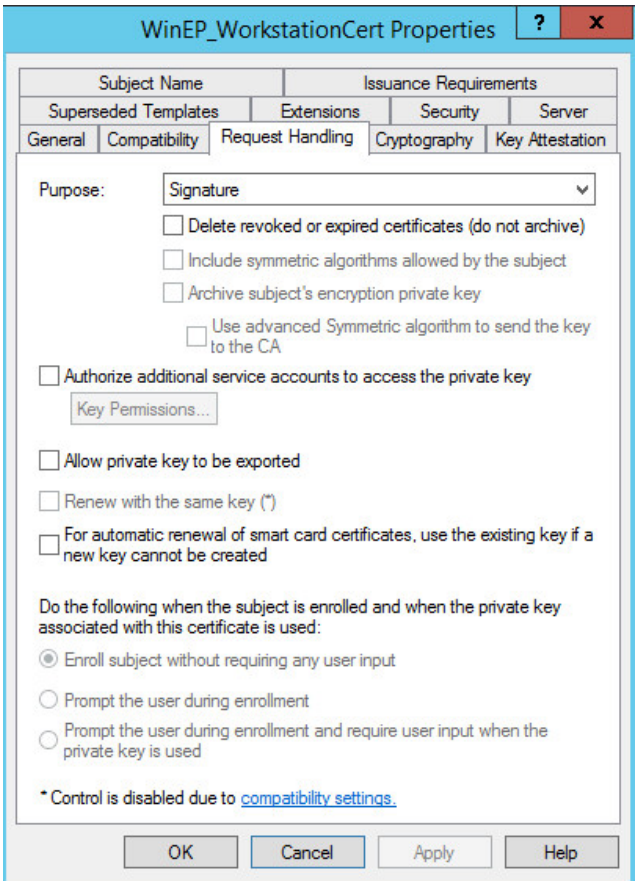


2. Compatibility:

Falls vorhanden (ab Active Directory Version 2008) gemäß Ihrer Umgebung anpassen

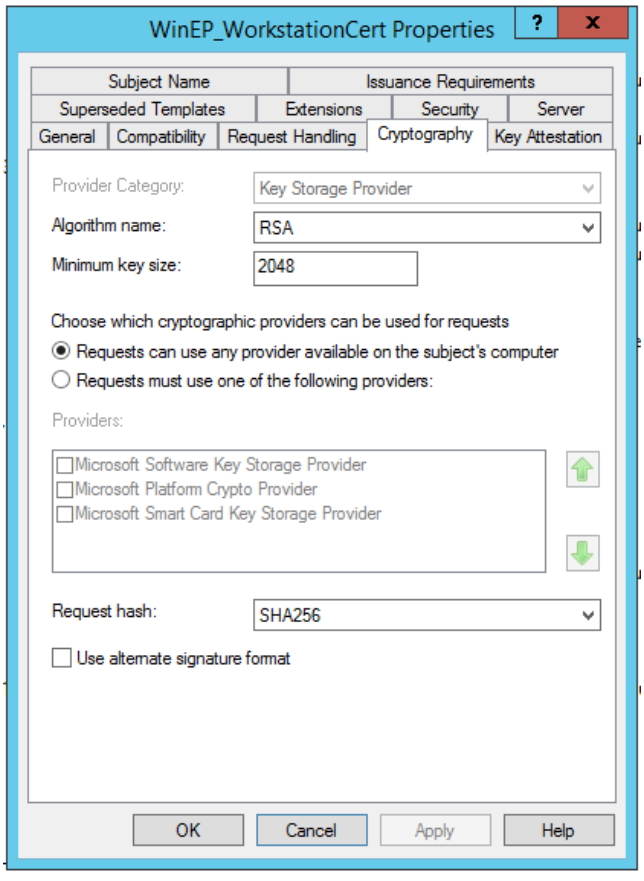


3. Request Handling:
   - Purpose: *Signature*

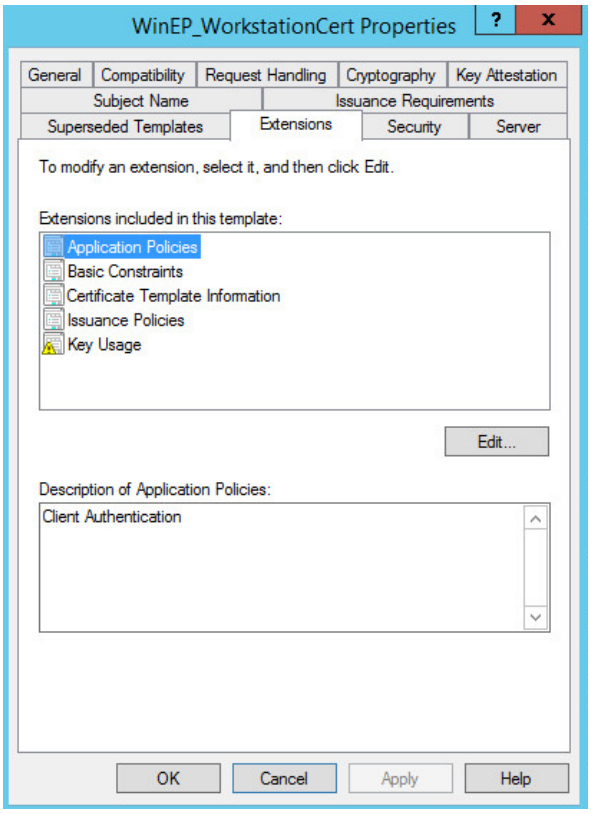


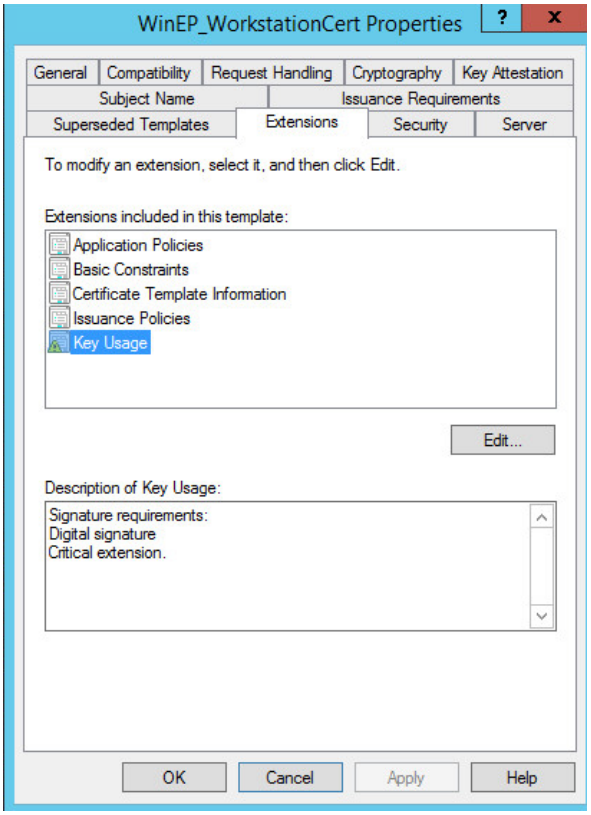
4. Cryptography:
   - Algorithm name: RSA
   - Minimum key size: 2048
   - Request hash: SHA 256

Bei älteren Active Directory Versionen ist dieser Menüpunkt unter *Request Handling* zu finden.
Bei Compatibility muss für RSA min. Windows Server 2008 ausgewählt sein.

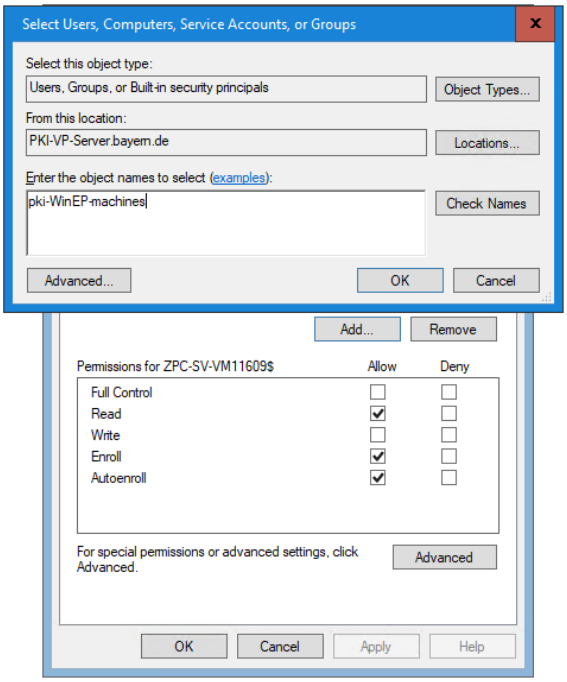


5. Extensions:
   - Application Policies: *Client Authentication*
   - Key Usage:
     - Digital signature
     - Critical extension

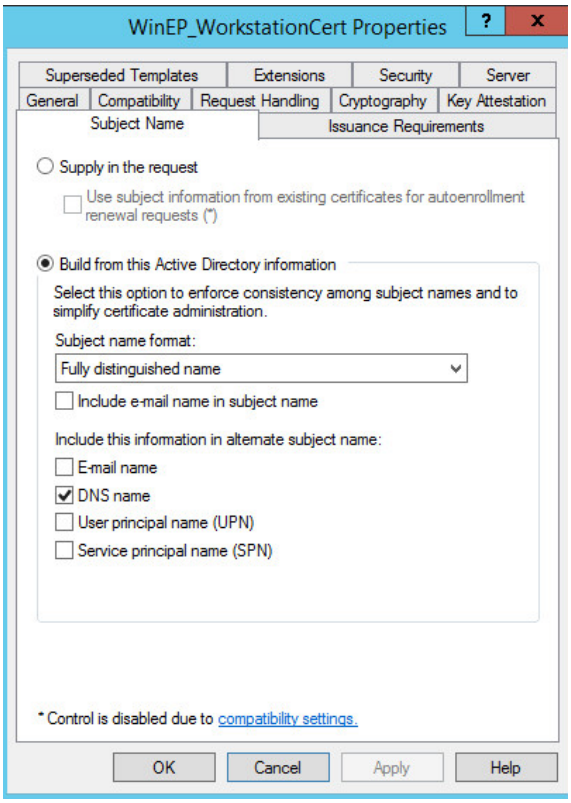




6. Security:
   Alle Computerobjekte, die Zertifikate beantragen können sollen, hinzufügen und die Rechte *Read*, *Enroll* und *Autoenroll* vergeben



7. Subject Name:
   - *Fully distinguished name* auswählen und Haken bei *DNS name* setzen



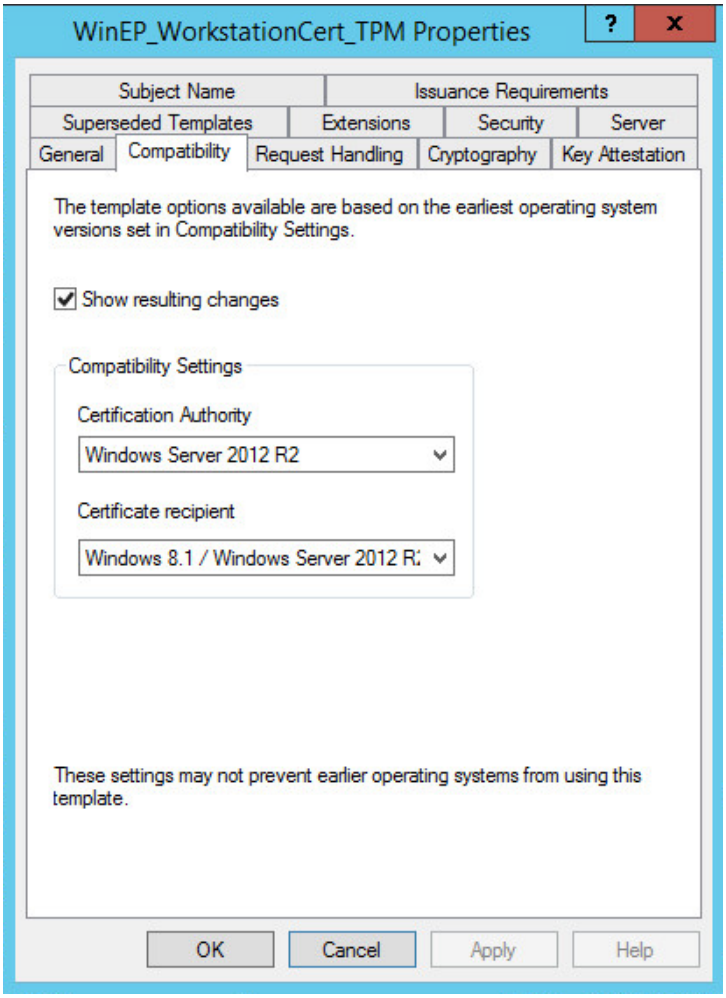
10.5 Maschinen-Zertifikat - WinEP_WorkstationCert_TPM

Sofern Ihre Maschinen einen TPM-Chip besitzen und bei Ihnen mind. Windows 8.1 und Windows Server 2012 R2 im Einsatz ist, können Sie diesen auch als Zertifikatsspeicher für Ihre Maschinenzertifikate nutzen.
Bei Nutzer-Zertifikate empfehlen wir die Nutzung des TPM nicht, da hier kein Backup des privaten Schlüssels des Verschlüsselungs-Zertifikats möglich ist.

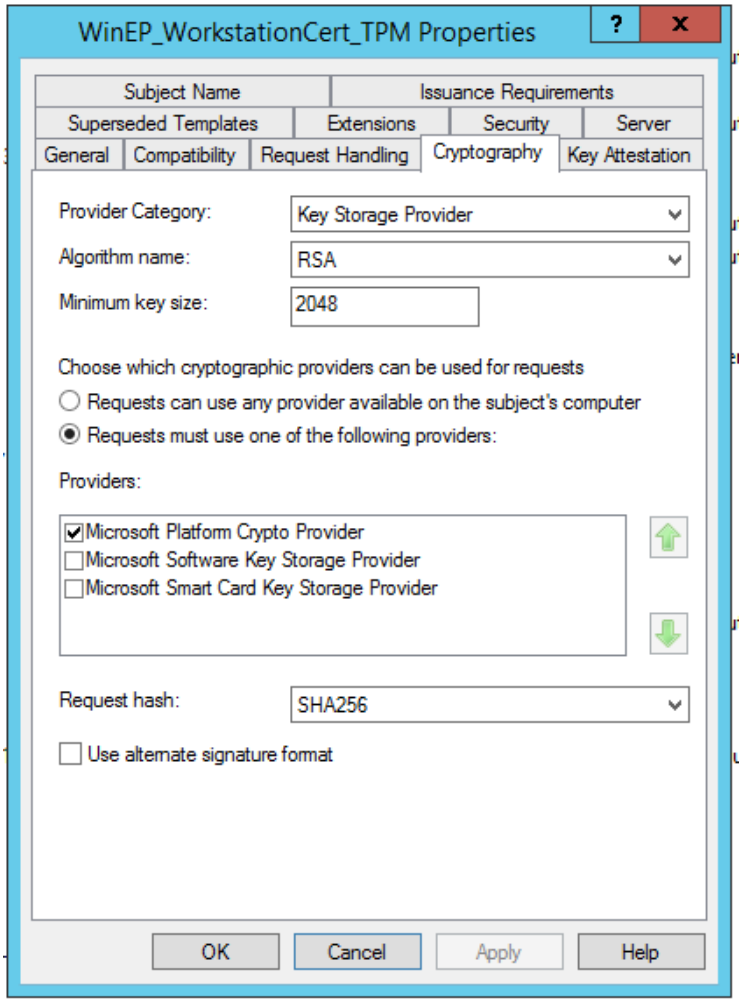
Legen Sie ein „WinEP_WorkstationCert_TPM“ Template an, indem Sie das vorhandene „WinEP_WorkstationCert“-Template duplizieren.

Folgende zusätzliche Einstellungen sind notwendig:

1. Compatibility:
   - Certification Authority: *Windows Server 2012 R2*
   - Certificate recipient: *Windows 8.1 /Windows Server 2012R2*



2. Cryptography:
   - Algorithm name: *RSA*
   - Minimum key size: 2048
   - Requests must use one of the following providers
     - *Microsoft Platform Crypto Provider*
   - Request hash: SHA256



11 Beantragung der Zertifikate

11.1 Nutzer Zertifikate (persönliche Zertifikate)

Damit ein Nutzer persönliche Zertifikate von der Bay. Verwaltungs-PKI erhalten kann, muss er mit der, dem AD-Eintrag entsprechenden, E-Mail-Adresse in Prime registriert sein und das Initalpasswort geändert haben.
Sind bereits aktive Zertifikate in Prime vorhanden (Softtoken oder Smartcard) erhält der Nutzer keine neuen. Die alten Zertifikate müssten zuerst gesperrt werden.

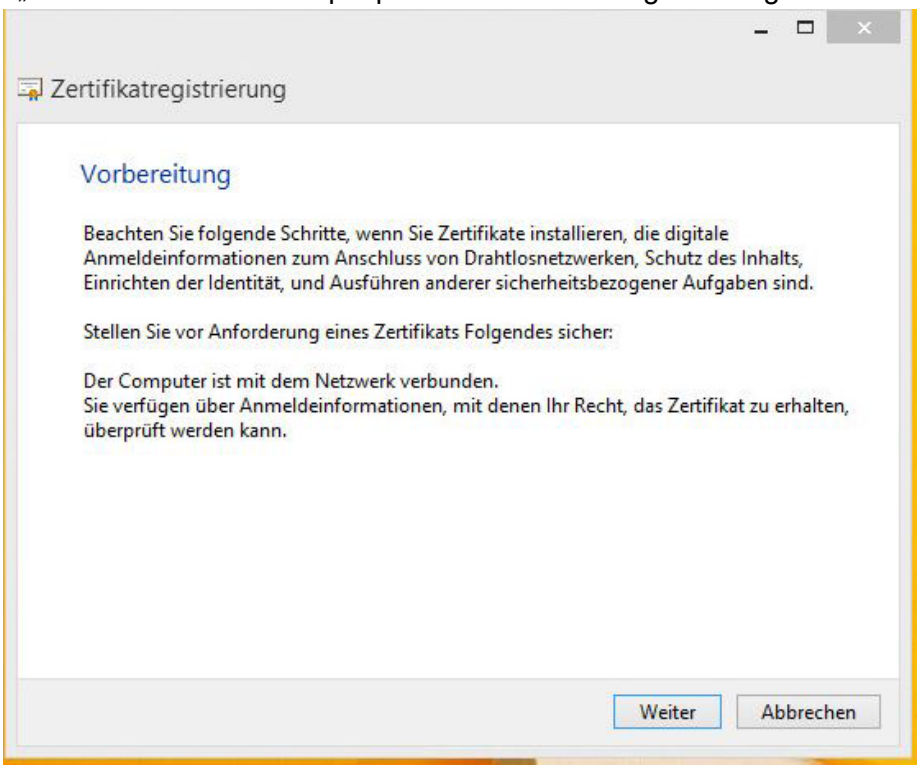
Bei der Beantragung von Nutzer-Zertifikaten ist die Vergabe einer PIN notwendig. Am besten vergeben Sie für alle 3 Zertifikatstypen (Verschlüsselung, Signatur und SSL) dieselbe PIN. Diese wird anschließend bei der Nutzung der Zertifikate/Schlüssel benötigt. Die ausgestellten Zertifikate sind in Prime dem entsprechenden Nutzer zugeordent und können dort auch gesperrt werden.

11.1.1 Automatische Beantragung

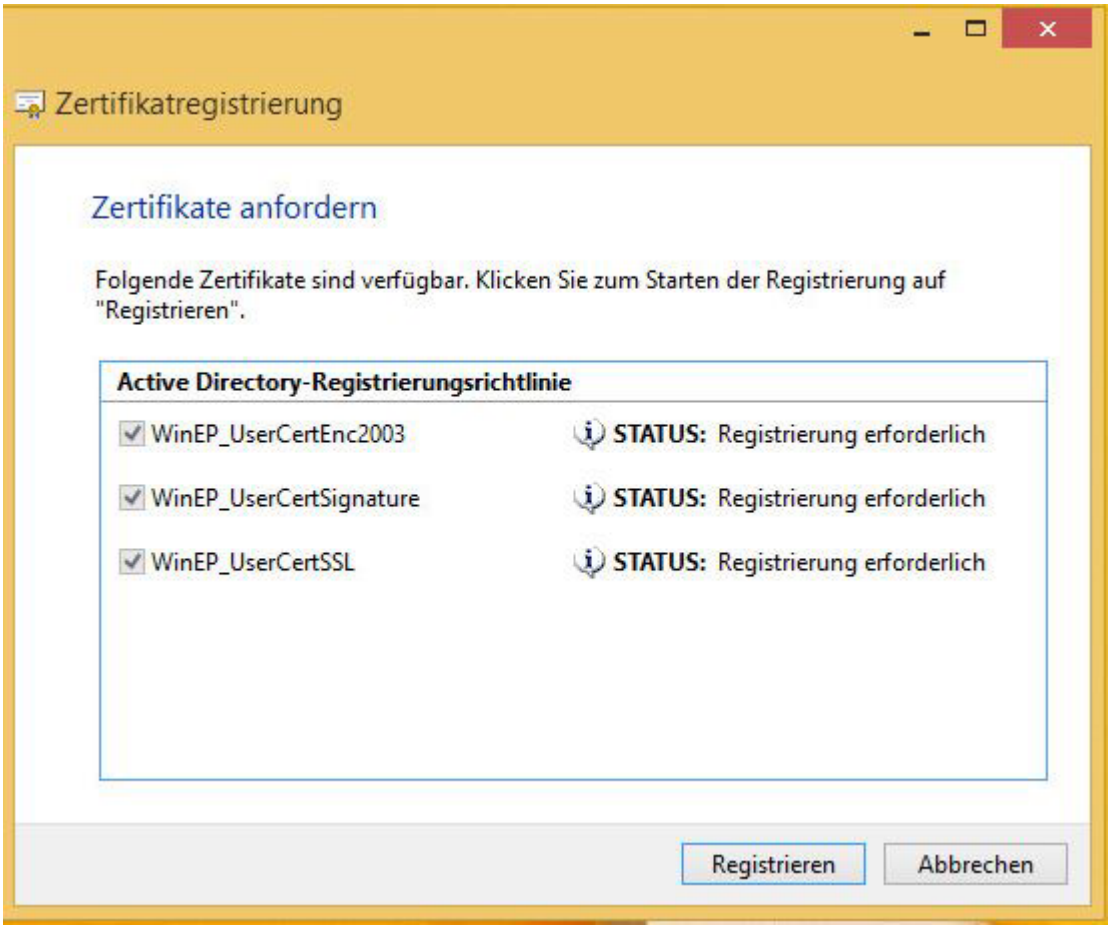
Ist das Autoenrollment von Zertifikaten per GPO aktiviert, sieht die automatische Beantragung von Zertifikaten ab Windows 8.1 wie folgt aus:

1. Bei Anmeldung am Client erscheint eine Meldung

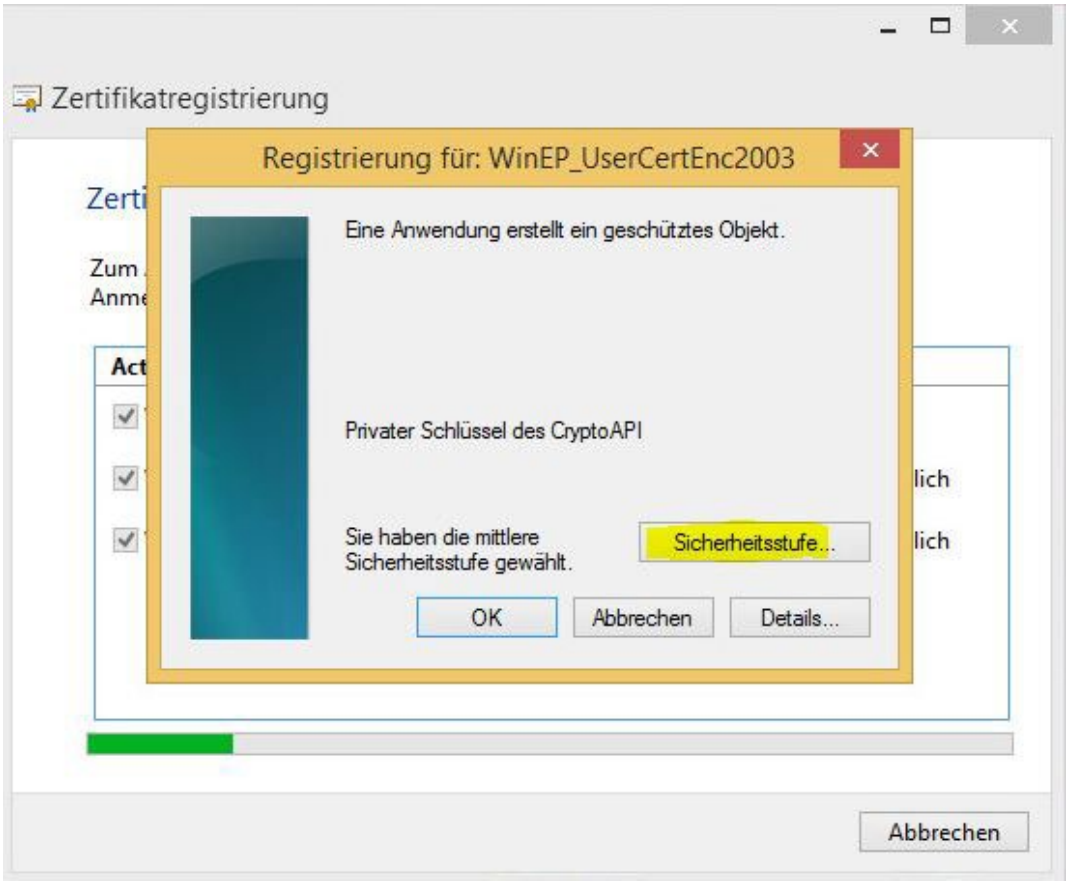
2. Auf das „Zertifikat“ klicken → Pop-Up für die Zertifikatsregistrierung öffent sich → *Weiter*



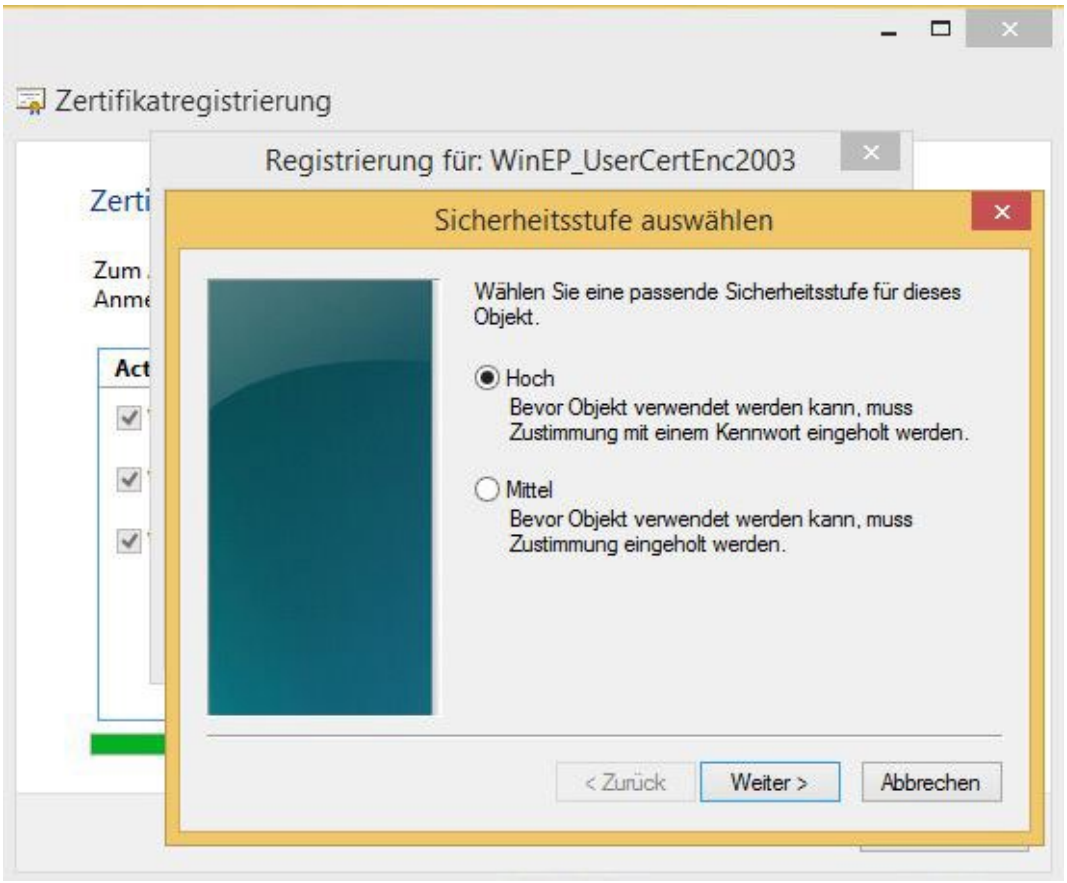
3. Verfügbare Template werden angezeigt (sind bereits ausgewählt) → *Registrieren*



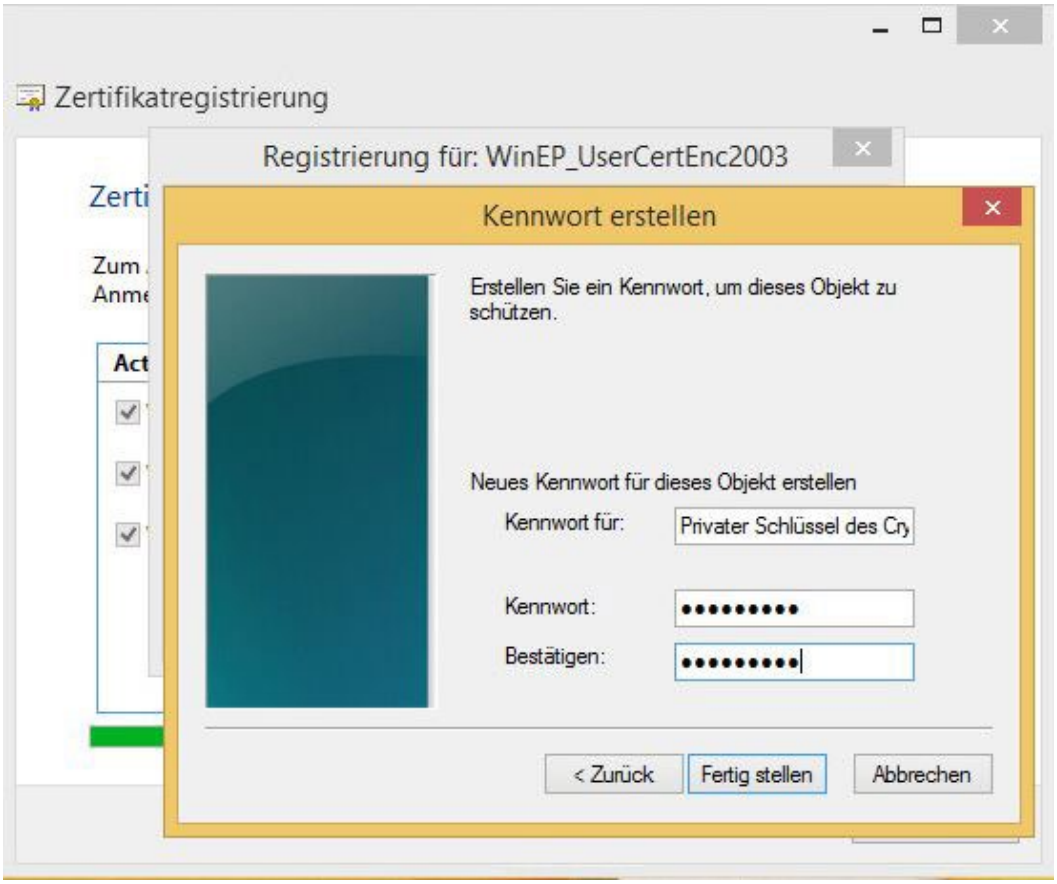
4. Registrierung für Verschlüsselungs Zertifikat → *Sicherheitsstufe*



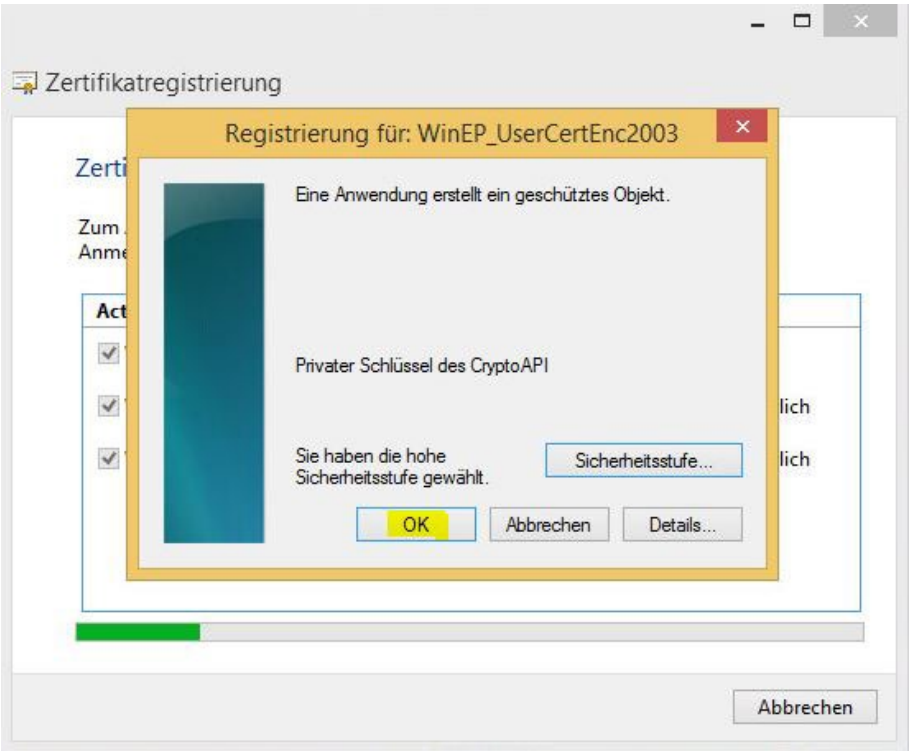
5. Aufgrund der Policy der Bay. Verwaltungs-PKI ist hier die Sicherheitsstufe „Hoch“ zu wählen → *Weiter*



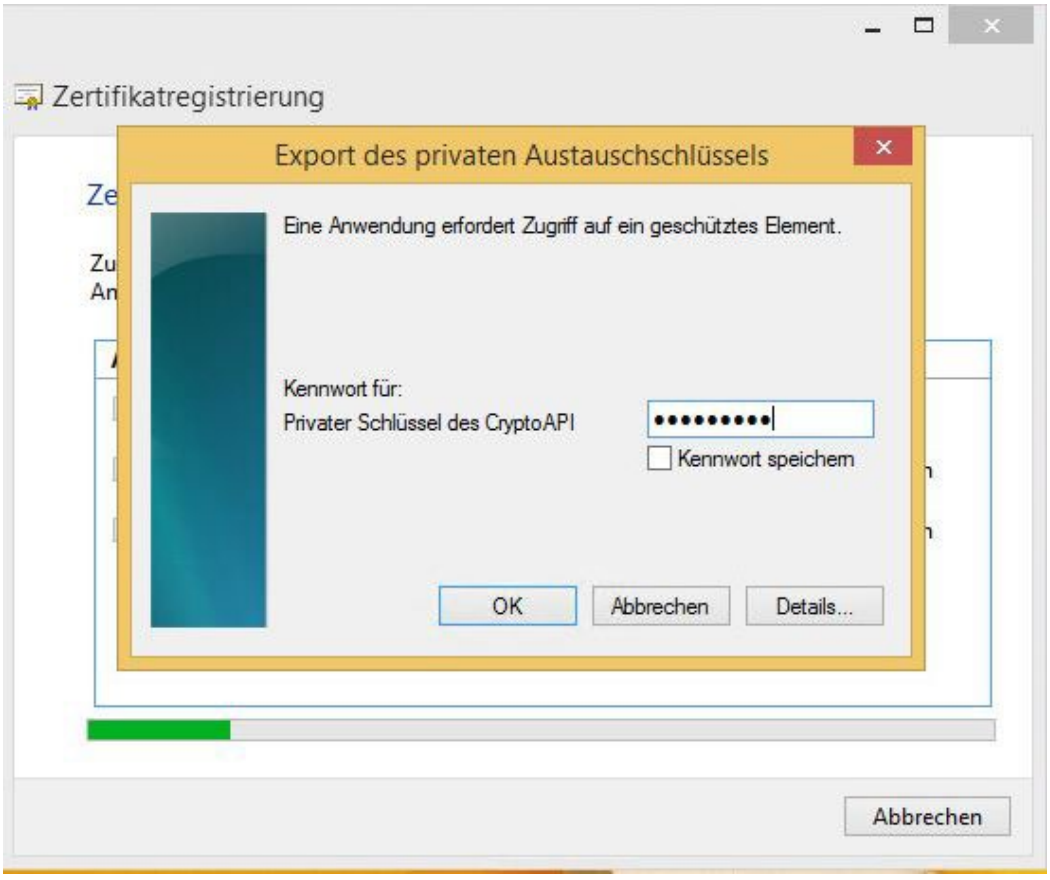
6. Vergabe einer PIN für den Verschlüsselungsschlüssel → *Fertig stellen*



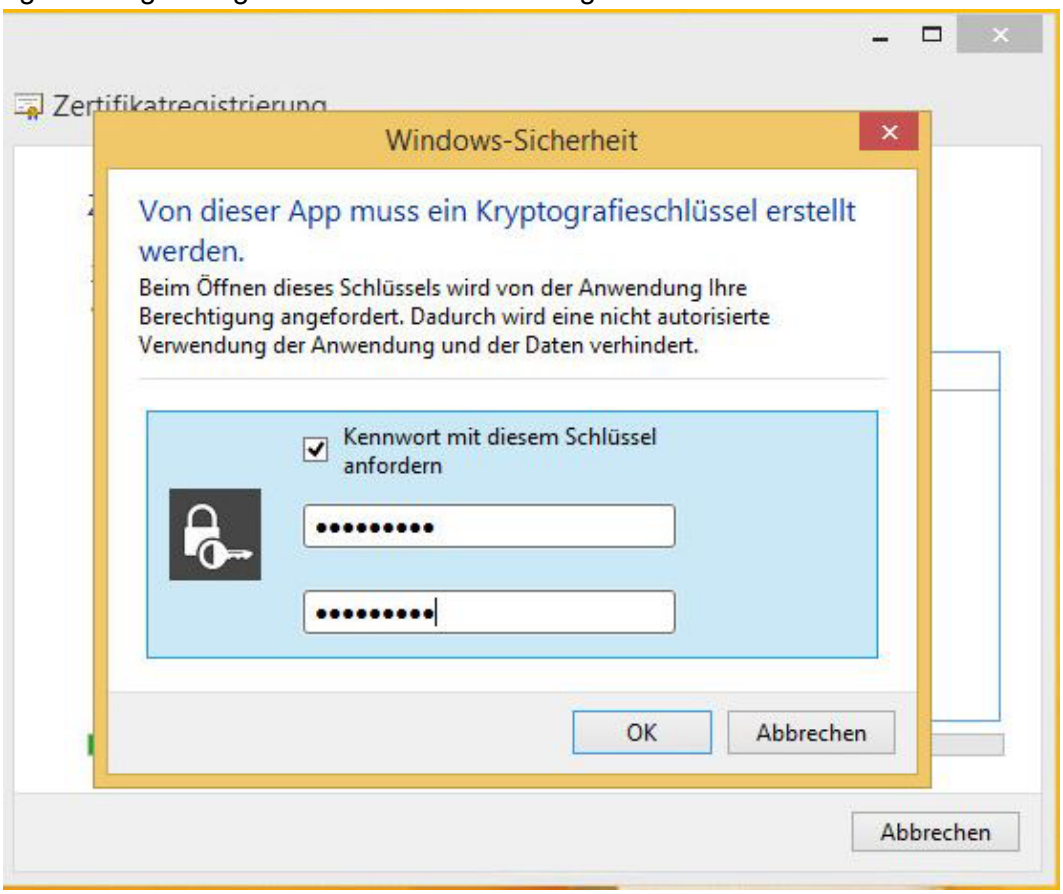
7. Mit *OK* bestätigen



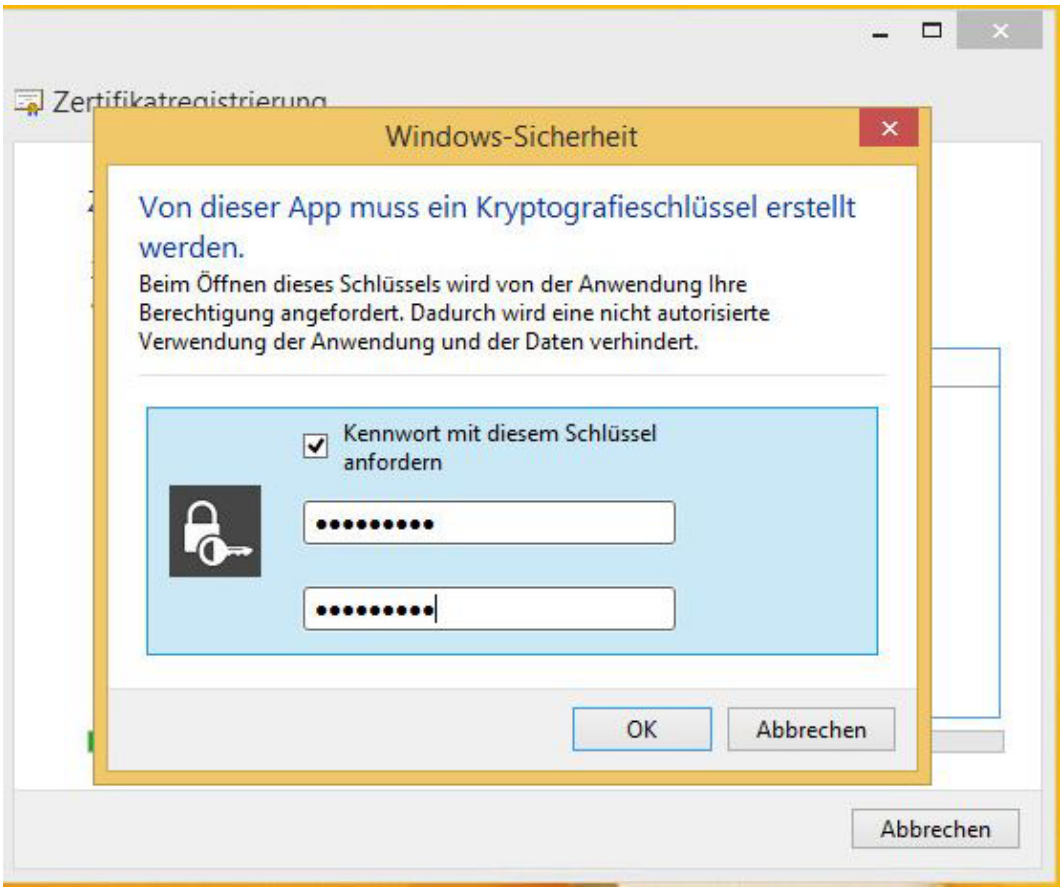
8. Für die Übermittlung des privaten Schlüssels an Prime wird die PIN benötigt → *OK*



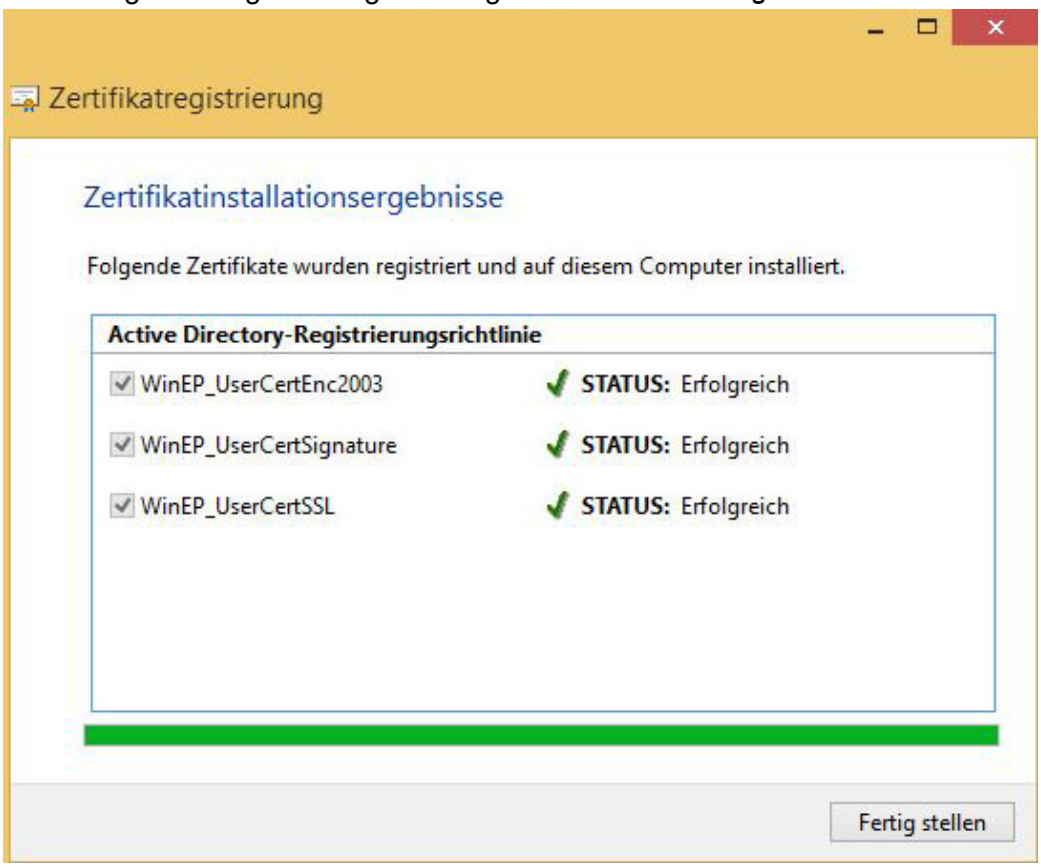
9. Registrierung für Signatur Zertifikat → PIN vergeben → *OK*



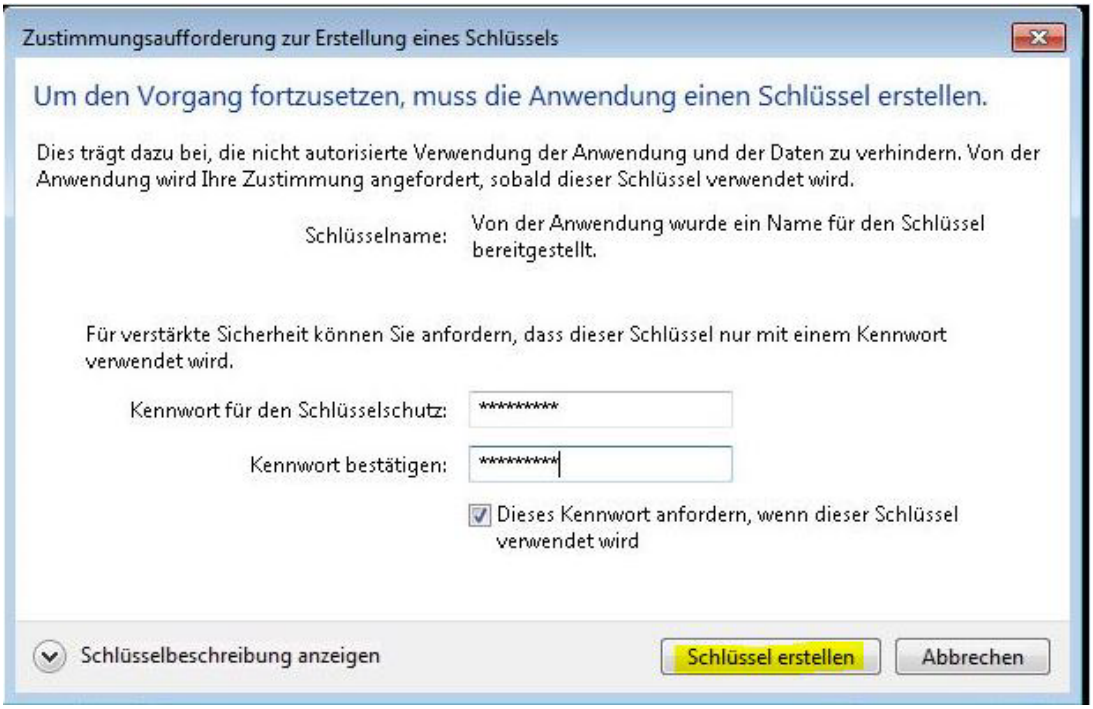
10. Registrierung für SSL Zertifikat → PIN vergeben → *OK*



11. Zertifikatsregistrierung ist erfolgreich abgeschlossen → *Fertig stellen*



Die Beantragung unter Windows 7 unterscheidet sich nur in Schritt 9 und 10. Hier sieht das Pop Up etwas anders aus:



11.1.2 Manuelle Beantragung

Die Zertifikate können auch manuell mittels mmc.exe beantragt werden:

1. File → Add/Remove Snap-in
2. Links auf *Certificates* klicken → *Add*
3. *My user account* → *Finish*
4. *OK* → Pop Up wird geschlossen
5. Links in der Konsolen Struktur *Certificates – Current User* ausklappen
6. Rechtsklick auf *Personal* → *All Tasks* → *Request New Certificate…*
7. Pop-Up für die Zertifikatsregistrierung öffent sich. Ähnlich zu Registrierung unter 10.1.1,mit dem Unterschied, dass die gewünschten Templates ausgewählt werden können. Zertifikate entsprechend beantragen.

Alle ausgestellten Zertifikate sind unter *Certificates – Current User* → *Personal* → *Certificates* zu finden.

11.1.3 Erneuerung der Zertifikate

Wenn die Zertifikatslaufzeit den Zeitraum von 6 Wochen unterschreitet wird bei aktivierten Autonenrollment automatisch ein neues Zertifikat beantragt. Beantragung läuft wie unter Punkt 11.1.1 ab. Manuell kann ein neuer Request auch in dieser 6 Wochen-Frist eingereicht werden.

11.2 Maschinen Zertifikate (Client Zertifikate)

Damit Client Zertifikate automatisch beantragt werden können, muss die Maschine mit dem Fully Qualified Domain Name (FQDN) in Prime registriert sein.
Die ausgestellten Zertifikate sind in Prime dem Client zugeordent und können dort auch gesperrt werden.

11.2.1 Automatische Beantragung

Ist das Autoenrollment von Client-Zertifikaten per GPO aktiviert, so erfolgt die Beantragung im Hintergrund. Es ist keine PIN Vergabe erforderlich.

11.2.2 Manuelle Beantragung

Manuell kann die Zertifikatsbeantragung mittels mmc.exe gestartet werden:

1. File → Add/Remove Snap-in
2. Links auf *Certificates* klicken → *Add*
3. *Computer account* → *Next* → *Local computer…* → *Finish*
4. *OK* → Pop Up wird geschlossen
5. Links in der Konsolen Struktur *Certificates (Local Computer)* ausklappen
6. Rechtsklick auf *Personal* → *All Tasks* → *Request New Certificate…*
7. Pop-Up für die Zertifikatsregistrierung öffent sich. Ähnlich zu Registrierung unter 10.1.1,mit dem Unterschied, dass die gewünschten Templates ausgewählt werden können. Zertifikate entsprechend beantragen.

Alle ausgestellten Zertifikate sind unter *Certificates (Local Computer)* → *Personal* → *Certificates* zu finden.

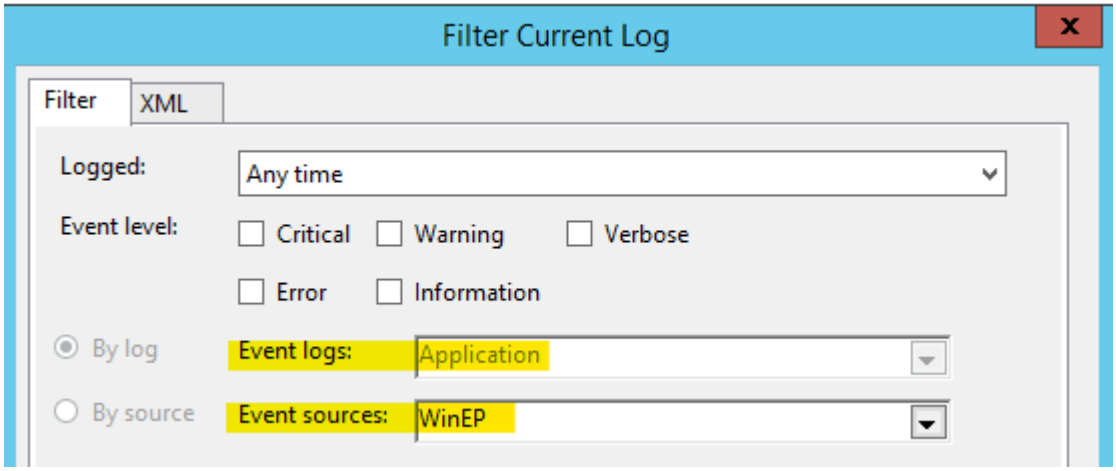
11.2.3 Erneuerung der Zertifikate

Wenn die Zertifikatslaufzeit den Zeitraum von 6 Wochen unterschreitet wird bei aktivierten Autonenrollment automatisch ein neues Zertifikat beantragt. Beantragung läuft wie unter Punkt 11.2.1 ab. Manuell kann ein neuer Request auch in dieser 6 Wochen-Frist eingereicht werden.

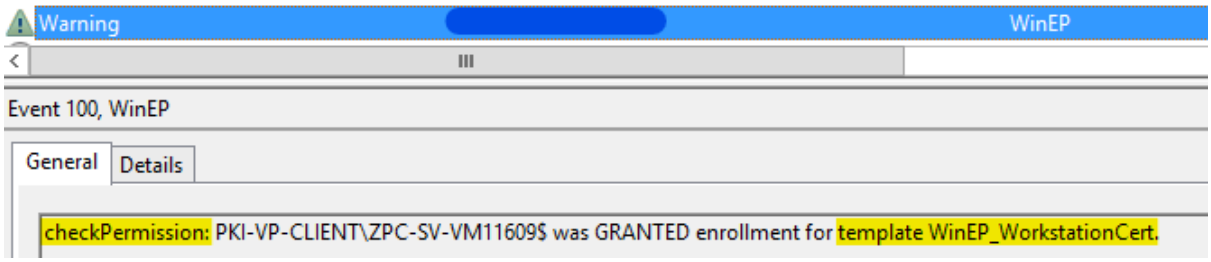
12 Bekannte Fehler

Der Dienst WinEP protokolliert im Windows Eventlog unter Application. Das Log-Level kann wie in Kapitel 7 beschrieben, geändert werden.

Man kann einen Filter im Eventlog über die Quelle „WinEP“ erstellen:



Eingehende Zertifikatsanträge werden als Warnung dokumentiert.
Im Meldungstext werden Benutzer bzw. Client und die beantragte Zertifikatsvorlage protokolliert:

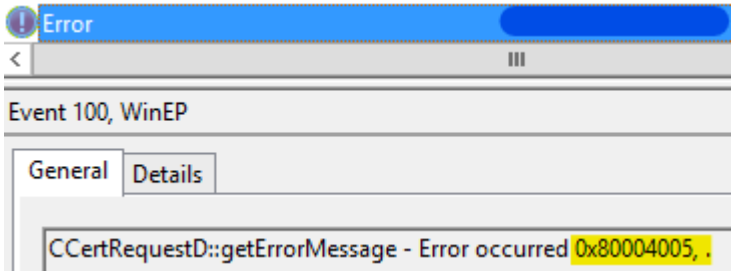


In den nachfolgenden Abschnitten werden einige häufig vorkommende Fehler und mögliche Ursachen genannt.

Sollte Ihr Fehler nicht dabei sein, starten Sie bitte einmal den WinEP-Dienst durch. Vielleicht handelt es sich um einen temporären Fehler, der nach dem Durchstarten verschwunden ist.

Besteht der Fehler danach weiter, hilft Ihnen gern unser PKI-Support-Team weiter (Kontaktdaten wie unter 1.1). Halten Sie dafür bitte Eventlogs, Zeitstempel und Daten zum Antragsteller (Name des Teilnehmers oder PCs) bereit.

12.1 Fehlercode 0x80004005



Dieser Fehlercode tritt häufig auf.

In den meisten Fällen ist die Fehlerursache in Prime zu finden. Bitte prüfen Sie zunächst in Prime:

- Ist der Benutzer bzw. Client in Prime registriert?
- Bei Benutzern: Hat sich der Teilnehmer mindestens einmal an Prime angemeldet und dabei sein Passwort geändert?
- Gibt es für diesen Benutzer bzw. Client bereits gültige (aktive) Zertifikate in Prime und sind diese noch länger als 6 Wochen gültig?

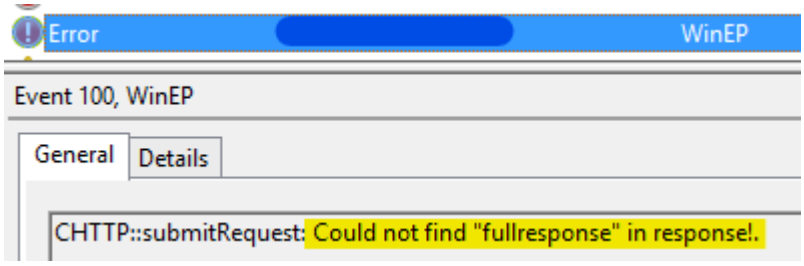
Handelt es sich um eine Zertifikatsverlängerung kommen auch die in Kapitel 12.2 dokumentierten Fehler in Betracht.

12.2 Fehler bei Zertifikatsverlängerungen

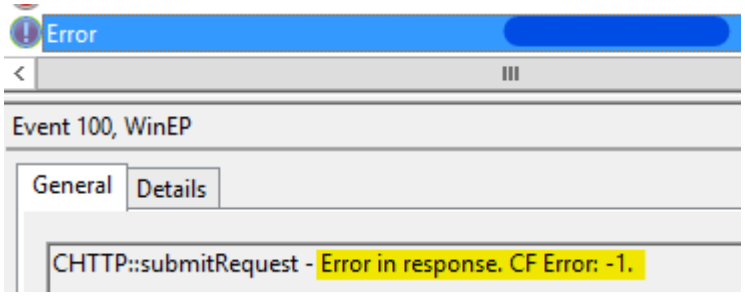
Bei Zertifikatsverlängerungen sind weitere Fehler bekannt.

12.2.1 Fehlercode 0x80004005 bei Zertifikatsverlängerung:

Handelt es sich um eine Zertifikatsverlängerung und sind die in Kapitel 12.1 benannten Fehler ausgeschlossen, sollten Sie nach einem der folgenden Fehlereinträge im WinEP Eventlog schauen:



Oder



Diese Fehlermeldungen sind zeitlich vor der Meldung 0x80004005 eingeordnet.
I.d.R. tritt nur eine der beiden Fehlermeldungen auf.

Der Fehler ist in der WinEP-Gegenstelle beim IT-DLZ (PGWY) begründet. Eine Lösung wurde beim Software-Hersteller angefordert.

Auswirkungen:

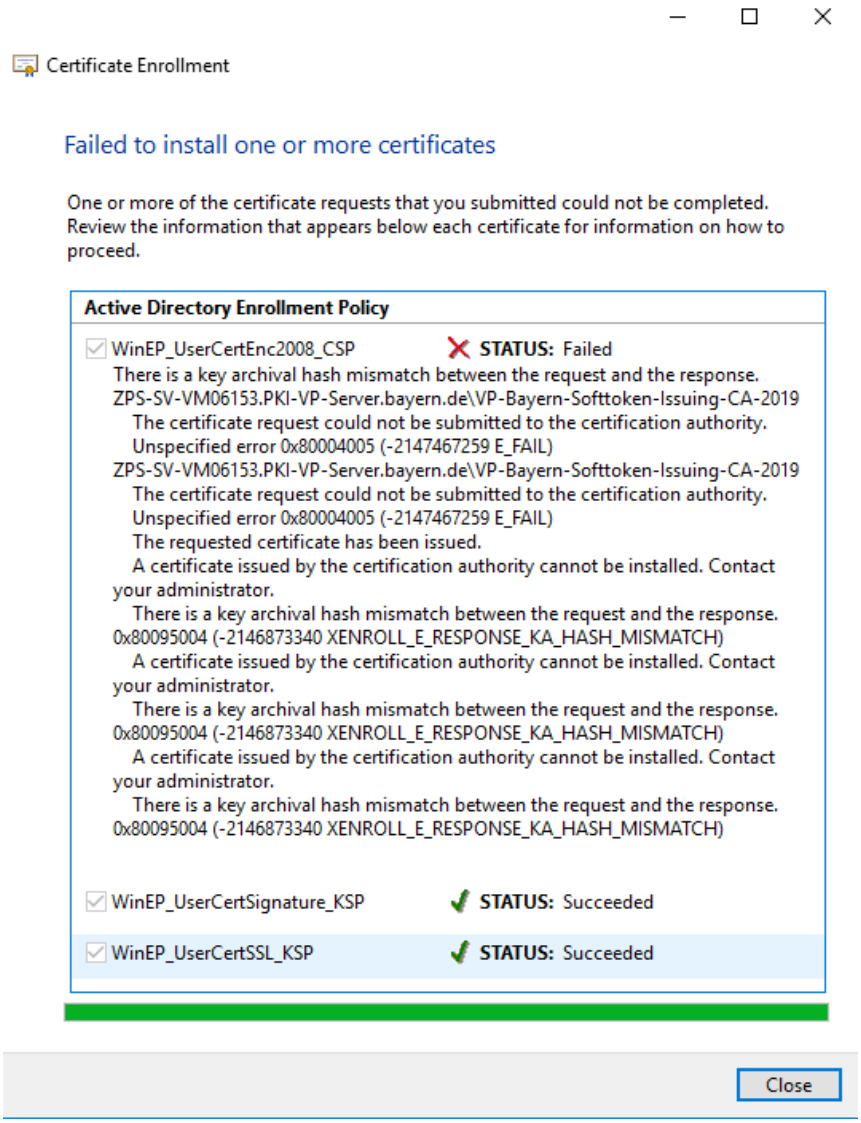
Unsere Tests haben zwei Varianten gezeigt:
In manchen Fällen muss der Benutzer die Fehlermeldung mit „Cancel“ bzw. „Abbrechen“ wegklicken. In anderen Fällen reagiert der Windows-Clients automatisch auf den zurückgemeldeten Fehler mit einem zweiten Zertifikatsantrag, der dann erfolgreich ist.
Der zweite Zertifikatsantrag ist anders aufgebaut und kann daher von der CA interpretiert und erfolgreich verarbeitet werden.

12.2.2 Fehler bei der Verlängerung eines Verschlüsselungszertifikates

Bei der Verlängerung (Erneuerung) von Verschlüsselungszertifikaten gibt es derzeit einen dauerhaften Fehler. Wir arbeiten noch an einer Lösung.

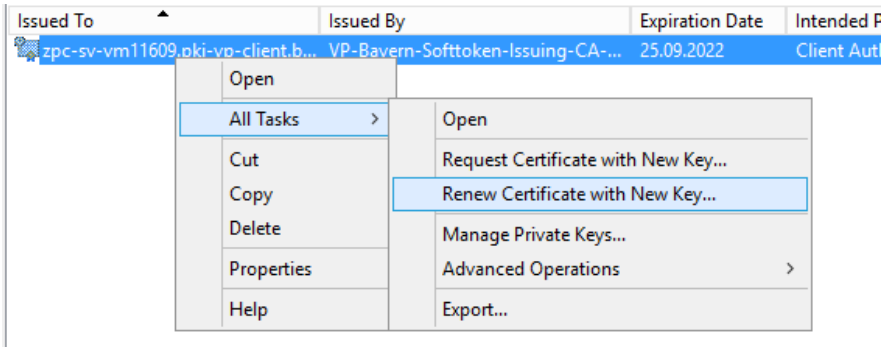
Verschlüsselungszertifikate werden im Unterschied zu allen anderen Zertifikaten während des Zertifizierungsprozesses an Komponenten des IT-DLZ übermittelt. Die Übermittlung erfolgt mit Bordmitteln des Windows Betriebssystems und verschlüsselt und zum Zweck der Archivierung und damit der Möglichkeit einer späteren Wiederherstellung (z.B. im Verlustfall).

Auf dem Client wird folgender Fehler angezeigt:



12.2.3 Workaround

Da beide o.g. Fehler nach unserer Kenntnis bisher nur auftreten, wenn der Windows-Client eine automatische Zertifikatserneuerung (Renew) beantragt wird, empfehlen wir statt der Erneuerung (Renew) einen Neuantrag (Request) durchzuführen.
Dies ist am einfachsten über die MMC und das Snap-In „Zertifikate“ bzw. certificates.msc umsetzbar.



Bei **Renew** kommt es zum Fehler.

Ein **Request** ist erfolgreich.

Standardbenutzer ohne lokale Administratorenrechte haben allerdings keinen Zugriff auf die MMC.

In diesen Fällen gibt es zwei weitere Optionen, die allerdings beide ihre Nachteile haben:

1. Sie sperren noch gültige Zertifikate in Prime. Der Client (PC) bemerkt dies und startet automatisch Neuanträge.
   Nachteil: Der Benutzer hat temporär keine gültigen Zertifikate. Wir können keine Aussage treffen, wie lange der Automatismus zur Neubeantragung dauert.
2. Sie entfernen vorhandene Zertifikate aus dem lokalen Zertifikatsspeicher des Benutzers (auf dessen PC). Der Client (PC) bemerkt dies und startet automatisch Neuanträge. Auch hier können wir keine genaue Aussage treffen, wie lange dies dauert.
   Nachteil: Dem Benutzer fehlen alte Verschlüsselungszertifikate. Sollen z.B. alte E-Mail entschlüsselt werden, muss das Verschlüsselungszertifikat aus Prime wiederhergestellt und am PC installiert werden.