



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

1	Übersicht	5
1.1	Anforderungen	5
1.2	Anlagen	6
2	Importieren der AD-Einträge	7
2.1	Certification Authorities Container	7
2.2	Enrollment Services Container	7
2.3	KRA Container	8
2.4	NTAuth Container	8
3	GPO für Autoenrollment der Zertifikate	9
3.1	GPO für Nutzerzertifikate	9
3.2	GPO für Maschinenzertifikate	10
3.3	GPO für Wurzel- und Sub-CA-Zertifikate	10
4	Global Catalog	11
5	WinEP-Serviceaccount	12
6	Installation WinEP	13
7	Konfiguration WinEP	17
8	Firewall Freischaltung	
8.1	WinEP Server	18
8.1.1	Zugriff Protocol Gateway	
8.1.2	RPC-Ports (nur AD intern)	
8.2	Clients (nur AD intern)	18
9	DCOM Konfiguration	19
10	Windows Zertifikats Templates für WinEP	20
10.1	Nutzer Verschlüsselungszertifikat - WinEP_UserCertEnc2003	20
10.2	Nutzer Signaturzertifikat - WinEP_UserCertSignature	25
10.3	Nutzer Authentifizierungszertifikat - WinEP_UserCertSSL	29

10.4	Maschinen-Zertifikat - WinEP_WorkstationCert	33
10.5	Maschinen-Zertifikat - WinEP_WorkstationCert_TPM	37
11	Beantragung der Zertifikate	. 39
11.1	Nutzer Zertifikate (persönliche Zertifikate)	39
11.1.1	Automatische Beantragung	39
11.1.2	Manuelle Beantragung	45
11.1.3	Erneuerung der Zertifikate	45
11.2	Maschinen Zertifikate (Client Zertifikate)	46
11.2.1	Automatische Beantragung	46
11.2.2	Manuelle Beantragung	46
11.2.3	Erneuerung der Zertifikate	46
12	Bekannte Fehler	47
12.1	Fehlercode 0x80004005	48
12.2	Fehler bei Zertifikatsverlängerungen	49
12.2.1	Fehlercode 0x80004005 bei Zertifikatsverlängerung:	49
12.2.2	Fehler bei der Verlängerung eines Verschlüsselungszertifikates	50
12.2.3	Workaround	51

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: <u>pki-support@ldbv.bayern.de</u>

1.2 Anlagen

- Root-CA-Zertifikate
 - Bayern-PKI: Bayern-Root-CA-2019.cer
- Sub-CA-Zertifikate
 - o 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:

WIN EP [DC-POL-01.POLIZEI-TOC.BAYERN.DE]	Object Type
🕀 🐏 Computer Configuration	Enterprise Trust
🖃 🕵 User Configuration	Trusted People
🖃 🧮 Policies	Certificate Services Client - Certificate Enrollment Policy
🕀 🚞 Software Settings	Certificate Services Client - Credential Roaming
🖃 🧮 Windows Settings	Certificate Services Client - Auto-Enrollment
a Scripts (Logon/Logoff)	
🖃 🚋 Security Settings	
🖃 🧮 Public Key Policies	
🧮 Enterprise Trust	Certificate Services Client - Auto-Enrollment Properties
🧮 Trusted People	Enrollment Policy Configuration
🕀 🚞 Software Restriction Policies	
E Folder Redirection	
🕀 📊 Policy-based QoS	Enroll user and computer certificates automatically
🛨 🎢 Internet Explorer Maintenance	
🕀 🚞 Administrative Templates: Policy defi	Configuration Models
🕀 🔛 Preferences	
	Renew expired certificates, update pending certificates, and remove
	Update certificates that use certificate templates
	Expiration notification
	Show expiry notifications when the percentage of remaining certificate
	lifetime is
	10 2 %
	Learn more about Automatic certificate management
	OK Cancel Apply
	1

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

dNSHostName Properties							
General							
di di	NSHostName						
Description:	DNS-Host-Name						
Common Name:	DNS-Host-Name						
X.500 OID:	1.2.840.113556.1.4.6	19					
Syntax and Range							
Syntax:	Unicode String		0				
Minimum:	0						
Maximum:	2048						
This attribute is sing	gle-valued.						
Attribute is active Index this attribute Ambiguous Name Resolution (ANR) Replicate this attribute to the Global Catalog Attribute is copied when duplicating a user Index this attribute for containerized searches							
ОК	Cancel	Apply	Help				

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 i	mportierten,	CAs	durchführen.
----------	---------	-------	-------	--------------	-----	--------------

📝 ADSI Edit				
File Action View Help				
🗢 🔿 🔁 🖬 🖻 🖻 🔂 🖬				
📝 ADSI Edit	Name	Class	Distinguished Name	Actions
Configuration [DC-POL-01.polizei-toc.bayern.de]	CN=Test-Issuing-CA-2016	pKIEnrolm	CN=Test-Issuing-CA-201	CN=Enrollment Services
CN=Configuration,DC=polizei-toc,DC=bayern,DC=de	CN=Test-Issuing-CA-2016-2	pKIEnrolm	CN=Test-Issuing-CA-201	
CN=DisplaySpecifiers				More Actions
CN=Extended-Rights				
CN=ForestUpdates				
CN=LostAndFoundConfig				
CN-Partuons				
CN-AuthN Policy Configuration				
CN=Claims Configuration				
CN=Group Key Distribution Service				
CN=Microsoft SPP				
CN=MsmqServices				
CN=NetServices				
🖃 🧰 CN=Public Key Services				
CN=AIA				
CN=CDP				
CN=Certificate Templates				
CN=Certification Authorities				
CN=Enrollment Services				
CN=KRA				
CN=OID				
CN=RRAS				
CN-Sites				
]

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\WinEF	² -User					
Password						
Back Next	Cancel					

👘 neXus Windows Enrolln	nent Proxy Setup	
Ready to install neXu	s Windows Enrollment Proxy	nexus
Click Install to begin the i settings. Click Cancel to e	nstallation. Click Back to review or change any xit the wizard.	of your installation
	Back 💱 Install	Cancel
02.07.2015 08:38	Windows Installer P 1.924 KB	
🎼 neXus Windows Enrollm	ent Proxy Setup	
Installing neXus Wind	lows Enrollment Proxy	SW2 ×
Do you want to publisher to ma	allow the following program from an unknow ke changes to this computer?	n The second sec
Program name: Publisher: File origin:	D:\20150710_WinEP\WinEP\WinEP\winep.msi Unknown Hard drive on this computer	
Show details	Yes	NO
	Change when these notification	ons appear
	Back Next	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* \rightarrow *Application* zu finden.

5. Auf *Ok* klicken \rightarrow Service wird neugestartet

Falls der Service nicht startet (Logon Failure), die WinEP Service Kennung über Services \rightarrow neXus WinEP \rightarrow Rechtsklick: Properties \rightarrow Log On neu berechtigen

9	neXus WinEP Configuration
Configuration	
- Protocol Gatew	ay Configuration
Hostname :	pgwy.pki.bybn.de
Port :	8449
URL :	/pgwy/winep
SSL Certificate	CN=WinEP-Officer-rzsued-toc, O=Freistaat Bayem, C=DE
	Set SSL Certificate Display SSL
Logging	
The log level sh	ould be changed for testing or diagnostic purposes only.
Log level :	2
<u></u>	
<u> </u>	Ok Cancel Apply

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: <u>https://support.microsoft.com/de-de/kb/832017</u>

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 \rightarrow Launch and Activation Permissions: Customize \rightarrow Edit
 - a. WinEP-User (Serviceaccount) hinzufügen und alle Berechtigungen auf Allow setzen
 - b. Everyone hinzufügen und alle Berechtigungen auf Allow setzen
- 6. Security Tab \rightarrow Configuration Permission: Customize \rightarrow Edit
 - a. WinEP-User (Serviceaccount) hinzufügen und *Full Control* und *Read*-Rechte vergeben
 - b. Authenticated Users hinzufügen und Read-Rechte zuweisen
- 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: <u>https://technet.microsoft.com/en-us/library/cc732445.aspx</u> 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* \rightarrow *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.

2

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

	VVIIIEP_	_oserce	entenczou	J3 PI	ropertie	SL	· ·	
	Subject Name		Issuance Requirements					
Super	seded Template	s	Extensions	Extensions Security			Server	
General	Compatibility	Reques	t Handling	Сгур	tography Key Attest			station
T								
	te display name							
WINEP	_UserCertEnc2	003						
Templa	te name:							
WinEP	UserCertEnc2	003						- 1
TANK TEL		005						
Validity	period:		Renewal	perio	d:			
β	years 🗸	'	2	week	s v			
	hala an anti-ana ta	A - 11 - 1						
	lish certificate in		nrectory				- 0-	
	Do not automatic Directory	cally reen	roll ir a duplid	cate c	ennicate e	XISTS I	n Ac	tive
	OK		Cancel		Apply		μ	alo
	UK		Cancel		- And		THE	aþ

2. Compatibility:

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

WinEP_Use	rCertEnc2003	Properties	?	x
Subject Name	Issi	iance Requirem	ents	
Superseded Templates	Extensions	Security	Se	rver
General Compatibility Req	uest Handling C	ryptography K	ey Atte	station
The template options availab versions set in Compatibility S	le are based on th Settings.	e earliest operati	ing syst	em
Show resulting changes				
Compatibility Settings				
Certification Authority		_		
Windows Server 2008 R	2 🕚	·		
Certificate recipient				
Windows 7 / Server 200	8 R2 🔹	·		
These settings may not preve template.	ent earlier operating	g systems from u	sing thi	S
ОК	Cancel	Apply	He	elp

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

Superseded Templates Extensions Security Server General Compatibility Request Handling Cryptography Key Attestation Purpose: Encryption Delete revoked or expired certificates (do not archive) Include symmetric algorithms allowed by the subject Include symmetric algorithms allowed by the subject Archive subject's encryption private key Image: Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used		Subject	t Name			Issuance Requirements				
General Compatibility Request Handling Cryptography Key Attestation Purpose: Encryption	Super	seded T	emplate	s	Extensions	Security		Server		
Purpose: Encryption Delete revoked or expired certificates (do not archive) Include symmetric algorithms allowed by the subject Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to compatibility settings.	General	Compa	atibility	Requ	est Handling	Cry	ptography	Key Attestation		
 Delete revoked or expired certificates (do not archive) Include symmetric algorithms allowed by the subject Archive subject's encryption private key Archive subject's encryption private key Archive subject is encryption private key Archive subject is encryption private key For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to compatibility settings. 	Purpose	e:	Encry	ption				~		
 Include symmetric algorithms allowed by the subject Archive subject's encryption private key Archive subject's encryption private key Allow private key to be exported Renew with the same key (") For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 			Del	ete rev	oked or expire	ed ce	ertificates (d	o not archive)		
 Archive subject's encryption private key Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to compatibility settings. 				ude sy	mmetric algori	thms	allowed by	the subject		
 Allow private key to be exported Renew with the same key (") For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 			✓ Arc	hive su	bject's encryp	tion	private key			
 Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 										
 Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to compatibility settings. 										
 Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 										
 Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 										
 Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 										
 Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 										
 Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 										
 Allow private key to be exported Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 	_		2		32					
Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to compatibility settings.	 Allow 	v private	e key to	be exp	orted					
Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to compatibility settings.	_				ontod					
For automatic renewal of smart card certificates, use the existing key if a new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to compatibility settings.										
new key cannot be created Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to compatibility settings.	Ren	ew with	the sam	e key (")					
Do the following when the subject is enrolled and when the private key associated with this certificate is used:	E Ren	ew with	the sam	e key (al of sr	") nat card certi	ficate	es use the r	existing key if a		
Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to compatibility settings.	For a	ew with automati	the sam	e key (al of sn	") nart card certif	ficate	es, use the e	existing key if a		
Do the following when the subject is enrolled and when the private key associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u>	For a new	ew with automati key car	the sam ic renew nnot be (e key (al of sn created	") nart card certi l	ficate	es, use the e	existing key if a		
associated with this certificate is used: Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u>	For a new	ew with automati key car	the sam ic renew nnot be (e key (al of sr created	") nart card certi I	ficate	es, use the e	existing key if a		
 Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 	Ren For a new Do the t	ew with automati key car following	the sam ic renew nnot be o g when t	e key (al of sr created he subj	(*) nart card certi d ject is enrolled	ficate	es, use the e I when the p	existing key if a private key		
 Enroll subject without requiring any user input Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 	Do the tassocia	ew with automati key car followin <u>c</u> ted with	the sam ic renew nnot be g when t this cert	e key (al of sr created he subj tificate	") nart card certi d ject is enrolled is used:	ficate	es, use the e I when the p	existing key if a private key		
 Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used Control is disabled due to <u>compatibility settings.</u> 	Do the fassocia	ew with automati key car following ted with	the sam ic renew nnot be g when t this cert	e key (al of sri created he subj tificate	") nart card certi j ject is enrolled is used:	ficate	es, use the e I when the p	existing key if a private key		
Prompt the user during enrollment Prompt the user during enrollment and require user input when the private key is used Control is disabled due to <u>compatibility settings.</u>	Do the transport	ew with automati key car following ted with	the sam ic renew nnot be g when t this cert ct withou	e key (al of sri created he subj ifficate it requir	(") nart card certi d ject is enrolled is used: ting any user ii	ficate I and	es, use the o	existing key if a orivate key		
 Prompt the user during enrollment and require user input when the private key is used * Control is disabled due to <u>compatibility settings.</u> 	Do the tassocia	ew with automati key car following ted with oll subjec	the sam ic renew nnot be g when t this cert ct withou	e key (al of sr created he subj ificate t requir	") nart card certil ject is enrolled is used: ing any user i	ficate I and	es, use the o	existing key if a private key		
private key is used Control is disabled due to <u>compatibility settings.</u>	Do the tassocia	ew with automati key car following ted with oll subject	the sam ic renew nnot be g when t this cert ct withou user duri	e key (al of sr created he subj ificate it requir ng enro	(7) nart card certi g ject is enrolled is used: ing any user i ollment	ficate I and nput	es, use the o	existing key if a private key		
*Control is disabled due to <u>compatibility settings</u> .	Do the tassocia	ew with automati key car following ted with ull subject npt the u	the sam ic renew nnot be g when t this cert ct withou user duri	e key (al of sr created he subj ifficate it requir ng enro	") nart card certii d is used: ing any user ii ollment ollment and rec	ficate I and nput	es, use the o	existing key if a private key when the		
* Control is disabled due to compatibility settings.	Do the tassocia	ew with automati key car following ted with ull subject npt the u	the sam ic renew not be g when t this cert ct withou user durin user durin is used	e key (al of sr created he subj ifficate it requir ng enro	") nart card certi d iect is enrolled is used: ing any user i ollment ollment and red	ficate I and nput quire	es, use the o I when the p user input v	existing key if a private key when the		
Control is disabled due to compatibility settings.	Do the tassocia Do the tassocia Enro Pror Pror priva	ew with automati key car following ted with oll subject onpt the u ate key i	the sam ic renew nnot be g when t this cert ct withou user durin is used	e key (al of sr created he sub; ificate it requir ng enro	") nart card certil j iect is enrolled is used: ing any user i ollment ollment and rea	ficate I and nput quire	es, use the o I when the p user input v	existing key if a private key when the		
	Ren For : new Do the : associa Enrc Pror priva	ew with automati key car following ted with ull subject npt the u npt the u ste key i	the sam ic renew nnot be o g when t this cert ct withou user durin user durin is used	e key (al of sr created he sub; tificate it requir ng enro	") nart card certif j ject is enrolled is used: ing any user i ollment ollment and red	ficate I and nput quire	es, use the o when the p user input v	existing key if a private key when the		
	Control Contr	ew with automatii key car following ted with oll subject npt the u npt the u npt the u ste key i	the sam ic renew nnot be o g when t this cert ct withou user durin user durin is used bled due	e key (al of sr created he subj ifficate it requir ng enro ng enro e to <u>cor</u>	") nart card certif ject is enrolled is used: ing any user i ollment ollment and red	ficate I and nput quire	es, use the o	existing key if a private key when the		
	Ren R	ew with automatii key car following ted with oll subject npt the u npt the u ate key i ol is disa	the sam ic renew not be o g when t this cent ct withou user durin is used bled due	e key (al of sm created he subj ificate it requir ng enro e to <u>cor</u>	") nart card certif ject is enrolled is used: ing any user i ollment ollment and red mpatibility setti	ficate I and nput quire	as, use the e	existing key if a private key when the Help		

- 4. Cryptography:
 - Minimum key size: 2048

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

	Subject Name		Issu	iance Requir	rements
Supers	seded Template	s Ext	ensions	Server	
ieneral	Compatibility	Request H	equest Handling Cryptography Key		
Provide	r Category:	Legac	y Cryptograp	hic Service	Provider V
Algorith	m name:	Determ	nined by CSI	P	Ý
Minimur	n keysize:	2048		1	
Micro Micro Micro Micro	osoft DH SChar osoft Enhanced osoft Enhanced osoft Enhanced	nnel Cryptogr I Cryptograph I DSS and D I RSA and A	aphic Provid nic Provider iffie-Hellman ES Cryptogra	der v1.0 Cryptograph aphic Provide	
Micr	osoft RSA SCha	annel Cryptod	graphic Prov	vider	 ✓
		Determ	nined by CSI	Р	v
Reques	st hash:				
Reque:	altemate signal	ture format			
Reque:	altemate signal	ure format			
Reque:	altemate signal	ture format			
Reques	altemate signal	ure format			
Reque:	altemate signal	ture format			

5. Extensions:

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

	WINEP_Us	erCertEnc200	3 Propertie	s 📑	
C.	Internet Manage		D		
General (ompatibility Re	uert Handling	Contography	Key Atte	etation
Supersec	led Templates	Extensions	Security	Se	rver
Tomatte					
To modify	an extension, sei	ect it, and then ci	ICK Edit.		
Extensions	s included in this	template:			
📺 Applic	ation Policies				
Basic	Constraints				
Certific	cate Template Inf	romation			
Key U	sage				
			Γ	Edit	
Description	n of Application F	'olicies:			
Jecule					<u> </u>
					\sim
	ОК	Cancel	Apply	H	elp
				2	
	WINEP Us	erCertEnc200	3 Properties	s 📑	×
	WINEP_Us	erCertEnc200	3 Properties	s [_f	x
Su General (WINEP_Us	erCertEnc200	3 Properties	ments	X
General C Supersed	WINEP_Us ubject Name Compatibility Re ded Templates	erCertEnc200	3 Properties ssuance Require Cryptography Security	ments Key Atte:	station
General C Supersec	WINEP_Us ubject Name Compatibility Re ded Templates	erCertEnc200	3 Properties ssuance Require Cryptography Security	ments Key Atter Se	station rver
General C Supersec To modify	WINEP_Us ubject Name Compatibility Re ded Templates an extension, sel	erCertEnc200	13 Properties ssuance Require Cryptography Security ick Edit.	ments Key Atte:	station
General C Supersec To modify Extensions	WINEP_Us ubject Name Compatibility Re ded Templates an extension, sel s included in this i	erCertEnc200	13 Properties ssuance Require <u>Cryptography</u> Security ck Edit.	ments Key Atte Se	station
Supersed To modify Extensions	WINEP_Us ubject Name Compatibility Re ded Templates an extension, sel s included in this i ation Policies	erCertEnc200	J3 Properties ssuance Require <u>Cryptography</u> Security ck Edit.	ments Key Atte	station
General C Supersec To modify Extensions Basic	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel s included in this ation Policies Constraints	erCertEnc200	13 Properties ssuance Require Cryptography Security ck Edit.	ments Key Atte:	station
Supersed General (Supersed To modify Extensions Applic Basic Cettific	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel s included in this ation Policies Constraints cate Template Infl ope Policies	erCertEnc200	33 Properties ssuance Require Cryptography Security ck Edit.	ments Key Atte:	station
Supersed Supersed To modify Extensions Basic Supersed Basic Supersed Issuar	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel s included in this ation Policies Constraints cate Template Infl coe Policies sage	erCertEnc200	33 Propertie: ssuance Require Cryptography Security ck Edit.	ments Key Atte: Se	station
Su General (Supersec To modify Extensions Basic Basic Certific Issuar	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel s included in this ' ation Policies ation Policies constraints cate Template Inf toce Policies sage	erCertEnc200	33 Propertie: ssuance Require Cryptography Security ck Edit.	ments Key Atte: Se	station
Supersect General C Supersect To modify Extensions Basic Certific Issuar	WINEP_US deject Name Compatibility Re ded Templates an extension, sel s included in this : ation Policies Constraints cate Template Inf ince Policies sage	erCertEnc200	13 Properties ssuance Require Cryptography Security ck Edit.	ments Key Atter Se	station
Supersec General C Supersec To modify Extensions Basic Certific Issuar	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel s included in this t ation Policies Constraints cate Template Inf ince Policies sage	erCertEnc200	3 Propertie: ssuance Require Cryptography Security ck Edit.	Key Atte: Key Atte: Se	station rver
Supersed General (Supersed To modify Extensions Applic Basic Cettific Issuar Key U	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel s included in this: ation Policies Constraints cate Template Inf nace Policies (sage)	erCertEnc200	3 Propertie: ssuance Require Cryptography Security ck Edit.	Key Attes	x station rver
Supersed Supersed To modify Extensions Applic Basic Supersed Issuar	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel ation Policies Constraints cate Template Info coe Policies sage n of Key Usage: exchance only w	erCertEnc200	3 Properties ssuance Require Cryptography Security ck Edit.	Key Atter	station rver
Supersect General C Supersect To modify Extensions Basic C Cettifu Issuar Key U Description Allow key Allow key Allow key	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel sincluded in this ation Policies constraints cate Template Info coe Policies sage n of Key Usage: exchange only v ryption of user data	erCertEnc200	3 Propertie: ssuance Require Cryptography Security ck Edit.	Key Atte	x station rver
Superser General C Superser To modify Extensions Basic Certific Issuar Key U Description Allow key Allow key Allow key	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel sincluded in this ation Policies constraints cate Template Inf ce Policies sage n of Key Usage: exchange only w nyption of user dat tension.	erCertEnc200	13 Properties	Key Atter	station rver
Su General C Supersec To modify Extensions Applic Basic Certific Issuar Key U Description Allow key Allow key Allow enc Critical ex	WINEP_US ubject Name Compatibility Re led Templates an extension, sel sincluded in this ation Policies Constraints constraints cate Template Inf ace Policies sage n of Key Usage: exchange only v ryption of user dat tension.	erCertEnc200	13 Properties: ssuance Require Cryptography Security ck Edit.	s r ments Key Atter Se Edit	station rver
Su General C Supersec To modify Extensions Basic Certific Issuar Key U Description Allow key Allow enc Critical ext	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel sincluded in this: ation Policies Constraints cate Template Inf nce Policies sage n of Key Usage: exchange only v ryption of user da tension.	erCertEnc200	3 Properties	Key Atte: Key Atte: Se	station rver
Supersed General C Supersed To modify Extensions Applic Basic Certific Issuar Key U Description Allow key Allow key	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel sincluded in this: ation Policies Constraints cate Template Inf nce Policies (sage) n of Key Usage: exchange only w tension.	erCertEnc200	3 Properties ssuance Require Cryptography Security ck Edit.	Key Attes	station rver
Su General C Supersec To modify Extensions Applic Basic Basic Susuar Key U Description Allow key Allow enc Critical ex	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel sincluded in this ation Policies Constraints cate Template Inf oce Policies Sage n of Key Usage: exchange only v tension.	erCertEnc200	3 Properties ssuance Require Cryptography Security ck Edit.	Key Atte	x station rver
Supersed Supersed To modify Extensions Basic Certific Issuar Key U Description Allow key Allow enc Critical ex	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel sincluded in this ation Policies Constraints cate Template Info ce Policies sage n of Key Usage: exchange only w ryption of user dat tension.	erCertEnc200	3 Propertie: ssuance Require <u>Cryptography</u> <u>Security</u> ck Edit.	Key Atte	x station rver
Su General C Supersec To modify Extensions Basic Basic Certific Issuar Key U Description Allow key Allow enc Critical ex	WINEP_US ubject Name Compatibility Re ded Templates an extension, sel sincluded in this ation Policies Constraints cate Template Inf oce Policies sage n of Key Usage: exchange only v ryption of user date tension.	erCertEnc200	33 Properties	Key Atter	x station rver

- 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

	Subject Name			ssuance Requi	rements
General	Compatibility	Reques	t Handling	Key Attestatio	
Supers	seded Template	s	Extensions	Security	Server
Group o	or user names:				
St. Au	thenticated Use	ers			~
🔏 Ad	ministrator				
Se Do	omain Users (FE	UERWE	HR-TOC\Do	main Users)	
& W	inEP Serviceke	nnung (wi	inep@polize	i-toc.bayem.de)	
🔏 Ad	ministrator				
😹 Do	omain Admins (P	OLIZEI-T	OC\Domain	Admins)	
Se Do	omain Users (PC	LIZEI-TO	C\Domain (Jsers)	
🔐 En	terprise Admins	(POLIZE	TOC\ Estar	(and the second	\sim
		II VEILE	I-TUC (Enter	Drise Admins)	
		II OLILL		Add	Remove
		II OLILL		Add	Remove
Permiss	ions for WinEP	Serviceke		Add Allow	Remove Deny
Permiss Full C	ions for WinEP	Serviceke	ennung	Add Allow	Remove Deny
Permiss Full C Read	ions for WinEP Control	Serviceke		Add Allow	Remove Deny
Permiss Full C Read Write	ions for WinEP Control	Serviceke	ennung	Add Allow	Remove Deny
Permiss Full C Read Write Enrol	ions for WinEP Control I	Serviceke	ennung	Add Allow	Remove Deny
Permiss Full C Read Write Enrol Autoe	ions for WinEP Control I I I enroll	Serviceke	ennung	Add Allow	Remove Deny
Permiss Full C Read Write Enrol Autoe	ions for WinEP Control I I I enroll	Serviceke	ennung	Add Allow	Remove Deny
Permiss Full C Read Write Enrol Autoe	ions for WinEP Control I I I enroll	Serviceke	ennung	Add Allow	Remove Deny
Permiss Full C Read Write Enrol Autoo	ions for WinEP Control I I enroll	Serviceke	ennung	Add Allow	Remove Deny
Permiss Full C Read Write Enrol Autoe	ions for WinEP Control I I enroll cial permissions	Serviceke	ced settings	Add Allow Allow Allow	Remove Deny
Permiss Full C Read Write Enrol Autor	ions for WinEP Control I I enroll cial permissions ved.	Serviceke	ced settings	Add Allow	Remove Deny
Permiss Full C Read Write Enrol Autoo	ions for WinEP Control I I enroll cial permissions cial permissions	Serviceke	ced settings	Add Allow Allow	Remove Deny
Permiss Full C Read Write Enrol Autoo	ions for WinEP Control I I enroll cial permissions cial permissions	Serviceke	ced settings	Add Allow Allow	Remove Deny

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

chicidi	Compatibility	Request	Handling	Cryptography	Key Attestation
Super	seded Template	s	Extensions	Security	Server
	Subject Name			Issuance Requi	rements
	ply in the reques Use subject info	st ormation fr	om existing	certificates for a	autoenrollment
Build Select simple	d from this Active	e Director enforce co	y informatio	n among subject n	names and to
Subj	ect name format	ininiistratio			
Fully	distinguished n	ame			~
	-mail name INS name Iser principal nar ervice principal	me (UPN) name (SP	'N)		
* Contro	ol is disabled due	e to <u>comp</u>	atibility setti	ngs.	

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

	WINEP_	UserCe	rtSignati	ire P	roperti	es L	
	Subject Name			ssuan	ce Requir	ement	s
Super	seded Template	s	Extensions		Security		Server
General	Compatibility	Reques	t Handling	Crypt	ography	Key	Attestatio
Templa	te displau name						
WinEP	UserCert Signa	ture					
WITLE		laro					
Templa	ite name:						
WinEP	UserCertSigna	ture					
Validity	period:	_	Renewal	perio	d:		
₿	years 🗸		2	week	s v		
Pub	lish certificate in	Active D	lirectory				
	Do not automatio Directory	cally reen	roll if a duplic	cate c	ertificate e	exists i	n Active
	Sheetory						
	0.1		• •				
	OK		Cancel		Apply		Help

2. Compatibility:

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

Superseded Templates Extensions Security Server Seneral Compatibility Request Handling Cryptography Key Attestation The template options available are based on the earliest operating system versions set in Compatibility Settings. Image: Server 2008 V Show resulting changes Versions Server 2008 V Certificate recipient Vindows Vista / Server 2008 V Versions set in Server 2008 V		Subject Name			ssua	nce Requir	eme	nts	
Seneral Compatibility Request Handling Ctyptography Key Attestation The template options available are based on the earliest operating system versions set in Compatibility Settings. Image: Compatibility Settings Image: Compatibility Settings Image: Compatibility Settings Image: Compatibility Settings Image: Certification Authority Image: Certificate recipient Image: Windows Vista / Server 2008 Image: Vertificate recipient Image: Vertificate recipient Image: These settings may not prevent earlier operating systems from using this template. Image: Vertificate recipient systems from using this template.	Super	seded Template	s	Extensions	T	Security		Se	rver
The template options available are based on the earliest operating system versions set in Compatibility Settings. Compatibility Settings Certification Authority Windows Server 2008 Certificate recipient Windows Vista / Server 2008 These settings may not prevent earlier operating systems from using this template.	General	Compatibility	Reques	t Handling	Cry	otography	Ke	y Atte:	station
Certification Authority Windows Server 2008 v Certificate recipient v Windows Vista / Server 2008 v These settings may not prevent earlier operating systems from using this template. V	Version:	nplate options a s set in Compati w resulting char atibility Settings	vailable a bility Sett	are based on ings.	the	earliest ope	eratin	g syst	em
Windows Server 2008 v Certificate recipient Windows Vista / Server 2008 Windows Vista / Server 2008 v	Certi	fication Authorit	y						
Certificate recipient Windows Vista / Server 2008 These settings may not prevent earlier operating systems from using this template.	Wir	dows Server 20	800		~				
Windows Vista / Server 2008 v These settings may not prevent earlier operating systems from using this template.	Certi	ficate recipient							
These settings may not prevent earlier operating systems from using this template.	Wir	ndows Vista / Se	erver 200	18	~				
	These : template	settings may not e.	prevent	earlier opera	ting	systems fro	m usi	ing thi	s

- 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

	Winf	EP_Use	erCe	rtSignat	ure	Properti	es	?	x
	Subject Na	ame			Issu	ance Requir	eme	nts	
Super	seded Temp	plates		Extensions		Security		Se	rver
General	Compatibi	ility Re	eques	t Handling	Cŋ	ptography	Ke	y Atte	station
Purpose	e: S	ignature							~
		Delete	revol	ced or expir	ed c	ertificates (d	o no	t archi	ve)
		Include	e sym	metric algor	ithms	allowed by	the	subjec	t
		Archiv	e subj	ect's encry	ption	private key			
		Use	e adva	anced Sym	metric	algorithm to	o sei	nd the	key
		- to t	he CA						
	v private ke	ey to be	export	ted					
Ren	ew with the	e same k	ey (*)						
For a new	automatic re key canno	enewal o t be cre	of sma ated	int card cert	ificat	es, use the e	exist	ing ke	yifa
Do the fassocia	following wh ted with this	hen the s certific	subje ate is	ct is enrolle used:	d and	d when the p	oriva	te key	
	ll subject w	ithout re	equirin	g any user	input				
O Pron	npt the user	r during	enrollr	ment					
Pron	npt the user	r during	enrollr	ment and re	quire	user input v	wher	the	
 priva 	ate key is us	sed							
 priva Control 	ate key is us ol is disabled	sed d due to	comp	atibility set	tings.				

- 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.

Win	EP_UserC	ertSignat	ur Propertie	es ? X
Subject Na	me		ssuance Requir	rements
Superseded Temp	lates	Extensions	Security	Server
General Compatibil	ity Reque	st Handling	Cryptography	Key Attestation
Provider Category:	Ke	ey Storage Pro	ovider	~
Algorithm name:	R	SA		~
Minimum key size:	20	48		
Choose which crypl Requests can u Requests must u Providers: Microsoft Softwa Microsoft Platfor Microsoft Smart	tographic pr se any provi use one of t are Key Stor m Crypto Pr Card Key St	oviders can b ider available ne following p age Provider ovider orage Provide	e used for requ on the subject's roviders:	s computer
Request hash:	SI	HA256		*
Use alternate sig	gnature form	at		
0	К	Cancel	Apply	Help

5. Extensions:

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

					es 📑
	Subject Name			ssuance Requir	ements
General	Compatibility	Request	t Handling	Cryptography	Key Attestation
Supers	eded Template	3	Extensions	Security	Server
Townad			and the set of	tal. Eda	
To mod	iy an extension,	Select IL,	and then c	ICK EUIL.	
Extensio	ons included in t	his templa	ate:		
🏢 Арр	lication Policies				
Bas	ic Constraints				
Cer	tificate l'emplate	Informat	ion		
Key	Usage				
					Eda
					Luit
Descript	tion of Applicatio	n Policie	s:		
Secure	Email				^
					~
	ОК		Cancel	Apply	Help
	WinEP_U	JserCe	rtSignat	ure Properti	es ? X
General	Subject Name	Paguast	Landing	Issuance Requi	Key Attestation
Supers	eded Templates	neques	Extensions	Security	Server
			1.1		
lo modif		select it,	and then c	lick Edit.	
	y an extension,				
Extensio	y an extension, ns included in tl	nis templa	ate:		
Extensio	y an extension, ns included in th lication Policies	nis templa	ate:		
Extensio Appl	y an extension, ns included in t lication Policies c Constraints	nis templa	ate:		
Extensio App Basi Certi	y an extension, ns included in tl lication Policies c Constraints ficate Template	nis templa Informat	ate: ion		
Extensio Appl Basi Certi	y an extension, ns included in ti lication Policies c Constraints ficate Template ance Policies	nis templa Informat	ate: ion		
Extensio Appl Basi Certi Issu	y an extension, ns included in t lication Policies c Constraints ficate Template ance Policies Usage	nis templa Informat	ate:		
Extensio Appl Basi Certi Issu Key	y an extension, ns included in tl lication Policies c Constraints fricate Template ance Policies Usage	nis templa Informat	ate: ion		
Extensio	y an extension, ns included in th lication Policies c Constraints ficate Template ance Policies Usage	nis templa	ion		54
Extensio	y an extension, ns included in til lication Policies c Constraints ficate Template ance Policies Usage	nis templa	ion		Edit
Extensio Appl Basi Certi Issu Key Descripti	y an extension, ns included in th lication Policies c Constraints ficate Template ance Policies Usage	nis templa Informat	ion		Edit
Extensio	y an extension, ns included in th lication Policies c Constraints ficate Template ance Policies Usage	nis templa Informat	ate:		Edit
Extensio Appi Basi Cert Issu Rey Descripti Signatu Digital s Signatu	y an extension, ns included in th lication Policies c Constraints ficate Template ance Policies Usage	e:	ion		Edit
Extensio Appi Basi Certi Issu Markey Descript Signatu Digital s Signatu Critical e	y an extension, ns included in th lication Policies c Constraints ficate Template ance Policies Usage	e:	ate: ion epudiation)		Edit
Extensio Appi Basi Certi Islau Key Descripti Signatu Digita is Signatu Critical e	y an extension, ns included in the lication Policies c Constraints fricate Template ance Policies Usage	nis templa Informat e:	ate: ion epudiation)		Edit
Extensio Appi Basi Certi Isusu Key Descripti Signatu Digtal s Signatu Crtical e	y an extension, ns included in th lication Policies c Constraints fricate Template ance Policies Usage	is templa Informat	ate: ion epudiation)		Edit
Extensio Appi Basi Certi Isusu Key Descript Signatu Digital s Signatu Critical e	y an extension, ns included in th lication Policies c Constraints fricate Template ance Policies Usage ion of Key Usag re requirements ignature re is proof of oni extension.	e:	ate: ion epudiation)		Edit
Extensio Appi Basi Certi Isu Isu Key Descripti Signatu Digital s Signatu Critical e	y an extension, ns included in th lication Policies c Constraints ficate Template ance Policies Usage	e:	ate: ion apudiation)		Edit
Extensio Appi Basi Cert Issu Key Descripti Signatu Digital s Signatu Critical e	y an extension, ns included in th lication Policies c Constraints ficate Template ance Policies Usage	e:	ate: ion epudiation)		Edit
Extensio Appi Basi Certi Issu Markey Descripti Signatu Digital s Signatu Critical e	y an extension, ns included in th lication Policies c Constraints ficate Template ance Policies Usage	e:	ate: ion epudiation)		Edit

6. Security:

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

	Subject Name			Issuance Requirements			
General	Compatibility	Request	Handling	Cryptography	Key Attestation		
Super	seded Template	s	Extensions	Security	Server		
Group	or user names:						
😹 AL	thenticated Use	ers					
Se Do	omain Users (FE	UERWE	IR-TOC\De	main Users)			
Sector Do	omain Admins (Po omain Users (Po iterprise Admins	LIZEI-TO (POLIZEI	C\Domain C\Domain	Jsers) prise Admins)			
				Add	Remove		
Permiss	ions for Domain	Users		Allow	Deny		
Full C	Control						
	4			\checkmark			
Read	•						
Read Write							
Read Write Enrol	- - -						
Read Write Enrol Auto	enroll			>			
Read Write Enrol Auto	; ; enroll cial permissions	oradvan	ced settings				
Read Write Enrol Autor	e I enroll cial permissions ciad.	or advan	ced settings	, click	Advanced		

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

Cunon	Compatibility	Request	Handling	Cryptography	Key Attestation
Super	seded Template	s	Extensions	Security	Server
	Subject Name		ls	suance Requir	ements
	ply in the reques	st			
	Use subject info renewal request	ormation fr s (*)	om existing o	ertificates for a	utoenrollment
Build	d from this Activ	e Director	y information		
Selec simpli	et this option to fy certificate ad	enforce co ministratio	onsistency a n.	mong subject n	ames and to
Subje	ect name format				
Fully	distinguished n	ame			~
Inclu Inclu	de this informati -mail name	on in alter	nate subject	name:	
	NS name				
	ser principal na	me (UPN)			
S	ervice principal	name (SP	N)		
			-		

2

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

	VVIIIE	P_Oser	CentSSL	PIC	perfies		<u> </u>	
	Subject Name			ssui	ance Requir	eme	ents	
Supers	eded Templates		Extensions	Τ	Security		Ser	ver
General	Compatibility	Request	Handling	Cŋ	ptography	phy Key Attestatio		
Templai	e displav name:							
WinEP	UserCertSSL							
Templa	e name:							
WinEP	UserCertSSL							
L								
Validity (period:		Renewal	per	iod:			
β	years 🗸		2	wee	eks ∨			
	ish certificate in <i>i</i>	Active Di	rectory					
)o not automatica)irectory	ally reenn	oll if a duplic	cate	certificate e	xist	s in Ac	tive
	hootory							
	OK		Cancel		Apply	1 [He	lo
	OR		00.1001		. 444.0		110	~P

2. Compatibility:

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

Subject Name Issuance Requirements Superseded Templates Extensions Security Server General Compatibility Request Handling Cryptography Key Attestation The template options available are based on the earliest operating system versions set in Compatibility Settings. Image: Compatibility Settings Image: Compatibility Settings Image: Compatibility Settings Certification Authority Image: Certificate recipient Image: Certificate recipient Image: Windows Vista / Server 2008 Image: Certificate recipient Image: Certificate recipient Image: Certificate recipient Image: These settings may not prevent earlier operating systems from using this template. Image: Certificate recipient systems from using this template.		WINE	P_Usei	rcentssi	Properties	
Superseded Templates Extensions Security Server General Compatibility Request Handling Cryptography Key Attestation The template options available are based on the earliest operating system versions set in Compatibility Settings. Image: Compatibility Settings Image: Compatibility Settings Image: Compatibility Settings Certification Authority Image: Certificate recipient Imag		Subject Name			Issuance Requir	rements
Seneral Compatibility Request Handling Cryptography Key Attestation The template options available are based on the earliest operating system versions set in Compatibility Settings. Image: Compatibility Settings Image: Compatibility Settings Image: Compatibility Settings Centification Authority Image: Centificate recipient Image: Centificate recipient Image: Windows Vista / Server 2008 Image: Centificate recipient Image: Centificate recipient Image: Centificate recipient Image: These settings may not prevent earlier operating systems from using this template. Image: Centificate recipient systems from using this template.	Supers	eded Template	s	Extensions	Security	Server
The template options available are based on the earliest operating system versions set in Compatibility Settings. Compatibility Settings Certification Authority Windows Server 2008 Certificate recipient Windows Vista / Server 2008 These settings may not prevent earlier operating systems from using this template.	General	Compatibility	Reques	t Handling	Cryptography	Key Attestation
Certification Authority Windows Server 2008 Certificate recipient Windows Vista / Server 2008 V These settings may not prevent earlier operating systems from using this template.	Version:	nplate options a s set in Compatil w resulting char atibility Settings	vailable a bility Setti nges	re based on ngs.	the earliest ope	rating system
Windows Server 2008 V Certificate recipient V Windows Vista / Server 2008 V These settings may not prevent earlier operating systems from using this template.	Certi	fication Authority	Y			
These settings may not prevent earlier operating systems from using this template.	Certi	ficate recipient idows Vista / Se	erver 200	8	v	
	These stemplate	settings may not e.	prevent	earlier opera	ting systems fro	m using this

- 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

	Subject Name			Issuance Requir	ements
Super	seded Template	s	Extensions	Security	Server
General	Compatibility	Reques	st Handling	Cryptography	Key Attestation
Purpos	e: Signa	ture			~
	De	lete revo	ked or expin	ed certificates (de	o not archive)
	🗌 Inc	lude sym	metric algori	thms allowed by	the subject
	Arc	chive sub	ject's encryp	otion private key	
		Use adv to the C/	anced Symm A	netric algorithm to	send the key
	w private key to	be expo	ted		
Allor	w private key to new with the sam	be expo ne key (*)	ted		
Allor Ren For new	w private key to new with the sam automatic renew v key cannot be	be expor ne key (*) val of sma created	ted) art card certi	ficates, use the e	existing key if a
Allor Ren For new Do the associa	w private key to new with the san automatic renew key cannot be following when i ted with this cer	be expon ne key (*) val of sma created the subje tificate is	ted art card certi ct is enrolled used:	ficates, use the e	existing key if a private key
Allor Ren For new Do the associa	w private key to new with the sam automatic renew key cannot be following when ited with this cer oll subject withou	be exponence (*) val of sma created the subje tificate is ut requirir	ted art card certi ct is enrolled used: ng any user i	ficates, use the e d and when the p nput	existing key if a vrivate key
Allor Ren For new Do the associa Enro	w private key to new with the sam automatic renew key cannot be following when ted with this cer oll subject withou mpt the user dur	be export ne key (") val of sma created the subje tificate is ut requirin ing enroll	tted art card certi act is enrolled used: ng any user i ment	ficates, use the e d and when the p nput	axisting key if a private key
Allor Ren For new Do the associa Enro Pror Pror privit	w private key to sew with the san automatic renew key cannot be following when ited with this cer oll subject withou npt the user dur npt the user dur ate key is used	be exponent wal of smatcreated the subjet tificate is ut requiring ing enroll	ted art card certi used: ng any user i ment ment and re	ficates, use the e I and when the p nput quire user input v	existing key if a private key when the
Allor Ren For new Do the associa Enro Pror Pror priv: * Contro	w private key to sew with the san automatic renew key cannot be following when ited with this cer oll subject withou mpt the user dur ate key is used ol is disabled du	be exponence wal of smatched (") val of smatched created the subjectificate is ut requiring ing enroll ing enroll e to <u>com</u>	ted art card certi used: ang any user i ment ment and re patibility sett	ficates, use the e d and when the p nput quire user input v ngs.	existing key if a Inivate key when the

- 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.

WinEP_UserCertSSL Properties ? ×							
	Subject Name		Issuance Requir	ements			
Supers	eded Template	es Extensions	Security	Server			
General	Compatibility	Request Handling	Cryptography	Key Attestation			
Provide	r Category:	Key Storage P	rovider	~			
Algorith	m name:	RSA		~			
Minimur	n keysize:	2048					
Req Req Provide Micn Micn Micn	Requests can use any provider available on the subject's computer Requests must use one of the following providers: Providers: Microsoft Software Key Storage Provider Microsoft Platform Crypto Provider Microsoft Smart Card Key Storage Provider						
Reques	t hash:	SHA256		~			
Use	altemate signal	ture format					
	ОК	Cancel	Apply	Help			

? X

5. Extensions:

- Application Policies: *Client Authentication*
- Key Usage:
 - o Digital signature
 - Critical extension

	Subject Name			Issu	iance Requir	ements		
General	Compatibility	Reque	est Handling	Cr	yptography	Key Attestation		
Supers	eded Template	s	Extensions		Security	Server		
To modi	fy an extension	, select	it, and then o	lick	Edit.			
Eddinad	lication Policies ic Constraints ificate Template ance Policies Usage	e Inform	nation					
Edit								
Descript	ion of Application	on Polic	ies:					
Client A	uthentication					× ×		
	ОК		Cancel		Apply	Help		
						2 7		
	Wint	:P_Us	erCertSSL	. Pr	operties			
	Subject Name			Issu	uance Requir	rements		
General	Compatibility	Reque	est Handling	0	ryptography	Key Attestation		
Supers	eded Template	S	Extensions		Security	Server		
To modi	fy an extension	, select	it, and then o	click	Edit.			
Extensio App Basi Cett Issu	ns included in t lication Policies ic Constraints ificate Template ance Policies <mark>Usage</mark>	his tem ; e Inform	plate:					
Descript	ion of Key Usa	de:				Edit		
Signatu Digital s Critical e	re requirements ignature extension.					<		
	ОК		Cancel][Apply	Help		

WinEP_UserCertSSL Properties

6. Security:

Alle Nutzerobjekte, die Zertifikate beantragen können sollen, hinzufügen und die Rechte Read, Enroll und Autoenroll vergeben

Subject Name	ls	suance Requir	ements
eneral Compatibility Requ	est Handling	Cryptography	Key Attestation
Superseded Templates	Extensions	Security	Server
aroup or user names:			
& Authenticated Users			
Somain Users (FEUERW	EHR-TOC\Dor	nain Users)	
👗 Administrator			
Comain Admins (POLIZE	I-TOC\Domain	Admins)	
Momain Users (POLIZEI-	TOC\Domain U	sers)	
Enterprise Admins (POLIZ	EI-TOC\Enter	orise Admins)	
		A.1.1	
			the second second second
		Add	Nemove
ermissions for Domain Users		Add	Deny
ermissions for Domain Users Full Control		Add	Deny
'emissions for Domain Users Full Control Read		Add	Deny
lemissions for Domain Users Full Control Read Write		Add	
Vermissions for Domain Users Full Control Read Write Enroll		Add	Deny
Vermissions for Domain Users Full Control Read Write Enroll Autoenroll		Add	Deny
Vermissions for Domain Users Full Control Read Write Enroll Autoenroll		Add	Deny
Vermissions for Domain Users Full Control Read Write Enroll Autoenroll		Add	Deny
Vermissions for Domain Users Full Control Read Write Enroll Autoenroll	anced settings,	Add Allow	Deny
Vermissions for Domain Users Full Control Read Write Enroll Autoenroll	anced settings,	Add Allow	Deny
emissions for Domain Users Full Control Read Write Enroll Autoenroll or special pemissions or adva dvanced.	anced settings,	Add Allow	Deny

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

Supp U U Re Build	Subject Name ly in the request se subject information newal requests (*)	on from existing ce	tificates for aut	nents
O Supp □ ^L re ● Build	ly in the request lse subject information newal requests (*)	on from existing ce	rtificates for aut	
Build				oenrollment
Coloct	from this Active Dire	ctory information		nee and to
simplify	certificate administ ct name format:	ration.	ong subject nar	nes and to
Fully	distinguished name		1	~
	e this information in nail name IS name er principal name (U	alternate subject n IPN)	ame:	
Se	rvice principal name	(SPN)		
* Control	is disabled due to <u>c</u>	ompatibility setting	<u>s.</u>	

2 V

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

	WINLF_	VVOIKS	lationce	IT FIC	operite	s 📑	
	Subject Name			ssuand	e Requir	ements	
Super	seded Template	s	r Extensions		Security	9	Server
General	Compatibility	Request	Handling	Crypto	ography	Key Att	testation
			2		2		
Templa	te display name:						
WinEP	_WorkstationCe	rt					
l empla	te name:						
WinEP	_WorkstationCe	rt					
Validity	period:		Renewal	period			
h	weare M	1	2	weeks			
	years +			weeks	Ť		
Pub	lish certificate in	Active Di	rectory				
	Do not automatic	ally reenn	oll if a duplic	ate ce	ertificate e	xists in /	Active
	Directory						
	ОК	(Cancel		Apply		Help

2. Compatibility:

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

	WinEP_	Works	tationCe	rt Prop	erties	s ?	x
	Subject Name			ssuance	Require	ements	
Supers	seded Templates		Extensions	Se	ecurity	Ser	ver
General	Compatibility	Request	t Handling	Cryptogr	aphy	Key Attes	tation
The ten version:	nplate options av s set in Compatib w resulting chan	vailable a vility Settin ges	re based on ngs.	the earlie	est oper	ating syste	em
Certi	fication Authority						
Win	dows Server 20	08		~			
Certi	ficate recipient ndows Vista / Se	rver 200	8	~			
These stemplate	settings may not e.	prevent e	earlier opera	ting syste	ms from	n using this	8
	ОК		Cancel	Арр	ply	He	lp

- 3. Request Handling:
 - Purpose: Signature

	Subject Name			Issuance Requir	ements		
Super	seded Template	s	Extensions	Security	Server		
General	Compatibility	Reques	t Handling	Cryptography	Key Attestation		
Purpose	e: Signa	ture		<u>A</u>	~		
	De	lete revol	ed or expire	ed certificates (de	not archive)		
		lude sym	metric algorit	thms allowed by	the subject		
Archive subject's encryption private key							
		Use adva to the CA	anced Symm	netric algorithm to	send the key		
Auth	norize additional	service a	ccounts to a	access the priva	te kev		
Ke	Permissions						
100	y i onnooiono						
	w private key to	be export	ed				
Ren	ew with the sam	ne key (*)					
For a new	automatic renew key cannot be	val of sma created	rt card certif	ficates, use the e	existing key if a		
Dethe	following when t	the subject	ct is enrolled used:	l and when the p	rivate key		
associa	ted with this cer						
 Enro 	ted with this cer all subject withou	ut requirin	g any user i	nput			
 Enro Pron 	ted with this cer oll subject withou npt the user duri	ut requirin ing enrollr	g any user i nent	nput			
 Enro Pron Pron priva 	ted with this cer oll subject withou npt the user duri npt the user duri ste key is used	ut requirin ing enrollr ing enrollr	g any user in nent nent and rec	nput quire user input v	when the		
 Enro Pron Pron priva 	ited with this cer all subject without mpt the user duri mpt the user duri ate key is used of is disabled du	ut requirin ing enrollr ing enrollr e to <u>comp</u>	g any user in nent nent and rec patibility setti	nput quire user input v <u>ngs.</u>	vhen the		
 Enro Pron Pron priva * Contro 	ted with this cer bill subject without onpt the user during the user during the key is used bill is disabled during	ut requirin ing enrollr ing enrollr e to <u>comp</u>	g any user in nent nent and rec natibility setti	nput quire user input v ngs.	when the		

- 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.

	WinEP_W	orkstation	Cert Pr	opertie	s	?	x	
Subje	ect Name		Issuan	ce Requir	ement	s		
Superseded	Templates	Extension	Extensions Security			Server		
General Corr	npatibility Re	equest Handling	Crypt	ography	Key I	Attes	station	
Provider Cate	Provider Category: Key Storage						~	
Algorithm nam	ne:	RSA					¥	
Minimum key	size:	2048		1				
Requests Requests Providers: Microsoft Microsoft Microsoft	Choose which cryptographic providers can be used for requests Requests can use any provider available on the subject's computer Requests must use one of the following providers: Providers: Microsoft Software Key Storage Provider Microsoft Platform Crypto Provider Microsoft Smart Card Key Storage Provider							
Request has	h:	SHA256					~	
Use alter	nate signature	format			1			

WinEP_WorkstationCert Properties ? X

5. Extensions:

- Application Policies: *Client Authentication*
- Key Usage:
 - o Digital signature
 - Critical extension

General	Compatibility	Reques	st Handling	Cryptogra	phy K	Key Attestation
	Subject Name			ssuance R	equirem	ients
Supers	eded Template	s	Extensions	Sec	urity	Server
To mod	fy an extension	, select it	, and then cl	ick Edit.		
Extensio	ons included in t	this temp	ate:			
App	lication Policies	3				
🔄 Bas	ic Constraints					
Cert	tificate Template	e Informa	tion			
	ance Policies					
M. Ney	Usage					
						Edit
Descript	tion of Applicati	on Policie	es:			
Client A	uthentication					^
						~
	OK		Cancel	Appl	y	Help
	WinFP	Mork				2 X
		VVOIK	stationCe	ert Prop	erties	
		_vvork	stationCe	ert Prop	erties	
General	Compatibility	Reque	stationCe	Cryptogra	erties	Key Attestation
General	Compatibility Subject Name	Reque	stationCo st Handling Extensions	Cryptogra	erties aphy Requirer	Key Attestation ments
General Super	Compatibility Subject Name seded Template	Reque	stationCe	Cryptogra Issuance I Se	erties aphy Requirer curity	Key Attestation ments Server
General Super To mod	Compatibility Subject Name seded Templati	Reque	est Handling Extensions it, and then o	Cryptogra Issuance F Se dick Edit.	erties aphy Requirer curity	Key Attestation ments Server
General Super To mod	Compatibility Subject Name seded Templat dify an extension	Reque	est Handling Extensions it, and then o	Cryptogra Issuance I Se dick Edit.	erties aphy Requirer curity	Key Attestation ments Server
General Super To mod Extensi	Compatibility Subject Name seded Templati dify an extension ions included in plication Policie	Reque	Ist Handling Extensions Date:	Cryptogra Issuance I Se slick Edit.	aphy Requirer curity	Key Attestation ments Server
General Super To moo Extensi Ba	Compatibility Subject Name seded Templat dify an extension ions included in plication Policie sic Constraints	Reque es n, select i this temp	stationCo st Handling Extensions it, and then o plate:	Cryptogra Issuance I Se dick Edit.	aphy Aphy Requirer	Key Attestation ments Server
General Super To mod Extensi Ba Extensi Ce	Compatibility Subject Name seded Templatu dify an extension ions included in plication Policie sic Constraints rtificate Templa	Reque es h, select i this temp es te Information	station st Handling Extensions it, and then o plate:	ert Prop	aphy Requirer	Key Attestation ments Server
General Super To mod Extensi Ba Ce Estensi Ba	Compatibility Subject Name seded Templatu dify an extension ons included in plication Policie sic Constraints rtificate Templa uance Policies	Reque es h, select i this temp is te Informa	Extensions Extensions it, and then o plate:	Cryptogra Issuance I Se dick Edit.	aphy Aphy Requirer curity	Key Attestation ments Server
General Super To moo Extensi Ba Ba Ce Isss Ke	Compatibility Subject Name seded Templatu dify an extension ions included in plication Policie sic Constraints rtificate Templa uance Policies y Usage	Reque es h, select i this temp ss te Inform	Ist Handling Extensions it, and then o plate:	Cryptogra Issuance I Se dick Edit.	erties aphy Requirer curity	Key Attestation ments Server
General Super To mod Extensi Ba Ba Censi Ss Ke	Compatibility Subject Name seded Templat dify an extension ions included in plication Policie sic Constraints rtificate Templa uance Policies y Usage	Reque es n, select i this temp is te Inform	Ist Handling text Handling Extensions it, and then o plate: ation	Cryptogr Issuance I Se dick Edit.	aphy Requirer	Key Attestation ments Server
General Super To moo Extensi Apa Cc Ss Ss Ke	Compatibility Subject Name seded Templat dify an extension ions included in plication Policie sic Constraints trificate Templa uance Policies y Usage	Reque es n, select i this temp is te Inform	Ist Handling Ist Handling Extensions it, and then of plate: ation	Cryptogr Issuance I Se dick Edit.	aphy Requirer	Key Attestation ments Server
General Super To moo Extensi Ap Ba Ce Ess ks	Compatibility Subject Name seded Templatu dify an extension ions included in plication Policie sic Constraints trificate Templa uance Policies y Usage	Reque es h, select i this temp s te Inform	Ist Handling Ist Handling Extensions It, and then o plate: ation	Cryptogri Issuance f Se dick Edit.	erties aphy Requirer curity	Key Attestation ments Server
General Super To mod Extensi Ba Ba Ce Iss S	Compatibility Subject Name seded Templat dify an extension ions included in plication Policies is Constraints rtificate Templa uance Policies y Usage	Reque es n, select i this temp is te Inform	ist Handling Extensions it, and then o plate: ation	Cryptogra Issuance f Se dick Edit.	aphy aphy aphy aphy aphy aphy aphy aphy	Key Attestation ments Server
General Super To mod Extensi Ba Ba Ce Signat	Compatibility Subject Name seded Templat dify an extension ions included in plication Policies is Constraints rtificate Templa uance Policies y Usage	Reque es	ist Handling Extensions it, and then o plate: ation	cryptogra Issuance f Se dick Edit.	erties aphy Requirer curity	Key Attestation ments Server
General Super To moo Extensi Ba Ba Ce Signat Descrip Signat Digital	Compatibility Subject Name seded Templat dify an extension ions included in plication Policie sic Constraints rtificate Templa uance Policies y Usage	Reque	stationConstruction	ert Prop Cryptogra Issuance I Se dick Edit.	aphy Requirer curity	Key Attestation ments Server
General Super To moo Extensi Ba Ce Signat Digital Crtical	Compatibility Subject Name seded Templat dify an extension ons included in plication Policie sic Constraints rtificate Templa uance Policies y Usage btion of Key Usa ure requirement signature extension.	Reque es h, select i this temp is te Information age: s:	stationConstruction	ert Prop	aphy Requirer curity	Key Attestation ments Server
General Super To mod Extensi Ba Ba Ce Signat Digital Critical	Compatibility Subject Name seded Templat dify an extension ons included in plication Policies sic Constraints rtificate Templa uance Policies y Usage stion of Key Usa ure requirement signature extension.	Reque es h, select i this temp is te Informa age: 	stationConstruction	ert Prop	aphy Requirer curity	Key Attestation ments Server
General Super To mod Extensi Ba Ce Signat Descrip Signat Digital Critical	Compatibility Subject Name seded Templat dify an extension ions included in plication Policies sic Constraints rtificate Templa uance Policies y Usage	Reque es	stationCo	ert Prop	aphy Requirer curity	Key Attestation ments Server
General Super To mod Extensi Ap Ba Cc Iss Ke Descrip Signat Digital Critical	Compatibility Subject Name seded Templat dify an extension ions included in plication Policie sic Constraints trificate Templa uance Policies y Usage stion of Key Usa ure requirement lextension.	Reque es h, select i this temp is te Informa	stationCo	Cryptogr Issuance I Se dick Edit.	aphy Requirer curity	Key Attestation ments Server
General Super To mod Extensi Ap Ba Cc Ess Ke Descrip Signat Digital Critical	Compatibility Subject Name seded Templat dify an extension ions included in plication Policie sic Constraints tificate Templa uance Policies y Usage	Reque es h, select i this temp is te Informa	It Handling Extensions it, and then o plate: ation	Cryptogr Issuance I Se dick Edit.	aphy Requirer curity	Key Attestation ments Server
General Super To mod Extensi Ba Ba Ce Ess Ess Ke Descrip Signat Dignat Critical	Compatibility Subject Name seded Templat dify an extension ions included in plication Policie sic Constraints trificate Templa uance Policies y Usage	Reque es	It Handling Extensions it, and then o plate: ation	Cryptogr Issuance I Se dick Edit.	aphy [1] Requirer curity	Key Attestation ments Server
General Super To mod Extensi Ap Ba Ba Ce Iss Signat Descrip Signat Digital Critical	Compatibility Subject Name seded Templat dify an extension ons included in plication Policie sic Constraints trificate Templa uance Policies y Usage	Reque es	It Handling Extensions it, and then on plate: ation	Cryptogr Issuance I Se dick Edit.	aphy 1 Requirer curity	Key Attestation ments Server
General Super To mod Extensi Ap Ba Ba Ce Iss Signat Descrip Signat Digital Critical	Compatibility Subject Name seded Templat dify an extension ions included in plication Policies sic Constraints trificate Templa uance Policies y Usage ation of Key Usa ure requirement signature extension.	Reque	stationConstruction	Cryptogr Issuance I Se dick Edit.	aphy 1 Requirer curity	Key Attestation ments Server

-

6. Security:

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

Select	t Users, Computers, Service Accounts, or Groups	x
Selec	t this object type: s, Groups, or Built-in security principals Object Types	
From t	this location:	_
PKI-	VP-Server.bayem.de	
Enter	the object names to select (examples):	-
pki-V	VinEP-machines Check Names	
Ad	dvanced OK Cancel	
	Add Remove Permissions for ZPC-SV-VM11609\$ Allow Deny Full Control	
	OK Cancel Apply Help	

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

	seded Template	s	Extensions	Security	Server
ieneral	Compatibility	Request	Handling	Cryptography	Key Attestation
	Subject Name			Issuance Requir	ements
	ply in the reque	st			
	Use subject info	mation fro	om existing	certificates for a	utoenrollment
	renewal request	:s (")			
Build	from this Activ	e Director	informatio	n	
Selec	t this option to	enforce co	insistency a	among subject n	ames and to
simpli	ify certificate ad	ministratio	n.		
Subje	ect name format	t:			
Fully	distinguished r	name			~
	nclude e-mail na	me in subj	ect name		
Inclu	de this informati	on in alter	nate subier	t name:	
	-mail name				
	INS name				
	lser principal na	me (UPN)			
	ervice principal	name (SP	N		
	or noo principal	name (or			
LS					
S					
S					
* Contro	ol is disabled du	e to <u>comp</u>	atibility setti	ngs.	

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

	t Name			Issuan	ce Requir	eme	nts	
Superseded	Templates	3	Extensions		Security		Se	rver
General Comp	atibility	Reques	st Handling	Crypt	ography	Ke	y Atte	statio
Versions set in Show result Compatibility Certification Windows S Certificate m Windows S These settings	compatib ting chan Settings Authority Server 20 ecipient 3.1 / Wind	ges / 12 R2 dows Se	earlier opera	v : v	stems fro	m us	ing thi	s

?

х

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

	Subject Name			lssui	ance Require	emen	its	
Supers	eded Template	s	Extensions		Security		Server	ľ
General	Compatibility	Request	Handling	Cŋ	/ptography	Key	Attestation	
Provide	r Category:	Key	Storage Pr	ovid	er		~	r
Algorithr	m name:	RS/	4				~	r
Minimun	n key size:	204	8					
Choose O Req I Req	which cryptogr uests can use a uests must use	aphic provid ny provid one of the	viders can b er available e following p	oe u: on f provi	sed for reque the subject's iders:	ests com	puter	E
	osoft Platform C osoft Software H osoft Smart Care	rypto Prov Key Storay I Key Sto	rider ge Provider rage Provid	er				r
Reques	t hash:	SH/	A256				~	
Use	altemate signat	ure forma	t					L
	_							
	ОК		Cancel		Apply		Help	

WinEP_WorkstationCert_TPM Properties

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*

ertifikate anfordern	
olgende Zertifikate sind verfügbar. Kl Registrieren".	icken Sie zum Starten der Registrierung auf
Active Directory-Registrierungsrid	htlinie
WinEP_UserCertEnc2003	i STATUS: Registrierung erforderlich
WinEP_UserCertSignature	i) STATUS: Registrierung erforderlich
WinEP_UserCertSSL	STATUS: Registrierung erforderlich

4. Registrierung für Verschlüsselungs Zertifikat → *Sicherheitsstufe*

	Eine Anwendung erstellt ein geschütztes Objekt.
Act	Privater Schlüssel des CryptoAPI lich Sie haben die mittlere Sicherheitsstufe gewählt.
	OK Abbrechen Details

_

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

Re	gistrierung für: WinEP_UserCertEnc2003	
Zerti	Kennwort erstellen	
Zum. Anme	Erstellen Sie ein Kennwort, um dieses schützen.	Objekt zu
Act		
	Neues Kennwort für dieses Objekt en	stellen
.	Kennwort für: Privater Schlü	issel des Cry
	Kennwort:	8
	Bestätigen:	
	< Zurück Fertig stelle	n Abbreche

7. Mit OK bestätigen

Privater Schlussel des CryptoAPI	
	lich
Sie haben die hohe Sicherheitsstufe Sicherheitsstufe gewählt.	lich
OK Abbrechen Details	

8. Für die Übermittlung des privaten Schlüssels an Prime wird die PIN benötigt $\rightarrow OK$

- Zertifikatregistrierung Windows-Sicherheit Von dieser App muss ein Kryptografieschlüssel erstellt werden. Beim Öffnen dieses Schlüssels wird von der Anwendung Ihre Berechtigung angefordert. Dadurch wird eine nicht autorisierte Verwendung der Anwendung und der Daten verhindert. Kennwort mit diesem Schlüssel • anfordern OK Abbrechen Abbrechen
- 9. Registrierung für Signatur Zertifikat \rightarrow PIN vergeben $\rightarrow OK$

10. Registrierung für SSL Zertifikat \rightarrow PIN vergeben \rightarrow OK

	Windows-Sicherheit	×
Von diese werden. Beim Öffnen Berechtigung	er App muss ein Kryptografieschlüssel erste dieses Schlüssels wird von der Anwendung Ihre gangefordert. Dadurch wird eine nicht autorisierte	llt
Verwendung	der Anwendung und der Daten verhindert.	
f	 Kennwort mit diesem Schlüssel anfordern 	
	•••••	
	OK Abbreck	hen
		-

Active Directory-Registrierungsrid	tlinie
WinEP_UserCertEnc2003	🗸 STATUS: Erfolgreich
WinEP_UserCertSignature	🖌 STATUS: Erfolgreich
WinEP_UserCertSSL	🗸 STATUS: Erfolgreich

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

Zustimmungsaufforderung zur Erstellung eines	Schlüssels		
Um den Vorgang fortzusetzen, mus	ss die Anwendung einen Schlüssel erstellen.		
Dies trägt dazu bei, die nicht autorisierte Verw Anwendung wird Ihre Zustimmung angeforde	rendung der Anwendung und der Daten zu verhindern. Von der ert, sobald dieser Schlüssel verwendet wird.		
Schlüsselname:	Von der Anwendung wurde ein Name für den Schlüssel bereitgestellt.		
Für verstärkte Sicherheit können Sie anfo verwendet wird.	ordern, dass dieser Schlüssel nur mit einem Kennwort		
Kennwort für den Schlüsselschutz:			
Kennwort bestätigen:	An international statements and the		
	Dieses Kennwort anfordern, wenn dieser Schlüssel verwendet wird		
Schlüsselbeschreibung anzeigen	Schlüssel erstellen Abbrechen		

11.1.2 Manuelle Beantragung

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

- 1. File \rightarrow Add/Remove Snap-in
- 2. Links auf *Certificates* klicken \rightarrow *Add*
- 3. My user account \rightarrow Finish
- 4. $OK \rightarrow Pop Up wird geschlossen$
- 5. Links in der Konsolen Struktur *Certificates Current User* ausklappen
- 6. Rechtsklick auf Personal \rightarrow All Tasks \rightarrow Request New Certificate...
- Pop-Up f
 ür die Zertifikatsregistrierung öffent sich. Ähnlich zu Registrierung unter 10.1.1,mit dem Unterschied, dass die gew
 ünschten Templates ausgew
 ählt werden k
 önnen. Zertifikate entsprechend beantragen.

Alle ausgestellten Zertifikate sind unter Certificates – Current User \rightarrow Personal \rightarrow 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 \rightarrow *Add*
- 3. Computer account \rightarrow Next \rightarrow Local computer... \rightarrow Finish
- 4. $OK \rightarrow Pop Up$ wird geschlossen
- 5. Links in der Konsolen Struktur Certificates (Local Computer) ausklappen
- 6. Rechtsklick auf Personal → All Tasks → Request New Certificate...
- Pop-Up f
 ür die Zertifikatsregistrierung öffent sich. Ähnlich zu Registrierung unter 10.1.1,mit dem Unterschied, dass die gew
 ünschten Templates ausgew
 ählt werden k
 önnen. Zertifikate entsprechend beantragen.

Alle ausgestellten Zertifikate sind unter *Certificates (Local Computer)* \rightarrow *Personal* \rightarrow *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:

Filter Current Log			
Filter XML			
Logged: Event level:	Any time Critical Warning Verbose		
	Error Information		
By log	Event logs: Application		
O By source	Event sources: WinEP		

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

A Warning			WinEP
<	ш		
Event 100, WinEP			
General Details			
checkPermission: PK	(I-VP-CLIENT\ZPC-SV-VM11609\$ was GRAN	ED enrollment for <mark>templa</mark>	te WinEP_WorkstationCert.

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 <u>Eventlogs, Zeitstempel und Daten zum</u> Antragsteller (Name des Teilnehmers oder PCs) bereit.

12.1 Fehlercode 0x80004005

<pre>Error</pre>	
<	
Event 100, WinEP	
General Details	
CCertRequestD::getErrorMessa	age - Error occurred <mark>0x80004005, .</mark>

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:

Error			WinEP
Event 100,	WinEP		
General	Details		
СНТТ	usubmitRequest <mark>: Cou</mark>	ıld not find "fullrespon	se" in response!.

Oder

Error	
<	Ш
Event 100, WinEP	
General Details	
CHTTP::submitRequest - Error	in response. CF Error: -1.

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:

– 🗆 🗙

🔄 Certificate Enrollment

Failed to install one or more certificates

One or more of the certificate requests that you submitted could not be completed. Review the information that appears below each certificate for information on how to proceed.

WinEP_UserCertEnc2008_CSP	X STATUS: Failed
There is a key archival hash mismate	ch between the request and the response.
ZPS-SV-VM06153.PKI-VP-Server.bay	ern.de\VP-Bayern-Softtoken-Issuing-CA-2019
The certificate request could not	be submitted to the certification authority.
Unspecified error 0x80004005 (-21	47467259 E_FAIL)
ZPS-SV-VM06153.PKI-VP-Server.bay	/ern.de\VP-Bayern-Softtoken-Issuing-CA-2019
The certificate request could not	be submitted to the certification authority.
Unspecified error 0x80004005 (-21	47467259 E_FAIL)
The requested certificate has been	n issued.
A certificate issued by the certific	ation authority cannot be installed. Contact
your administrator.	
There is a key archival hash mism	atch between the request and the response.
0x80095004 (-2146873340 XENROLL_	E_RESPONSE_KA_HASH_MISMATCH)
A certificate issued by the certific	ation authority cannot be installed. Contact
your administrator.	
There is a key archival hash mism	atch between the request and the response.
0x80095004 (-2146873340 XENROLL_	E_RESPONSE_KA_HASH_MISMATCH)
A certificate issued by the certificate	ation authority cannot be installed. Contact
your administrator.	
There is a key archival hash mism	atch between the request and the response.
0x80095004 (-21468/3340 XENROLL_	E_RESPONSE_KA_HASH_MISMATCH)
✓ WinEP UserCertSignature KSP	STATUS: Succeeded
WinEP_UserCertSSL_KSP	STATUS: Succeeded

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.

Issued To	Issue	l By		Expiration Date	Intended F
🕵 zpc-sv-vm1160	9 <mark>.pki-vp-client.b VP-B</mark>	avern-So	ofttoken-Issuing-CA	25.09.2022	Client Aut
	Open				
	All Tasks	>	Open		
	Cut		Request Certificate with	h New Key	
	Сору		Renew Certificate with	New Key	
	Delete		Manage Private Keys		
	Properties		Advanced Operations		>
	Help		Export		
	-				

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:

- 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.