



# **Amazonen Werke H. Dreyer GmbH & Co. KG**

---

**„Einrichtung einer zweistufigen PKI-Struktur auf  
64bit Technologie mit Schwerpunkt auf externen  
Zugriff auf Domänen-Exchange Postfach“**

**Projektdokumentation**

**Moritz Buntrock**



## **Inhaltsverzeichnis**

1. Projektvorfeld .....	1
1.1 Projekteinleitung .....	1
1.2 Projektauftrag .....	1
1.3 Projektschnittstellen .....	1
2. IST-Analyse .....	2
3. Sollkonzept .....	3
4. Organisatorische Einteilung .....	4
4.1 Ablaufplanung / Zeitliche Gliederung .....	4
4.1 Personalplanung .....	5
5. Sachmittelbedarf ermitteln .....	6
6. Kostenplanung .....	7
7. Installationsphase .....	8
7.1 Installationen der Host-Server .....	8
7.2 Einrichtung der Root- und Issuing-Zertifizierungsstelle .....	8
7.3 Erstellung des Zertifikates für den Webserver .....	11
7.4 Konfiguration des RPC-Proxys .....	12
7.6 Einstellung des Exchange Servers .....	12
7.7 Anpassung der RPC-Einstellungen auf dem AD .....	12
7.8 Zertifikatsanforderung des Webserver auf dem der RPC-Proxy läuft .....	12
8. Abschluss .....	15
8.1 Test der Funktionalität .....	15
8.2 Soll- / Ist- Vergleich .....	15
8.3 Fazit .....	15

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit  
Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

## Tabellenverzeichnis

Tabelle 1: Zeitliche Gliederung .....	4
Tabelle 2: Aufwand der PKI bei Einrichtung durch Dienstleister .....	5
Tabelle 3: Aufwand bei eigener Einrichtung und Konfiguration der PKI .....	5

## Abbildungsverzeichnis

Abbildung 1: IST-Zustand der PKI-Struktur .....	2
Abbildung 2: (Gesamt-)Soll-Konzept der PKI-Struktur .....	3
Abbildung 3: Amazone RootCA Zertifikat .....	8
Abbildung 4: Zertifikatsanforderung .....	9
Abbildung 5: Austellen des Zertifikates für die SubCA .....	10
Abbildung 6: Zertifizierungstellenzertifikat auf der IssuingCA installieren .....	10
Abbildung 7: Amazone SubCA Zertifikat .....	10
Abbildung 8: Eigenschaften/Allgemein der Amazone Webserver Vorlage .....	11
Abbildung 9: Eigenschaften/Sicherheit der Amazone Webserver Vorlage .....	11
Abbildung 10: Eigenschaften/Exchange-Features eines Benutzers im Active Directory .....	12
Abbildung 11: Zertifikatsanforderung des Webserver über die Zertifizierungskonsole .....	13
Abbildung 12: Angefordertes Amazone Webserver Zertifikat .....	14
Abbildung 13: Eigenschaften/Antragstellers des Webserver Zertifikats .....	14

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

## **1. Projektvorfeld**

### **1.1 Projekteinleitung**

Die AMAZONE-Gruppe ist ein Familienunternehmen der Landmaschinen- und Kommunalmaschinenindustrie in der 4. Generation der Familie Dreyer. Die Amazone Gruppe ist mit Ihren 6 Standorten deutschlandweit vertreten. Das Augenmerk bei diesem Projekt liegt auf dem Produktionsstandort in Hude bei Oldenburg für aktive Bodenbearbeitung und Sätechnik. Dieser wurde im Jahre 1957 gegründet und beschäftigt derzeit ca. 420 Mitarbeiter.

In Bezug auf die eigentliche Dokumentation werden alle Begriffe, die in folgender Schriftart „**Courier New**“ formatiert sind, im Glossar in alphabetischer Reihenfolge näher erklärt. Etwaige Passwortangaben, Computernamen, interne IP-Adressen und Zertifikatsinformationen sind aus Datenschutzgründen absichtlich entfernt worden, da diese nur den jeweils involvierten Personen bekannt sein sollten. Die Passwörter sind allerdings ausreichend lang, bestehen aus Groß- und Kleinbuchstaben, sowie Zahlen bzw. Sonderzeichen.

### **1.2 Projektauftrag**

Bei einem Vorgespräch mit Herrn Rittel (Administrator der Amazone Gruppe) wurde die derzeitige Situation und das grob abgesteckte Soll-Konzept besprochen. Der Auftrag besteht daraus, die bereits bestehende 32bit PKI-Struktur, deren Zertifikate zum 31.12.2011 auslaufen, durch eine zweistufige **Certification Authority** (kurz CA) auf Basis von 64bit abzulösen.

### **1.3 Projektschnittstellen**

Als direkte Ansprechpartner in diesem Projekt stehen der Auftraggeber Herr Clemens Rittel und Herr Matthias Bonk, der in Hinsicht auf organisatorische und technische Richtlinien hinzugezogen wurde, zur Verfügung.

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

## 2. IST-Analyse

Die Amazonen-Gruppe besitzt derzeit eine zweistufige PKI-Infrastruktur (Enterprise RootCA / Enterprise SubCA) auf Basis von Windows Server 2003 R2. Die RootCA befindet sich im Stammwerk Gaste, die SubCA ist in den Standorten Gaste, Hude und Leipzig verteilt. Das Pilotprojekt wird nur im Zusammenspiel Gaste/Hude durchgeführt. Der angedachte Einsatzzweck ist die Anbindung von externen Mitarbeitern ohne Domänenmitgliedschaft (bevorzugt aus dem Standort Samara / Russland) durch Outlook RPC over HTTP. Da es im Frühjahr 2010 zu Problemen auf dem Server kam, auf dem sich die Stammzertifizierungsstelle befand, konnte man die auslaufenden Zertifikate nicht verlängern (speziell: das am 03.2011 auslaufende Zertifikat für Outlook RPC over HTTP). Nach Reaktivierung im Januar 2011 der Stammzertifizierungsstelle und der RootCA wurde das für Outlook RPC over HTTP zuständige Zertifikat bis zum 31.12.2011 verlängert.

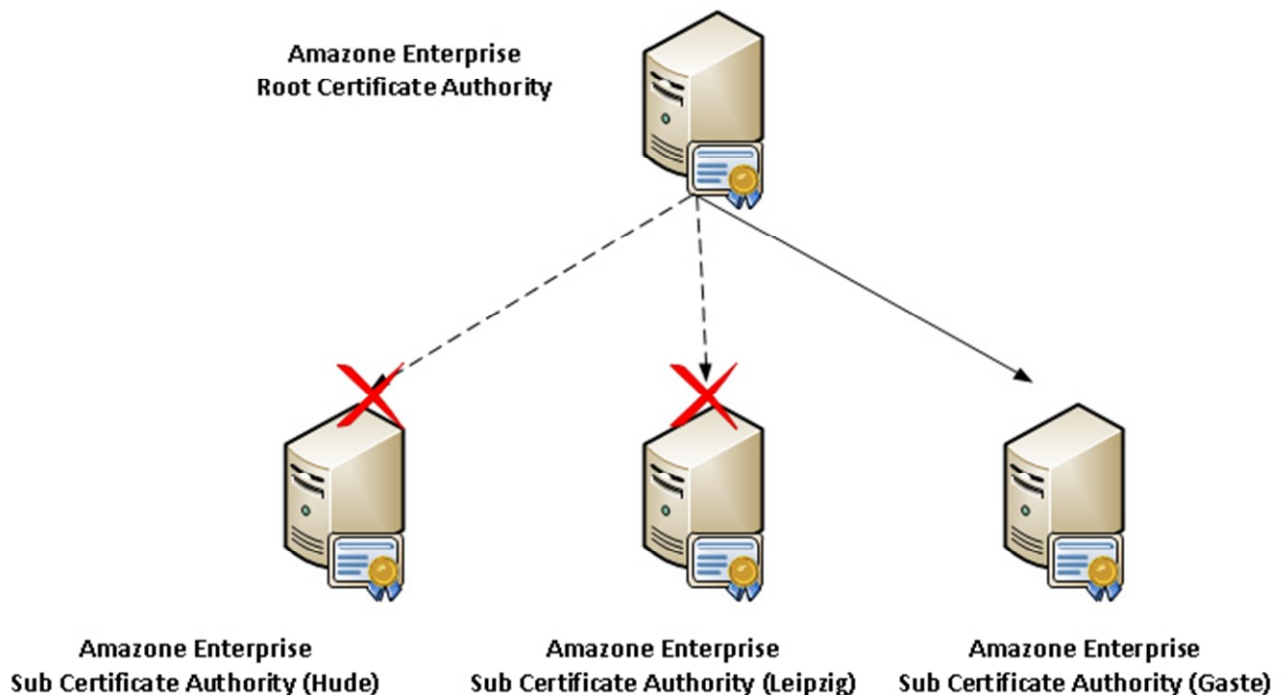


Abbildung 1: IST-Zustand der PKI-Struktur

Derzeit ist nur die RootCA und die SubCA in dem Werk Gaste verfügbar. Diese läuft auf einem Domain Controller der mit Windows Server 2003 Enterprise Edition R2 betrieben wird.

### 3. Sollkonzept

Zum Abschluss des Projektes soll die Amazone-Gruppe eine zweistufige PKI-Intrastruktur besitzen, die auf Windows Server 2008 R2 Technologie funktioniert. Da der Betrieb analog eine Hochstufung von Windows Server 2003 auf 2008 R2 in der Domänencontroller Umgebung vollzieht, liegt es nahe, dass die zukünftige Stammzertifizierungsstelle direkt auf Windows Server 2008 R2 aufgesetzt wird.

<sup>1</sup>Zusätzlich sollen die Laufzeiten der Zertifikate für Outlook RPC over HTTP verlängert werden und im gleichen Schritt die Vorarbeit für offene Schnittstellen in Hinsicht auf Endgeräteauthentifizierung, sowie E-Mail Verschlüsselung und Dateiverschlüsselung in der Firmenlandschaft gegeben werden. Es muss sichergestellt werden, dass ein externer Mitarbeiter durch ein verbessertes Sicherheitskonzept einen gesicherten Zugriff auf seine im Standort Hude befindlichen Exchange Postfächer bekommt. Dies beinhaltet eine Sicherheitsabfrage über ein gültiges Zertifikat. Zusätzlich sollen neue Verschlüsselungsverfahren angewandt werden. Nach erfolgreicher Einrichtung und Implementierung kann die derzeit vorhandene Zertifikatsstelle (Windows Server 2003 R2) abgeschaltet werden.

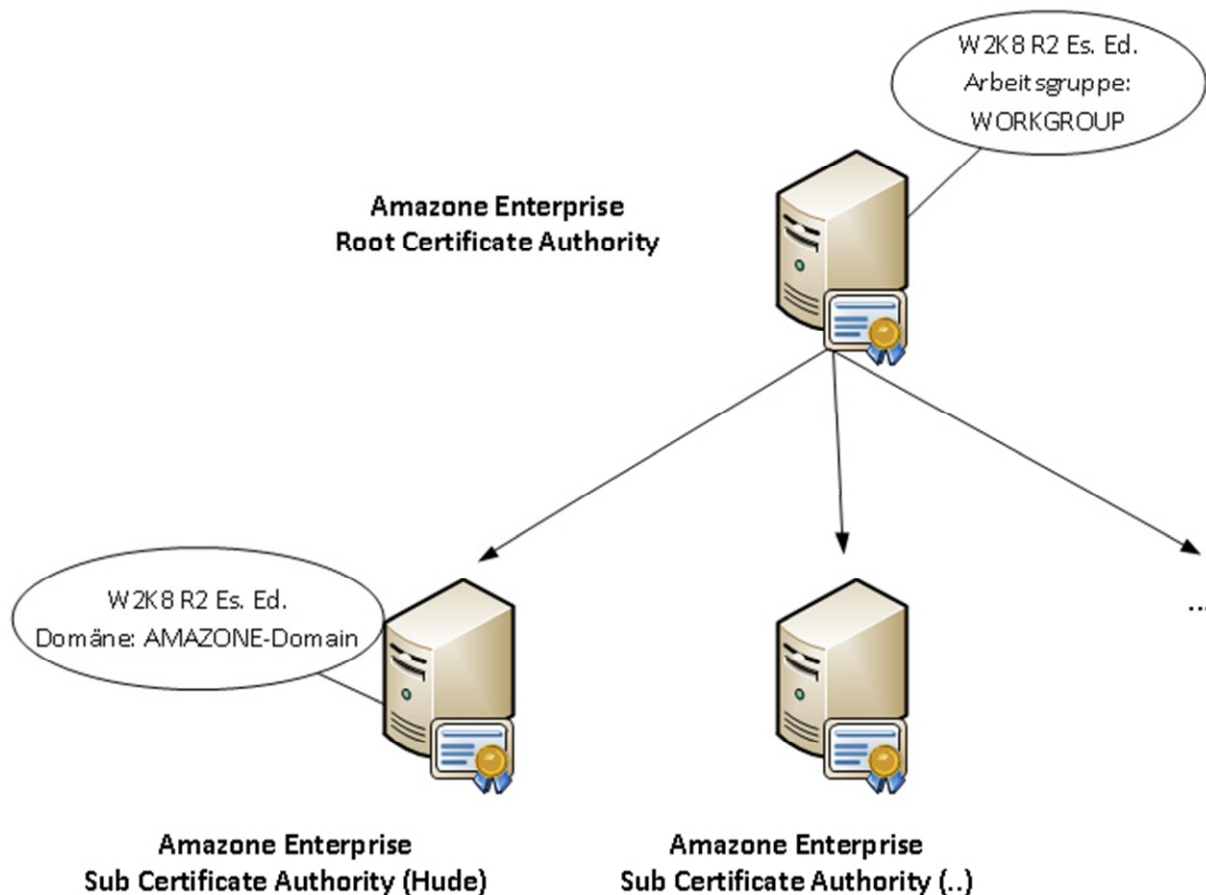


Abbildung 2: (Gesamt-)Soll-Konzept der PKI-Struktur

<sup>1</sup> (Anm.: an dieser Stelle weise ich darauf hin, dass im Folgenden das Kürzel W2K8 R2 genutzt wird)

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt  
auf externen Zugriff auf Domänen-Exchange Postfach

## 4. Organisatorische Einteilung

### 4.1 Ablaufplanung / Zeitliche Gliederung

Das Projekt soll den Umfang von 35 Stunden nicht überschreiten.  
Der Starttermin war für den 01.03.2011 festgelegt, das Ende war für den 15.04.2011 datiert.

Tabelle 1: Zeitliche Gliederung

	Handlungsschritte	Dauer in Stunden		
		IST-Zeit	Soll-Zeit	
<b>1. Definition</b>				
	1.1 Kundengespräch / Zielsetzung	6	6	
	1.2 IST-Zustand ermitteln	1	1	
	1.3 Soll-Konzept erstellen	3	3	
	1.4 Sachmittelbedarf ermitteln	1	1	
	1.5 Kundengespräch	2	2	
	1.6 Pflichtenheft	1	1	
	<b>Gesamt:</b>	<b>14</b>	<b>14</b>	
<b>2. Planung</b>				
	2.1 Ablaufplanung	3	3	
	2.2 Zeitplanung	1	1	
	2.3 Personalplanung	1	1	
	2.4 Angebote einholen	1	1	
	2.5 Kostenplanung	1	1	
	2.6 Bestellung	1	1	
	<b>Gesamt:</b>	<b>8</b>	<b>8</b>	
<b>3. Durchführung</b>				
	3.1 Installation des Host-Servers	2	1	-1
	3.2 Einrichtung der Zertifizierungsstelle	1	1	
	3.3 Erstellung der Zertifikate	2	2	
	3.4 Einstellung des Exchange Servers	1	1	
	3.5 Anpassung der RPC-Einstellungen am Active Directory Domain Controller	1	1	
	3.6 Einstellung bzw. Anpassung der Endgeräte	1	2	+1
	<b>Gesamt:</b>	<b>8</b>	<b>8</b>	
<i>Der Kunde hat ein vorinstalliertes W2K8 R2 Es. Ed. Image zur Verfügung gestellt, weswegen sich die Dauer von Punkt 3.1 verkürzt hat. Im gleichen Zug haben die Arbeiten an den Endgeräten mehr Zeit verbraucht, da dort Fehler aufgetreten waren.</i>				
<b>4. Abschluss</b>				
	4.1 Test der Funktionalität	1 ½	1 ½	
	4.2 Soll- / Ist- Vergleich	1	1	
	4.3 Fazit	1	1	
	4.4 Betriebsdokumentation erstellen	1	1	
	4.5 Kundendokumentation erstellen	½	½	
	<b>Gesamt:</b>	<b>5</b>	<b>5</b>	

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

#### 4.1 Personalplanung

Da im Vorfeld eine Implementierung und Einrichtung der PKI durch einen Dienstleister angedacht war, werden zur Differenzierung der Arbeitsaufwand bei einer Einholung von Dienstleistern und der Arbeitsaufwand bei der Umsetzung einer Eigenlösung in den folgenden zwei Tabellen veranschaulicht:

<div style="text-align: center;">             ↑  <b>Leistung für den Kunden</b>              ↓                ↑  <b>Aufwand des Kunden</b>              ↓         </div>	<b>Infrastruktur</b>	Hardware aufbauen
		Hardware-Upgrades
		Software installieren
	<b>Personaleinsatz</b>	Technologische Grundlagen
		Erstellung von Zertifikaten
		Verteilung der Zertifikate
	<b>Recht</b>	Pflichten / Haftung PKI Betreiber
		Pflichten PKI Benutzer
		Softwareupdates
		Backup / Recovery
		Betrieb und Wartung

Tabelle 2: Aufwand der PKI bei Einrichtung durch Dienstleister

Als Gegenbeispiel folgen die zusammengefassten Handlungsschritte für eine eigenständige Einrichtung und Konfiguration der PKI. Im dem angedachten Szenario werden alle Schritte durch Eigenleistung erbracht bzw. erlernt:

<div style="text-align: center;">             ↑  <b>Aufwand des Kunden</b>              ↓         </div>	<b>Infrastruktur</b>	Hardware aufbauen
		Software installieren
		Hardware-Upgrades
		Softwareupdates
	<b>Personaleinsatz</b>	Technologische Grundlagen
		Erstellung von Zertifikaten
		Verteilung der Zertifikate
		Backup / Recovery
		Betrieb und Wartung
	<b>Recht</b>	Pflichten / Haftung PKI Betreiber
		Pflichten PKI Benutzer

Tabelle 3: Aufwand bei eigener Einrichtung und Konfiguration der PKI

Aus den oben aufgezeigten Beispielen wird recht schnell deutlich, dass die aufgewendete Zeit für eine selbstbetriebene PKI in Bezug auf Planung und den Aufbau eine sehr hohe Bindung der Kapazitäten des eigenen Personals darstellt. Allerdings kann durch eine selbsteingerichtete und konfigurierte PKI-Lösung wesentlich flexibler auf zusätzliche Anforderungen reagiert werden.

Die Kosten zu den jeweiligen Modellen werden im nächsten Kapitel analysiert.



Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

## **5. Sachmittelbedarf ermitteln**

Da die derzeitige PKI-Instanz auf veralteter Serverhardware (Dell Powerededge 1850) liegt und der Auftraggeber sich momentan in einer Migrationsphase von Windows Server 2003 R2 (32bit) auf W2K8 R2 befindet, muss neue Hardware beschafft werden. Aufgrund des angedachten Einsatzzweckes und der Unternehmensphilosophie, muss der neue Server für eine erhöhte Anzahl an virtuellen Maschinen ausgelegt werden. Es kommt hinzu, dass im Amazone Unternehmen durchgängig Hardware von Dell verbaut wird, weswegen bei der Angebotseinholung hauptsächlich die dort angebotenen Server analysiert wurden. Durch diesen Schritt ist es möglich weitere Rabatte auf Hardware einzukalkulieren und Geld zu sparen.

Das sind die Komponenten des Servers (Dell PowerEdge T610):

*4x Intel Xeon E5645 2,40 Ghz; 24 GB DDR3; 2x 870W Netzteil; 6x 300 GB Festplatte in einem RAID 5 Verbund, wobei eine Festplatte als Hotspare fungiert; 1x Broadcom NetXtreme 1 GbE Nic 2x Port ; 1x Broadcom NetXtreme 1 GbE Nic 4x Port.*

Zusätzlich zu der Serverhardware werden noch zwei weitere, virtuelle Server eingerichtet (Root-CA bzw. die Sub-CA). Der Kunde wünscht, dass dieses Szenario mittels der Virtualisierungsplattform Hyper-V bewerkstelligt wird. Die Zertifikatsdienste der Root-CA und der Sub-CA werden mit dem Betriebssystem W2K8 R2 Es. Ed.<sup>2</sup> bereitgestellt. Für die Root-CA kann eigentlich auch das Betriebssystem W2K8 R2 St. Ed.<sup>3</sup> verwendet werden, da die erweiterten Funktionen der Enterprise Edition an dieser Stelle nicht benötigt werden. Vom Kunden wird allerdings gewünscht, dass wir auf beiden Zertifikatsstellen einheitlich die W2K8 R2 Es nutzen. Die Kosten für 2 x W2K8 R2 Es. Ed. Lizenzen werden in der nachfolgenden Tabelle „Kostenanalyse“ unter dem Punkt „Lizenzkosten“ aufgeführt.

---

<sup>2</sup> Windows Server 2008 R2 Enterprise Edition

<sup>3</sup> Windows Server 2008 R2 Standard Edition

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt  
auf externen Zugriff auf Domänen-Exchange Postfach

## 6. Kostenplanung<sup>4</sup>

Um mögliche Alternativen im Blick zu haben, werden in der folgenden Tabelle die Kosten von zwei Alternativen aufgeführt; Outsourcing (extern beglaubigte Zertifikate einer vertrauenswürdigen Stammzertifizierungsstelle (z.B. „Thawte“) oder eine Implementierung durch Dienstleistung (z.B. „Controlware“)

	Outsourcing (Zertifikate „kaufen“)	Implementierung durch Dienstleistung	Eigenleistung
Hardwarekosten	-	1x 6324,85 €	1x 6324,85 €
Lizenzkosten	-	2x 2.376,37€ = 4752,74 €	2x 2.376,37€ = 4752,74 €
Supportkosten	-	-	-
Schulungskosten	-	3 Tage * 980,00 € = 2940,00 €	-
Einrichtungskosten (extern)	-	3 Tage * 980,00 € = 2.940,00 €	-
Einrichtungskosten (intern)	-	6 Std. * 98,00 € = 588,00 €	35 Std. * 98,00 € = 3430,00 €
Zertifikatskosten	1 Stk = 659,00 €	-	-
<b>Summe</b>	<b>659,00 €</b>	<b>17.545,59 €</b>	<b>14.507,59 €</b>

Tabelle 4: Kostenanalyse

Die Kostenanalyse verdeutlicht, dass in dem angedachten Projekt die Lösung Outsourcing, genauer - extern verifizierte Webserverzertifikate mit 2 Jahren Laufzeit - kostengünstiger wäre, als die Einrichtung durch einen Dienstleister oder durch eine komplette Eigenleistung. Zu beachten ist allerdings, dass in diesem Szenario nur die Webserverzertifikate eine Rolle spielen. Da aber das Projekt auch in Zukunft von den Kosten her überschaubar bleiben soll und die Zertifikate in dem Beispiel über das komplette Unternehmen verteilt werden (verschiedene Zwecke der Zertifikate), steigen auch die Kosten durch eingekaufte Zertifikate auf Dauer in die Höhe.

Kriterium	Faktor	Outsourcing		Eingekaufte Dienstleistung		Eigenleistung	
		Punkte	P * F	Punkte	P * F	Punkte	P * F
Kosten	3	3	9	1	3	1	3
Support	3	2	6	2	6	3	9
Einarbeitungszeit	1	3	3	2	2	1	1
Flexibilität	3	1	3	2	6	3	9
Erweiterbarkeit	2	2	4	2	4	3	6
Zentrale Verwaltung	1	2	2	2	2	2	2
Ausfallsicherheit	2	3	6	2	2	2	4
<b>Ergebnis</b>		<b>33</b>		<b>25</b>		<b>34</b>	

Tabelle 5: Entscheidungsmatrix

<sup>4</sup> Kosten sind den im Anhang befindlichen Angeboten zu entnehmen

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

## **7. Installationsphase**

### **7.1 Installationen der Host-Server**

An den vorkonfigurierten Hyper-V Imageplatten mit W2K8 R2 Es Ed. müssen lediglich kleinere Einstellungen vorgenommen werden. Im ersten Arbeitsschritt werden alle erforderlichen Programme installiert. Anschließend bekommen die virtuellen Server, die vorgesehenen selbsterklärenden Namen und feste IP-Adressen. Ist dies erledigt wird, die SubCA in die bestehende Amazone-Domäne aufgenommen. Der RootCA Server, bleibt in der Standard-Arbeitsgruppe „Workgroup“, da dieser nur für die Zertifikatsverlängerung eingeschaltet werden muss.

### **7.2 Einrichtung der Root- und Issuing-Zertifizierungsstelle**

Vor der Installation der RootCA (Servername: {ROOTCA-Server}) wurde die Datei CAPolicy.inf erstellt, die auf dem Server in das Verzeichnis C:\Windows\ des Servers kopiert wird. <sup>5</sup>Diese Datei muss nicht zwingend erstellt werden, Sie vereinfacht die Einrichtung der CA, da während der Installation die dort angegebenen Optionen gleich eingetragen werden. Die Zertifikatsdienste selbst werden über den Server Manager des WS2K8 R2 installiert. Diese wird als Zertifikatsstelle installiert, welche als Option „Eigenständig“ fungiert. Der Zertifizierungsstellentyp ist „Stammzertifizierungsstelle“, da diese die erste Zertifizierungsstelle der PKI wird. Das bedeutet auch, dass bei der Konfiguration der Serverrolle ein neuer privater Schlüssel erstellt werden muss. Die Schlüssellänge dieses Schlüssels beträgt 4096 Bit. Am Ende der Einstellungen wird ein selbsterklärender Name vergeben, bei der RootCA „Amazone Root Certification Authority“. Die genaue Auflistung des Suffixes ist dem Anhang zu entnehmen. Um die weiteren Parameter der RootCA zu definieren, wird nach der Installation ein Skript mit entsprechend vorgefertigten Werten ausgeführt. <sup>6</sup> Nach dem Ausführen dieses Skriptes ist die eigentliche Installation und Einrichtung abgeschlossen. Das ausgestellte Zertifikat kann abschließend geprüft werden:

**Ausgestellt für:** Amazone Root Certification Authority

**Ausgestellt von:** Amazone Root Certification Authority

**Gültig ab** 18. 04. 2011 **bis** 18. 04. 2022

Abbildung 3: Amazone RootCA Zertifikat

Damit den Zertifikaten der PKI vertraut werden kann, muss das Zertifikat der Root-CA in den Zertifikatsspeicher für vertrauenswürdige Stammzertifizierungsstellen aufgenommen werden. Durch eine Veröffentlichung des Zertifikates im Active

---

<sup>5</sup> (Anm.: siehe Anhang B.3.1)

<sup>6</sup> (Anm.: siehe Anhang B.4.1)

### Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

Directory wird dieses automatisch bei allen Domänenmitgliedern als vertrauenswürdig gekennzeichnet. Dies wird über den folgenden Befehl in der Kommandozeile durchgeführt:

```
certutil -dspublish -f "C:\Windows\System32\certsrv\certenroll\AmazonRoot Certification Authority.crt"
```

Für die Installation der SubCA (Servername: {ROOTCA-Server}) kann abermals die Datei CAPolicy.inf genutzt werden. Die Einstellung der Datei weicht allerdings von der \*.inf-Datei ab, die auf dem Server hinterlegt ist. Vor der Installation wird diese in das Verzeichnis C:\Windows\ des Servers kopiert.<sup>7</sup> Die Zertifikatsdienste selbst werden über den Server Manager installiert. Bei der Issuing-CA ist zu beachten, dass neben der Zertifikatsstelle zusätzlich die Zertifikatsstellen-Webregistrierung mit installiert wird. Dadurch ist es möglich, für Computer, die kein Mitglied der Amazone-Domäne sind, Zertifikate auszustellen und zu registrieren. Da im vorherigen Handlungsschritt bereits die „Stammzertifizierungsstelle“ (RootCA) installiert wurde, arbeitet die IssuingCA als Installationstyp „Unternehmen“. Dieser Server ist, im Gegensatz zu der RootCA, Mitglied der Amazone-Domäne. Als Zertifizierungsstellentyp wird „untergeordnete Zertifizierungsstelle“ ausgewählt. Auch dort benötigt man einen neuen privaten Schlüssel mit der Schlüssellänge 4096 Bit. Der Name dieser SubCA lautet „Amazone Internal Certification Authority“. Die genaue Auflistung des Suffixes ist dem Anhang zu entnehmen.<sup>8</sup> Bei dieser SubCA ist allerdings zu beachten, dass das Zertifikat für diesen Server erst bei der RootCA zu beantragen ist. Alle weiteren Einstellungen bleiben auf Standard. Bei der erfolgreichen Installation der Zertifikatsdienste wurde ein „Zertifikatsrequest“ erstellt. Dieser muss jetzt auf der RootCA über die Zertifizierungsstellenkonsole eingereicht werden:

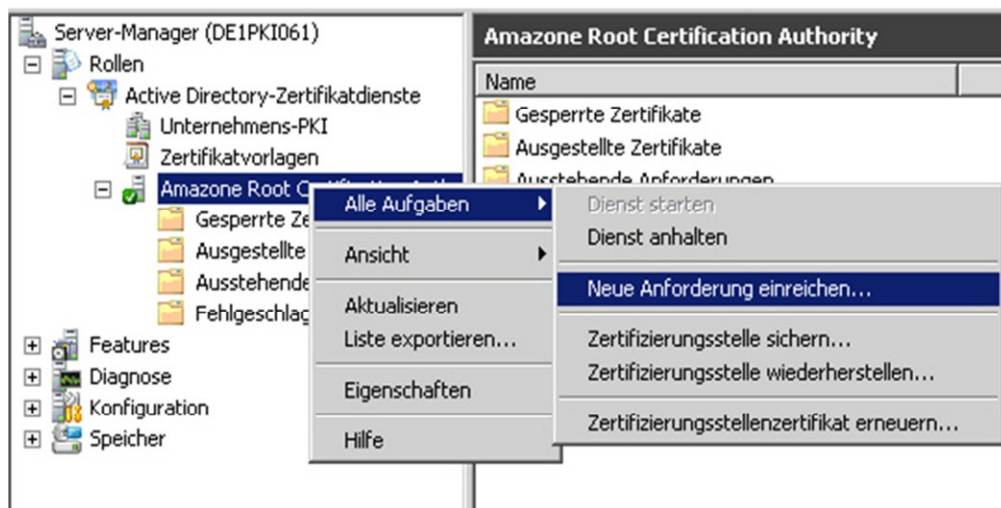


Abbildung 4: Zertifikatsanforderung

<sup>7</sup> (Anm.: siehe Anhang B.6.1)

<sup>8</sup> (Anm.: siehe Anhang B.6.2)

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

Anschließend taucht das Zertifikat unter „Ausstehende Anforderungen“ auf und muss dort manuell genehmigt werden.



Abbildung 5: Ausstellen des Zertifikates für die SubCA

Ist das erfolgt, kann das Zertifikat exportiert und auf dem {SUBCA-Server} in der Zertifizierungsstellenkonsole installiert werden.

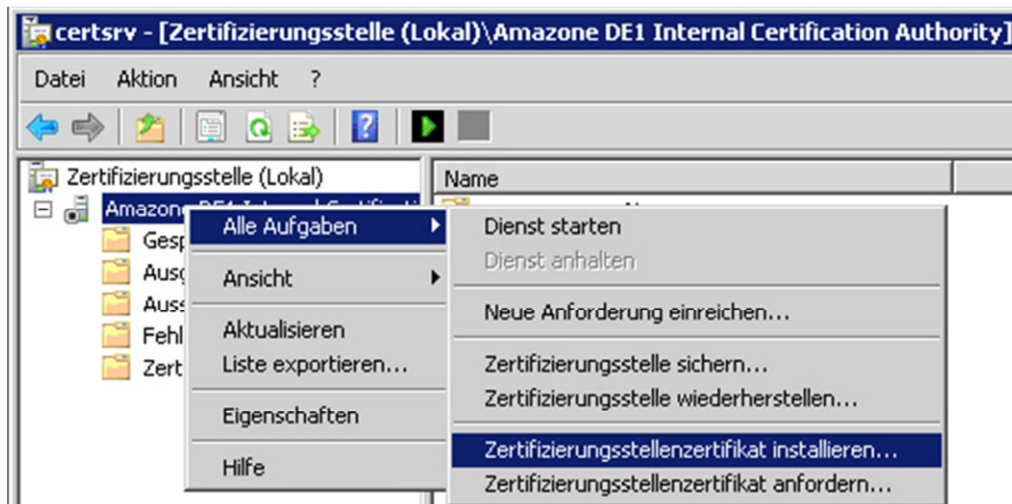


Abbildung 6: Zertifizierungsstellenzertifikat auf der IssuingCA installieren

Danach können die Zertifikatsdienste gestartet werden. Um die festgelegten Parameter für die SubCA zu definieren, wird nach der Installation ein Skript ausgeführt.<sup>9</sup> Abschließende Prüfung des Zertifikates der SubCA:

**Ausgestellt für:** Amazone DE1 Internal Certification Authority

**Ausgestellt von:** Amazone Root Certification Authority

**Gültig ab** 18. 04. 2011 **bis** 18. 04. 2016

🔑 Sie besitzen einen privaten Schlüssel für dieses Zertifikat.

Abbildung 7: Amazone SubCA Zertifikat

<sup>9</sup> (Anm.: siehe Anhang B.7.1)

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

### 7.3 Erstellung des Zertifikates für den Webserver

Als erstes werden sämtliche Zertifikatsvorlagen aus der Konsole der Sub-CA entfernt, um anschließend alle benötigten Vorlagen mit den angepassten Informationen neu zu erstellen. Zuerst wählt man die entsprechende Vorlage aus der Konsole Zertifikatsvorlagen. Mit einem Klick auf „Doppelte Vorlage“ im Kontextmenü kann anschließend eine neue Vorlage erstellt werden. Alle erstellten Vorlagen werden nach „Windows Server 2003“ erstellt. Die verschlüsselte Kommunikation mit einem Webserver wird nicht über HTTP sondern über HTTPS durchgeführt. Dafür benötigt der Server ein Zertifikat mit dem Verwendungszweck „Serverauthentifizierung“. Für die erforderlichen Webserverzertifikate wird also eine Vorlage „Amazon Webserver“ erstellt.

The screenshot shows the 'Amazon Webserver' certificate template properties. The 'Vorlagenanzeigename:' field contains 'Amazon Webserver'. The 'Unterstützte Zertifizierungsstellen (Min.):' field contains 'Windows Server 2003 Enterprise'. The 'Vorlagenname:' field also contains 'Amazon Webserver'. At the bottom, there are two dropdown menus: 'Gültigkeitsdauer:' set to '2 Jahre' and 'Erneuerungszeitraum:' set to '6 Wochen'.

Abbildung 8: Eigenschaften/Allgemein der Amazon Webserver Vorlage

The screenshot shows the 'Amazon Webserver' certificate template properties, Security tab. The 'Abgelöste Vorlagen' tab is selected. The 'Gruppen- oder Benutzernamen:' list contains the following entries: 'Authentifizierte Benutzer', 'Administrator PKI (admin\_pki@AURDXP.amazonen-werke.com)', 'PKI\_Webserver (AURDXP\PKI\_Webserver)', 'Domänen-Admins (AURDXP\Domänen-Admins)', and 'Organisations-Admins (AURDXP\Organisations-Admins)'. The 'PKI\_Webserver (AURDXP\PKI\_Webserver)' entry is selected. Below the list are 'Hinzufügen...' and 'Entfernen' buttons. The 'Berechtigungen für "PKI\_Webserver"' table is shown below.

Berechtigungen für "PKI_Webserver"	Zulassen	Verweigern
Vollzugriff	<input type="checkbox"/>	<input type="checkbox"/>
Lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Schreiben	<input type="checkbox"/>	<input type="checkbox"/>
Registrieren	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Automatisch registrieren	<input type="checkbox"/>	<input type="checkbox"/>

Abbildung 9: Eigenschaften/Sicherheit der Amazon Webserver Vorlage



Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

Die Berechtigung zur Registrierung solcher Zertifikate werden der Gruppe „PKI-Webserver“ erteilt. Diese Gruppe wurde im Vorfeld auf dem AD-Controller des Werkes Gaste erstellt.

#### **7.4 Konfiguration des RPC-Proxys**

Bevor „RPC over HTTP“ eingesetzt werden kann, muss auf einem Webserver in der **DMZ** ein bestimmter Netzwerkdienst installiert werden. Dies geschieht über „Software“ in der Option „Assistent für Windows-Komponenten“ unter „Netzwerkdienste“. Dort gibt es die Auswahlmöglichkeit „RPC-über-HTTP-Proxy“. Nach der Installation nimmt dieser Dienst die Anfragen der Clients aus dem Internet entgegen. Zusätzlich müssen in den Eigenschaften die Authentifizierungsmethoden abgeändert werden. Dazu ist über den Reiter „Verzeichnissicherheit“ die Option „Standardauthentifizierung“ zu aktivieren.

#### **7.6 Einstellung des Exchange Servers**

Auf den Exchange 2003 Servern ist es erforderlich die Einstellung für die „RPC over HTTP“ Konfiguration zu überarbeiten. Dazu aktiviert man auf dem Mailserver über den Exchange Server Manager die Option „RPC-HTTP Back-End-Server“.

#### **7.7 Anpassung der RPC-Einstellungen auf dem AD**

Damit die Benutzer „RPC over HTTP“ auch nutzen können, müssen drei Bedingungen erfüllt sein: 1. Benutzer muss im Verzeichnisdienst existieren, 2. Benutzer muss ein Postfach besitzen und 3. Benutzer muss die Berechtigung besitzen RPC zu nutzen. Die ersten beiden Punkte sind bei dem bestehenden Benutzer erfüllt, also bearbeitet man die 3. Bedingung. Dazu wird in dem Verzeichnisdienst auf dem Konto des Mitarbeiters unter dem Reiter „Exchange-Features“ die Option „Outlook Web Access“ aktiviert.

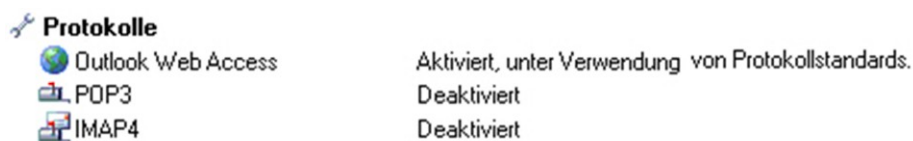


Abbildung 10: Eigenschaften/Exchange-Features eines Benutzers im Active Directory

#### **7.8 Zertifikatsanforderung des Webserver auf dem der RPC-Proxy läuft**

Ein Webserverzertifikat kann über unterschiedliche Wege angefordert werden. Möglich ist die Registrierung über eine Webseite (intern: `https://{SUBCA-Server}.{AMAZONE-DOMAIN}.com/certsrv`), die Registrierung über die Internetdienste-Manager Konsole oder die Registrierung über die Zertifikatskonsole. Es folgt ein Beispiel für die Anforderung eines Webserverzertifikates mittels der Zertifikatskonsole:

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

Die Zertifikatskonsole wird über MMC gestartet. Dort wird dann das Snap-In „Zertifikate“ hinzugefügt. Dieses kann für Benutzer oder Computer hinzugefügt werden. Da ein Webserverzertifikat für einen Computer beantragt werden soll, wird „Zertifikatskonsole für Computer“ ausgewählt. Dort kann jetzt unter „Eigene Zertifikate“ ein Zertifikat angefordert werden.

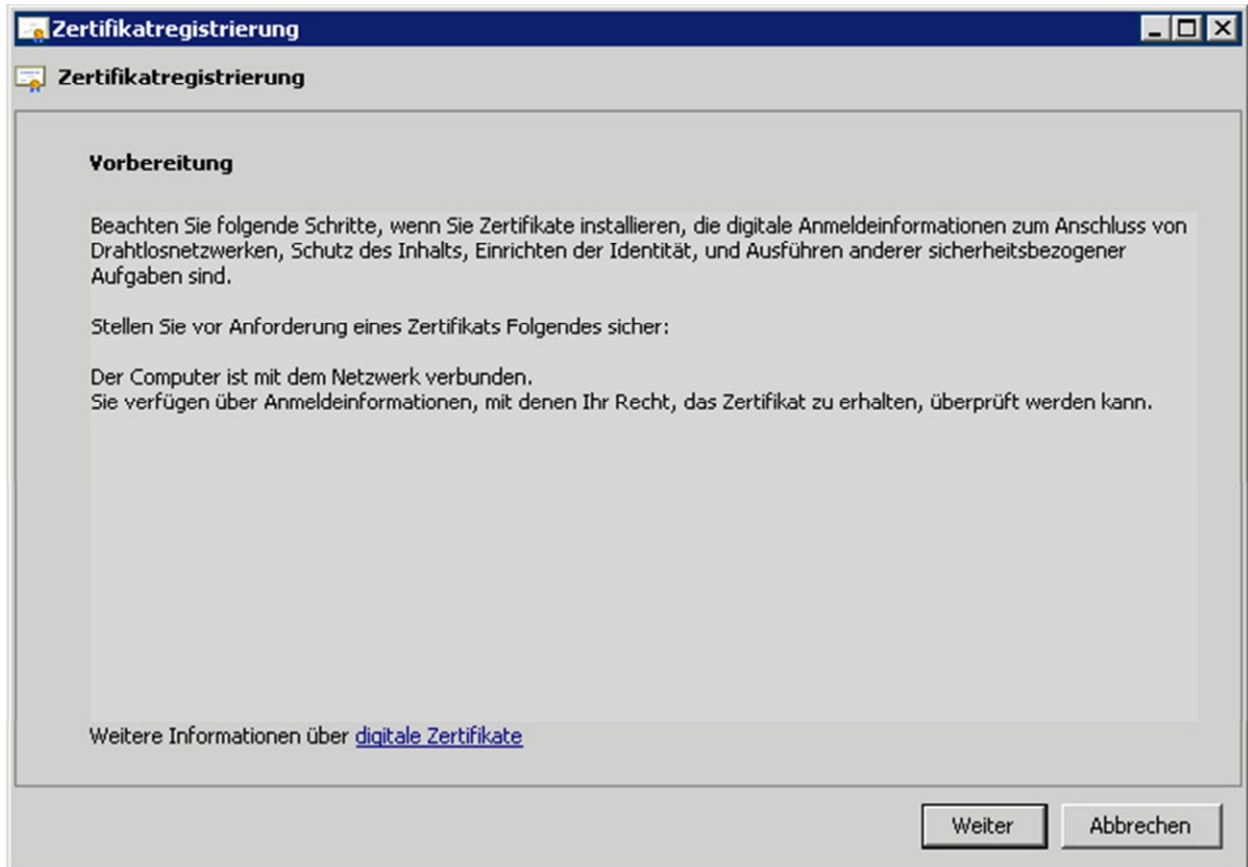


Abbildung 11: Zertifikatsanforderung des Webservers über die Zertifizierungskonsole



Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt  
auf externen Zugriff auf Domänen-Exchange Postfach

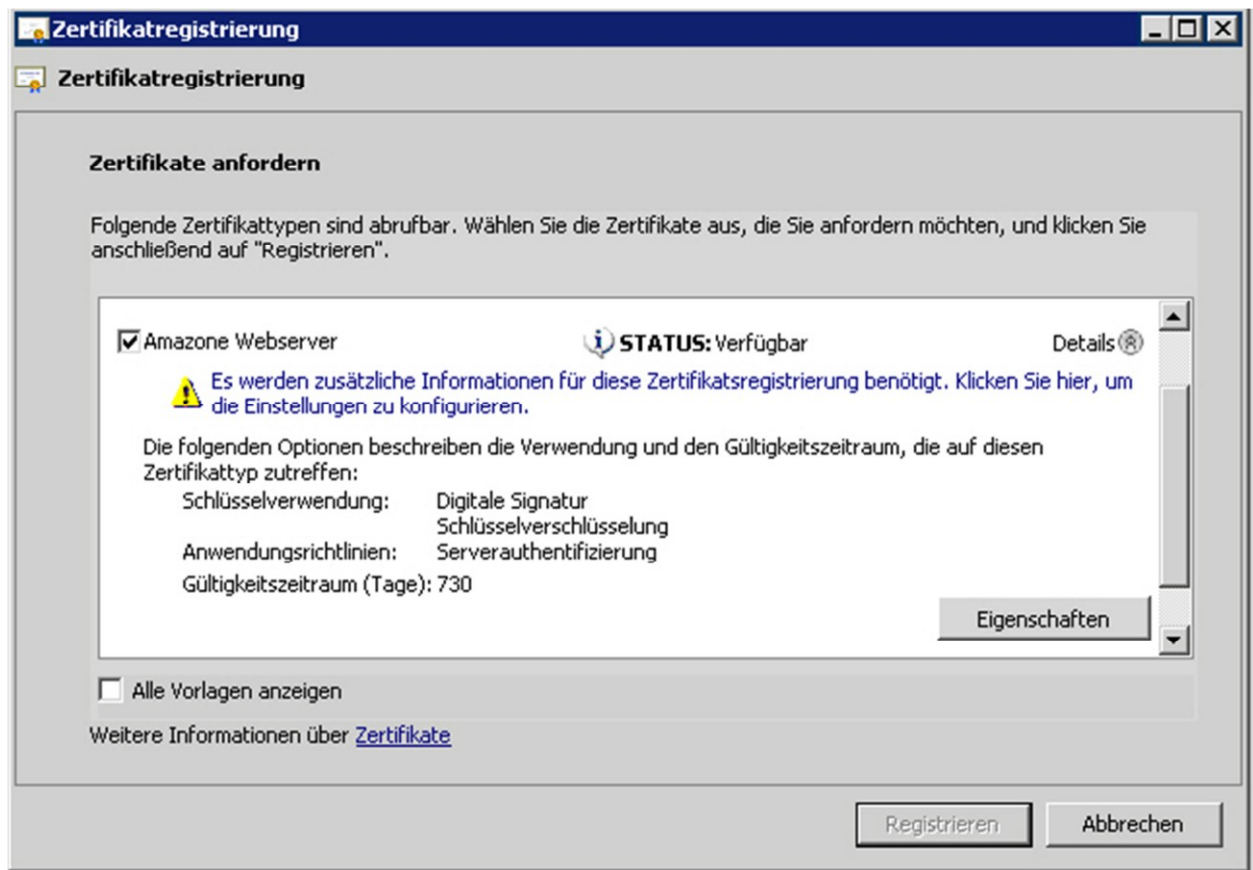


Abbildung 12: Angefordertes Amazon Webserver Zertifikat

Über den Punkt „Eigenschaften“ ist die Möglichkeit gegeben zusätzliche Informationen für den Webserver anzugeben (bspw. wird dazu der FQDN des Servers ausgewählt, der das Zertifikat beantragt).

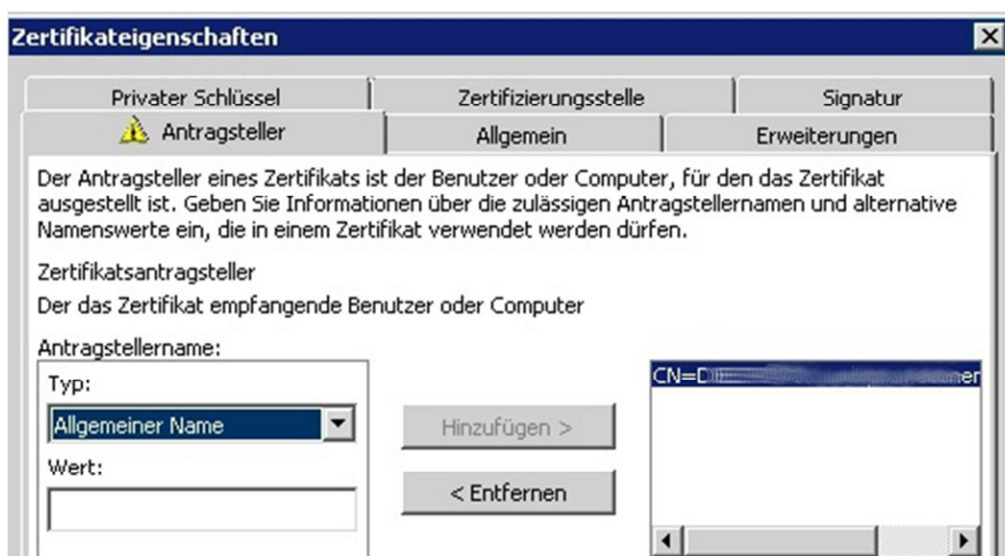


Abbildung 13: Eigenschaften/Antragstellers des Webserver Zertifikats

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

## **8. Abschluss**

### **8.1 Test der Funktionalität**

Auf einem externen Client eines Amazone-Mitarbeiters, der nicht im Amazone-Netzwerk ist, wird der Internet-Explorer geöffnet. Man kann Outlook RPC over HTTP über folgende Adressen erreichen:

<https://{AMAZONE-URL}/amazone> oder <https://{AMAZONE-IP-extern}/amazone>

Darauf folgt ein Sicherheitshinweis. Dieser wird mit „Ja“ bestätigt. Anschließend ist es dem Mitarbeiter möglich, wie gewohnt auf sein Postfach zuzugreifen.

### **8.2 Soll- / Ist- Vergleich**

Genau wie vor der Umstellung besitzt die Amazone-Gruppe eine zweistufige PKI-Infrastruktur. Die neue PKI läuft nach Projektabschluss auf Basis von W2K8 R2 und erfüllt alle Anforderungen in Hinsicht auf zukünftige Sicherheitsprojekte. Die RootCA und SubCA befindet sich weiterhin im Stammwerk Gaste. Die Standorte Hude und Leipzig werden folgen. Die für die Webserver, auf denen die Anbindung der Outlook RPC over HTTP Anbindung läuft, ausgestellten Zertifikate, deren Ablaufdatum auf den 31.12.2011 datiert sind, wurden durch die neu ausgestellten Zertifikate (Webserverzertifikatslaufzeit = 2 Jahre) ersetzt.

### **8.3 Fazit**

Durch die Einrichtung der neuen Amazone-PKI ist es der Amazone-Gruppe möglich verstärkt Sicherheitsrichtlinien für Ihr internes Netzwerk durchzusetzen. Zusätzlich kann auf neu hinzukommende Anforderungen hinsichtlich Zertifikatsauthentifizierungen, für den Zugriff aufs WLAN (802.1X), schnell und effizient reagiert werden. Nach Abschluss des Projektes wird die alte Amazone-PKI abgeschaltet.

## **Inhaltsverzeichnis Anhang**

<u>A. Auszüge der Angebote</u> .....	i
<u>A.1. Dell / Serverhardware</u> .....	i
<u>A.2. SoftwareONE / Windows Server 2008 R2 Lizenzen</u> .....	ii
<u>A.3. Angebot Zertifikate</u> .....	iii
<u>A.4. Controlware / Dienstleistung:</u> .....	iv
<u>B. Auszüge der Dateien</u> .....	v
<u>B.1. Namenskonvention</u> .....	v
<u>B.2. Installation der Root-CA</u> .....	v
<u>B.3. Vorbereitung der Installation</u> .....	vi
<u>B.3.1. Inhalt CAPolicy.inf</u> .....	vi
<u>B.4. Nachinstallationskonfiguration</u> .....	vi
<u>B.4.1. Parameter-Script Root-CA</u> .....	vi
<u>B.5. Installation der Sub-CA DE1</u> .....	vii
<u>B.6. Vorbereitung der Installation</u> .....	vii
<u>B.6.1. Inhalt CAPolicy.inf</u> .....	vii
<u>B.7. Nachinstallationskonfiguration</u> .....	viii
<u>B.7.1. Parameter-Script Sub-CA</u> .....	viii
<u>C. Administrationshandbuch</u> .....	ix
<u>C.1. Gültigkeitsdauer der Zertifikate</u> .....	ix
<u>C.2. Verlängerung/Erneuerung der Zertifizierungsstellenzertifikate</u> .....	ix
<u>C.3. Gültigkeit der Zertifikatssperrlisten</u> .....	ix
<u>C.4. Verlängerung des Zertifizierungsstellenzertifikates</u> .....	ix
<u>C.5. Sicherung einer Zertifizierungsstelle</u> .....	x
<u>C.7. Wiederherstellung einer Zertifizierungsstelle</u> .....	xiii
<u>C.8. Sperren eines Zertifikates</u> .....	xiv
<u>C.9. Manuelles veröffentlichen der Zertifikatssperrliste</u> .....	xv
<u>C.10. Exportieren eines Zertifikates aus der Zertifikatskonsole</u> .....	xv
<u>C.11. Importieren eines Zertifikates aus der Zertifikatskonsole</u> .....	xvii
<u>D. Kundenhandbuch</u> .....	xviii
<u>E. Glossar</u> .....	xix
<u>F. Quellenverzeichnis</u> .....	xx
<u>G. Literaturverzeichnis</u> .....	xx

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt  
auf externen Zugriff auf Domänen-Exchange Postfach

**A. Auszüge der Angebote**

**A.1. Dell / Serverhardware**

Angebot		Amazonen-Werke H. Dreyer GmbH & Co. KG			
Angebots Nr:	Kunde Nr:	Datum:	Ansprechpartner:		
24810181		14.03.2011			
				Telefon: 06997923941	
				Fax: 069256233941	
Kunde:		Gültigkeit des Angebots:			
Amazonen-Werke H. Dreyer GmbH & Co. KG		14 Tage			
Adresse:		Vorr. Lieferdatum:			
Heinrich Dreyer Straße		11.04.2011			
27798 Hude		Zahlungsbedingungen:			
Germany		30 Tage netto			
<hr/>					
Sehr geehrte/r 					
vielen Dank für Ihre Anfrage und das Interesse an unseren Produkten und Dienstleistungen. Nachfolgend unterbreiten wir Ihnen unser Angebot, welches wir speziell auf die von Ihnen beschriebenen Anforderungen hin erstellt und abgestimmt haben.					
Für Rückfragen stehe ich Ihnen jederzeit gerne telefonisch unter 06997923941 bzw. per E-Mail Aliaksei_Tsarou@Dell.com zur Verfügung.					
Mit freundlichen Grüßen					
					
Dell Angebot 24810181 - Amazonen-Werke H. Dreyer					
Ansprechpartner:  (Telefon 06997923941)					
<hr/>					
<b>1 Preisübersicht</b>					
Beschreibung:	Menge:	Einzelpreis:	Preis:		
PowerEdge T610 Tower Gehäuse für bis zu 8x 3,5Zoll Festplatten und Intel 55xx/56xx Prozessoren	1	EUR 5.315,00	EUR 5.315,00		
<b>Zwischensumme</b>			<b>EUR 5.315,00</b>		
19% MWSt (EUR 5.315,00)			EUR 1.009,85		
<b>Gesamt</b>			<b>EUR 6.324,85</b>		
<hr/>					
<b>Auftrag Informationen</b>					
Rechnungsadresse:			Lieferadresse:		
Amazonen-Werke H. Dreyer GmbH & Co. KG			Amazonen-Werke H. Dreyer GmbH & Co. KG		
Heinrich Dreyer Straße			Heinrich Dreyer Straße		
27798 Hude			27798 Hude		
Germany			Germany		

## Amazonen Werke H. Dreyer GmbH & Co. KG

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt  
auf externen Zugriff auf Domänen-Exchange Postfach

### A.2. SoftwareONE / Windows Server 2008 R2 Lizenzen



SoftwareONE Deutschland GmbH, Bismarckstrasse 67, D-74074 Heilbronn

Amazonen-Werke H. Dreyer GmbH & Co KG  
Heinrich-Dreyer-Straße  
27798 Hude (Oldenburg)

Datum: 07.01.2010  
Kundennr.: DE-SCU-100521  
UmSt ID: DE257433435  
Account Manager: [Name]  
Ihre Kontaktperson: [Name]  
E-Mail: [Email]  
Telefonnr. direkt: [Phone]  
Debitor ID Nr.: DE117583895

#### Angebot DE-QUO-102129

##### Rechnungsadresse

Amazonen-Werke H. Dreyer GmbH & Co KG  
Heinrich-Dreyer-Straße  
27798 Hude (Oldenburg)

##### Lieferadresse

Amazonen-Werke H. Dreyer GmbH & Co KG  
Heinrich-Dreyer-Straße  
27798 Hude (Oldenburg)

##### Lizenz Adresse

Amazonen-Werke H. Dreyer GmbH & Co KG  
Heinrich-Dreyer-Straße  
27798 Hude (Oldenburg)



Pos. Nr.	Beschreibung	Hersteller	Liz.Mod	Rab.-Stufe	Format	Version	Sprache	Menge	VK-Preis	MWST %	Betrag (EUR)
10	<p>Mit SA, da aufgrund der MUI Option Win Enterprise benötigt wird. Die MUI Option bekommen Sie nur über Windows Enterprise.</p>										
20	SL										
30	P72-04219	Windows Server Enterprise License					SL				
	Microsoft	OPEN	NON	LIC	2008 R2	Windows		1	2.376,37	19	2.376,37
Total EUR ohne UmSt											
19% MWST											
Total EUR inkl. UmSt											

Berücksichtigte Verträge

Microsoft Open License // Amazonen Werke H. Dreyer GmbH & Co KG

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt  
auf externen Zugriff auf Domänen-Exchange Postfach

**A.3. Angebot Zertifikate**

<input checked="" type="radio"/> <b>SSL Web Server Certificate with EV</b> Standardverschlüsselung Höchste Vertrauensstufe	 <ul style="list-style-type: none"><li>Grüne Adressleiste</li><li>Extended Validation</li><li>128-Bit- (Minimum) bis 256-Bit-SSL-Verschlüsselung</li></ul> <a href="#">Weitere Informationen</a>
<input type="radio"/> <b>SGC SuperCert</b> Bestmögliche Verschlüsselung Gängige Vertrauensstufe	 <ul style="list-style-type: none"><li>Vollständige Validierung der Organisation</li><li>128-Bit- (Minimum) bis 256-Bit-SSL-Verschlüsselung</li></ul> <a href="#">Weitere Informationen</a>
<input type="radio"/> <b>SSL Web Server Certificate</b> Standardverschlüsselung Gängige Vertrauensstufe	<ul style="list-style-type: none"><li>Vollständige Validierung der Organisation</li><li>128-Bit- (Minimum) bis 256-Bit-SSL-Verschlüsselung</li></ul> <a href="#">Weitere Informationen</a>
<input type="radio"/> <b>SSL 123 Certificate</b> Standardverschlüsselung Ausgestellt in Minuten	<ul style="list-style-type: none"><li>Domain-Validierung</li><li>128-Bit- (Minimum) bis 256-Bit-SSL-Verschlüsselung</li></ul> <a href="#">Weitere Informationen</a>

**Gültigkeitsdauer auswählen** ?

2 Jahre ▼

**Anzahl der Server-Lizenzen eingeben** ?

Geben Sie die Anzahl der Server ein, die mit diesem Zertifikat gesichert werden sollen:

**Gesamt: 659 EUR**

**SSL Web Server Certificate with EV**  
Gültigkeitsdauer: 2 Jahre  
Anzahl der Serverlizenzen: 1  
Anzahl der Subject Alternative Names: 0

**Verfügen Sie bereits über Anmeldeinformationen für das Certificate Center?**

\* Benutzername

\* Passwort

**Anmelden**

[Haben Sie Ihren Benutzernamen vergessen?](#)

[Haben Sie Ihr Passwort vergessen?](#)

Falls Sie kein Certificate Center-Konto besitzen, klicken Sie unten auf der Seite auf „Weiter“, um fortzufahren und später ein Konto zu erstellen.



## Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

### A.4. Controlware / Dienstleistung:

Angebot Nr. AN1006110

Zuständig  
Telefon



Seite 3

Dieses Angebot wurde erstellt für:  
Amazonen Werke H. Dreyer GmbH & Co. KG - 27798 Hude

#### Angebotsdetails

Pos	Bezeichnung	Menge	Preis/Stück	Wert
10		1,00		980,00 EUR
20	Dienstleistungstage Einführung in die PKI-Technologie	1,00	980,00	optional EUR
30	Dienstleistungstage Workshop Konzeptionierung einer neuen PKI	1,00	980,00	980,00 EUR
40	Dienstleistungstage Erstellung eines PKI- bzw. Cryptokonzepts	1,00	980,00	980,00 EUR
50	Dienstleistungstage Aufbau der PKI	1,00	980,00	980,00 EUR
60	Anfahrtpauschale je Anfahrt zusätzlich angefallene Dienstleistung wird nach tatsächlich erbrachtem Aufwand zu dem hier ausgewiesenen Tagessatz abgerechnet	1,00	150,00	150,00 EUR
Steuersätze		Warenwert ohne Steuer	Betrag MwSt.	Brutto
19,00		4.070,00	773,30	4.843,30 EUR
		4.070,00	773,30	4.843,30 EUR

Dieses Angebot ist gültig bis:

Zahlungsbedingungen Netto - 10 Tage

Gewährleistung: 12 Monate

Lieferzeit: 4-6 Wochen

Alle Preise verstehen sich ausschließlich Verpackung und gesetzlicher Mehrwertsteuer.

Sitz Dietzenbach, Registergericht Offenbach a. M.  
HRB-Nr. 6431, USt-IdNr. DE 113 539 225  
Steuernummer 3523035235  
WEEE Reg.-Nr. DE 90262751  
Geschäftsführung: Helmut E. Wörner (Vorsitzender),  
Hubert Potthoff, Bernd Schwefing

Firmenzentrale  
Controlware GmbH  
Waldstraße 92  
63128 Dietzenbach  
Deutschland

Telefon +49 6074 858-0  
Telefax +49 6074 858-108  
E-Mail [info@controlware.de](mailto:info@controlware.de)  
[www.controlware.de](http://www.controlware.de)  
Es gelten die AGB's der Controlware GmbH  
AGB <http://www.controlware.de/sonstiges/agb>

Controlware GmbH GS-Hamburg  
Esplanade 6  
20354 Hamburg

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

## **B. Auszüge der Dateien**

### **B.1. Namenskonvention**

Die Attribute der Zertifikate der einzelnen CA-Systeme werden wie folgt genutzt:

#### **Root-CA**

*CN = Amazone Root Certification Authority*

*O = AMAZONEN-Werke H. Dreyer GmbH und Co. KG*

*L = Hasbergen-Gaste*

*S = Niedersachsen*

*C = DE*

#### **Sub-CA DE1**

*CN = Amazone DE1 Internal Certification Authority*

*O = AMAZONEN-Werke H. Dreyer GmbH und Co. KG*

*L = Hasbergen-Gaste*

*S = Niedersachsen*

*C = DE*

### **B.2. Installation der Root-CA**

Für die Stammzertifizierungsstelle sind folgende Parameter festgelegt worden:

Computername:	= {ROOTCA-Server}
IP-Adresse:	= {AMAZONE-IP-intern}
Schlüssellänge des Root-Zertifikats:	= 4096
Gültigkeitsdauer des Root-Zertifikats:	= 11 Jahre
Veröffentlichungszeitraum der Zertifikatsperrliste:	= 26 Wochen
Veröffentlichungszeitraum der Deltasperrliste:	= keine Deltasperrliste
Veröffentlichungspunkt der Zertifikatsperrliste:	= <a href="http://root-ca.amazonen-werke.com/certenroll">http://root-ca.amazonen-werke.com/certenroll</a>
Veröffentlichungspunkt des Root-Zertifikats:	= <a href="http://root-ca.amazonen-werke.com/certenroll">http://root-ca.amazonen-werke.com/certenroll</a>
Gültigkeitsdauer der auszustellenden Zertifikate:	= 2 Jahre



Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt  
auf externen Zugriff auf Domänen-Exchange Postfach

### **B.3. Vorbereitung der Installation**

#### **B.3.1. Inhalt CAPolicy.inf**

*[Version]*

*Signature="\$Windows NT\$"*

*[certsrv\_server]*

*Renewalkeylength=4096*

*RenewalValidityPeriodUnits=11*

*RenewalValidityPeriod=years*

*CRLPeriod=weeks*

*CRLPeriodUnits=26*

*CRLDeltaPeriodUnits=0*

*CRLDeltaPeriod=days*

*[PolicyStatementExtension]*

*Policies=Amazone*

*[Amazone]*

*OID={AMAZONE-OID}*

*NOTICE=Amazonen Werke Ausstellererklärung*

*URL=http://www.cps.amazonen-werke.com/cps/CPStatement.pdf*

*[CRLDistributionPoint]*

*Empty=True*

*[AuthorityInformationAccess]*

*Empty=True*

### **B.4. Nachinstallationskonfiguration**

#### **B.4.1. Parameter-Script Root-CA**

*::Declare Configuration NC*

*certutil -setreg CA\DSConfigDN*

*CN=Configuration,DC={AMAZONE},DC={DOMAIN},DC=com*

*::Define CRL Publication Intervals*

*certutil -setreg CA\CRLPeriodUnits 26*

*certutil -setreg CA\CRLPeriod "weeks"*

*certutil -setreg CA\CRLDeltaPeriodUnits 0*

*certutil -setreg CA\CRLDeltaPeriod "Hours"*

*::Apply the required CDP Extension URLs*

*certutil -setreg CA\CRLPublicationURLs*

*"65:%windir%\system32\CertSrv\CertEnroll\%%3%%8%%9.cr\n6:http://root-ca.amazonen-werke.com/certenroll/%%3%%8%%9.cr\n6:http://www.cps.amazonen-werke.com/cps/crlde0/%%3%%8%%9.cr"*

*::Apply the required AIA Extension URLs*

*certutil -setreg CA\CACertPublicationURLs*

*"1:%windir%\system32\CertSrv\CertEnroll\%%3%%4.crt\n2:http://root-ca.amazonen-*

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt  
auf externen Zugriff auf Domänen-Exchange Postfach

*werke.com/certenroll/%%3%%4.crt\n2:http://www.cps.amazonen-  
werke.com/cps/aiade0/%%3%%4.crt"*

*::Enable all auditing events for the Amazone-Root-CA  
certutil -setreg CA\AuditFilter 127*

*::Set Validity Period for Issued Certificates  
certutil -setreg CA\ValidityPeriodUnits 5  
certutil -setreg CA\ValidityPeriod "Years"*

*::Restart Certificate Services  
net stop certsvc & net start certsvc*

### **B.5. Installation der Sub-CA DE1**

Für die Sub-CA sind folgende Parameter festgelegt worden:

Computername:	= {SUBCA-Server}
IP-Adresse:	= {AMAZONE-IP-intern}
Schlüssellänge des Root-Zertifikats:	= 4096
Gültigkeitsdauer des Root-Zertifikats:	= 05 Jahre
Veröffentlichungszeitraum der Zertifikatsperrliste:	= 7 Tage
Veröffentlichungszeitraum der Deltasperrliste:	= 1 Tag
Veröffentlichungspunkt der Zertifikatsperrliste:	=http://sub-ca-de1.amazonen- werke.com/certenroll
Veröffentlichungspunkt des Root-Zertifikats:	=http://sub-ca-de1.amazonen- werke.com/certenroll
Gültigkeitsdauer der auszustellenden Zertifikate:	= 2 Jahre

### **B.6. Vorbereitung der Installation**

#### **B.6.1. Inhalt CAPolicy.inf**

*[Version]  
Signature="\$Windows NT\$"  
[certsrv\_server]  
renewalkeylength=4096  
RenewalValidityPeriodUnits=5  
RenewalValidityPeriod=years  
CRLPeriod=days  
CRLPeriodUnits=7  
CRLDeltaPeriodUnits=1  
CRLDeltaPeriod=days*

*[PolicyStatementExtension]  
Policies=Amazone*

*[Amazone]  
OID={AMAZONE-OID}  
NOTICE=Amazonen Werke Ausstellererklärung  
URL=http://www.cps.amazonen-werke.com/cps/CPStatement.pdf*

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt  
auf externen Zugriff auf Domänen-Exchange Postfach

## **B.7. Nachinstallationskonfiguration**

### **B.7.1. Parameter-Script Sub-CA**

*::Declare Configuration NC*

*certutil -setreg CA\DSConfigDN*

*CN=Configuration,DC={AMAZONE},DC={DOMAIN},DC=com*

*::Define CRL Publication Intervals*

*certutil -setreg CA\CRLPeriodUnits 7*

*certutil -setreg CA\CRLPeriod "days"*

*certutil -setreg CA\CRLDeltaPeriodUnits 1*

*certutil -setreg CA\CRLDeltaPeriod "Days"*

*::Apply the required CDP Extension URLs*

*certutil -setreg CA\CRLPublicationURLs*

*"65:%windir%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n6:http://subde1-  
ca.amazonen-werke.com/certenroll/%%3%%8%%9.crl\n6:http://www.cps.amazonen-  
werke.com/cps/crlde1/%%3%%8%%9.crl"*

*::Apply the required AIA Extension URLs*

*certutil -setreg CA\CACertPublicationURLs*

*"1:%windir%\system32\CertSrv\CertEnroll\%%3%%4.crl\n2:http://subde1-  
ca.amazonen-werke.com/certenroll/%%3%%4.crl\n2:http://www.cps.amazonen-  
werke.com/cps/aiade1/%%3%%4.crl"*

*::Enable all auditing events for the Amazone-Sub-CA DE1*

*certutil -setreg CA\AuditFilter 127*

*::Set Validity Period for Issued Certificates*

*certutil -setreg CA\ValidityPeriodUnits 2*

*certutil -setreg CA\ValidityPeriod "Years"*

*::Restart Certificate Services*

*net stop certsvc & net start certsvc*

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

## **C. Administrationshandbuch**

### **C.1. Gültigkeitsdauer der Zertifikate**

Für die Zertifikate, die von der Amazone-PKI ausgestellt werden, sind folgende Gültigkeitsdauern festgelegt:

- |  |          |
|--|----------|
| • Amazone - Root CA:                                     | 11 Jahre |
| • Amazone - Sub CA (gilt für alle drei):                 | 05 Jahre |
| • Längste Gültigkeitsdauer für ausgestellte Zertifikate: | 02 Jahre |

### **C.2. Verlängerung/Erneuerung der Zertifizierungsstellenzertifikate**

Die Gültigkeitsdauern der Zertifikate sind so gewählt und aufeinander abgestimmt, dass alle drei Jahre ein Erneuerungsprozess für mindestens eine der Zertifizierungsstellen durchgeführt werden muss. Hierbei ist besonders darauf geachtet worden, dass die Verlängerungstermine sich regelmäßig wiederholen. Hier müssen

- |   |              |
|---|--------------|
| • die Maschinenzertifikate:                         | alle 2 Jahre |
| • das Zertifikat der Issuing CAs:                   | alle 3 Jahre |
| • das Zertifikat der Zwischenzertifizierungsstelle: | alle 6 Jahre |

verlängert werden.

### **C.3. Gültigkeit der Zertifikatssperrlisten**

Für die CRL werden folgende Gültigkeitszeiträume festgelegt:

- |                        |  |
|------------------------|--|
| • Root CA:             | 26 Wochen (es werden keine Deltasperrlisten verwendet) |
| • CRL Sub CA DE1-3:    | 7 Tage   |
| • DeltaCRL Sub-CA DE1: | 1 x Täglich  |

Für den Betrieb der PKI sind einige regelmäßige Tätigkeiten notwendig, die hier beschrieben werden.

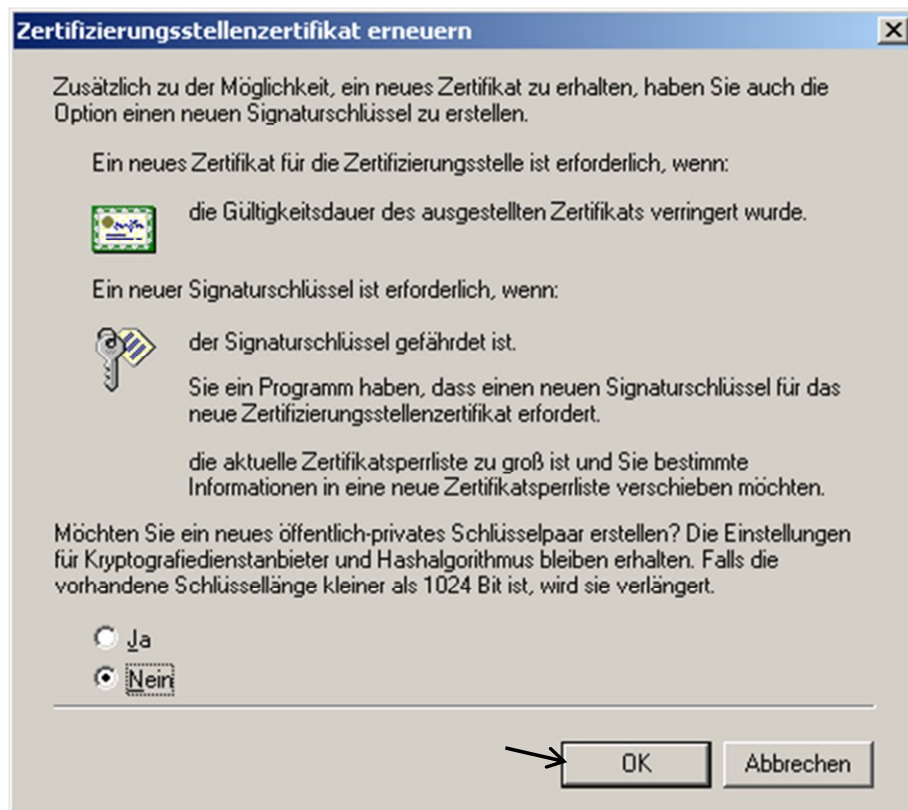
### **C.4. Verlängerung des Zertifizierungsstellenzertifikates**

Die Zertifizierungsstellenzertifikate müssen in regelmäßigen Abständen verlängert werden. Dies erfolgt über die Zertifizierungsstellenkonsole. Dort kann man im Kontextmenü der Zertifizierungsstelle ein neues Zertifikat anfordern.



Für eine Verlängerung müssen die Zertifikatsdienste beendet werden.

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach



HINWEIS:

Das neue Zertifikat sollte immer mit dem gleichen Schlüssel erstellt werden. **(Nein)**

### **C.5. Sicherung einer Zertifizierungsstelle**

Die Sicherung kann entweder über

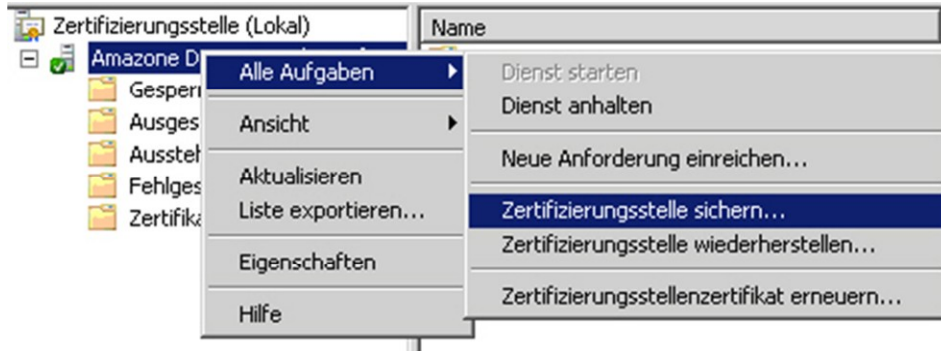
- eine manuelle Sicherung in der Zertifizierungsstellen-Konsole (Kontextmenü: Zertifizierungsstelle sichern)
- mittels des Werkzeuges  
„certutil –privatkey –backup p:\ath\to\empty\backup\directory“
- über einen Backup-Agenten zur Integration in die vorhandene Backup-Lösung
- 

geschehen.

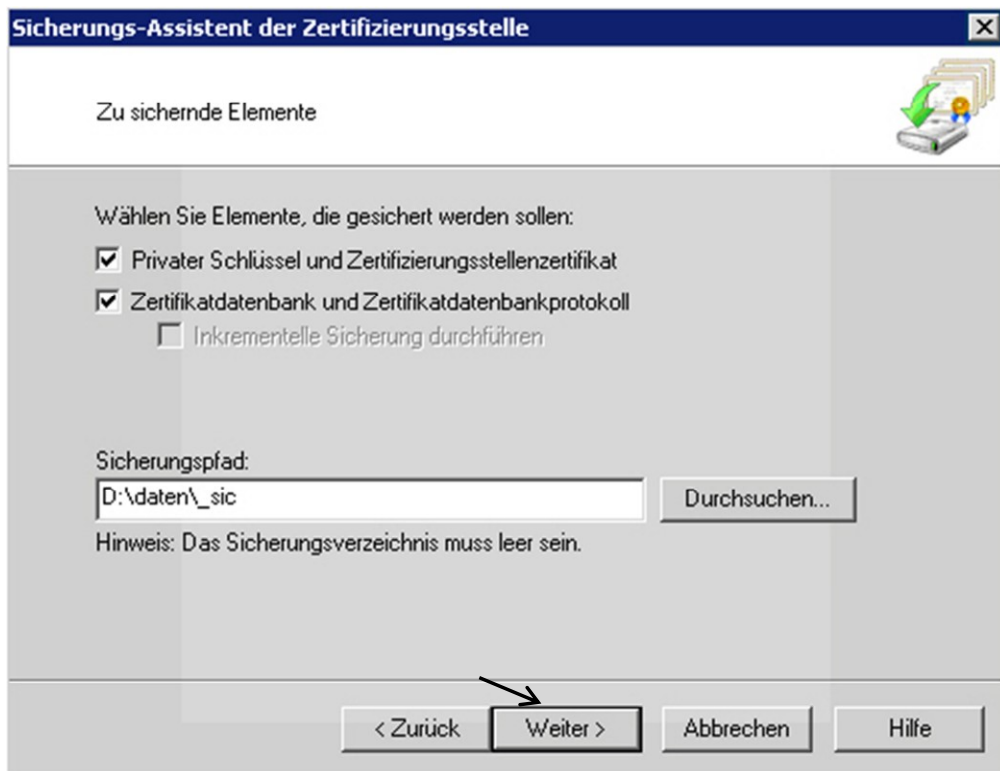
Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

### Beispiel Manuelle Sicherung:

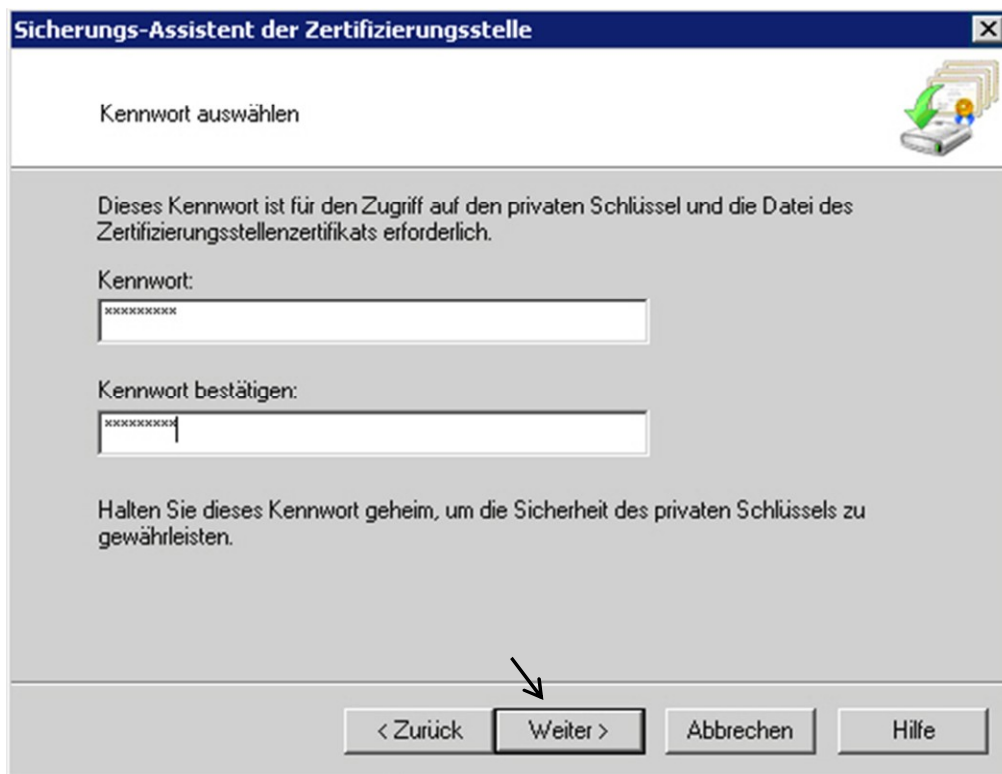
Aus dem Kontextmenü der Zertifizierungsstelle den Punkt „Zertifizierungsstelle sichern“ auswählen



Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt  
auf externen Zugriff auf Domänen-Exchange Postfach



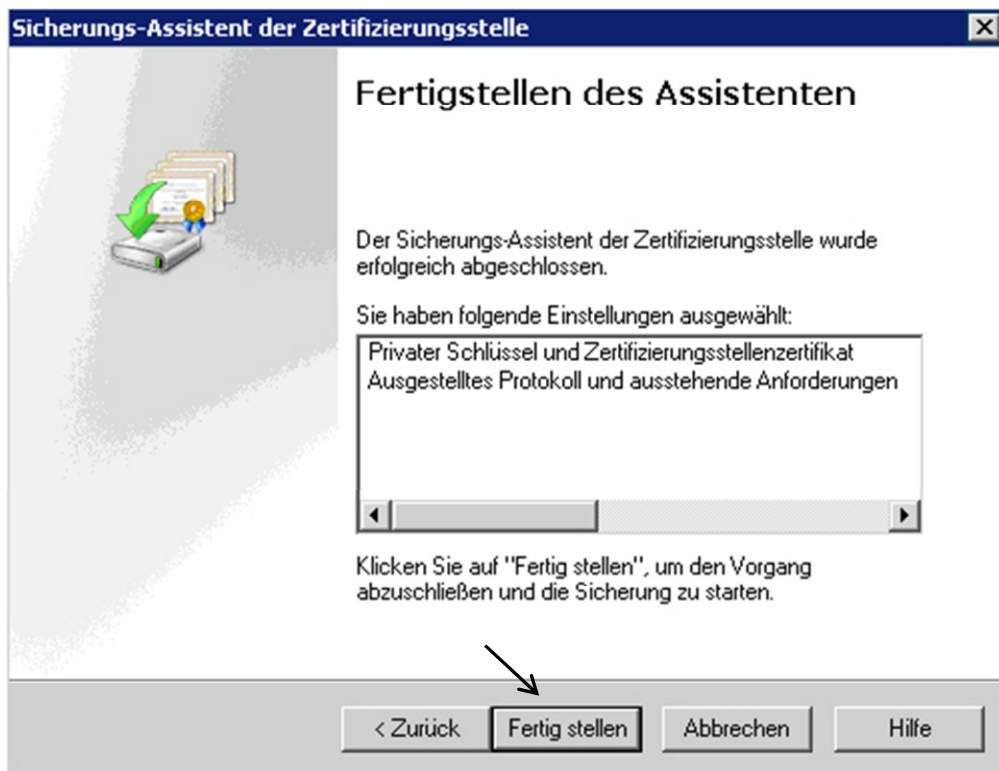
Sicherungspfad angeben!



Weiter



Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach



Fertig stellen

### **C.7. Wiederherstellung einer Zertifizierungsstelle**

Die Rücksicherung einer Zertifizierungsstelle kann je nach Sicherungsverfahren wie folgt durchgeführt werden.

1. Bereitstellung eines Windows 2008 R2 Servers Enterprise Edition mit gleichem Patch-/Servicepack-Level wie zum Zeitpunkt der Erstellung der Sicherung
  - a. Benennung des Servers wie zum Zeitpunkt der Sicherung
  - b. Der Server als AD-integrierte CA darf **nicht** in die Domäne aufgenommen werden, wenn die Rücksicherung über den „Systemstate“ geschehen soll!
2. Kopieren der dem Server zugeordneten CAPolicy.inf in das Verzeichnis C:\Windows
3. Installation der Zertifikatsdienste über das Software-Applet der Systemsteuerung
4. Ausführen des Post-Install-Skriptes
5. Wiederherstellung der Zertifikatsdatenbank und der privaten Schlüssel entweder über
  - a. das Kontextmenü der Zertifizierungsstellen-Konsole
  - b. das Werkzeug „certutil –privatekey -recover p:\ath\to\empty\backup\directory “
  - c. Rückspielen des “Systemstate”.

Nach einem Neustart des Systems ist zu prüfen, ob alle Dienste, insbesondere die Zertifikatsdienste, ohne kritische Fehlermeldungen starten.



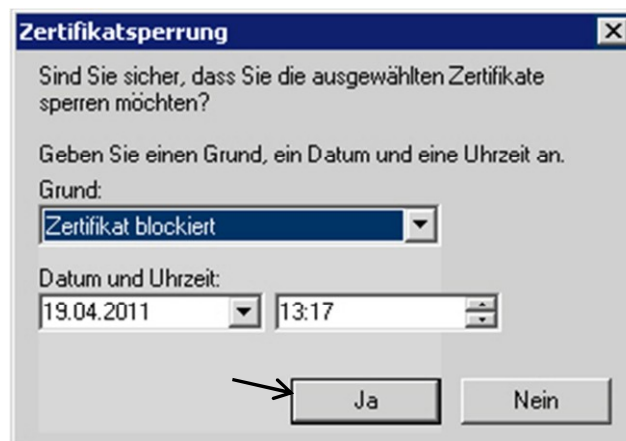
Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

### **C.8. Sperren eines Zertifikates**

Die von der Sub-CA ausgestellten Zertifikate werden in der Zertifizierungsstellenkonsole aufgelistet. Um ein Zertifikat zu sperren, muss man das betreffende Zertifikat aus der Liste ermitteln. Wenn man dann mit der rechten Maustaste auf das Zertifikat klickt, kann man über das Menü „Alle Aufgaben“ den Menüpunkt „Zertifikat sperren“ auswählen.



Nach der Auswahl „Zertifikat sperren“ wird man nach dem Grund für die Sperrung gefragt.



Es wird empfohlen, die Zertifikate ohne Angabe von Gründen zu sperren, da man diese Informationen in der Sperrliste wiederfindet. Die einzige Ausnahme ist eine Blockierung des Zertifikates. Wenn ein Zertifikat mit der Begründung „Blockiert“ gesperrt wird, kann die Sperrung wieder aufgehoben werden. Das Zertifikat ist anschließend wieder gültig.

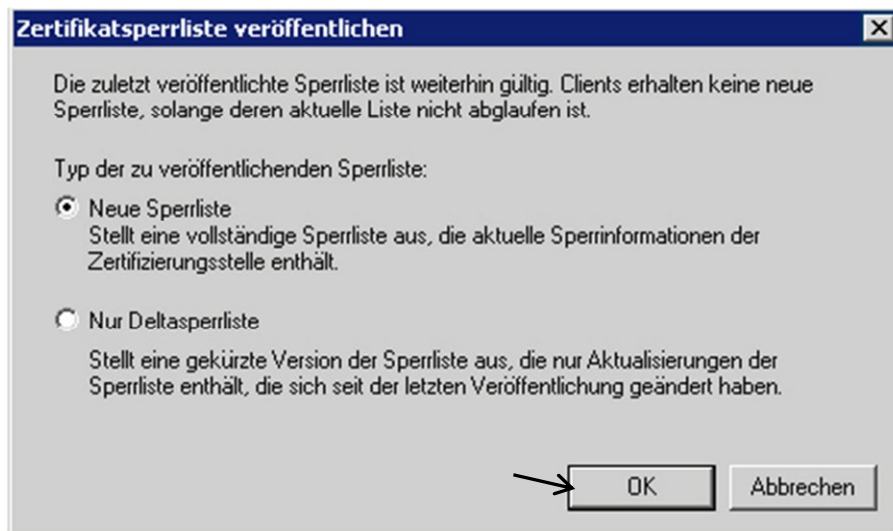
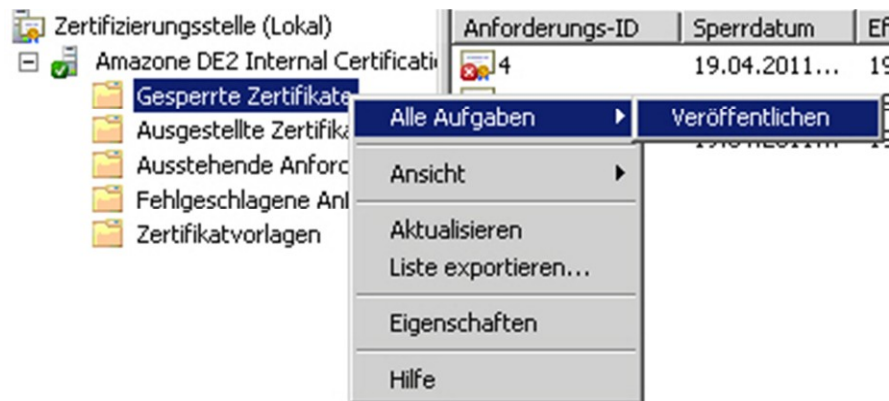


Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

Die gesperrten Zertifikate werden dadurch aus der Liste „Ausgestellte Zertifikate“ in die Liste „Gesperrte Zertifikate“ verschoben. Dort können dann auch alle Zertifikate, die mit der Begründung „Blockiert“ gesperrt wurden, wieder freigegeben werden.

### **C.9. Manuelles veröffentlichen der Zertifikatssperrliste**

Wenn ein Zertifikat auf der Sub-CA gesperrt wurde, muss die Sperrliste aktualisiert / neu veröffentlicht werden. Das gleiche gilt für die Sperrliste der Root CA. Diese ist ein Jahr gültig und muss dann neu erstellt werden. Das kann man in der Zertifizierungsstellenkonsole durchführen. Dazu wechselt man in den Bereich „Gesperrte Zertifikate“ und wählt den Punkt „Veröffentlichen“.



### **C.10. Exportieren eines Zertifikates aus der Zertifikatskonsole**

Zertifikate können über die Zertifikatskonsole exportiert werden. Dabei ist auch ein Export des privaten Schlüssels möglich, wenn die Zertifikatsvorlage dieses erlaubt. Um ein Zertifikat zu exportieren, wählt man das entsprechende Zertifikat aus und klickt im Kontextmenü auf „exportieren“. Beispiel ohne privaten Schlüssel:

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt  
auf externen Zugriff auf Domänen-Exchange Postfach

**Zertifikatexport-Assistent**

**Format der zu exportierenden Datei**  
Zertifikate können in verschiedenen Dateiformaten exportiert werden.

Wählen Sie das gewünschte Format:

- ☒ DER-codiert-binär X.509 (.CER)
- ☐ Base-64-codiert X.509 (.CER)
- ☐ Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
  - ☐ Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- ☐ Privater Informationsaustausch - PKCS #12 (.PFX)
  - ☐ Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
  - ☐ Privaten Schlüssel nach erfolgreichem Export löschen
  - ☐ Alle erweiterten Eigenschaften exportieren
- ☐ Microsoft Serieller Zertifikatspeicher (.SST)

Weitere Informationen über [Zertifikatdateiformate](#)

< Zurück Weiter > Abbrechen

**Zertifikatexport-Assistent**

**Privaten Schlüssel exportieren**  
Sie können den privaten Schlüssel mit dem Zertifikat exportieren.

Private Schlüssel sind kennwortgeschützt. Wenn Sie den privaten Schlüssel mit dem ausgewählten Zertifikat exportieren möchten, müssen Sie auf einer der folgenden Seiten ein Kennwort eingeben.

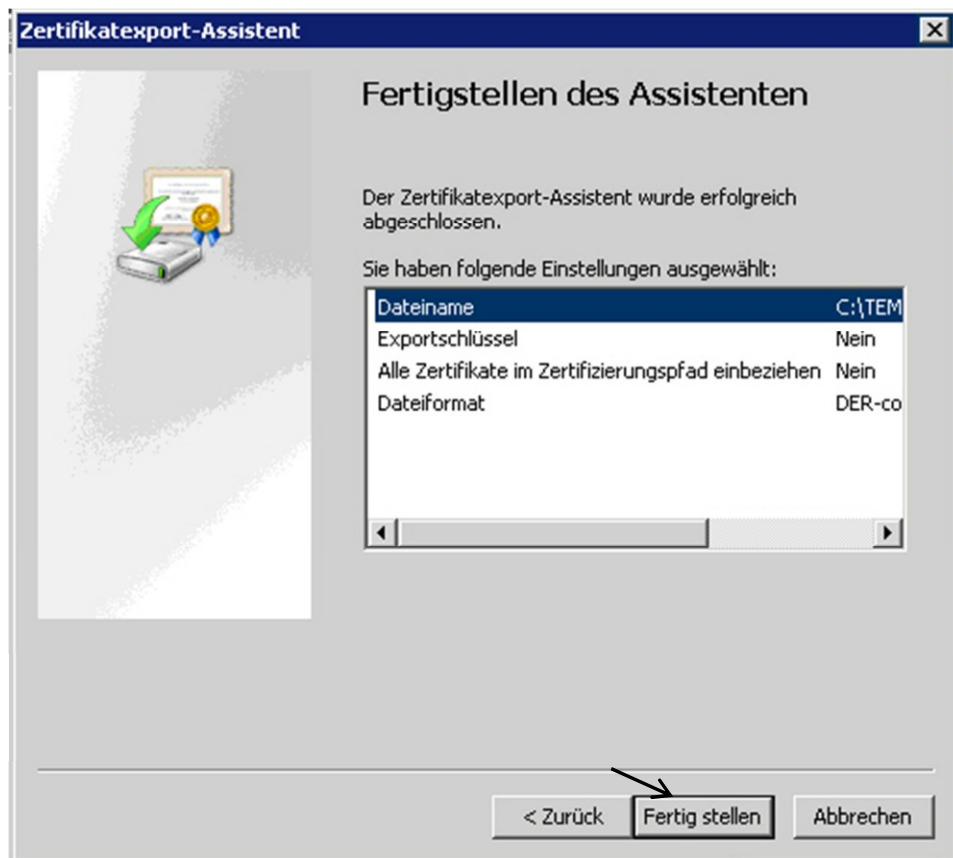
Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?

- ☐ Ja, privaten Schlüssel exportieren
- ☒ Nein, privaten Schlüssel nicht exportieren

Weitere Informationen über [das Exportieren privater Schlüssel](#)

< Zurück Weiter > Abbrechen

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach



### **C.11. Importieren eines Zertifikates aus der Zertifikatskonsole**

Zertifikate können über die Zertifikatskonsole importiert werden. Dabei ist auch ein Import des privaten Schlüssels möglich, wenn die Datei im PFX-Format vorliegt. Um ein Zertifikat zu importieren, wählt man den entsprechenden Zertifikatsspeicher aus und klickt im Kontextmenü auf „importieren“.

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

### D. Kundenhandbuch

Wie melde ich mich in Outlook Web Access an:

Von einem PC, der nicht im Amazone-Netzwerk ist, den Internet-Explorer öffnen; <https://{AMAZONE-URL}/amazone> oder <https://{AMAZONE-IP-extern}/amazone> eingeben. Darauf folgt ein Sicherheitshinweis. Dieser umschreibt, dass der angesprochene Webserver ein ungültiges Sicherheitszertifikat verwendet. Dem Zertifikat wird nicht vertraut, weil das Aussteller-Zertifikat nach außen nicht glaubwürdig ist. (Beispiel: Mozilla Firefox) Der Sicherheitshinweis kann allerdings nach manuellem Prüfen des Zertifikates bestätigt werden.



#### Dieser Verbindung wird nicht vertraut

Sie haben Firefox angewiesen, eine gesicherte Verbindung zu **dmzms.amazone.de** aufzubauen, es kann aber nicht überprüft werden, ob die Verbindung sicher ist.

Wenn Sie normalerweise eine gesicherte Verbindung aufbauen, weist sich die Website mit einer vertrauenswürdigen Identifikation aus, um zu garantieren, dass Sie die richtige Website besuchen. Die Identifikation dieser Website dagegen kann nicht bestätigt werden.

#### Was sollte ich tun?

Falls Sie für gewöhnlich keine Probleme mit dieser Website haben, könnte dieser Fehler bedeuten, dass jemand die Website fälscht. Sie sollten in dem Fall nicht fortfahren.

[Diese Seite verlassen](#)

#### ▼ Technische Details

dmzms.amazone.de verwendet ein ungültiges Sicherheitszertifikat.

Dem Zertifikat wird nicht vertraut, weil das Aussteller-Zertifikat unbekannt ist.

(Fehlercode: sec\_error\_unknown\_issuer)

#### ► Ich kenne das Risiko



Microsoft Office

# Outlook Web Access

Provided by Microsoft Exchange Server 2003

Domäne\Benutzername: {AMAZONE-DOMAIN}\User

Kennwort: .....

[Anmelden](#)

#### Sicherheit

- ☒ Öffentlicher oder gemeinsam genutzter Computer

Wählen Sie diese Option, falls dieser Computer von mehreren Personen verwendet wird.

- ☐ Privater Computer

Wählen Sie diese Option, falls dieser Computer nur von Ihnen verwendet wird.

**Achtung:** Mit der Auswahl dieser Option bestätigen Sie, dass dieser Computer die Sicherheitsrichtlinien Ihrer Organisation erfüllt.

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

## **E. Glossar**

### **CA (Certification Authority):**

autorisierte Zertifizierungsstelle die beglaubigte digitale Zertifikate herausgeben kann

### **Deltasperrlisten:**

Die Deltasperrlisten beinhalten nicht den ganzen Umfang der gesperrten Zertifikate, sondern nur aktuelle Änderungen.

### **DMZ (demilitarized zone):**

handelt es sich um einen geschützten Serververbund, der sich zwischen 2 abgeschotteten Netzwerken befindet

### **FQDN (fully qualified domain name):**

Vollständiger DNS-Name, bestehend aus Host-Namen und dem Domänen-Suffix

### **Issuing-CA:**

ausstellende Zertifizierungsstelle für Computer- und Benutzerzertifikate

### **Outlook RPC over HTTP:**

Aufruf von Outlook (2003) mittels RPC-Anbindung am internen Exchange Server über HTTP/s

### **RootCA:**

oberste Stammzertifizierungsstelle in einem Unternehmen, stellt Stammzertifikate für SubCA aus

### **SubCA:**

Zertifizierungsstelle hierarchisch unter der RootCA angesiedelt, stellt Zertifikate für Benutzer und Computer aus

### **Zertifikatsrequest (CSR, Certificate Signing request):**

Das Zertifikatsrequest ist ein kryptischer Text, der auf dem jeweiligen Server der den Antrag für das Zertifikat stellt, generiert wird. Dieser beinhaltet weitere Informationen wie Organisationsname, Standort, etc.

### **Zertifikatssperrliste (CRL):**

Sperrlisten beinhalten eine Auflistung aller zurückgezogener oder gesperrter Zertifikate/Schlüssel

Einrichtung einer zweistufigen PKI-Struktur auf 64bit Technologie mit Schwerpunkt auf externen Zugriff auf Domänen-Exchange Postfach

## **F. Quellenverzeichnis**

### **Planung einer PKI – Integration in die Firmenstruktur:**

[http://www.tecchannel.de/sicherheit/identity\\_access/402051/public\\_key\\_infrastrukturen/index7.html](http://www.tecchannel.de/sicherheit/identity_access/402051/public_key_infrastrukturen/index7.html)

### **Die Zertifikatsstelle in der eigenen Firma**

<http://www.msxfaq.de/signcrypt/firmenca.htm>

### **RPC over HTTP**

<http://www.msxfaq.de/clients/rpchttp.htm>

### **Konfigurieren eines Back-End-Servers**

[http://technet.microsoft.com/de-de/library/bb124951\(EXCHG.65\).aspx](http://technet.microsoft.com/de-de/library/bb124951(EXCHG.65).aspx)

### **Optimale Methoden zum Implementieren einer Infrastruktur mit öffentlichen Schlüssel (PKI) unter Windows Server 2003**

<http://www.microsoft.com/germany/technet/datenbank/articles/600683.mspx>

## **G. Literaturverzeichnis**

**Microsoft Press (2008), Brian Komar:** Windows Server 2008 PKI- und Zertifikat-Sicherheit – Entwerfen und Einführen von zertifikatsbasierenden Sicherheitslösungen für Ihr Netzwerk