

INSTITUT FÜR INFORMATIK
DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN



Bachelorarbeit

**Aufbau einer
Public Key Infrastruktur
bei der
M-net Telekommunikations GmbH**

Daniel Leimig



Bachelorarbeit

**Aufbau einer
Public Key Infrastruktur
bei der
M-net Telekommunikations GmbH**

Daniel Leimig

Aufgabensteller: Prof. Dr. Helmut Reiser
Betreuer: Dr. Michael Brenner
Marcel Breuer
Filipe Pinto Correia (M-net Telekommunikations GmbH)
Abgabetermin: 14. Februar 2018

Hiermit versichere ich, dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 14. Februar 2018

.....
(Unterschrift des Kandidaten)

Abstract

Um den sicheren und vertraulichen Austausch von Daten in einem Netzwerk zu erhöhen, gibt es verschiedene kryptografische Verfahren, wie z. B. eine Public-Key-Infrastruktur (PKI). Das ist ein Kryptosystem, welches zur Ausstellung, Verteilung und Prüfung von Zertifikaten genutzt wird, um eine sichere Kommunikation und Authentifizierung zu ermöglichen. Dabei stellt eine Zertifizierungsstelle jedem Client bzw. Server, der Mitglied des Netzwerkes ist, ein Zertifikat aus, welches zur Authentifizierung im Netzwerk dient. Will nun ein Client auf einen Server zugreifen, wird das Zertifikat des Clients an eine Validierungsstelle übermittelt, die überprüft, ob das Zertifikat authentisch und gültig ist. Nach einer positiven Rückmeldung erhält der Client Zugriff auf den Server. Aufbauend auf einer PKI lassen sich unter anderem E-Mail-Verschlüsselungen mit Secure/Multipurpose Internet Mail Extensions (S/MIME) und Virtual Private Network (VPN) Lösungen mit Authentifizierung umsetzen.

Das WLAN-Netzwerk der M-net Telekommunikations GmbH ist derzeit wegen seiner schwachen Authentifizierung als reiner Internetzugang eingerichtet. Durch die Implementierung einer PKI wird die WLAN-Sicherheit erhöht und somit der Weg zu einem mobilen Arbeitsplatz mit den gleichen Zugriffsrechten wie ein stationärer Arbeitsplatz ermöglicht.

In dieser Bachelorarbeit soll eine zweischichtige Zertifizierungsstellenhierarchie umgesetzt werden. Zum Schutz der kryptografischen Schlüssel der Zertifizierungsstellen und zur sicheren Ausführung der kryptographischen Operationen kommt in dieser Realisierung ein Hardwaresicherheitsmodul (HSM) zum Einsatz.

Inhaltsverzeichnis

| | |
|---|-----------|
| 1. Einleitung | 1 |
| 2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI) | 3 |
| 2.1. Verschlüsselung | 3 |
| 2.1.1. Symmetrische Verschlüsselung | 3 |
| 2.1.2. Asymmetrische Verschlüsselung | 3 |
| 2.1.3. Kombination asymmetrische und symmetrische Verschlüsselung | 5 |
| 2.1.4. Hash-Algorithmus | 5 |
| 2.1.5. Signatur-Algorithmus | 6 |
| 2.1.6. Signatur-Hash-Algorithmus | 6 |
| 2.1.7. Kryptografieanbieter | 7 |
| 2.2. Funktionsweise einer Public Key Infrastruktur (PKI) | 7 |
| 2.2.1. Zertifizierungsstelle (CA) | 11 |
| 2.2.1.1. Zertifikatvorlagen | 12 |
| 2.2.1.2. Sperrlisten | 15 |
| 2.2.1.3. Sperrlistenverteilungspunkte (CDP) | 18 |
| 2.2.1.4. Authority Information Access (AIA) | 19 |
| 2.2.1.5. Subject Alternative Names (SANs) | 19 |
| 2.2.1.6. Microsoft Internet Information Services (IIS) | 20 |
| 2.2.1.7. Online Certificate Status Protocol (OCSP) | 20 |
| 2.2.1.8. Sperrlisten Webserver | 21 |
| 2.2.1.9. Network Device Enrollment Service (NDES) | 21 |
| 2.2.1.10. Datenbank und Log Files | 23 |
| 2.2.2. Hardware-Sicherheitsmodul (HSM) | 23 |
| 2.2.3. Topologie einer Public Key Infrastruktur (PKI) | 25 |
| 2.2.3.1. Zertifikatkette | 27 |
| 2.2.3.2. Offline Zertifizierungsstellen | 28 |
| 2.2.3.3. CA Clustering | 30 |
| 2.2.4. Gültigkeitsdauer Zertifikate | 31 |
| 2.3. Zusammenfassung | 31 |
| 3. Konzept | 33 |
| 3.1. Anforderung M-net an die Public Key Infrastruktur (PKI) | 33 |
| 3.2. Konzeptdetails | 34 |
| 3.2.1. Pfadlänge | 34 |
| 3.2.2. Root CA | 35 |
| 3.2.3. Untergeordnete Zertifizierungsstellen | 35 |
| 3.2.4. Verwendung zweier Hardware-Sicherheitsmodule | 37 |
| 3.2.5. Berechtigungen | 38 |
| 3.2.6. Zertifikatdetails | 38 |

| | |
|---|-----------|
| 3.2.7. Sperrlisten | 39 |
| 3.2.8. Publikationspunkte | 39 |
| 3.2.9. Registrierungsmethoden | 40 |
| 3.2.10. Zertifikatvorlagen | 41 |
| 3.2.11. CA Clustering | 41 |
| 3.2.12. Wiederherstellbarkeit | 41 |
| 3.2.13. Verfügbarkeit | 41 |
| 3.3. Zusammenfassung | 42 |
| 4. Umsetzung | 43 |
| 4.1. Einrichtung Hardware-Sicherheitsmodul | 43 |
| 4.2. Anbindung der Zertifizierungsstelle an das Hardware-Sicherheitsmodul High Availability-Cluster | 44 |
| 4.2.1. Konfiguration SafeNet Luna Client 6.2.0-15 mit der Virtual Token Library und High Availability | 44 |
| 4.2.2. Key Storage Provider und Cryptographic Service Provider | 45 |
| 4.3. Zertifizierungsstellen | 45 |
| 4.3.1. Konfigurationsskripte für Windows Zertifizierungsstellen | 45 |
| 4.3.1.1. CAPolicy.inf | 45 |
| 4.3.1.2. Zertifizierungsstellenkonfigurationsskript | 47 |
| 4.3.2. Installation | 52 |
| 4.3.3. Veröffentlichung Root CA Zertifikat und Sperrliste | 53 |
| 4.3.3.1. Überwachung Zertifizierungsdienste | 54 |
| 4.3.3.2. Aktivierung der SANs | 54 |
| 4.4. Zertifikatvorlagen | 54 |
| 4.4.1. Zertifikatvorlage für SSL Zertifikate | 55 |
| 4.4.2. Zertifikatvorlagen für den NDES | 55 |
| 4.4.3. Zertifikatvorlage für das MDM | 56 |
| 4.4.4. Zertifikatvorlage für den OCSP Responder | 56 |
| 4.5. Konfiguration Zertifizierungsdienste | 57 |
| 4.5.1. Microsoft Internet Information Services (IIS) | 57 |
| 4.5.2. OCSP Responder | 57 |
| 4.5.3. Network Device Enrollment Service (NDES) | 58 |
| 4.6. Backup der Datenbank und der Konfiguration der Zertifizierungsstellen | 59 |
| 4.7. Offlinenehmen der Root CA | 60 |
| 4.8. Erstellung des Schlüsselpaares der Backup Root CA | 60 |
| 4.9. Backup der Partitionen des Hardware-Sicherheitsmoduls | 62 |
| 4.10. Zusammenfassung | 63 |
| 5. Verifikation | 65 |
| 5.1. Hardware-Sicherheitsmodul | 66 |
| 5.1.1. Schlüssel in Hardware-Sicherheitsmodul Partitionen | 66 |
| 5.1.2. High Availability-Cluster | 67 |
| 5.1.3. Backup und Wiederherstellung der Schlüssel der Hardware-Sicherheitsmodule | 68 |

| | | |
|-----------|--|-----------|
| 5.2. | Zertifikate | 69 |
| 5.2.1. | Ausstellung Zertifikate | 69 |
| 5.2.1.1. | Manuelles Ausstellen über die Microsoft Management Console auf der Zertifizierungsstelle | 69 |
| 5.2.1.2. | Manuelles Ausstellen über die Microsoft Management Console auf dem Zertifikatempfänger | 69 |
| 5.2.1.3. | Manuelles Ausstellen mit dem Programm Certreq auf der Zertifizierungsstelle | 70 |
| 5.2.1.4. | Manuelles Ausstellen über die Zertifizierungsstellen-Webregistrierung | 71 |
| 5.2.1.5. | Automatische Verteilung der Zertifikate durch Gruppenrichtlinien | 72 |
| 5.2.1.6. | Network Device Enrollment Service (NDES) | 73 |
| 5.2.2. | Zertifikatsperrung und Gültigkeitsüberprüfung | 74 |
| 5.2.2.1. | Active Directory | 74 |
| 5.2.2.2. | Webserver | 75 |
| 5.2.2.3. | Online Certificate Status Protocol (OCSP) | 75 |
| 5.3. | Ergebnis der Verifikation | 76 |
| 6. | Fazit und Ausblick auf weitere Einsatzmöglichkeiten | 79 |
| A. | Screenshot gestützte Implementierungsdokumentation | 81 |
| A.1. | Einrichtung Hardware-Sicherheitsmodul (HSM) | 81 |
| A.2. | Anbindung Zertifizierungsstelle an das Hardware-Sicherheitsmodul High Availability-Cluster | 81 |
| A.2.1. | Installation und Konfiguration des Safenet Luna Clients | 81 |
| A.2.2. | Key Storage Provider (KSP) und Cryptographic Service Provider (CSP) | 86 |
| A.3. | Einrichtung Active Directory-Zertifikatsdienste der Root CA | 89 |
| A.4. | Veröffentlichen des Zertifikats und der Sperrliste der Root CA | 95 |
| A.4.1. | Konfiguration Root CA und Veröffentlichung Zertifikat und Sperrliste der Root CA in der NTMNET Domäne | 96 |
| A.4.2. | Konfiguration Root CA und Veröffentlichung Zertifikat und Sperrliste der Root CA in der ACI Domäne | 97 |
| A.4.3. | Konfiguration Root CA und Veröffentlichung Zertifikat und Sperrliste der Root CA für eine domänenlose Umgebung | 97 |
| A.5. | Einrichtung Active Directory-Zertifikatsdienste der Sub CAs | 97 |
| A.5.1. | Signieren des Sub CA Zertifikats und Konfiguration Sub CA | 103 |
| A.5.2. | Aktivierung der Systemüberwachungsrichtlinien auf den Sub CAs | 107 |
| A.5.3. | Aktivierung der Subject Alternative Names (SANs) in Zertifikaten | 108 |
| A.5.4. | Installation der Zertifikatvorlagen | 108 |
| A.5.5. | Konfiguration der Zertifikatvorlagen | 108 |
| A.5.5.1. | M-net_Domain-Webserver | 109 |
| A.5.5.2. | M-net_Exchange-Enrollment-Agent(offlinerequest) | 110 |
| A.5.5.3. | M-net_CEP-Encryption | 111 |
| A.5.5.4. | M-net_SCEP-MobileIron | 111 |
| A.5.5.5. | M-net_OCSP-Response_Signing | 113 |
| A.5.6. | Konfiguration des Microsoft Internet Information Services (IIS) | 114 |

Inhaltsverzeichnis

| | |
|--|------------|
| A.5.7. Konfiguration des OCSP Responders | 117 |
| A.5.8. Konfiguration des Network Device Enrollment Services (NDES) | 123 |
| Abkürzungsverzeichnis | 127 |
| Abbildungsverzeichnis | 129 |
| Listingsverzeichnis | 131 |
| Tabellenverzeichnis | 133 |
| Literaturverzeichnis | 135 |

1. Einleitung

In Zeiten steigender Kriminalität in der Informationstechnik (IT) wird das Sicherheitsbewusstsein und die Notwendigkeit seine Daten vor fremden Zugriff zu sichern immer wichtiger. Die Integrität, Vertraulichkeit und Authentizität von Daten oder den Zugriff zu einem Netzwerk zu schützen, ist ein entscheidender Faktor. Dafür werden unter anderem Authentifizierungs-, Verschlüsselungs-, Signatur- und Prüfsummenverfahren benutzt. Authentifizierungsverfahren dienen dazu sicherzustellen, dass die Eigenschaft einer Datei, Person oder Gerät dem entspricht, was erwartet bzw. behauptet wird. Ein Verschlüsselungsverfahren verschleiert den Inhalt einer Datei. Das Signaturverfahren stellt die Herkunft oder den Autor fest, während das Prüfsummenverfahren die Unverfälschtheit einer Datei garantiert.

Um diese Verfahren anwenden zu können, werden sogenannte Schlüsselpaare benötigt, welche aus einem privaten und einem öffentlichen Schlüssel bestehen. Der private Schlüssel bleibt immer beim Besitzer, während der öffentliche Schlüssel herausgegeben werden kann. Ist jemand z. B. im Besitz eines signierten Dokuments von einem Unternehmen, kann er mit Hilfe des öffentlichen Schlüssels des Unternehmens überprüfen, ob das Dokument wirklich von dem Unternehmen stammt. Inzwischen sind diese Schlüssel, auch Zertifikate genannt, allgegenwärtig und werden u. a. für die Absicherung einer Hypertext Transfer Protocol (HTTP) Verbindung benutzt, wenn beispielsweise Onlinebanking genutzt wird. Zum Erzeugen dieser Schlüsselpaare kann eine Public Key Infrastruktur (PKI) verwendet werden. Die PKI erstellt und verwaltet Schlüssel und fungiert somit als Sicherheitsinstanz.

In dieser Bachelorarbeit wird auf die Funktionsweise einer PKI eingegangen, ein Konzept zur Implementierung vorgestellt und erläutert. Anschließend wird, anhand von Screenshots, die durchgeführte Implementierung beschrieben.

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

In diesem Kapitel wird das generische Konzept der Verschlüsselungsarten und die Funktionsweise einer PKI und ihrer Komponenten erläutert. Dabei ist zu beachten, dass diese Bachelorarbeit den Fokus hauptsächlich auf eine Microsoft Windows PKI und weniger auf eine PKI unter Verwendung von Unix/Linux setzt.

2.1. Verschlüsselung

Es gibt verschiedene Arten der Verschlüsselung, wobei alle einen mathematischen Algorithmus benutzen. Wird ein Algorithmus angewendet um etwas zu verschlüsseln, wird dazu ein sogenannter Schlüssel benutzt. Dieser Schlüssel repräsentiert das Kennwort für die verschlüsselten Daten, analog zu einem Schlüssel für ein Schloss, das Daten in einem Tresor sichert. Die Sicherheit der Verschlüsselung hängt dabei von dem verwendeten Algorithmus und der Länge des Schlüssels ab. Je nach Verschlüsselungsart, Algorithmus und Länge des Schlüssels wird für eine Ver- oder Entschlüsselung unterschiedlich viel Zeit benötigt. Bei der Wahl eines Algorithmus muss zusätzlich die Kompatibilität mit den eingesetzten Geräten und Programmen beachtet werden, da diese nicht alle Algorithmen unterstützen.

2.1.1. Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird der gleiche Schlüssel sowohl für die Ver- als auch Entschlüsselung verwendet. Dieser Schlüssel ist sowohl dem Empfänger als auch dem Sender bekannt und darf auch nur diesen beiden bekannt sein, da ansonsten eine dritte Partei die Daten ebenfalls entschlüsseln könnte. Der Sender verschlüsselt seine Nachricht mit dem Schlüssel und schickt die verschlüsselte Nachricht an den Empfänger. Dieser entschlüsselt die Nachricht mit dem gleichen Schlüssel und kann sie nun lesen. Ein Beispiel ist in Abbildung 2.1 dargestellt.



Abbildung 2.1.: Symmetrische Verschlüsselung

2.1.2. Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung besitzen sowohl Sender als auch Empfänger einen privaten und einen öffentlichen Schlüssel. Beide Schlüssel werden zusammen generiert, wobei der private Schlüssel nicht in Umlauf gelangen darf, während der öffentliche Schlüssel zur

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

Ver- bzw. Entschlüsselung veröffentlicht werden kann. Der Sender benutzt zum Verschlüsseln den öffentlichen Schlüssel des Empfängers und schickt die verschlüsselte Nachricht an den Empfänger. Dieser entschlüsselt mit seinem privaten Schlüssel die Nachricht. Ein Beispiel ist in Abbildung 2.2 dargestellt.

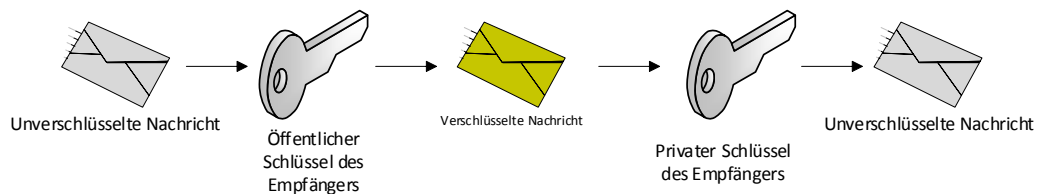


Abbildung 2.2.: Asymmetrische Verschlüsselung

Einer der am häufigsten benutzten Vertreter der asymmetrischen Verschlüsselung ist der Rivest, Shamir und Adleman (RSA) Algorithmus. In einer Empfehlung der Bundesnetzagentur [Bun14] werden RSA Schlüssel mit einer Schlüssellänge von 2048 Bit mindestens bis Ende 2020 als sicher angegeben. Schlüssel mit 1024 Bit und weniger werden seit Ende 2007 nicht mehr empfohlen. Microsoft schreibt für seine Zertifizierungsstellen ab Windows Server 2012 eine Mindestschlüssellänge bei RSA von 1024 Bit vor, ansonsten startet der Zertifizierungsstellendienst nicht [Mic16a]. Eine Verdoppelung der Schlüssellänge bei RSA führt zu einer sechs- bis siebenmal langsameren Ver- bzw. Entschlüsselung, siehe Listing 2.1.

Listing 2.1: Ausführen des OpenSSL Speed Befehls für RSA 512 Bit, 1024 Bit, 2048 Bit und 4096 Bit auf einem AMD Phenom II X6 1090T mit 3,2 Ghz

```
1 D:\Program Files (x86)\OpenSSL-Win32\bin>openssl speed rsa512 rsa1024
  rsa2048 rsa4096
2
3 Doing 512 bit private rsa's for 10s: 45186 512 bit private RSA's in
  10.00s
4 Doing 512 bit public rsa's for 10s: 534987 512 bit public RSA's in
  9.98s
5 Doing 1024 bit private rsa's for 10s: 8016 1024 bit private RSA's in
  10.00s
6 Doing 1024 bit public rsa's for 10s: 179278 1024 bit public RSA's in
  10.00s
7 Doing 2048 bit private rsa's for 10s: 1297 2048 bit private RSA's in
  10.00s
8 Doing 2048 bit public rsa's for 10s: 51063 2048 bit public RSA's in
  9.95s
9 Doing 4096 bit private rsa's for 10s: 193 4096 bit private RSA's in
  10.00s
10 Doing 4096 bit public rsa's for 10s: 13475 4096 bit public RSA's in
  10.00s
11 OpenSSL 1.1.0f 25 May 2017
12 built on: reproducible build, date unspecified
13 options:bn(64,32) rc4(8x,mmx) des(long) aes(partial) idea(int)
  blowfish(ptr)
14 compiler: cl "VC-WIN32
15          sign    verify    sign/s  verify/s
16 rsa  512 bits  0.000221s 0.000019s  4518.6  53582.4
17 rsa 1024 bits  0.001248s 0.000056s   801.6  17927.8
18 rsa 2048 bits  0.007710s 0.000195s   129.7   5130.3
19 rsa 4096 bits  0.051813s 0.000742s    19.3   1347.5
```


2.1.3. Kombination asymmetrische und symmetrische Verschlüsselung

Eine weitere Art der Verschlüsselung ist das Anwenden einer Kombination von asymmetrischer und symmetrischer Verschlüsselung. Hierbei wird die asymmetrische Verschlüsselung genutzt, um einen symmetrisch verschlüsselten Schlüssel sicher zwischen zwei Parteien auszutauschen. Anschließend können die beiden Parteien mit dem symmetrischen Schlüssel ihre Nachrichten verschlüsseln.

2.1.4. Hash-Algorithmus

Bei der Anwendung eines Hash-Algorithmus auf ein eingelestes Dokument wird ein mathematisches Ergebnis generiert, ein sogenannter Hashwert. Dieser Hashwert ist eindeutig. Sollte das Dokument verändert werden, stimmt ein daraufhin neu generierter Hashwert nicht mehr mit dem ursprünglichen Hashwert überein. Dadurch wird, wenn der originale Hashwert vorliegt, eine Möglichkeit zur Überprüfung der Unverfälschtheit eines Dokumentes möglich. Ein Hashwert einer Datei oder eines Textes kann mit geeigneten Programmen, z. B. dem Hash Tool leicht erstellt und somit überprüft werden.

Als Algorithmus wird dabei oftmals der Secure Hash Algorithm (SHA) verwendet. Von diesem gibt es vier Varianten, die wiederum unterteilt werden. Die vier Varianten sind SHA-0, SHA-1, SHA-2 und SHA-3, wobei die Zahl für die Version des Algorithmus steht, d. h. SHA-0 ist die älteste Version. Da SHA-0 schon 1995 durch SHA-1 abgelöst wurde, hat SHA-0 in der Praxisverwendung keine nennenswerte Bedeutung mehr. [Wik17]

SHA-0 und SHA-1 haben immer eine 160 Bit Hashlänge, während die Hashlänge von SHA-2 und SHA-3 durch ein Suffix, welches der Länge des Hashwerts in Bit entspricht, genauer spezifiziert wird. D. h. SHA-256 gehört der SHA-2 Familie an und hat einen 256 Bit Hashwert, während SHA3-256 der SHA-3 Familie mit 256 Bit Hashwertlänge angehört.

Die Bundesnetzagentur [Bun14] hält die SHA-1 Hashfunktion seit Ende 2007 für nicht mehr geeignet, während Hashfunktionen der SHA-2 Familie von SHA-256 und aufwärts bis mindestens Ende 2020 für Signaturen geeignet sein sollen.

Der American Standard Code for Information Interchange (ASCII) ordnet Zeichen, wie z. B. Buchstaben, einem Code zu, um einen Text zu übertragen und darzustellen. Dabei repräsentiert der Code 0x61 den Buchstaben „a“, 0x62 den Buchstaben „b“, 0x63 den Buchstaben „c“, usw. In Tabelle 2.1 werden die Hashwerte zweier Texte verglichen, die sich nur um ein Bit unterscheiden. Der ASCII-Code des Buchstabens „h“ ist 0x68, während „g“ durch 0x67 repräsentiert wird.

Tabelle 2.1.: Beispiel zweier Hashwerte mit SHA-256

| |
|---|
| Alle Kinder haben Haare; nur nicht Klaus, dem fallen sie aus. |
| da932cbb8d2d508d3757420129545420c888610a297e3f7bfbfd495eca6d82326 |
| Alle Kinder gaben Haare; nur nicht Klaus, dem fallen sie aus. |
| c868981a5742590f5902a71f4ee8d4fa4d50982747317cf6c71f0f089032957a |

2.1.5. Signatur-Algorithmus

Ein Signatur-Algorithmus wird verwendet, um dem Empfänger die Herkunft des Senders zu garantieren. Dabei verschlüsselt der Sender seine Nachricht mit seinem privaten Schlüssel und schickt die verschlüsselte Nachricht an den Empfänger. Dieser kann nun diese Nachricht mit dem öffentlichen Schlüssel des Senders entschlüsseln. Da nur der Sender Zugriff auf seinen privaten Schlüssel hat, ist somit sichergestellt, dass die Nachricht vom Sender kommt. Die Nachricht wird hierbei zwar verschlüsselt übertragen, aber jeder der im Besitz des öffentlichen Schlüssel des Senders ist, kann die Nachricht mitlesen. Ein Beispiel ist in Abbildung 2.3 dargestellt.

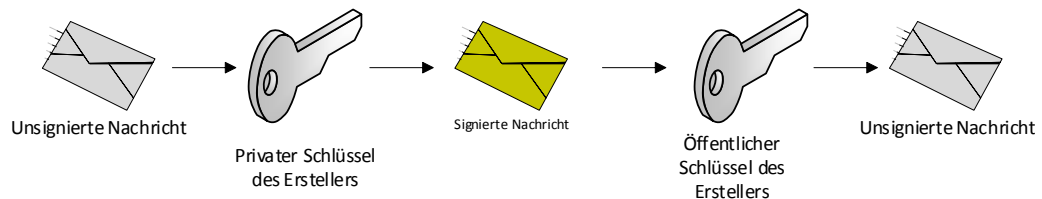


Abbildung 2.3.: Anwendung des Signatur-Algorithmus

2.1.6. Signatur-Hash-Algorithmus

Bei der Verschlüsselung mit einem Signatur-Hash-Algorithmus wird die Unverfälschtheit einer Datei garantiert, indem ausgeschlossen wird, dass sowohl die Nachricht als auch der Hashwert manipuliert wurden. Der Ersteller der Nachricht generiert den Hashwert seiner Datei und verschlüsselt diesen Hashwert mit seinem privaten Schlüssel, signiert ihn also. Dann werden die unverschlüsselte Nachricht und der Hashwert an den Empfänger geschickt. Dieser kann nun mit dem öffentlichen Schlüssel des Senders den Hashwert entschlüsseln, einen neuen Hashwert der Nachricht generieren und vergleichen. Sollten die beiden Hashwerte nicht übereinstimmen, wurde entweder der Hashwert oder die Nachricht manipuliert. Diese Kombination aus Signatur- und Hash-Algorithmus hat den Vorteil des geringeren Rechenaufwandes, da statt der Nachricht nur der Hashwert verschlüsselt werden muss. Durch die Hashwert-Signatur mittels privatem Schlüssel ist garantiert, dass die Nachricht vom Ersteller kommt. Ein Beispiel ist in Abbildung 2.4 dargestellt.

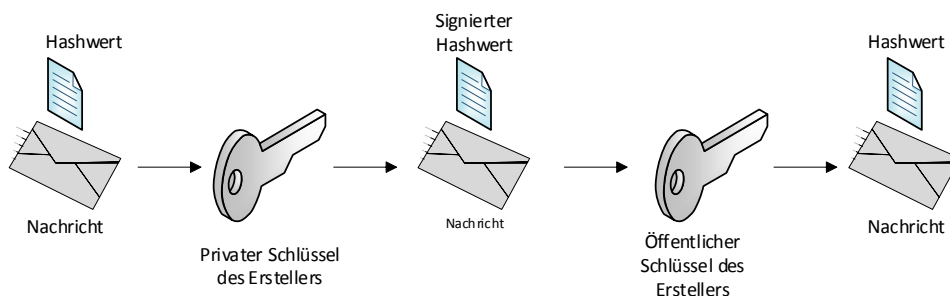


Abbildung 2.4.: Anwendung des Signatur-Hash-Algorithmus

2.1.7. Kryptografieanbieter

Ein Kryptografieanbieter ist ein Programm, das ein Anwenden von Kryptografieoperationen, wie z. B. einer Verschlüsselung oder einer Signatur, möglich macht. Dabei unterscheiden sich die Kryptografieanbieter unter anderem in ihrer Geschwindigkeit oder der unterstützten Kryptografiealgorithmen.

Kryptografieanbieter werden in zwei Anbieterkategorien unterteilt. Diese sind der Kryptografiediensteanbieter (Cryptographic Service Provider, CSP) und der Schlüsselspeicheranbieter (Key Storage Provider, KSP). Microsoft nennt den KSP teilweise auch Cryptography API: Next Generation (CNG). Der KSP ist der Nachfolger des CSPs und bietet unter anderem die Unterstützung von SHA-2 an. Der KSP kann ab Windows Server 2008 und Vista benutzt werden [Micntb]. Der RSA#Microsoft Software Key Storage Provider unterstützt beispielsweise SHA-1 bis SHA-512 mit Schlüssellängen bis 16384 Bit [Mienta].

2.2. Funktionsweise einer Public Key Infrastruktur (PKI)

Eine PKI besteht hauptsächlich aus drei Komponenten:

- Zertifizierungsstelle (Certificate Authority, CA)
- Registrierungsstelle (Registration Authority, RA)
- Validierungsstelle (Validation Authority, VA)

Das Zusammenspiel dieser drei Komponenten wird im folgenden Abschnitt erklärt.

Ein Benutzer erstellt meist seinen privaten Schlüssel lokal auf dem PC, aus dem dann ein öffentlicher Schlüssel generiert wird. Benötigt man jedoch einen signierten öffentlichen Schlüssel, muss eine Zertifikatanforderung an eine Zertifizierungsstelle gesendet werden, welche dann ein signiertes Zertifikat passend zu dem privaten Schlüssel erstellt. Dies geschieht, indem der Benutzer bei der RA ein von der PKI signiertes Zertifikat anfordert. Die RA überprüft dann, ob der Benutzer dazu berechtigt ist und leitet, bei positiver Überprüfung, die Anfrage an die Zertifizierungsstelle weiter, welche nun das Zertifikat erzeugt und an den Benutzer zurückschickt. [Kom04] Dies ist in Abbildung 2.5 dargestellt.

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

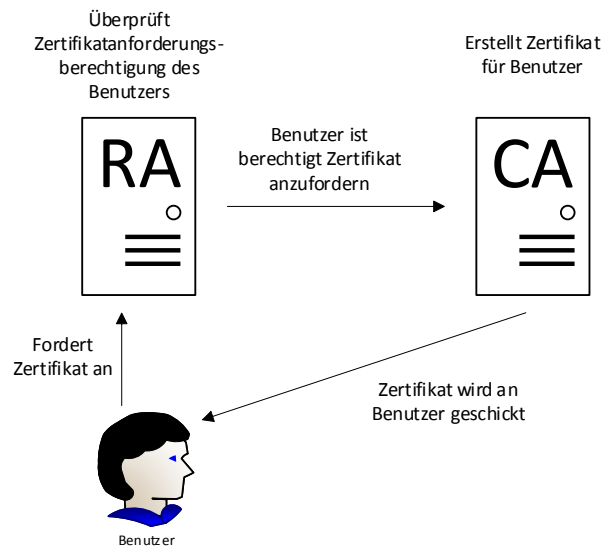


Abbildung 2.5.: Zertifikatanforderung

Hat nun der Benutzer ein Zertifikat von dieser PKI bekommen und schickt das Zertifikat an ein anderes System, kann dieses System durch eine Abfrage bei der Validierungsstelle feststellen, ob das Zertifikat von ihr stammt und dessen Gültigkeit prüfen. Die Zertifikatvalidierung ist in Abbildung 2.6 dargestellt.

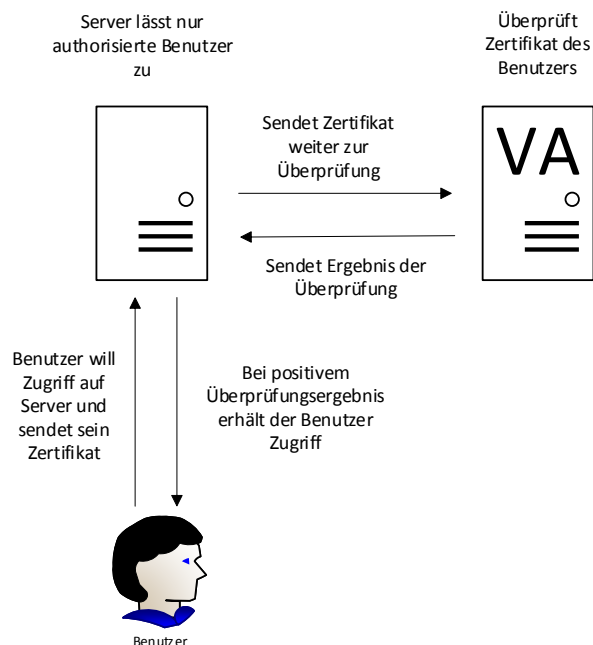


Abbildung 2.6.: Zertifikatvalidierung

Es gibt diverse Arten von Zertifikaten für verschiedene Anwendungen. Zertifizierungsstellenzertifikate sind Zertifikate, die einer Zertifizierungsstelle gehören und dazu berechtigen ebenfalls Zertifikate auszustellen. Teilnehmerzertifikate sind Zertifikate, die von einer Zertifizierungsstelle ausgestellt werden, aber keine ausstellende Funktion innehaben. Diese

2.2. Funktionsweise einer Public Key Infrastruktur (PKI)

Teilnehmerzertifikate unterteilen sich wiederum in Benutzer-, Client-, Server- und Dienstzertifikate. Benutzerzertifikate sind an eine Person, Client- und Serverzertifikate an ein Gerät und Dienstzertifikate an einen Dienst gebunden. Diese Zertifikattypen unterteilen sich dann nochmals in ihren jeweiligen Verwendungszweck, wie z. B. Signatur von Dokumenten oder Verschlüsselung von Dateien.

Die meisten digitalen Zertifikate einer PKI basieren auf dem X.509 Standard, welcher in Version 1 im Jahr 1988 definiert wurde [Kom04]. Die in Zertifikaten der X.509 Version 1 enthaltenen Informationen sind in Tabelle 2.2 aufgelistet.

Tabelle 2.2.: Zertifikatdetails der X.509 Version 1

| Feld | Beschreibung |
|---|--|
| Version (Version) | Hier steht die Versionsnummer des X.509 Zertifikats, in diesem Fall V1 |
| Seriennummer (Serial Number) | Eindeutige numerische Kennung, die von der CA erstellt wird |
| Signaturalgorithmus (Signature Algorithm) | Hier steht der Signaturalgorithmus mit dem die CA das Zertifikat signiert hat und die verwendete Hashfunktion. |
| Aussteller (Issuer) | Enthält den Distinguished Name der CA, die das Zertifikat ausgegeben und signiert hat. |
| Gültigkeitsdauer (Validity) | Hier wird der Zeitraum definiert, in dem das Zertifikat gültig ist. |
| Antragsteller (Subject) | Hier wird der Distinguished Name des Antragstellers definiert. |
| Öffentlicher Schlüssel (Subject Public Key) | Enthält den öffentlichen Schlüssel und den Algorithmus mit der verwendeten Schlüssellänge, mit der der öffentliche Schlüssel erstellt wurde. |
| Signaturwert (Signature Value) | Enthält den Signaturwert der durch das Anwenden des Signaturalgorithmus von der CA auf die Informationen aller Felder generiert wurde. |

In der im Jahr 1993 eingeführten Version 2 sind zusätzlich zwei optionale Felder definiert worden, um das Erneuern eines Zertifizierungszertifikats zu verbessern, siehe Tabelle 2.3 [Kom04].

Tabelle 2.3.: Zusätzliche Zertifikatdetails der X.509 Version 2

| Feld | Beschreibung |
|---|--|
| Eindeutige ID Aussteller (Issuer Unique ID) | Hier steht eine von der CA für sich selber generierte eindeutige Kennung, meistens eine hexadezimale Zeichenkette. |
| Eindeutige ID Antragsteller (Subject Unique ID) | Hier steht eine von der CA generierte eindeutige Kennung für den Antragsteller, meistens eine hexadezimale Zeichenkette. |

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

Der X.509 Version 3 Standard ist im Jahr 1996 veröffentlicht worden und fügt das Feld Erweiterungen dem Zertifikat hinzu [Kom04]. Ein Beispiel für eine Erweiterung sind die Baseinschränkungen (Basic Constraints). In dieser sollte z. B. „CA:true“ stehen, wenn es sich um ein Zertifizierungsstellenzertifikat handelt.

Der X.509 Standard wird laufend weiterentwickelt, wobei aktuell nur zusätzliche Erweiterungen hinzukommen oder aktualisiert werden und im Zertifikat immer noch Version V3 angezeigt wird. In Listing 2.2 ist ein selbst-signiertes Zertifizierungsstellenzertifikat zu sehen, d. h. in diesem Zertifikat sind Aussteller und Antragsteller identisch.

Listing 2.2: Selbst-signiertes Zertifizierungsstellenzertifikat

```
1 Certificate:
2   Data:
3     Version: 3 (0x2)
4     Serial Number:
5       f8:5c:0e:e8:8f:0a:76:39
6     Signature Algorithm: sha256WithRSAEncryption
7     Issuer: C = DE, ST = Bavaria, L = Munich, O = Family Leimig,
8       CN = MyRoot
9     Validity
10      Not Before: Feb  3 19:48:52 2018 GMT
11      Not After : Feb  3 19:48:52 2019 GMT
12     Subject: C = DE, ST = Bavaria, L = Munich, O = Family Leimig
13       , CN = MyRoot
14     Subject Public Key Info:
15       Public Key Algorithm: rsaEncryption
16       Public-Key: (1024 bit)
17       Modulus:
18         00:f4:8f:12:ba:2f:5f:60:2e:48:71:35:89:ec:0b:
19         4b:c8:1c:67:d0:ed:25:64:0e:1d:56:7e:39:7c:3f:
20         11:a2:1c:b7:4a:2d:19:fc:b7:4c:82:c9:e1:3b:bc:
21         af:c4:9f:4d:ce:80:69:cb:35:e0:a3:ed:53:7b:08:
22         da:6b:7d:7d:5d:e3:8f:d6:08:d5:e0:a5:e5:22:50:
23         e9:8d:f9:fe:f8:32:6c:74:e0:37:08:b0:22:04:a5:
24         09:41:6f:b6:8f:55:d3:ed:3d:cc:43:a3:1e:16:09:
25         21:0c:73:0e:88:c4:d1:ac:c1:07:95:b3:b7:c9:2b:
26         80:71:6d:45:f7:9a:41:28:3b
27       Exponent: 65537 (0x10001)
28     X509v3 extensions:
29       X509v3 Basic Constraints:
30         CA:TRUE
31     Signature Algorithm: sha256WithRSAEncryption
32     6e:53:d2:8b:d6:2a:c5:91:42:5a:72:52:91:98:c5:1b:b5:00:
33     b0:7a:4e:3b:ef:49:0b:4a:d8:06:30:88:e8:72:0d:98:14:2c:
34     84:ba:9b:67:a5:a5:bc:7f:c7:d6:94:81:34:1f:27:ac:ac:69:
35     07:7c:87:e9:36:34:bc:d5:32:96:9e:93:b9:b0:05:f2:4e:06:
36     b0:86:f7:2c:76:19:b1:d9:6f:66:e4:79:6e:c2:c4:01:d3:a8:
37     db:73:c8:ec:00:93:7b:93:62:9c:76:5d:5b:29:e2:b1:89:a8:
38     e1:f1:c5:4e:39:24:37:20:a3:66:59:6c:81:4a:7b:16:d0:7e:
39     76:28
```

Es gibt mehrere Dateiformate für Zertifikate, z. B. PKCS#7 oder DER. DER Zertifikate sind an der Dateiendung .pem, .cer, .crt oder .der erkennbar. Häufig sind DER Zertifikate Base64 codiert, was eine schönere Formatierung der Datei bewirkt, wenn sie mit dem Editor

geöffnet werden. Das in Listing 2.2 gezeigte Zertifikat ist in Listing 2.3 als Base64 codierte Datei zu sehen.

Listing 2.3: Selbst-signiertes Zertifizierungsstellenzertifikat Base64 codiert

```

1 -----BEGIN CERTIFICATE-----
2 MIICQDCCAamgAwIBAgIJAPhcDuiPCnY5MA0GCSqGSIb3DQEBCwUAMFkxCzAJBgNV
3 BAYTAkRFMRwDgYDVQQIDAdCYXZhcmlhMQ8wDQYDVQQHDAZNdW5pY2gxZjAUBgNV
4 BAoMDUZhWlseSBMZWltaWcxZDZANBgNVBAMMBk15Um9vdDAeFw0xODAyMDMxOTQ4
5 NTJaFw0xOTAyMDMxOTQ4NTJaMFkxCzAJBgNVBAYTAkRFMRwDgYDVQQIDAdCYXZh
6 cmlhMQ8wDQYDVQQHDAZNdW5pY2gxZjAUBgNVBAoMDUZhWlseSBMZWltaWcxZDZAN
7 BgNVBAMMBk15Um9vdDCBnzANBjkiG9w0BAQEFAAOBjQAwgYkCgYEA9I8Sui9f
8 YC5IcTWJ7AtLyBxn0O0LZA4dVn45fD8Rohy3Si0Z/LdMgsnhO7yvxJ9NzoBpyzXg
9 o+1Tewjaa319XeOP1gjV4KX111Dpjfn++DJsdoA3CLAIbKUJQW+2j1XT7T3MQ6Me
10 FgkhDHMOiMTRrMEHlbO3ySuAcW1F95pBKDsCAwEAAMQMA4wDAYDVR0TBAAUwAwEB
11 /zANBgkqhkiG9w0BAQsFAAOBgQBuu9KL1irFkUJaclKRmMUbtQCwek4770kLStgG
12 MIjocg2YFCyEuptnpaW8f8fWIE0HyesrGkHfIfpNjS81TKWnpO5sAXyTgawhves
13 dhmx2W9m5HluwsQB06jbc8jsAJN7k2Kcdl1bKeKxiajh8cVOOSQ3IKNmWWyBSnsW
14 0H52KA==
15 -----END CERTIFICATE-----

```

2.2.1. Zertifizierungsstelle (CA)

Die Zertifizierungsstelle hat folgende Aufgaben:

- Ausstellen von Zertifikaten
- Verlängern von Zertifikaten
- Sperren von Zertifikaten
- Erstellung und Bereitstellen von Zertifikatvorlagen
- Veröffentlichen der Zertifikatsperrliste

Das Ausstellen von Zertifikaten kann entweder manuell direkt auf der CA, manuell oder automatisiert durch Zertifikatvorlagen oder über eine von den Microsoft Internet Information Services (IIS) bereitgestellte Webseite erfolgen. Eine manuelle Zertifikaterstellung auf der CA erfolgt durch Einreichen einer vom Anforderer des Zertifikats erstellten Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) und dem anschließenden Ausstellen des Zertifikats. Dieses muss dann von der CA exportiert und dem Anforderer übermittelt werden. Die manuelle Zertifikatausstellung ist die einzige Möglichkeit für Computer, die keinen Netzwerkzugriff auf die CA oder den IIS der CA haben, ein Zertifikat zu erhalten.

Zertifikate haben eine Gültigkeitsdauer, die bei Ablauf das Zertifikat als ungültig deklariert. Zertifikate können allerdings erneuert oder verlängert werden.

Ein Zertifikat kann auch gesperrt werden. Sollte z. B. ein privater Schlüssel eines Clients kompromittiert worden sein, muss das zugehörige Zertifikat auf der CA gesperrt werden. Verlässt ein Mitarbeiter mit einem Benutzerzertifikat das Unternehmen, sollte dessen Benutzerzertifikat ebenfalls gesperrt werden.

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

2.2.1.1. Zertifikatvorlagen

Eine Zertifikatvorlage dient dazu, bestimmte Konfigurationen des angeforderten Zertifikats zu definieren. In den Zertifikatvorlagen werden unter anderem die Gültigkeitsdauer, der Erneuerungszeitraum, der Verwendungszweck, die Schlüssellänge, der Verschlüsselungsalgorithmus und die zugriffsberechtigten Computer bzw. Personen oder Gruppen definiert.

Die Gültigkeitsdauer gibt an, wie lange das Zertifikat gültig ist, während der Erneuerungszeitraum angibt, wie viele Tage vor Ablauf der Gültigkeitsdauer ein neues Zertifikat angefordert werden soll.

Der Verwendungszweck definiert die Berechtigung des ausgestellten Zertifikats für einen der folgenden Punkte:

- Signatur
- Verschlüsselung
- Signatur und Verschlüsselung
- Signatur und Smartcard-Anmeldung

Wird die Signatur ausgewählt, kann das Zertifikat zur Signierung und zum Überprüfen der Signaturen benutzt werden. Bei der Verschlüsselung kann das Zertifikat zum Ver- und Entschlüsseln eingesetzt werden. Die Verwendung als Signatur und Verschlüsselung erlaubt sowohl die Signatur als auch die Verschlüsselung, während Signatur und Smartcard-Anmeldung die Anmeldung mit Smartcard und die Signatur erlaubt. [Mic12b]

Um die Zertifikatvorlagen im vollen Umfang nutzen zu können, muss die CA, auf der die Zertifikatvorlagen genutzt werden sollen, Mitglied einer Domäne sein, da die Zertifikatvorlagen Microsoft Active Directory Objekte sind, welche auf den Domaincontrollern gespeichert werden. Dies hat auch zur Folge, dass alle Zertifikatvorlagen von allen CAs in einer Domäne benutzt werden können. Ist nun eine CA Mitglied einer Domäne, können Zertifikatvorlagen individuell angepasst werden und als neue Zertifikatvorlagen abgespeichert werden. Sollten mehrere Domaincontroller in einer Domäne zum Einsatz kommen, ist zu beachten, dass die Zertifikatvorlagen auf jedem Domaincontroller gespeichert werden und die CA immer auf die Zertifikatvorlagen zugreift, die auf dem Domaincontroller liegen, mit dem die CA gerade verbunden ist. Dies wird dann relevant, wenn eine Zertifikatvorlage verändert oder neu erstellt wird und die Domaincontroller diese Änderung zuerst synchronisieren müssen, bevor die aktuelle Zertifikatvorlage jeder CA vorliegt.

Bei den Zertifikatvorlagen muss zwischen vier Schemaversionen unterschieden werden. Schemaversion 1 dient zur Zertifikatverteilung an Computer, die mindestens Windows 2000 oder Windows Server 2000 installiert haben. Schemaversion 2 erlaubt die Verteilung von Zertifikaten nur an PCs, die mindestens Windows XP oder Windows Server 2003 installiert haben. Schemaversion 3 setzt mindestens Windows Vista oder Windows Server 2008 voraus. [Mic09a] Mit Windows Server 2012 wird Schemaversion 4 unterstützt, welche als Zertifikatempfänger mindestens Windows 8 fordert [Mic13c]. Je höher die Schemaversion gewählt

2.2. Funktionsweise einer Public Key Infrastruktur (PKI)

wird, desto mehr Konfigurationen sind in der Zertifikatvorlage möglich. KSP Kryptografieanbieter werden beispielsweise erst ab Schemaversion 3 unterstützt. Mit der Benutzung von Zertifikatsignierungsanforderungen können auch für nicht Windows Rechner Zertifikatvorlagen genutzt werden, um Zertifikate auszustellen.

In Abbildung 2.7 ist ein Teil einer Zertifikatvorlage abgebildet. In Tabelle 2.4 ist eine Kurzübersicht der Funktionen der einzelnen Reiter der Zertifikatvorlagen aufgelistet.

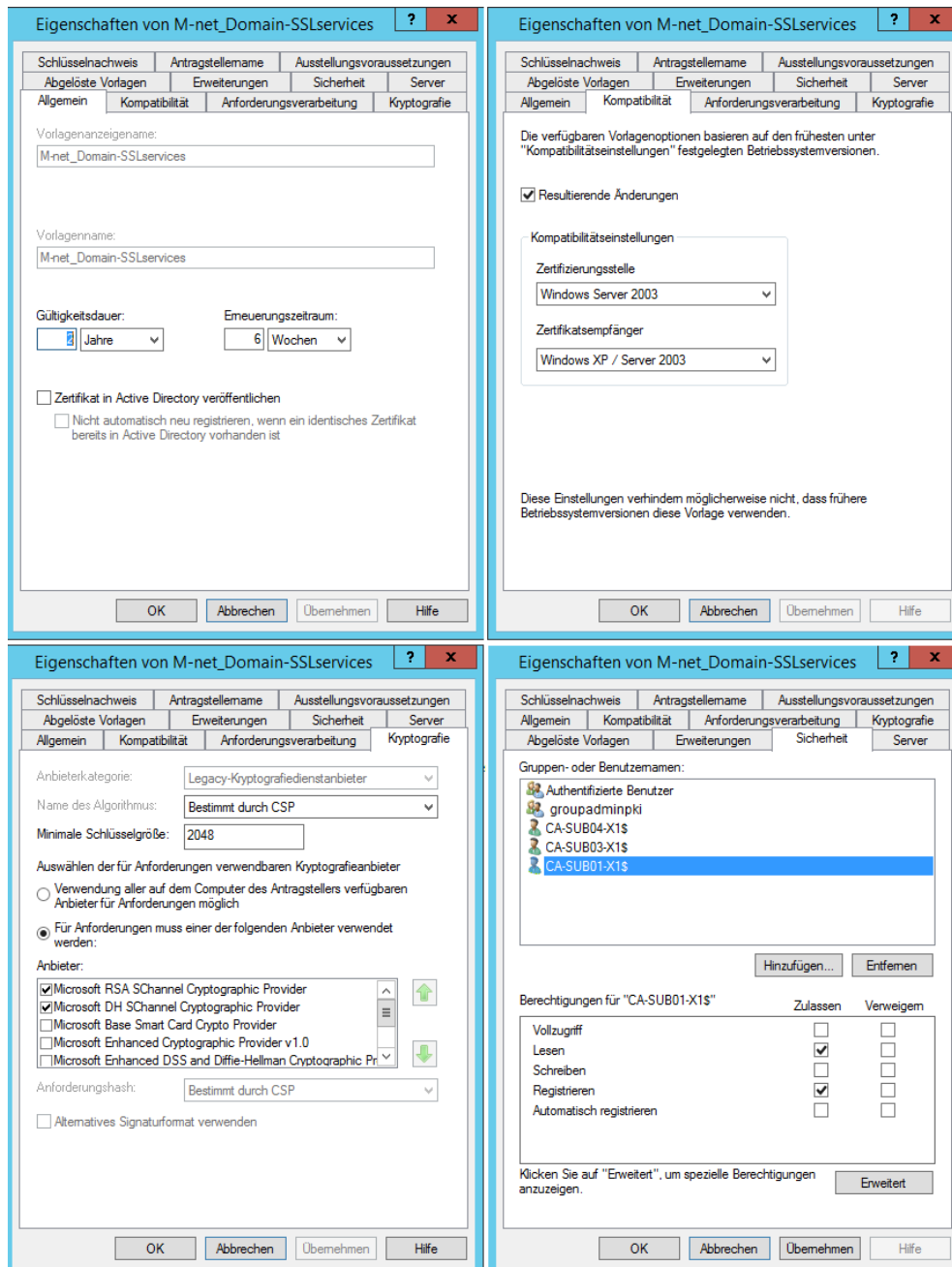


Abbildung 2.7.: Beispiel einer Zertifikatvorlage von Schemaversion 4

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

Tabelle 2.4.: Kurzbeschreibung der Reiter der Zertifikatvorlagen von Schemaversion 4

| Reiter Zertifikatvorlage | Beschreibung |
|---------------------------|---|
| Allgemein | Festlegung der Gültigkeitsdauer, dem Erneuerungszeitraum und der Veröffentlichung im Active Directory. |
| Kompatibilität | Einstellungen zur Kompatibilität der Windowsversionen der Zertifizierungsstelle und der Zertifikatempfänger. |
| Anforderungsverarbeitung | Einstellungen zum Zweck des Zertifikats und der Nutzung des privaten Schlüssels. |
| Kryptografie | Festlegung der verwendeten Schlüssellänge, der erlaubten Kryptografieanbieter und Angabe, ob KSP oder CSP verwendet werden soll. |
| Abgelöste Vorlagen | Auflistung der Vorlagen, die von dieser Vorlage abgelöst werden. |
| Erweiterungen | Hier können verschiedene Richtlinien für das auszustellende Zertifikat konfiguriert werden. Bei der Anwendungsrichtlinie kann beispielsweise der beabsichtigte Zweck des Zertifikats angegeben werden, z. B. Serverauthentifizierung. |
| Sicherheit | Hier wird festgelegt, wer diese Zertifikatvorlage benutzen darf und welche Berechtigungen er hat. |
| Server | Bietet die Möglichkeit, die Zertifikatinformationen, die standardmäßig in der Datenbank gespeichert werden, zu deaktivieren. Auch die Möglichkeit zu verhindern, dass die Gültigkeit des Zertifikats überprüft wird, kann hier konfiguriert werden. |
| Schlüsselnachweis | Hier kann vom Zertifikatempfänger ein Nachweis gefordert werden, dass der Schlüssel in einem Trusted Platform Module (TPM) gespeichert wird [Mic16c]. Ein TPM ist ein Chip auf dem Mainboard, der einfache kryptografische Operationen ermöglicht und Zertifikate mit 2048 Bit Schlüssellänge speichern kann [Bunwn]. |
| Antragstellername | Legt fest, ob die Informationen zum Antragsteller manuell, aus dem Active Directory oder bei einer Zertifikaterneuerung aus einem bereits installierten Zertifikat erfasst werden. |
| Ausstellungsvoraussetzung | Festlegung der Kriterien für die Ausstellung des Zertifikats, z. B. der Besitz eines bereits gültigen Zertifikats. |

Eine genauere Erklärung der einzelnen Komponenten einer Zertifikatvorlage kann unter

der Quelle [Mic09b] nachgelesen werden.

2.2.1.2. Sperrlisten

Zertifikate werden anhand ihrer Gültigkeit und ihres Sperrstatus als gültig betrachtet, wenn die aktuelle Zeit in der Gültigkeitsdauer des Zertifikats liegt und das Zertifikat nicht gesperrt ist. Bei einer Zertifikatsperrung wird das Zertifikat in die sogenannte Sperrliste, der Certificate Revocation List (CRL), aufgenommen. Die Sperrliste wird in regelmäßigen Zeitpunkten von der CA veröffentlicht und damit aktualisiert. Jede CA erstellt eine eigene von ihr signierte CRL, die die Seriennummern, den Sperrgrund und den Sperrzeitpunkt von Zertifikaten enthält, die von ihr ausgestellt und gesperrt wurden. Die Größe einer CRL entspricht ca. einem Megabyte pro 30.000 bis 40.000 gesperrten Zertifikaten.

Eine CRL wird in regelmäßigen Abständen veröffentlicht, dem sogenannten Veröffentlichungs- oder Erneuerungsintervall, welches individuell konfiguriert wird. Dabei hat jede CRL eine Gültigkeitsdauer. Die Gültigkeitsdauer der CRL ist die Summe aus dem Veröffentlichungsintervall und einem Überschneidungszeitraum, dem so genannten Overlap Intervall. Die Gültigkeitsdauer muss hierbei länger als das Veröffentlichungsintervall sein.

Bei einer Windows CA ist die Gültigkeitsdauer der CRL in der Standardkonfiguration um 10 Prozent länger als das Veröffentlichungsintervall, jedoch höchstens 12 Stunden länger [Mic13b]. Die maximale Gültigkeitsdauer entspricht dem doppelten Erneuerungsintervall, d. h. bei einem Erneuerungsintervall von einem Tag beträgt die maximale Gültigkeitsdauer zwei Tage. Wenn die Gültigkeitsdauer auf der Standardeinstellung gelassen wird, beträgt sie 26 Stunden und 24 Minuten. Es empfiehlt sich die Gültigkeitsdauer der CRL ausreichend lang zu setzen, um genug Reaktionszeit für den Ausfall einer CA zu haben, da nur mit einer funktionierenden CA eine CRL erstellt werden kann. Beträgt die Gültigkeit einer CRL zwei Tage und das Erneuerungsintervall ist täglich, so hat man mindestens einen Tag Zeit, ein vorhandenes Problem zu finden und eine neue CRL zu veröffentlichen, bevor die alte CRL ungültig wird.

Durch das Anpassen von Registrierungsschlüsseln unter „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<Name der CA>“ lässt sich das Erneuerungsintervall und der Überschneidungszeitraum manuell anpassen. Der Schlüssel „CRLPeriod“ gibt die Einheit des Erneuerungsintervalls an: „Hours“, „Days“, „Weeks“, „Months“ oder „Years“. Der Schlüssel „CRLPeriodUnits“ gibt den Wert der „CRLPeriod“ an. Der Schlüssel „CRLOverlapPeriod“ gibt die Einheit des Überschneidungszeitraums an, während „CRLOverlapUnits“ den zugehörigen Wert definiert.

Eine Windows CA speichert ihre CRL in der Standardkonfiguration unter „C:\Windows\System32\CertSrv\CertEnroll“ ab. Ist die CA ein Mitglied einer Domäne, kann die CRL zusätzlich in der Domäne im AD veröffentlicht werden. Sollen Geräte oder Benutzer außerhalb des Netzwerkes ein Zertifikat verwenden, muss die CRL auch von außerhalb des Netzwerkes erreichbar sein. Dies kann entweder durch einen Webserver, der die CRL bereitstellt oder durch einen OCSP Responder geschehen. Nicht zu empfehlen ist es, die CA über das Internet erreichbar zu machen und auf ihr einen Webserver zu hosten, um dort die CRL verfügbar zu machen, da dies die Angriffsmöglichkeiten auf die CA erhöht.

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

Muss ein Zertifikat mit hoher Priorisierung gesperrt werden, kann die Veröffentlichung der Zertifikatssperrliste auch manuell auf der CA ausgeführt werden. Wird eine Sperrliste manuell veröffentlicht, beginnen die Veröffentlichungsintervalle ab diesem Zeitpunkt von vorne.

Wird ein Zertifikat gesperrt, kann zur besseren Dokumentation der Grund dafür angegeben werden. In der Tabelle 2.5 sind mögliche Sperrgründe mit ihrem Sperrlistengrundcode (reason code) aufgelistet.

Tabelle 2.5.: Sperrgründe

| Sperrgrund (reason code) | Beschreibung |
|--|--|
| Nicht angegeben (0) | Es wird kein Sperrgrund angegeben. |
| Schlüsselkompromittierung (1) | Dem Schlüssel kann nicht mehr vertraut werden. |
| Kompromittierung der Zertifizierungsstelle (2) | Der Zertifizierungsstelle kann nicht mehr vertraut werden. |
| Zuordnung geändert (3) | Das Zertifikat wird nicht mehr benötigt, da z. B. der Client, der das Zertifikat zur Authentifizierung für einen Server benutzt hat, auf den Server nicht mehr zugreifen muss. |
| Abgelöst (4) | Das Zertifikat wurde durch ein neues ersetzt, weil sich z. B. die Zertifikatvorlage geändert hat. |
| Vorgangsende (5) | Die Zertifizierungsstelle wurde außer Betrieb gestellt. |
| Zertifikat blockiert (6) | Dieser Sperrgrund erlaubt es, das Zertifikat nach seiner Sperrung wieder zu reaktivieren. Dadurch ist eine zeitliche Sperrung möglich. |
| (7) | Dieser Sperrgrund wird nicht verwendet. |
| Aus Zertifikatssperrliste entfernen (8) | Die Sperrung eines Zertifikats, mit dem Sperrgrund „Zertifikat blockiert“, wurde aufgehoben und noch keine neue Basissperrliste generiert. Siehe Kapitel 2.2.1.2. |

Wenn ein gesperrtes Zertifikat zeitlich ungültig wird, wird es, bei der Standardkonfiguration einer Windows CA, in einer neu erstellten CRL nicht mehr aufgelistet.

Deltasperrlisten

Zusätzlich zu der Sperrliste, auch Basissperrliste genannt, gibt es Deltasperrlisten (Delta CRLs). Die Deltasperrliste ist im Gegensatz zu der Basissperrliste nicht in jeder PKI konfiguriert und hat die Aufgabe, alle Zertifikate aufzulisten, die nach der letzten Veröffentlichung der Basissperrliste gesperrt wurden. Deltasperrlisten werden in der Regel häufiger veröffentlicht als die Basissperrlisten und sind deutlich kleiner, da sie nur die gesperrten Zertifikate enthalten, die zwischen den Veröffentlichungen der Basissperrlisten gesperrt werden. Ein Beispiel zur Deltasperrliste ist in Abbildung 2.8 gegeben. In diesem Beispiel ist das Veröffentlichungsintervall der Basissperrliste auf vier Zeiteinheiten und das Veröffentlichungsintervall der Deltasperrliste auf drei Zeiteinheiten konfiguriert.

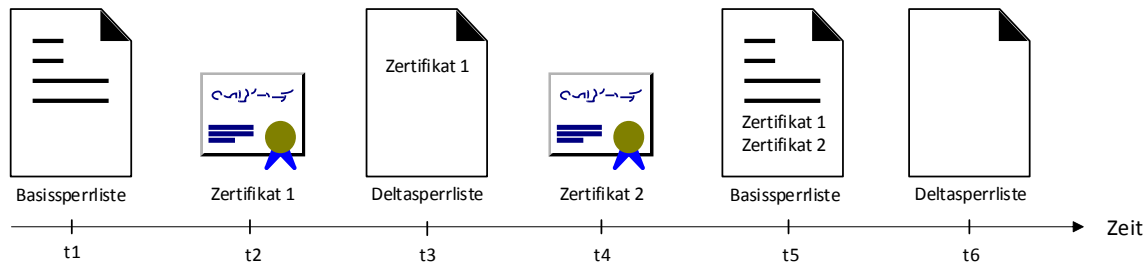


Abbildung 2.8.: Veröffentlichung der Deltasperrriste

- Zeitpunkt t1: Es wird eine Basissperrriste veröffentlicht, die bereits gesperrte Zertifikate enthält.
- Zeitpunkt t2: Zertifikat 1 wird gesperrt.
- Zeitpunkt t3: Es wird eine neue Deltasperrriste veröffentlicht, die nun das Zertifikat 1 enthält, da es nach Veröffentlichung der Basissperrriste gesperrt wurde.
- Zeitpunkt t4: Zertifikat 2 wird gesperrt.
- Zeitpunkt t5: Da das Veröffentlichungsintervall der Basissperrriste vier Zeiteinheiten beträgt und seit der Veröffentlichung der Basissperrriste vier Zeiteinheiten vergangen sind, wird nun eine neue Basissperrriste veröffentlicht. Diese enthält alle gesperrten Zertifikate, also im Vergleich zu der Basissperrriste von t1 nun zusätzlich noch die Zertifikate 1 und 2.
- Zeitpunkt t6: Seit der letzten Deltasperrristenveröffentlichung sind drei Zeiteinheiten vergangen, was zur Ausstellung einer neuen Deltasperrriste führt. Da im Zeitraum zwischen t5 und t6 kein Zertifikat gesperrt wurde, wird eine leere Deltasperrriste veröffentlicht.

Bekommt ein Zertifikat den Status „Zertifikat blockiert“, kann die Sperrung später aufgehoben werden. Wenn nach Aufhebung der Sperrung eine Deltasperrriste vor der Basissperrriste ausgestellt wird, wird das Zertifikat in der Delta CRL mit dem Sperrlistengrund „Aus Zertifikatsperrriste entfernen (8)“ aufgelistet. Da jedoch auch die Deltasperrriste nur in regelmäßigen Abständen veröffentlicht wird, ist der Status der gesperrten Zertifikate nicht aktuell. Deltasperrristen werden nicht von allen Programmen unterstützt, weswegen es Sinn machen kann, das Veröffentlichungsintervall der Basissperrriste zu verkürzen, um auf eine Deltasperrriste verzichten zu können. Veröffentlichungsintervalle und der Überschneidungszeitraum lassen sich analog zu der Basissperrriste in der Windows Registrierungsdatenbank anpassen.

Partitionierte Sperrlisten

Partitionierte Sperrlisten sind Sperrlisten, die in mehrere kleinere Sperrlisten aufgeteilt werden. Durch mehrere kleinere Sperrlisten sinkt die Zeit der Zertifikatsstatusüberprüfung, da nur die relevante Sperrliste betrachtet wird und diese weniger Einträge enthält, als eine einzige große CRL. Eine Möglichkeit, Sperrlisten zu partitionieren, ist die Erneuerung des CA Schlüsselpaares. Bei einer Erneuerung des CA Schlüsselpaares wird für das neue Schlüsselpaar eine neue CRL erstellt, die keine Einträge des alten Schlüsselpaares enthält. Werden

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

nun Zertifikate gesperrt, die von dem neuen privaten Schlüssel ausgestellt wurden, erscheinen diese nur in der CRL des neuen Schlüsselpaares. Wenn Zertifikate, die mit dem alten privaten Schlüssel ausgestellt wurden, gesperrt werden, so werden diese nicht in die CRL des neuen Schlüsselpaares eingetragen, sondern in die CRL des alten Schlüsselpaares. [DC04] Eine CA muss für alle jemals benutzten und noch gültigen privaten Schlüsseln in den konfigurierten Erneuerungsintervallen Basissperrlisten und ggf. Deltasperrlisten erstellen.

Sperrlistenenerweiterung Issuing Distribution Point (IDP)

Enthalten CRLs die Issuing Distribution Point (IDP) Erweiterung, handelt es ebenfalls sich um partitionierte Sperrlisten. In dieser Erweiterung wird spezifiziert, ob die Sperrliste nur gesperrte Zertifizierungsstellenzertifikate oder nur gesperrte Endzertifikate (dies sind alle Nicht-Zertifizierungsstellenzertifikate) oder nur gesperrte Zertifikate, die den gleichen Sperrgrund haben, enthält. Dies bewirkt eine Aufteilung einer großen CRL in mehrere kleine CRLs. Nicht alle Anwendungen unterstützen durch IDP partitionierte Sperrlisten.

2.2.1.3. Sperrlistenverteilungspunkte (CDP)

In den Sperrlistenverteilungspunkten (CRL Distribution Point, CDP) wird die Reihenfolge der Orte festgelegt, an denen eine Zertifikatüberprüfung mit Hilfe der CRL stattfindet bzw. die CRL heruntergeladen werden kann. Diese Orte werden auch Publikationspunkte genannt. Folgende Veröffentlichungsprotokolle werden unterstützt:

- File: Mit dem Server Message Block (SMB) und dem Common Internet File System (CIFS) stehen zwei Netzwerkprotokolle für den Dateizugriff auf einen Server zur Verfügung. Diese beiden Protokolle werden von allen Windows Betriebssystemen und von vielen Unix/Linux Betriebssystemen unterstützt.
- FTP: Mit dem File Transfer Protocol steht ein weiteres Netzwerkprotokoll für den Zugriff auf einen Server zur Verfügung. Nahezu alle Computer sind FTP kompatibel.
- HTTP: Das Hypertext Transfer Protocol wird von nahezu allen Geräten unterstützt und erlaubt, die Sperrliste von einem Webserver herunterzuladen. Das Gerät braucht lediglich Zugang zum Internet und dem Webserver, um die Sperrliste herunterzuladen. Eine Absicherung des Webserver per SSL ist nicht nötig, da die Sperrliste eine digital signierte Datei ist und somit nicht auf geschützte Transportwege angewiesen ist. Eine Absicherung per SSL kann auch zu einem Henne-Ei-Problem führen, da das Gerät, das auf den Webserver zugreift, zur Überprüfung des Webserver-Zertifikats eine aktuelle Sperrliste benötigt. Sollte die eigene Sperrliste jedoch abgelaufen sein, kann das Gerät unter Umständen keine neue Sperrliste herunterladen, da es das SSL Zertifikat des Webserver nicht überprüfen und somit die Verbindung nicht aufbauen kann.
- LDAP: Das Lightweight Directory Access Protocol ist ein Netzwerkprotokoll für den Zugriff auf einen Verzeichnisdienst, z. B. das Microsoft Active Directory. In einer Domäne werden die CRLs in der Active Directory-Datenbank auf den Domänencontrollern abgelegt und sind so für Clients mit Zugriff auf einen Domänencontroller per LDAP schnell erreichbar. [Bod13]

In den Sperrlistenverteilungspunkten wird eine Reihenfolge angegeben. Kann von dem ersten Sperrlistenverteilungspunkt keine CRL abgerufen werden, wird mit dem nächsten

Sperrlistenverteilungspunkt fortzuführen. Da die Sperrlistenverteilungspunkte in der CA konfiguriert sind und in die ausgestellten Zertifikate geschrieben werden, ist eine nachträgliche Änderung möglicherweise kompliziert. Es empfiehlt sich daher entweder einen Teil der alten CDP Infrastruktur stehen zu lassen oder eine neue CDP Infrastruktur zu konfigurieren und danach alle Zertifikate neu auszustellen.

2.2.1.4. Authority Information Access (AIA)

In der Zertifikaterweiterung Zugriff auf Stelleninformationen (Authority Information Access, AIA) stehen die Pfade für das Abrufen der Zertifizierungsstellenzertifikate. Es werden die gleichen Veröffentlichungsprotokolle unterstützt wie bei den Sperrlistenverteilungspunkten und auch das Abarbeiten der Reihenfolge ist identisch. Allerdings wird hier keine CRL sondern das CA Zertifikat heruntergeladen. Obwohl die Reihenfolge der Publikationspunkte des AIA und des CDP nicht identisch sein müssen, werden sie meistens identisch gewählt, da die Zertifikate oftmals auf den gleichen Servern und unter den gleichen Adressen wie die CRLs verfügbar gemacht werden.

Auch bei den AIA ist eine nachträgliche Änderung möglicherweise kompliziert und verläuft analog zu der nachträglichen Änderung des CDP.

2.2.1.5. Subject Alternative Names (SANs)

Der Alternative Antragstellernamen (Subject Alternative Name, SAN) ist eine Zertifikaterweiterung, die es ermöglicht erweiterte Informationen zu dem Antragsteller anzugeben, z. B. die IP-Adresse, eine E-Mail-Adresse, mehrere DNS oder URLs. Während alte Programme teilweise keine SANs unterstützen, gibt es aktuelle Programme, wie z. B. der Browser Google Chrome, der ab Version 58 vor Zertifikaten warnt, die keine SANs enthalten [Med17]. Ein Beispiel eines Zertifikats, das SANs enthält ist in Abbildung 2.9 zu sehen.

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

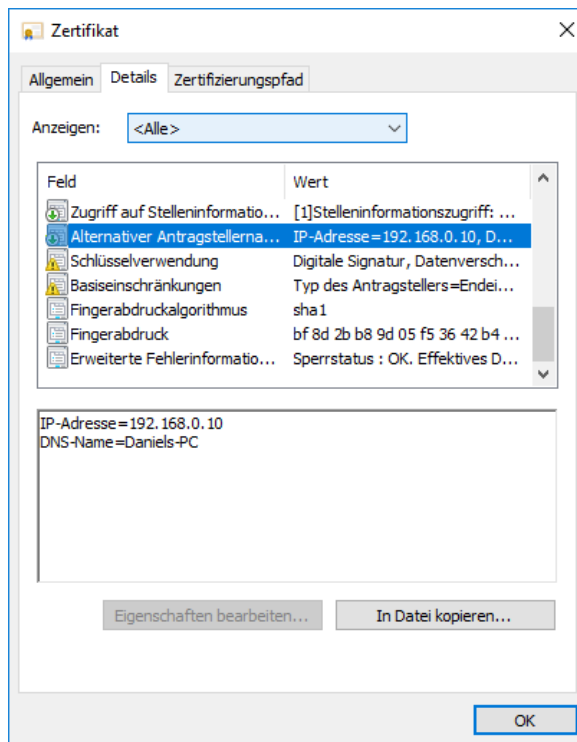


Abbildung 2.9.: Zertifikat mit angegebenen SANs

2.2.1.6. Microsoft Internet Information Services (IIS)

Die Internetinformationsdienste (Internet Information Services, IIS) sind ein Microsoft Webserverdienst, der es erlaubt, mehrere Microsoft Dienste online anzubinden. Unter anderem kann die Zertifizierungsstellen-Webregistrierung eingebunden werden, was es ermöglicht, das Zertifizierungsstellenzertifikat, die Zertifikatkette und die Basisperlliste herunterzuladen sowie Zertifikate anzufordern. Damit Zertifikate angefordert werden können, müssen entsprechend konfigurierte Zertifikatvorlagen veröffentlicht werden. Die Zertifikatanforderung benötigt eine Autorisierungsüberprüfung, weshalb die Webseite nur über HTTPS erreichbar und mit einem SSL Zertifikat abgesichert sein sollte. Über den IIS wird ebenfalls der OCSP Responder, welcher in Kapitel 2.2.1.7 beschrieben wird, online verfügbar gemacht. Um die Zertifizierungsstellen-Webregistrierung mit dem IIS nutzen zu können, darf der Signatur-Hash-Algorithmus maximal SHA-256 sein.

Wenn die Zertifizierungsstellen-Webregistrierung über das Internet erreichbar sein soll, sollte dieser Dienst auf einen anderen Computer ausgelagert werden, um die CA nicht von außen zugänglich machen zu müssen.

2.2.1.7. Online Certificate Status Protocol (OCSP)

Das Online Certificate Status Protocol (OCSP) dient dazu, den Status von Zertifikaten abzufragen. Hierfür wird der Dienst auf einem Server, dem sogenannten OCSP Responder oder auch Online-Responder, installiert. Dies kann entweder direkt auf der CA erfolgen oder auf einem anderen Server. Möchte man den OCSP Responder über das Internet erreichbar ma-

chen, ist es empfehlenswert, ihn auf einen separaten Server auszulagern, um die CA nicht über das Internet erreichbar machen zu müssen. Sollte man den Schutz noch weiter erhöhen wollen, kann man den IIS des OCSP Responders auch noch auslagern, so dass man den OCSP Responder nicht über das Internet ansprechbar machen muss.

Kontaktiert ein Client den OCSP Responder, schickt er ihm per HTTP eine Zertifikatsanforderung. Daraufhin kontaktiert der OCSP Responder entweder die CA und schaut in ihrer Zertifikatsdatenbank nach oder greift auf eine CRL zurück, ermittelt dort den Zertifikatsstatus und schickt einen von ihm signierten Zertifikatsstatus an den Client zurück. Greift der OCSP Responder direkt auf die CA zu, ist der an den Client zurückgeschickte Zertifikatsstatus immer aktuell und nicht, wie bei einer CRL, möglicherweise veraltet. [Mic13a] Microsoft Online-Responder beziehen ihre Sperrinformationen immer von einer CRL und können die Datenbank einer CA nicht direkt ansprechen [Mic09c]. Hat der OCSP Responder eine Anfrage zu einem Zertifikatsstatus erhalten, speichert er diese Information in seinem Cache, um bei der nächsten Zertifikatsstatusanfrage für dieses Zertifikat schneller die Antwort zurücksenden zu können. Beachtet werden muss, dass nicht alle Programme den OCSP Dienst unterstützen.

Der OCSP Responder wird als HTTP URL in den AIA Erweiterungen der CA aufgelistet, jedoch nicht in den AIA Erweiterungen des Zertifikats einbezogen, sondern in den OCSP-Erweiterungen einbezogen. Siehe Bild in Schritt Nr. 80 der Implementierungsdokumentation.

2.2.1.8. Sperrlisten Webserver

Um eine Ausfallsicherheit des OCSP Responders zu gewährleisten und um Probleme mit Programmen zu vermeiden, die keinen OCSP Dienst benutzen, ist es sinnvoll, die CRL auf einem Webserver bereitzustellen. Einen direkten Zugriff auf die CA durch den Webserver sollte vermieden werden, da dies die Sicherheit der CA, bei einem kompromittierten Webserver, schwächen könnte. Um dies zu vermeiden, kann entweder direkt von der CA die CRL weiterkopiert oder die CA so konfiguriert werden, dass sie die CRL zusätzlich auf einen zweiten Speicherort, z. B. einem Netzwerkordner, veröffentlicht. Von dort kann dann der Webserver die CRL einbinden.

2.2.1.9. Network Device Enrollment Service (NDES)

Der Registrierungsdienst für Netzwerkgeräte (Network Device Enrollment Service, NDES) ist ein Dienst, der eine Zertifikatsregistrierungsanfrage an eine Zertifizierungsstelle weiterleitet und das dann erstellte Zertifikat an den Sender der Anfrage zurück übermittelt.

Für den NDES wird das Simple Certificate Enrollment Protocol (SCEP) benutzt, welches zur sicheren und skalierbaren Ausstellung von Zertifikaten an Netzwerkgeräte verwendet wird. Zu beachten ist, dass KSP Kryptografieanbieter bei NDES nicht unterstützt werden und daher der CSP verwendet werden muss [Mic16b].

Der NDES funktioniert wie folgt: Der Administrator meldet sich auf der Webseite `https://<Servername>/CertSrv/mscep_admin/` des NDES an. Der NDES kontaktiert einen Domain Controller, der die Anmeldedaten und die Berechtigungen des Administrators auf den vorhandenen Zertifikatsvorlagen überprüft. Bei Erfolg wird ihm auf der Webseite ein

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

60 Minuten gültiges Registrierungskennwort angezeigt, siehe Abbildung 2.10. Das Registrierungskennwort muss der Administrator an das Netzwerkgerät übermitteln, damit dieses eine Zertifikatanfrage an die Webseite `https://<Servername>/CertSrv/mscep` des NDES schicken kann. Der NDES signiert diese Anfrage mit seinem Zertifikat und schickt sie an die CA, welche das Zertifikat des Netzwerkgerätes ausstellt. Anschließend schickt die CA das Zertifikat an den NDES, der es an das Netzwerkgerät schickt. [Mic18]

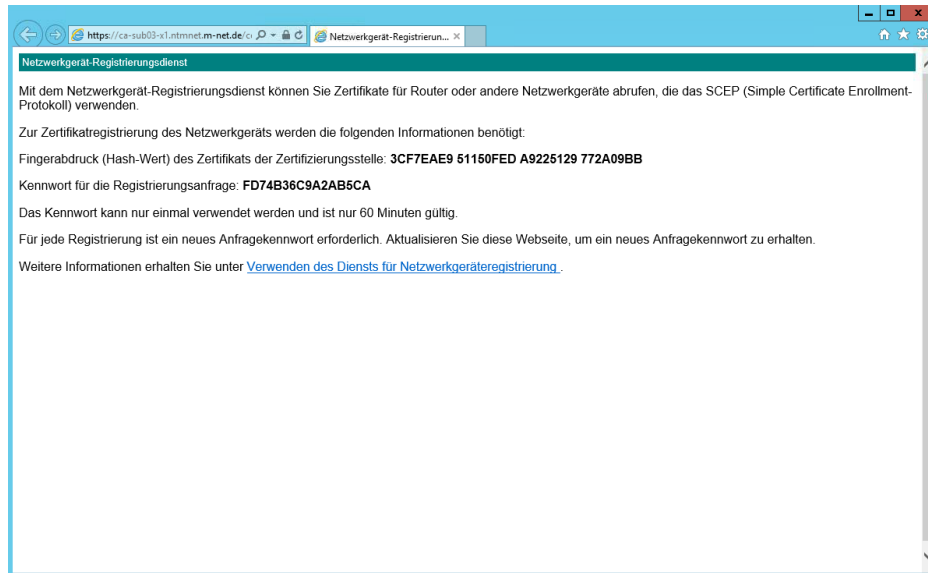


Abbildung 2.10.: NDES Administratorseite

Ein Netzwerkgerät kann dabei z. B. ein Handy sein. Statt dem Administrator wird oftmals ein Mobile Device Management Programm verwendet, das dessen Aufgaben automatisiert ausführt. Der Prozess der Zertifikatanforderung über NDES ist in Abbildung 2.11 dargestellt.

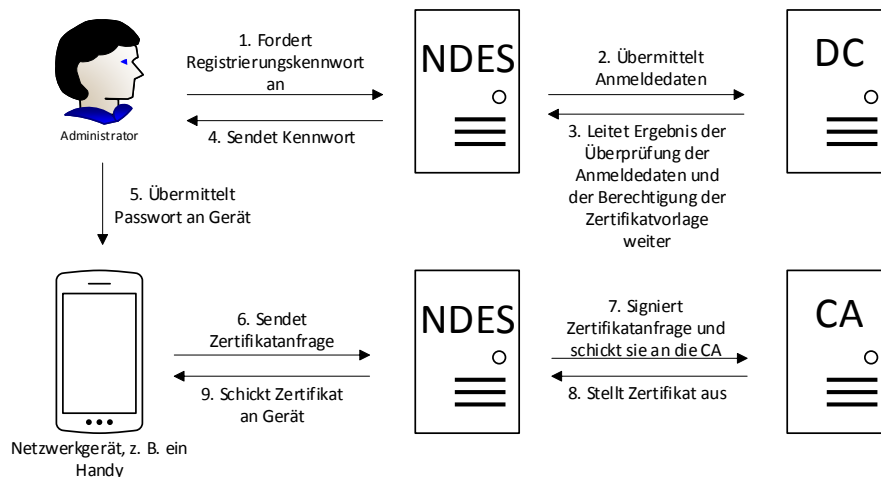


Abbildung 2.11.: Zertifikatanforderung über NDES

2.2.1.10. Datenbank und Log Files

Die CA legt eine Datenbank an, in der u. a. ausgestellte Zertifikate, fehlgeschlagene Zertifikatanforderungen oder gesperrte Zertifikate gespeichert werden. Diese Daten können z. B. auf einen Fileserver ausgelagert werden, um ein einfacheres Backup zu ermöglichen und um die Festplattenkapazität auf der CA nicht unnötig groß wählen zu müssen, da die Datenbank mit der Zeit durchaus in den mittleren zweistelligen Gigabyte Bereich anwachsen kann. Sollte die Datenbank mit der Zeit zu groß werden, kann mit dem Microsoft Kommandozeilenprogramm Certutil, welches standardmäßig auf allen Windows Server Betriebssystemen ab Windows Server 2003 installiert ist, die Datenbank wieder verkleinert werden. Dabei können dann weniger relevante Daten, z. B. fehlgeschlagene Zertifikatanforderungen oder abgelaufene Zertifikate, entfernt werden.

Ebenfalls werden, falls konfiguriert, von der CA Log Files angelegt, die Fehler und Aktionen der CA protokollieren. Diese können u. a. zur Fehlersuche benutzt werden oder mit einer Monitoring Software zum Überprüfen der Lauffähigkeit der CA verwendet werden. Die Log Files können ebenfalls ausgelagert werden, um z. B. eine Überprüfung zu erleichtern.

Ein Backup der Datenbank kann ebenfalls mit Hilfe von Certutil von der CA gemacht werden, wenn die Datenbank auf der CA verbleiben sollte. Ein regelmäßiges Backup der Datenbank ist notwendig, da bei einem Datenverlust der CA die kompletten Informationen über ausgestellte und gesperrte Zertifikate verloren gehen können. Alle Konfigurationen einer Windows CA werden in der Windows-Registrierungsdatenbank gespeichert, weshalb ein Backup der Konfiguration durch den Export der relevanten Windows-Registrierungsdatenbankschlüssel geschieht.

2.2.2. Hardware-Sicherheitsmodul (HSM)

Ein Hardware-Sicherheitsmodul (Hardware Security Module, HSM) ist ein Gerät, das dazu optimiert ist, kryptografische Operationen sicher und effizient auszuführen und Informationen verschlüsselt zu speichern.

Eine wichtige Funktion des HSMs ist die Generierung und Speicherung der privaten Schlüssel in der HSM, wodurch es einem Angreifer deutlich erschwert wird, den privaten Schlüssel zu manipulieren oder gar zu exportieren. Selbst bei einer Kompromittierung der CA gelangt der Angreifer nicht in den Besitz des privaten Schlüssels, da dieser nicht auf der CA liegt. Der sogenannte Key-in-Hardware-Ansatz erweitert dies, indem der private Schlüssel während des gesamten Key-Lebenszyklus in der HSM verbleibt, d. h. von der Generierung des Schlüsselpaares bis hin zu allen kryptografischen Operationen, die mit dem privaten Schlüssel geschehen. Das HSM wird dabei als eigener Kryptografieanbieter in das Betriebssystem eingebunden.

Da es viele verschiedene HSMs gibt, die sich hinsichtlich der angebotenen Funktionen unterscheiden, ist eine genaue Sondierung der gewünschten Fähigkeiten einer HSM notwendig. Beispielsweise unterstützen nicht alle HSMs den Key-in-Hardware-Ansatz, bei dem die Schlüssel in einem Trusted Layer bewegt werden, um z. B. eine Signierung durchzuführen. HSMs gibt es als PCI Karten, PCI-Express Karten, Smartcards, Serielle Karten, USB- oder

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

Netzwerkgeräte. Auch muss z. B. die Betriebssystemkompatibilität, die Unterstützung der zu verwendenden Algorithmen und die Geschwindigkeit des HSMs betrachtet werden. Die Geschwindigkeit wird dabei in Transaktionen pro Sekunde angegeben. Eine typische Angabe wären z. B. 350 Transaktionen pro Sekunde bei RSA-2048, d. h. es können z. B. 350 Signieroperationen pro Sekunde durchgeführt werden. Manche HSMs, wie die Gemalto Luna Network HSM 6 [Gemwn] oder die Cavium LiquidSecurity HSM CNL35XX [Cavwn] haben die Option Partitionen zu erstellen. Dies führt zu einer erhöhten Sicherheit, da jede Zertifizierungsstelle ihr Schlüsselpaar auf einer eigenen Partition speichern kann, auf die nur sie Zugriff hat. Bekannte Hersteller von HSMs sind z. B. Atos, Cavium, Gemalto, Thales oder Futurex.

Bei Verwendung eines HSMs, muss über ein Backup nachgedacht werden, da bei einem Defekt des HSMs der private Schlüssel verloren gehen könnte. Hierzu werden von Firmen wie Gemalto offline Backup Hardware-Sicherheitsmodule angeboten, welche nur den Zweck haben, ein Backup des HSMs zu erstellen, es ggf. wiederherzustellen und die Daten verschlüsselt zu speichern. Diese sind im Vergleich zu normalen HSMs oftmals günstiger.

Eine andere Möglichkeit für Redundanz zu sorgen, ist das Verwenden von mehreren HSMs mit identischem Inhalt. Hierbei gibt es bei manchen HSMs, wie z. B. den Gemalto Luna HSMs, die Möglichkeit, diese miteinander zu einem sogenannten High Availability-Cluster zu verbinden. Bei einem HA-Cluster wird das Schlüsselpaar auf jede der HSMs abgelegt, was zu einer erhöhten Ausfallsicherheit führt, da dadurch der Defekt einer HSM kompensiert wird. Als zweiter Effekt entsteht eine Leistungssteigerung, weil die kryptografischen Operationen auf beiden HSMs ausgeführt werden.

Im Fall der Gemalto Luna HSM werden die HSMs direkt an die Zertifizierungsstellen angebunden und haben keinen Kontakt untereinander. Abbildung 2.12 zeigt ein HSM, an das mehrere Zertifizierungsstellen angebunden sind, wobei jede CA eine eigene Partition verwendet, um dort ihren privaten Schlüssel zu speichern. Abbildung 2.13 zeigt eine Zertifizierungsstelle, die zwei HSMs als HA-Cluster konfiguriert hat.

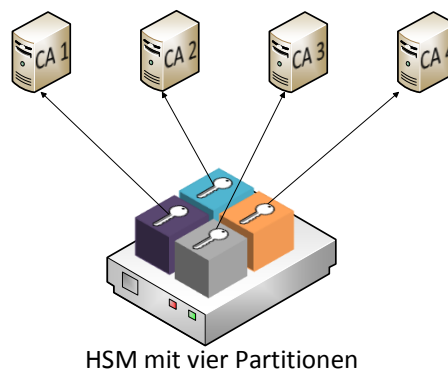


Abbildung 2.12.: HSM mit vier Partitionen, auf die jeweils eine CA zugreift

2.2. Funktionsweise einer Public Key Infrastruktur (PKI)

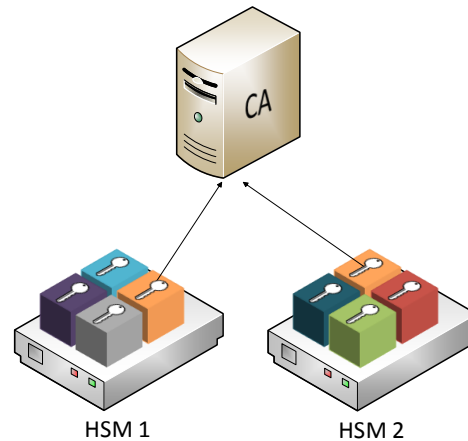


Abbildung 2.13.: Zertifizierungsstelle mit zwei angebundenen HSMs als HA-Cluster konfiguriert

2.2.3. Topologie einer Public Key Infrastruktur (PKI)

Eine einfache PKI besteht nur aus einer Zertifizierungsstelle, der Root CA, während komplexere PKIs aus mehreren Zertifizierungsstellen bestehen. Bei der streng hierarchischen PKI existieren mehrere Schichten in die die Zertifizierungsstellen eingeordnet werden. Die Zertifizierungsstelle der obersten Schicht wird Root CA, Wurzel- oder Stammzertifizierungsstelle genannt. In der Schicht darunter befinden sich untergeordnete Zertifizierungsstellen bzw. Zwischenzertifizierungsstellen, auch Intermediate CAs oder Sub CAs genannt. Eine Zwischenzertifizierungsstelle ist eine untergeordnete Zertifizierungsstelle, die eine oder mehrere ihrer untergeordnete Zertifizierungsstellen kontrolliert, welche als ausstellende Zertifizierungsstellen fungieren.

In einer Zertifikatkette, siehe Abbildung 2.14, fungiert die Root CA als höchster Bezugspunkt, während die untergeordneten CAs, die an der Erstellung des Zertifikats beteiligt sind und darunter aufgelistet werden. Im konkreten Fall bedeutet dies bei der Abbildung 2.14, dass die M-net-Root-X1 die Wurzelzertifizierungsstelle und die M-net-Sub-Intern-01 eine untergeordnete Zertifizierungsstelle ist, die das Zertifikat für den Computer NBMUC559 ausgestellt hat.

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

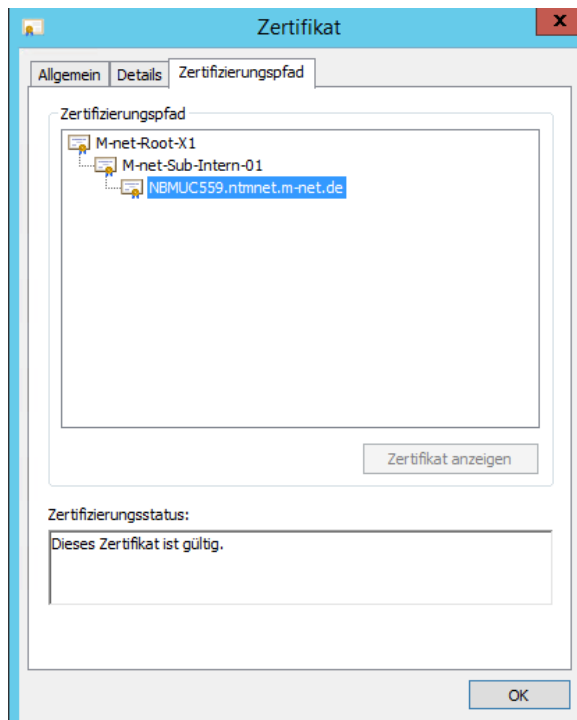


Abbildung 2.14.: Zertifikatkette

Durch diese Struktur ist eine hohe Skalierbarkeit und erweiterte Sicherheit garantiert, da nicht ausstellende Zertifizierungsstellen offline genommen werden können und so schwerer angreifbar sind. Aus diesem Grund ist bei Verwendung einer hierarchischen Struktur die Root CA oftmals offline. Als weiterer Vorteil kann die Zuteilung verschiedener Verwaltungsaufgaben an bestimmte CAs erfolgen, z. B. die Verwaltung von Benutzerzertifikaten nur durch eine CA, während eine andere CA alle Serverzertifikate verwaltet.

Besteht eine PKI aus mehreren untergeordneten Zertifizierungsstellen, wird sie mehrschichtige oder mehrstufige PKI genannt. Eine zweistufige PKI besteht also aus einer Root CA und mindestens einer Sub CA, während bei einer dreistufigen PKI zusätzlich noch mindestens eine der Sub CAs eine weitere, ihr untergeordnete CA hat. Dies ist in Abbildung 2.15 dargestellt.

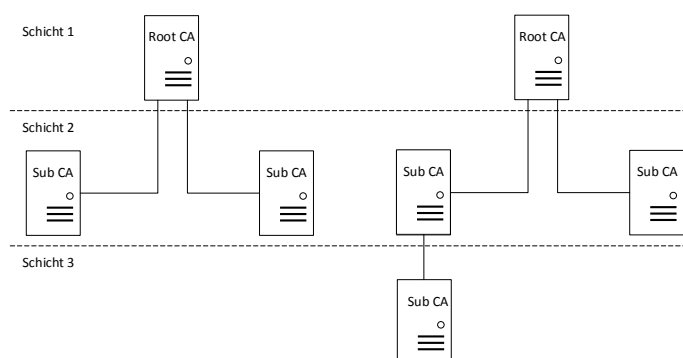


Abbildung 2.15.: Mehrstufige PKI; links eine zweistufige PKI, rechts eine dreistufige PKI

2.2. Funktionsweise einer Public Key Infrastruktur (PKI)

Sollte in einer mehrstufigen PKI eine Sub CA oder ihr privater Schlüssel kompromittiert worden sein, kann in der Root CA das Zertifikat der kompromittierten Sub CA gesperrt werden, womit dann alle von dieser Sub CA ausgestellten Zertifikate ungültig werden. Sollten mehrere Sub CAs im Einsatz sein, ist der restliche Betrieb der anderen Sub CAs und deren bereits ausgestellten Zertifikatsempfängern ohne weitere Einschränkung gegeben. Je weniger Zertifikate eine Zertifizierungsstelle ausstellt, desto weniger Zertifikate werden bei einer Sperrung dieser Zertifizierungsstelle ungültig.

Sollte jedoch keine mehrstufige PKI existieren und somit die einzige vorhandene CA oder ihr vorhandener privater Schlüssel kompromittiert werden, wird das Vertrauen in die komplette PKI zerstört, da es keine übergeordnete Instanz über der Root CA gibt, die das Zertifikat der Root CA sperren könnte. Dann müssen alle Zertifikate der PKI neu ausgestellt werden, statt nur die Zertifikate der kompromittierten CA.

Aufbauend auf einer hierarchischen PKI kann diese zu einer Kreuzzertifizierungs-PKI ausgebaut werden. Dabei werden zwei vorhandene Zertifizierungsstellen, die keine gemeinsame übergeordnete Zertifizierungsstelle haben, miteinander kreuzzertifiziert und stellen so ein Vertrauensverhältnis her. In Abbildung 2.16 ist eine PKI von Unternehmen A und eine PKI von Unternehmen B abgebildet.

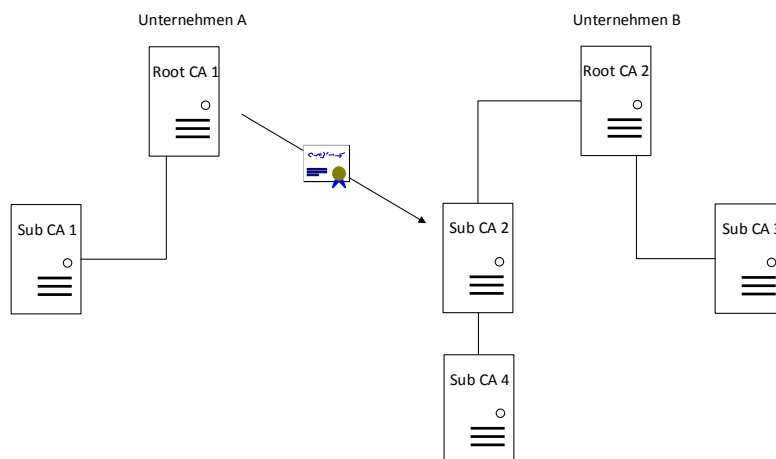


Abbildung 2.16.: Kreuzzertifizierung

Wenn nun die Root CA 1 von Unternehmen A der Sub CA 2 von Unternehmen B ein Kreuzzertifizierungsstellenzertifikat ausstellt, bewirkt dies, dass alle Inhaber, die von der Sub CA 2 ein Zertifikat ausgestellt bekommen haben, der Root CA 1 von Unternehmen A vertrauen. Die Sub CA 2 wirkt für diese Geräte dann wie eine untergeordnete Zertifizierungsstelle von der Root CA 1. [Kom08] Dies wird z. B. bei einer Firmenfusion angewandt, wenn beide Firmen bereits eine eigene PKI in Betrieb haben, die sie nicht verändern wollen. Eine Neuausstellung bereits ausgestellter Zertifikate ist hierbei nicht nötig.

2.2.3.1. Zertifikatkette

Ist eine Zertifikatkette wie in Abbildung 2.14 gegeben, überprüft der Client diese vom untersten Zertifikat bis zum Root CA Zertifikat. Der Client schaut nach, ob in seinem lokalen

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

Zertifikatspeicher die Zertifikate enthalten sind und lädt sie, wenn sie nicht vorhanden sind, von einem der Standorte der Stelleninformationen des Zertifikats herunter. Nun werden alle Zertifikate überprüft, ob die Signatur und der Gültigkeitsbereich valide ist und ob die Zertifikate gesperrt, beschädigt oder fehlerhaft sind. Der Sperrstatus der Zertifikate wird über die Standorte der Sperrlisten-Verteilungspunkte der Zertifikate überprüft.

Eine Überprüfung der Zertifikatkette wird allerdings nicht von allen Programmen unterstützt und umgesetzt. Diese überprüfen dann oftmals nur das unterste Zertifikat. Eine zu hohe Schlüssellänge einer Zertifizierungsstelle kann bei der Überprüfung der Zertifikatkette auch zu Problemen führen. Unterstützt ein Programm z. B. nur eine maximale Schlüssellänge von 4096 Bit, wobei die Zertifizierungsstelle einen 8192 Bit Schlüssel hat, so kann dieses Zertifikat unter Umständen nicht überprüft werden. Dies verhindert somit eine Überprüfung der kompletten Kette und führt zu einer Einstufung des Zertifikats als ungültig.

2.2.3.2. Offline Zertifizierungsstellen

Ist eine mehrstufige PKI im Einsatz, empfiehlt es sich die Root CA offline zu nehmen, um ihren Schutz vor Netzwerkangriffen zu erhöhen. Sollte die Root CA kompromittiert oder gar ihr privater Schlüssel entwendet werden, wird das Vertrauen in die komplette PKI zerstört, da es keine übergeordnete Instanz gibt, die das Zertifikat sperren könnte. Bei einer großen, mehrstufigen PKI kann es auch vorkommen, dass mehrere untergeordnete Zertifizierungsstellen offline genommen werden.

Eine Offline Root CA muss dann nur für folgende Operationen kurzzeitig in Betrieb genommen werden:

- Verlängern des eigenen Zertifikats
- Widerrufen des eigenen Zertifikats
- Veröffentlichen der Zertifikatssperrliste
- Ausstellen von untergeordneten Zertifizierungsstellenzertifikaten
- Verlängern von untergeordneten Zertifizierungsstellenzertifikaten
- Widerrufen von untergeordneten Zertifizierungsstellenzertifikaten

Sollte es sich nicht um eine Root CA handeln, entfällt der Punkt „Widerrufen des eigenen Zertifikats“, da dies dann von der ihr übergeordneten Zertifizierungsstelle aus erfolgt.

Je nachdem wie die Laufzeiten der Zertifikate und der Sperrliste der Zertifizierungsstellen gewählt werden, kann es sein, dass eine offline CA mehrere Jahre nicht in Betrieb genommen werden muss.

Es gibt mehrere Möglichkeiten, eine CA offline zu lagern. Hierbei muss zuerst unterschieden werden, ob der private Schlüssel der CA zusammen mit der Zertifizierungsstelle gesichert werden soll oder nicht. Auch gibt es verschiedene Möglichkeiten, die Zertifizierungsstelle zu sichern.

2.2. Funktionsweise einer Public Key Infrastruktur (PKI)

Eine minimale Sicherung besteht aus dem privaten Schlüssel, der Datenbank und der Konfiguration der Zertifizierungsstelle. Da die offline Zertifizierungsstelle idealerweise nur Zertifikate für ihr direkt untergeordnete Zertifizierungsstellen ausstellt, ist die Datenbank nur mehrere Megabyte groß. Daraus resultiert bei einer minimalen Sicherung eine zu sichernde Datengröße von unter einem Gigabyte. Nach der Sicherung kann die Zertifizierungsstelle von dem Computer deinstalliert werden. Zur Wiederinbetriebnahme ist es nötig, einen PC mit einer Zertifizierungsstelle neu aufzusetzen und die gesicherte Konfiguration, die Datenbank und den privaten Schlüssel dort einzuspielen. Bei Verwendung eines HSMs mit Backuplösung, wie in Kapitel 2.2.2 beschrieben, muss nur die Datenbank und die Konfiguration der Zertifizierungsstelle gesichert werden, da der private Schlüssel in der HSM liegt. Um den Schutz des privaten Schlüssels der offline Zertifizierungsstelle weiter zu erhöhen, kann auch das HSM offline genommen werden.

Es besteht allerdings auch die Möglichkeit, die Zertifizierungsstelle nicht zu deinstallieren, sondern diese auf dem Computer zu belassen, da durch den Export des privaten Schlüssels dieser im Anschluss von der Maschine gelöscht werden kann und die Zertifizierungsstelle ohne privaten Schlüssel funktionslos ist. Dasselbe gilt bei der Verwendung eines HSMs, denn ist der Kontakt zu dem HSM unterbunden, so ist die Zertifizierungsstelle ebenfalls funktionslos. Dennoch sollte der Zugriff auf die Zertifizierungsstelle abgesichert werden, da bei einer Wiederinbetriebnahme ein nicht kompromittierter Zustand der Maschine gegeben sein muss. Dies hat den Vorteil, dass eine Wiederinbetriebnahme schneller erfolgen kann, als eine komplette Neuinstallation der Zertifizierungsstelle. Das ist ein wichtiger Punkt, da z. B. das Sperren eines Zertifizierungsstellenzertifikats eine zeitkritische Aktion ist.

Wenn die Zertifizierungsstelle eine virtuelle Maschine ist, d. h. das sie in einer virtualisierten Umgebung ohne eigene physische Hardware läuft, lässt sich die CA auf ein externes Medium, z. B. einen USB Stick, verschieben, der dann beispielsweise in einen Tresor gesperrt wird. Ist die CA auf einem physischen Gerät, wie z. B. einem PC installiert, kann das Gerät heruntergefahren und weggesperrt werden.

Sollen die Datenbank und die Konfiguration oder gar der private Schlüssel exportiert werden, muss der Zugriff auf diese Dateien eingeschränkt und die Dateien idealerweise verschlüsselt werden. Die Verschlüsselung des privaten Schlüssels sollte so gewählt werden, dass angenommen werden kann, dass die Verschlüsselung nicht vor Ablauf der Gültigkeitsdauer des Zertifizierungsstellenzertifikats ausgehebelt wird.

Als Aufbewahrungsmedien bieten sich z. B. Magnetbänder, USB Sticks, optische Medien, Hardware-Sicherheitsmodule oder ein Fileserver an.

Magnetbänder bieten eine hohe Lebensdauer, teilweise über 30 Jahre und eine Unempfindlichkeit gegenüber Stößen und Stürzen. Nachteile sind Empfindlichkeiten gegen Staub, Feuchtigkeit, magnetische Felder und teilweise Temperatur. Fujifilm setzt bei seinen LTO Ultrium 1 - 5 Magnetbändern für das Erreichen der über 30-jährigen Lebensdauer eine Lagertemperatur zwischen 16° und 25° Celsius voraus [Fujwn]. Ebenfalls nachteilig sind lange Zugriffszeiten, da ggf. erst zu einer bestimmten Stelle des Bandes gespult werden muss und das notwendige Vorhandensein eines Bandlaufwerks und dessen Software [Wik18].

2. Allgemeine Erklärung einer Public Key Infrastruktur (PKI)

Als USB Stick eignet sich z. B. der SanDisk Memory Vault, der laut Herstellerangaben Daten für bis zu 100 Jahre sicher aufbewahrt [San11].

Die meisten Optischen Medien sind anfällig gegenüber Kratzern, Licht, Temperatur und Feuchtigkeit [ct08]. Von Verbatim sind die Archival Grade Gold DVD-R [Verwna] und Archival Grade Gold CD-R [Verwnb] erhältlich, die laut Hersteller für eine Archivierungszeit von 100 Jahren ausgelegt sind und einen erhöhten Schutz gegenüber Kratzern und Korrosion haben. Die Verbatim MDISC ist mit einer durchschnittlichen Speicherzeit von 1000 Jahren angegeben. Dabei werden die Daten in eine steinähnliche Speicherschicht eingraviert, welche laut Hersteller wärme- und lichtbeständig ist [Verwnc].

Gemalto gibt für die Lesbarkeit der Daten der Safenet Hardware-Sicherheitsmodule bei einer konservativen worst-case Schätzung eine Lebensdauer von 20 Jahren an. Voraussetzung ist ein Temperaturbereich im Betrieb zwischen 0° Celsius und +40° Celsius bzw. ein Temperaturbereich zwischen -20° Celsius und +65° Celsius bei der Lagerung. [Gem15a]

Die Dateien auf einen Dateiserver abzulegen, ggf. zu verschlüsseln und die Zugriffsberechtigungen darauf einzuschränken, ist eine der komfortabelsten Methoden. Es erleichtert das Erstellen eines Backups und ermöglicht einen schnellen Zugriff auf die Daten. Jedoch ist dies weniger sicher als ein, z. B. in einem Tresor abgesperartes Speichermedium, auf dem die Dateien verschlüsselt abgespeichert sind.

Bei der Wahl des Speichermediums und der ggf. eingesetzten Verschlüsselung muss auch darauf geachtet werden, ob die Verfügbarkeit der Technologie in der Zukunft noch gegeben sein wird.

2.2.3.3. CA Clustering

Bei einem Ausfall einer CA ist das Ausstellen von Zertifikaten oder Sperrlisten dieser CA nicht mehr möglich. Dies sollte theoretisch keine schwerwiegenden Probleme nach sich ziehen, da Zertifikate deutlich vor dem Ablaufdatum erneuert werden sollten.

Wenn keine neue CRL ausgestellt werden kann und die Gültigkeit der Sperrliste abgelaufen ist, schlägt die Überprüfung der Zertifikatkette fehl. Dadurch wird die Nutzbarkeit aller von dieser CA ausgestellten Zertifikate eingeschränkt, da diese als ungültig betrachtet werden. Das ist somit das größte Problem, was durch das CA Clustern verhindert werden kann. Es gibt allerdings auch Programme, die eine abgelaufene Sperrliste ignorieren und diese als gültig betrachten.

CA Clustern geschieht dabei durch einen Aktiv/Passiv Cluster, d. h. es ist immer nur eine Zertifizierungsstelle aktiv. Wenn die aktive CA eine Funktionsstörung hat, wird die bis dahin passive CA aktiv geschaltet um den Betrieb aufrecht zu erhalten. [Kom08]

Diese Technik wird u. a. von Microsoft Windows Server 2012 unterstützt. Das CA Clustern unterstützt weder einen OCSP Responder noch den NDES. Des Weiteren wird von Microsoft empfohlen, die Zertifizierungsstellen-Webregistrierung nicht auf einem Computer laufen zu lassen, der Teil des Clusters ist. [Mic15]

2.2.4. Gültigkeitsdauer Zertifikate

Die Gültigkeitsdauer von Zertifikaten sollte so gewählt werden, dass diese nicht länger als die voraussichtliche Zeit beträgt, in der das Zertifikat entschlüsselt werden kann. Das Certification Authority and Browser (CA/Browser) Forum, zu dem u. a. Apple, Cisco, Digi-Cert, Entrust, GlobalSign, Google und Microsoft gehören, veröffentlicht Branchenrichtlinien für IT-Sicherheit und Zertifizierungsstellen [cab17]. Das CA/Browser Forum empfiehlt für Zertifizierungsstellenzertifikate und Teilnehmerzertifikate eine Verwendung von mindestens SHA-256 mit einer Länge von 2048 Bit bei RSA. Für Teilnehmerzertifikate wird außerdem eine maximale Gültigkeit von 39 Monaten empfohlen. [CA/14]

Zu beachten ist auch, dass eine CA nur Zertifikate mit einer maximalen Gültigkeitsdauer bis zu ihrer eigenen Restlaufzeit ausstellen kann. D. h. beträgt die Restlaufzeit des Zertifizierungsstellenzertifikats 32 Monate, kann die maximale Gültigkeitsdauer der auszustellenden Zertifikate maximal 32 Monate betragen.

Für eine erleichterte Administration und um Einschränkungen bei der Ausstellung von Zertifikaten zu vermeiden, empfiehlt es sich jedes Zertifikat einer Zertifizierungsstelle nach der Hälfte der Laufzeit um die ursprüngliche Gültigkeitsdauer zu verlängern. Dadurch wird sichergestellt, dass die CA bis zum Ende der ursprünglichen Gültigkeitsdauer noch alle Zertifikate mit der gewünschten Gültigkeitsdauer ausstellen kann und diese nicht durch die maximale Gültigkeitsdauer der CA beschränkt wird. Um die Entschlüsselung zu verhindern, sollte nach Ablauf der ursprünglichen Gültigkeitsdauer das Zertifizierungsstellenzertifikat erneuert werden.

2.3. Zusammenfassung

In Kapitel 2.1 werden die notwendigen Grundlagen der Verschlüsselung erläutert. Hierzu wird auf die symmetrische und asymmetrische Verschlüsselung eingegangen und die Funktionsweise des Hash- und Signatur-Algorithmus sowie der Kryptografieanbieter erklärt. Die Funktionsweise einer PKI und ihrer einzelnen Bestandteile beschreibt Kapitel 2.2. Konkret wird hierbei auf die Zertifizierungsstelle und einige ihrer Komponenten eingegangen, z. B. Zertifikatvorlagen, Sperrlisten, der NDES und die Zertifikaterweiterungen CDP und AIA. Im nächsten Kapitel werden die Anforderungen der M-net Telekommunikations GmbH an die PKI und das Konzept zur Umsetzung vorgestellt.

3. Konzept

In diesem Kapitel wird das Designkonzept der zu implementierenden Public Key Infrastruktur bei der M-net Telekommunikations GmbH, im Folgenden nur M-net genannt, erläutert. Dabei wird auf die Anforderungen von M-net an die PKI eingegangen und anschließend das daraus resultierende Konzept beschrieben.

3.1. Anforderung M-net an die Public Key Infrastruktur (PKI)

Die PKI soll bei M-net primär als Sicherheitskonzept für Client- und Serverauthentifizierung eingesetzt werden. Die dazu notwendigen Anforderungen der Firma M-net an die PKI wurden in Workshops mit ca. 10 Teilnehmern am 21.03.2017 und 27.03.2017 erörtert und sind nachfolgend aufgelistet:

| | |
|-------------------------------|--|
| Ausbaumöglichkeiten | Ausbaumöglichkeit der PKI für u. a. eine sicherere WLAN Authentifizierung und die Authentifizierung von VPN Zugängen. Auch für weitere, eventuell später kommende Anforderungen wie z. B. E-Mail- oder Dateiverschlüsselung soll die PKI eingesetzt werden können. |
| Betriebssysteme | Da die PKI bei M-net von zwei Abteilungen administriert wird, wovon die eine Windows Zertifizierungsstellen einsetzt und die andere auf Unix und Linux basierende Zertifizierungsstellen setzt, muss als Anforderung eine Kompatibilität mit mehreren Betriebssystemen gegeben sein. |
| Ausstellbarkeit | Ausstellbarkeit von Zertifikaten für Windows, Linux und Unix PCs. Die Windows Computer befinden sich dabei entweder in einer von zwei Domänen oder sind autark. |
| MDM | Ausstellbarkeit von Zertifikaten für das Mobile Device Management über den MobileIron Dienst. |
| Zertifikattypen | Durch die unterschiedlichen Anforderungen an die PKI müssen verschiedene Zertifikattypen wie z. B. SSL oder Serverauthentifizierung ausgestellt werden können, die auch Subject Alternative Names unterstützen. |
| Netzwerkcompatibilität | Netzwerkcompatibilität zu der bei M-net vorhanden Netzwerkstruktur, in welcher mehrere VLANs und durch Firewalls getrennte Netzwerkbereiche vorhanden sind. |

3. Konzept

| | |
|------------------------------|---|
| Schlüssellänge | Durch die sehr heterogene Client-Landschaft, die verschiedene Programme, Betriebssysteme und Computer umfasst, welche teilweise auch nicht aktuell sind, ist auf eine hohe Kompatibilität, insbesondere auf die der Schlüssellänge, zu achten. |
| Zertifikatanforderung | Da mit der Standardkonfiguration einer Windows Zertifizierungsstelle nur Windows Maschinen, die Mitglied einer Domäne sind, automatisch Zertifikate anfordern können, muss zusätzlich eine Möglichkeit zur einfachen Zertifikatanforderung und -erstellung implementiert werden. |
| Zertifikatstatus | Es muss sichergestellt werden, dass der Zertifikatstatus für die sehr heterogene Client-Landschaft überprüfbar ist. Da nur Windows Computer einer Domäne einen Zertifikatstatus über das Active Directory überprüfen können, wird für die übrigen PCs eine Möglichkeit benötigt, den aktuellen Status zu überprüfen. Eine CRL alleine ist hierbei nicht ausreichend, denn diese ist nicht immer aktuell. Die CRL soll zusätzlich redundant verfügbar sein, da ein regelmäßiger Zugang zum internen Netz oder dem Internet nicht für alle Clients vorausgesetzt werden kann. |
| Verfügbarkeit | Die Verfügbarkeit jeder Zertifizierungsstelle soll 99,5 % und die Verfügbarkeit ihrer Sperrliste soll 99,9 % betragen. |
| Wiederherstellbarkeit | Eine möglichst schnelle Wiederherstellbarkeit der CA soll erreicht werden, so dass bei einem Ausfall die Funktionsfähigkeit innerhalb von zwei Arbeitstagen wiederhergestellt werden kann. |
| AltCA | Bei M-net ist aktuell eine Root CA im Einsatz, die einige Zertifikate ausgestellt hat. Diese Zertifikate sollen durch Zertifikate der neuen PKI ausgetauscht werden. Dadurch müssen eventuelle Komplikationen beim Zertifikataustausch berücksichtigt werden. |

3.2. Konzeptdetails

Die zu implementierende PKI wird als eine zweischichtige Zertifizierungsstellenhierarchie umgesetzt und besteht aus einer Wurzelzertifizierungsinstanz (Root CA) und sechs untergeordneten Zertifizierungsstellen (Sub CAs). Als Backupplan wird zusätzlich ein zweites Root CA Schlüsselpaar generiert. Deren Zertifikat wird simultan mit den anderen Zertifikaten ausgerollt, aber nicht verwendet. Dies soll erst dann geschehen, wenn die Root CA kompromittiert werden sollte. Drei der Sub CAs sind für den Backbone Bereich der M-net zuständig und werden in dieser Bachelorarbeit nicht weiter betrachtet. Das Erstellen des Schlüsselpaares der zweiten Root CA ist eine Umsetzung der Anforderung Wiederherstellbarkeit.

3.2.1. Pfadlänge

Um eine hohe Flexibilität zu ermöglichen, wird die Pfadlänge der Root CA nicht beschränkt. Die Pfadlänge der Sub CAs wird hingegen auf 0 beschränkt, um eine Inbetriebnahme einer untergeordneten Zertifizierungsstelle zu verhindern.

3.2.2. Root CA

Die Root CA (M-net-Root-X1) ist eine offline Zertifizierungsstelle, die nur zum Signieren der sechs Sub CAs hergenommen und anschließend offline genommen wird.

Die Root CA ist eine Windows Server 2016 Datacenter Maschine, allerdings kein Mitglied einer Domäne. Dies ermöglicht ihr, beliebige Zertifizierungsstellen mit beliebiger Domänenzugehörigkeit und beliebigem Betriebssystem zu zertifizieren. Somit ist die Anforderung Betriebssysteme, welche die Unterstützung von Zertifizierungsstellen mit unterschiedlichen Betriebssystemen verlangt, erfüllt. Die Root CA wird als eine virtuelle Maschine eingerichtet und nach dem offline nehmen auf einen PGP verschlüsselten Dateiserver verschoben.

Das Schlüsselpaar der Backup Root CA wird mit dem Programm OpenSSL auf einem Laptop erzeugt, auf dem extra für diesen Zweck Ubuntu installiert wird.

3.2.3. Untergeordnete Zertifizierungsstellen

Alle Windows Sub CAs und OCSP Responder haben als Betriebssystem Windows Server 2012 R2 Datacenter installiert und sind virtuelle Maschinen, die in Rechenzentren laufen, welche von der M-net betrieben werden. Die Windows Computer sind in einem eigenen VLAN, um die Sicherheit der CAs zu erhöhen.

Die erste Sub CA ist die M-net-Sub-Intern-01, welche Mitglied der Hauptdomäne „ntmnet.m-net.de“ ist. Dadurch können Zertifikate und die Zertifikatsperrliste automatisch in das Active Directory (AD) publiziert werden. Auf der CA laufen die Zertifizierungsstelle, der IIS und ein ausgelagerter OCSP Responder, welcher von außerhalb des internen Netzwerkes erreichbar ist. Durch die Auslagerung des OCSP Responders kann für Clients, die nicht im internen Netzwerk angeschlossen sind, eine aktuellere Zertifikatüberprüfung als per CRL realisiert werden. Mit Hilfe dieser CA sollen alle Domänenclients wie PCs und Laptops sowie Domänenserver signiert werden.

Durch das Vorhandensein zweier Domänen wird auch in der zweiten Domäne eine CA aufgebaut. Daher ist die zweite Sub CA M-net-Sub-ServiceLan-01 Mitglied der „mnet.aci“ Domäne. Auf ihr laufen die Zertifizierungsstelle, der IIS und ein OCSP Responder. Da in dieser Domäne alle Server und Clients innerhalb des internen Netzwerkes sind, besteht keine Notwendigkeit, hier den OCSP Responder auszulagern.

Auf der dritten Sub CA M-net-Sub-MDM-01 laufen die Zertifizierungsstelle, der IIS, NDES und ein ausgelagerter OCSP Responder. Diese CA ist Mitglied der „ntmnet.m-net.de“ Domäne. Ihr Zweck ist einzig die Bereitstellung der Zertifikate für mobile Geräte, z. B. Handys und Tablets. Über den Network Device Enrollment Service (NDES) bzw. das Simple Certificate Enrollment Protocol (SCEP) ist ein MobileIron Dienst angebunden, der für die Verwaltung der mobilen Geräte zuständig ist. MobileIron greift dabei per SCEP auf die CA zu und fordert gemäß der Zertifikatvorlage M-net_SCEP_MobilIron für das Gerät ein Zertifikat an. Dies erfüllt die Anforderung MDM. Der OCSP Responder wird ebenfalls ausgelagert, während der NDES Dienst auf der CA bleibt, da der MobileIron Server nur im internen Netzwerk angebunden ist.

3. Konzept

Eine Übersicht der Computer ist in Abbildung 3.1 zu sehen. Zusätzlich existieren noch drei weitere CAs in einer anderen Abteilung, welche allerdings in dieser Bachelorarbeit nicht behandelt werden.

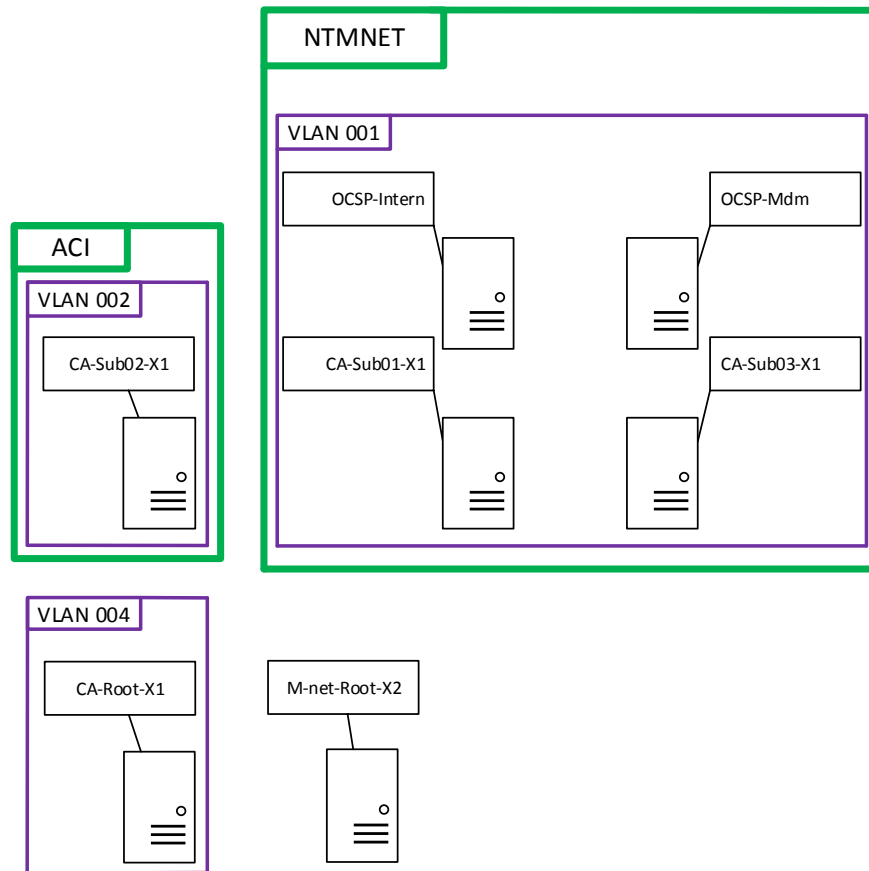


Abbildung 3.1.: Teilübersicht der PKI

Eine Konfiguration der Zertifizierungsstellen für die Unterstützung von SANs ist notwendig, um den Teil der Anforderung Zertifikattypen zu erfüllen, der dessen Unterstützung fordert.

Die Anforderung Ausstellbarkeit, die die Ausstellbarkeit von Zertifikaten an unterschiedliche Betriebssysteme und Domänenzugehörigkeiten verlangt, ist somit durch untergeordnete Zertifizierungsstellen, die verschiedenen Domänen angehören, erfüllt.

Durch die zweistufige PKI und keiner vorhandenen Einschränkung bezüglich der auszustellenden Zertifikate, kann die PKI für weitere Sicherheitsbausteine wie z. B. WLAN Authentifizierung, VPN Anbindung oder E-Mail- und Dateiverschlüsselung ausgebaut werden. Die für diese Sicherheitsbausteine benötigten Gerätezertifikate oder Benutzerzertifikate, wie beispielsweise für die E-Mailverschlüsselung benötigt, können durch Zertifikatvorlagen über die Domäne oder per NDES an die Geräte ausgestellt werden. Die Anforderung der Ausbaumöglichkeiten ist hiermit erfüllt.

3.2.4. Verwendung zweier Hardware-Sicherheitsmodule

Die Schlüssel der CAs und der OCSP Responder werden in zwei HSMs gespeichert, die per High Availability(HA) geclustert sind. Bei den HSMs handelt es sich um zwei Gemalto Luna SA 1700, die in zwei verschiedenen Rechenzentren installiert sind, welche von der M-net betrieben werden. Das ist eine Umsetzung der Anforderung Verfügbarkeit.

Die Wahl des HSMs beruht auf der Unterstützung für Partitionen, des HA-Clusters, der Netzwerkanbindung, des Key-in-Hardware-Ansatzes, der ausreichenden Geschwindigkeit von 350 tps bei RSA-2048, der Unterstützung gängiger Kryptografiealgorithmen wie RSA-4096 und der Unterstützung für Windows und Linux. [Gemwn]

Um die Anforderung Netzwerkkompatibilität zu erfüllen, die eine Kompatibilität zur Netzwerkinfrastruktur der M-net voraussetzt, befinden sich die HSMs in einem eigenen VLAN. Die Anbindung des HSMs an eine CA erfolgt mittels Virtual Trust Link, welcher über den Port 1792 läuft. Dies erlaubt es, den Zugriff auf die HSMs einzuschränken und nur den CAs und ausgewählten Servern den Zugriff zu ermöglichen.

Folgende Partitionen und zugriffsberechtigte Clients sind auf jeder HSM eingerichtet:

Tabelle 3.1.: HSM Partitionen und deren zugriffsberechtigte Clients

| Partitionsname | Zugriffsberechtigte Clients |
|----------------|--|
| parroot | Root CA |
| parrootbu | Backup RootX2 |
| parit | Sub-CA-Intern, Sub-CA-MDM, Sub-CA-ServiceLAN |
| parbackbone | CAs der Backbone Abteilung |
| parocsp | OCSP-Intern, OCSP-Mdm |

An die CA wird immer nur die Partition angebunden, in der der eigene private Schlüssel liegt, womit die CA auch nur Zugriff auf diese Partition erhält. Jede CA speichert ihre Schlüssel und die Schlüssel ihrer Dienste in der ihr zugeteilten Partition. Im Falle der Sub-CA-MDM liegen daher die NDES Schlüssel noch in der casubitx1 Partition. Die Partition carootx2 beinhaltet nur das Schlüsselpaar der RootX2 und wird erst bei Kompromittierung der Root CA an eine Zertifizierungsstelle angebunden.

Um eine zusätzliche Sicherheit zu garantieren, wird ein offline Backup HSM Modul zum Einsatz kommen, welches die Schlüssel aller CAs speichert. Der Aufbewahrungsort des Backup HSM Moduls wird ein Tresor, dessen Zugriff auf eine ausgewählte Personengruppe eingeschränkt ist. Ein Plan der PKI mit eingezeichneten HSMs ist in Abbildung 3.2 zu sehen.

Durch die Verwendung zweier HSMs in einem HA-Cluster, wobei die HSMs an zwei verschiedenen Standorten installiert werden, wird eine hohe Verfügbarkeit realisiert, die in der Anforderung Verfügbarkeit gefordert wird. Zusätzlich wird jede HSM noch um ein weiteres Netzteil erweitert, um die Ausfallwahrscheinlichkeit noch weiter zu senken.

3. Konzept

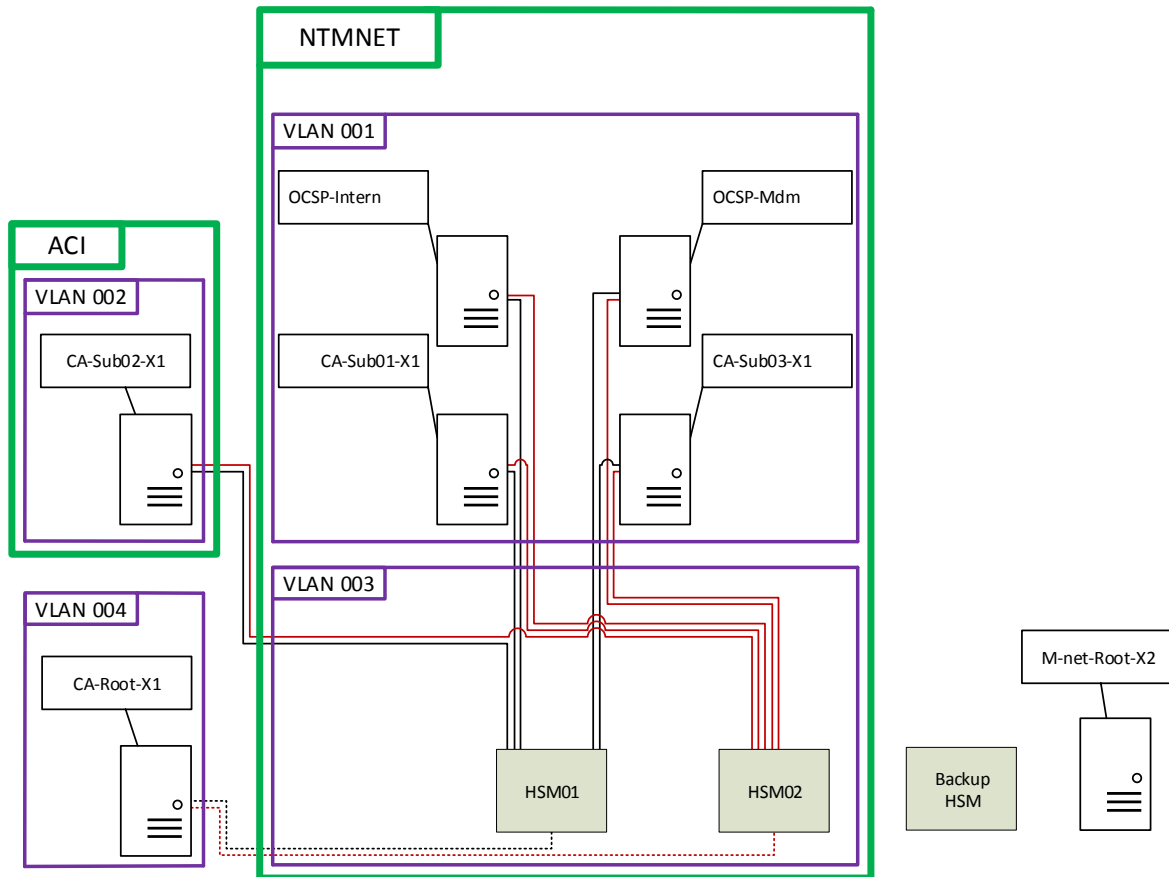


Abbildung 3.2.: Teilübersicht der PKI mit den HSMs

3.2.5. Berechtigungen

Nur eine stark eingeschränkte Gruppe von Administratoren hat Zugriff auf das HSM, die CAs und den PGP verschlüsselten Dateiserver, auf dem die Root CA, nachdem sie offline genommen wurde, gespeichert wird. Diese Gruppe wird im Folgenden `groupadminpki` genannt. Zudem ist ein Domänenadministratoraccount `adminpki` angelegt worden, der lokaler Administrator auf den Sub CAs und Mitglied der Gruppe `groupadminpki` ist.

3.2.6. Zertifikatdetails

Als Schlüssellänge werden für alle Zertifizierungsstellen 4096 Bit und für alle Clientzertifikate, die maximal zwei Jahre gültig sein dürfen, 2048 Bit verwendet. Dies stellt einen Kompromiss aus Sicherheit und Kompatibilität dar, da nicht alle vorhandenen Programme mit einer größeren Schlüssellänge kompatibel sind. Die hohe Kompatibilität wird in der Anforderung Schlüssellänge gefordert und ist durch eine Schlüssellänge von 4096 Bit für die CAs somit gegeben. Als Signatur-Hash-Algorithmus wird SHA-256 benutzt, um den Zertifikatsdienst mit dem IIS verwenden zu können, da dieser kein SHA-512 unterstützt. Die Zertifizierungsstellen-Webregistrierung ist notwendig, um die Anforderung Zertifikatanforderung, die eine unkomplizierte Zertifikatanforderung für nicht Domänenmitglieder fordert, zu erfüllen.

Die Zertifikate bzw. Sperrlisten haben folgende Gültigkeitsdauer:

Tabelle 3.2.: Gültigkeitsdauer Zertifikate bzw. Sperrlisten

| | | |
|------------------|----|-------|
| Root CAs | 20 | Jahre |
| Sub CAs | 10 | Jahre |
| Computer | 2 | Jahre |
| Mobile Endgeräte | 1 | Jahr |
| CRL Root CA | 5 | Jahre |
| CRL Sub CAs | 2 | Tage |

Das Veröffentlichungsintervall der CRL ist ein Tag. Allerdings soll alle sechs Stunden automatisiert per Skript eine CRL ausgestellt werden. Dies erlaubt eine Überprüfung der PKI, da die CRL nur bei Funktionsfähigkeit der CA erstellt wird und erhöht somit die Aktualität der CRL. Die zweitägige Gültigkeit ist Teil der Anforderung Wiederherstellbarkeit.

Jedes Zertifizierungsstellenzertifikat wird nach der Hälfte der Laufzeit um die ursprüngliche Gültigkeitsdauer verlängert. Nach Ablauf der ursprünglichen Gültigkeitsdauer wird das Zertifikat erneuert.

3.2.7. Sperrlisten

Die Zertifikate und Sperrlisten der CAs werden über das AD und über einen intern und extern erreichbaren Webserver verteilt, wodurch auch nicht Domänenmitglieder oder nicht an das interne Netzwerk angeschlossene Geräte Zugriff bekommen.

Die Sub-CA-Intern, die Sub-CA-MDM und die Sub-CA-ServiceLAN veröffentlichen ihre Sperrliste auf einen Netzwerkordner, der auf einem internen Dateiserver liegt. Schreibende Zugriffsrechte auf diesen Ordner haben nur die drei CAs und die groupadminpki. Auf diesen Ordner greifen die beiden redundanten Webserver zu, welche die öffentlichen Schlüssel und die Sperrlisten intern und extern als URL zur Verfügung stellen.

Da die Sperrliste täglich ausgestellt wird, jede CA über einen OCSP Responder verfügt und nicht mehrere Zehntausend gesperrte Zertifikate erwartet werden, wird auf den Einsatz einer Delta CRL verzichtet.

Um die Sperrlisten zusätzlich unter <http://pki.m-online.de> und die Sperrlisten der Backbone Abteilung zusätzlich unter <http://pki.m-net.de> erreichen zu können, werden Reverse Proxys eingesetzt.

Damit wird die Anforderung Zertifikatstatus, welche eine aktuelle Zertifikatstatusprüfung fordert, erfüllt.

3.2.8. Publikationspunkte

Die Reihenfolge der Publikationspunkte ist folgende: AD, OCSP, URL. Auf der Sub-CA-Intern und der Sub-CA-MDM kommt jeweils ein ausgelagerter OCSP Responder zum Einsatz, welche momentan noch innerhalb des internen Netzes stehen, allerdings langfristig in

3. Konzept

die DMZ verschoben werden sollen. Der OCSP Responder der Sub-CA-ServiceLAN ist auf der Sub-CA-ServiceLan installiert, da diese CA nur in einem intern schon stark zugriffsbeschränkten Netz aktiv ist. CA Zertifikate und CRLs der Sub-CA-MDM und der Sub-CA-Intern werden in der „ntmnet.m-net.de“ Domäne veröffentlicht und per Gruppenrichtlinie verteilt, analog mit der CA-ServiceLan in der „mnet.aci“ Domäne.

Die URLs für die öffentlichen Schlüssel der CAs und der CRLs lauten:

- *http://pki.m-net.de/<Dateiname>*
- *http://pki.m-online.net/<Dateiname>*

Die URL *http://pki.m-net.de/<Dateiname>* wird dabei von den zwei redundanten Webservern (Webserver-01 und Webserver-02) bereitgestellt. Die URL *http://pki.m-online.net/<Dateiname>* wird von einem Webserver der Backbone Abteilung bereitgestellt.

Die URLs für die OCSP Responder der Sub-CA-Intern und der Sub-CA-MDM lauten:

- *http://pki-intern.m-net.de/ocsp*
- *http://pki-mdm.m-net.de/ocsp*

Durch die verschiedenen Sperrlistenverteilungspunkte wird eine hohe Verfügbarkeit ermöglicht, da nur einer der Sperrlistenverteilungspunkte erreicht werden muss, um den Betrieb der Geräte bzw. Dienste, die die Zertifikate bereits besitzen und benutzen, zu ermöglichen. Dies ist seitens der Anforderung Verfügbarkeit gefordert.

3.2.9. Registrierungsmethoden

Folgende Registrierungsmethoden sollen unterstützt werden:

- Automatische Registrierung über Zertifikatvorlagen und Windows Gruppenrichtlinien
- Automatische Registrierung über NDES für mobile Geräte (MobileIron)
- Manuelle Registrierung mit Windows Enrollment bzw. einem CSR
- Manuelle Registrierung über die Zertifizierungsstellen-Webregistrierung

Der IIS, auf der die Zertifizierungsstellen-Webregistrierung läuft, soll nur intern verfügbar sein und nicht außerhalb des M-net Netzwerks. Deshalb ist eine Auslagerung auf einen externen IIS Server nicht notwendig.

Durch die verschiedenen Registrierungsmethoden ist die Anforderung Zertifikatanforderung, die genau dies fordert, erfüllt. Ebenso ist durch die Umsetzung von NDES die Anforderung MDM, die eine Anbindung an den MobileIron Dienst fordert, erfüllt. Durch die Möglichkeit einer manuellen Registrierung und der dadurch höheren Kontrolle über die vorhandenen Zertifikate im Zertifikatspeicher der Maschinen, lässt sich ein Austausch von alten Zertifikaten durch neue störungsfreier umsetzen. Dies wird in Anforderung AltCA gefordert.

3.2.10. Zertifikatvorlagen

Für folgende Geräte und Dienste werden Zertifikatvorlagen benötigt:

- Windows Clients
- Mobile Geräte
- Server
- OCSP Responder
- SSL-Verbindungen
- NDES

Durch die Zertifikatvorlagen ist ein einheitliches Ausstellen von verschiedenen Zertifikattypen möglich, was zum Teil in der Anforderung Zertifikattypen gefordert wurde. Durch die Verwendung von Windows Server 2012 bei den Sub CAs werden Schemaversion 4 Zertifikatvorlagen unterstützt.

3.2.11. CA Clustering

Durch das CA Clustern wird die Verfügbarkeit des OCSP Responders und des NDES nicht erhöht und eine Zertifizierungsstellen-Webregistrierung auf der Zertifizierungsstelle nicht empfohlen. Das Clustern würde zwar in die Anforderung Verfügbarkeit fallen, jedoch der Anforderung Zertifikatanforderung wegen der Zertifizierungsstellen-Webregistrierung widersprechen bzw. würde diese Anforderung dann eine Auslagerung der Zertifizierungsstellen-Webregistrierung von allen CAs auf neue Maschinen verlangen. Da durch die zweitägige Gültigkeit der Sperrliste genügend Zeit gegeben ist, die CA wieder in Betrieb zu nehmen, wird das CA Clustering nicht implementiert.

3.2.12. Wiederherstellbarkeit

Dieses Kapitel beschreibt die Umsetzung der Anforderung Wiederherstellbarkeit.

Die eingesetzten Maschinen und Programme sollen so konfiguriert werden, dass bei einem Neustart der Maschinen automatisch alle Dienste wieder starten und kein manueller Eingriff notwendig ist. Dies ist notwendig, um eine Wiederherstellbarkeit des Systems nach z. B. einem Stromausfall oder einem gewollten Neustart zur Fehlerbehebung zu vereinfachen. Ein Backup der virtuellen Maschinen wird alle drei Stunden automatisiert durchgeführt.

3.2.13. Verfügbarkeit

Die Maschinen sollen auf zwei Rechenzentren aufgeteilt werden, so dass der Ausfall eines Rechenzentrums möglichst wenig Auswirkungen auf die PKI hat. Durch den Anschluss der Maschinen an die unterbrechungsfreie Stromversorgung (USV) in den Rechenzentren soll eine Erhöhung der Verfügbarkeit realisiert werden. Beide Punkte sind notwendig um der Anforderung Verfügbarkeit zu entsprechen.

3.3. Zusammenfassung

Zuerst wurden in Kapitel 3.1 die spezifischen Anforderungen der M-net an die PKI dargestellt, z. B. der Ausstellbarkeit der Zertifikate für das Mobile Device Management oder Computer mit verschiedenen Betriebssystemen und Domänenzugehörigkeiten. Anschließend sind in Kapitel 3.2 die genauen Details zur Umsetzung der PKI festgelegt worden, z. B. die Verwendung zweier HSMs in einem HA-Cluster. Eine Übersicht, der aus diesem Konzept entwickelten PKI, wird in Abbildung 3.3 dargestellt. Im nächsten Kapitel wird die Umsetzung des Konzepts durchgeführt.

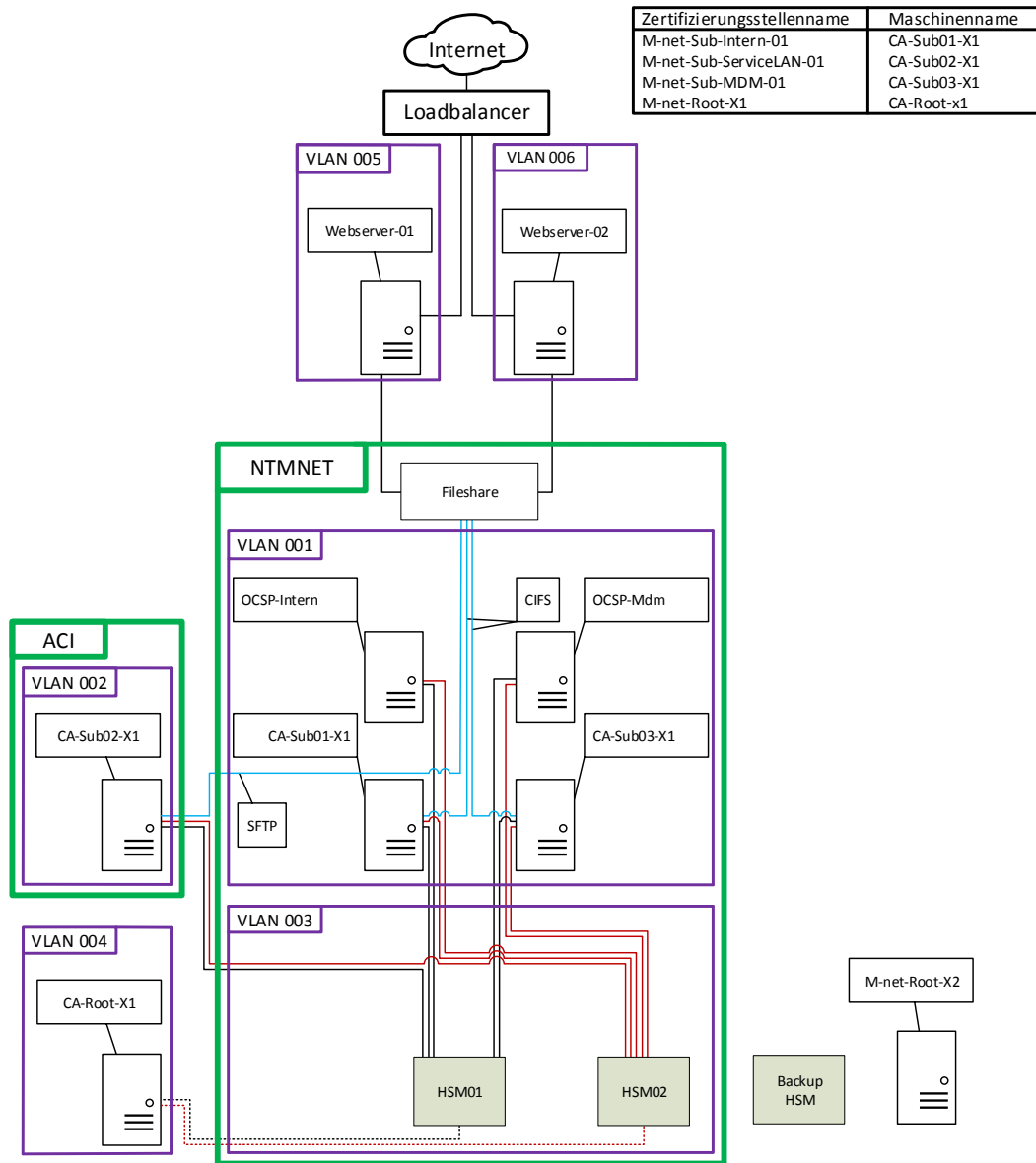


Abbildung 3.3.: Übersicht der PKI

4. Umsetzung

In diesem Kapitel wird die Implementierung der Public Key Infrastruktur unter Berücksichtigung der Konzeptdetails aus Kapitel 3.2 beschrieben. Eine durch Screenshots gestützte Implementierungsdokumentation befindet sich im Anhang A.

4.1. Einrichtung Hardware-Sicherheitsmodul

Für die Konfiguration der Luna HSM wird diese an einen Computer per seriellen Kabel angeschlossen und ein Terminal, z. B. PuTTY, geöffnet. Für die serielle Verbindung muss die Verbindung folgendermaßen konfiguriert werden:

- Baudrate 115200
- acht Datenbits
- ein Stopbit
- kein Paritybit
- Aktivierung des VT100 Befehlssatzes
- Aktivierung der Hardware Flow Control

Mit den voreingestellten Anmeldedaten meldet man sich nun an und gibt bei der erscheinenden Aufforderung ein neues Administratorpasswort ein.

Nun wird die Zeit des HSMs mit dem Befehl „`sysconfig time <HH:MM YYYYMMDD>`“ eingestellt. Im Fall von M-net wird zusätzlich die HSM mit dem NTP Server verbunden. Der NTP Server ist ein Server, der mit dem Network Time Protocol die Uhrzeiten von Geräten mit seiner eigenen Zeit synchronisiert. Dadurch ist sichergestellt, dass alle Geräte die richtige Uhrzeit haben. Dies geschieht mit den Befehlen „`sysconfig ntp addserver <FQDN des NTP Servers>`“ und „`sysconfig ntp enable`“.

Mit dem Befehl „`network hostname <Gerätename>`“ wird der Gerätename des HSMs festgelegt. Der Befehl „`net dns add nameserver <IP-Adresse des DNS-Servers>`“ bindet den DNS Server an das HSM an. Der DNS Server hat die Aufgabe Gerätenamen auf IP-Adressen abzubilden. Die Konfiguration der Netzwerkeinstellungen geschieht mit dem Befehl „`net interface -device <Netzwerkport> -ip <IP-Adresse> -netmask <Netzwerkmaske> -gateway <Gateway>`“. Mit dem Befehl „`network show`“ kann die Konfiguration anschließend angezeigt werden. Damit ist die Netzwerkkonfiguration abgeschlossen und das HSM kann über das Netzwerk angesprochen werden.

4. Umsetzung

Bevor Partitionen erstellt werden können, muss das HSM initialisiert werden. Dazu wird der Befehl „hsm -init -label <Name der HSM>“ eingegeben und bei der nun erscheinenden Aufforderung zum Erstellen eines Passworts, das Passwort für das Benutzerkonto des „Security Officers“ der HSM vergeben. Dieser „Security Officer“ ist eine Benutzerrolle auf der HSM mit spezielleren Rechten als der Administrator. Das Erstellen, Löschen und Verändern von Partitionen kann z. B. nur mit angemeldetem „Security Officer“ erfolgen. Die Erstellung von Partitionen erfolgt mit dem Befehl „partition create -partition <Partitionsname>“, der nach Eingabe ein Partitions Passwort fordert. Da bei der M-net fünf Partitionen benötigt werden, wird der Befehl fünfmal ausgeführt.

Damit ist die Konfiguration der ersten HSM abgeschlossen. Die zweite HSM wird komplett analog eingerichtet, wobei darauf geachtet werden muss, dass Partitionsnamen und Partitions passwörter identisch sein müssen.

4.2. Anbindung der Zertifizierungsstelle an das Hardware-Sicherheitsmodul High Availability-Cluster

In diesem Kapitel wird der Luna Client installiert, die Verbindung zu den HSMs eingerichtet und konfiguriert. Diese Konfiguration wird analog auf allen Windowsmaschinen durchgeführt. Alle Programme und Eingabeaufforderungen müssen mit Administratorrechten ausgeführt werden.

4.2.1. Konfiguration SafeNet Luna Client 6.2.0-15 mit der Virtual Token Library und High Availability

Zum Zeitpunkt der Implementierung war bereits der Luna Client 6.2.2-4 verfügbar, der jedoch nicht stabil lief und somit den Einsatz der älteren Luna Client 6.2.0-15 Version erforderlich machte.

Eine detaillierte Konfiguration des Luna Clients befindet sich in Kapitel A.2.1 der Screenshot gestützten Dokumentation.

Die Installation des Luna Clients setzt .Net Framework 3.5 voraus. Dies kann z. B. über den Assistenten zum Hinzufügen von Rollen und Features installiert werden. Da zwei SafeNet-Netzwerk-HSM 1700 zum Einsatz kommen, wird im Installationsprozess des Luna Clients das Luna CSP/Luna KSP Paket ausgewählt und der Luna Client installiert.

Für die Verbindung zwischen den HSMs und den Windows Maschinen wird ein Network Trust Link (NTL) mit Hilfe der Virtual Token Library (vtl) verwendet und eingerichtet. Da der Network Trust Link Service (NTLS) über den Port 1792 läuft, muss dieser in den entsprechenden Firewalls freigeschaltet werden.

Dabei werden die Serverzertifikate der HSMs auf den Clients installiert, auf diesen ein Clientzertifikat generiert und in den HSMs registriert. Nun kann der Client in der HSM einer Partition zugeordnet werden, um auf diese Zugriff zu erhalten. Da der Client dadurch

nur per FQDN registriert wurde, wird noch zusätzlich dessen IP eingetragen.

Das Kommandozeilenprogramm Lunacm, welches bei der Installation des Luna Clients mitinstalliert wird, wird auf dem Client ausgeführt. Damit wird eine HA-Gruppe erstellt und dieser die jeweilige Partition der beiden HSMs zugeteilt. Um eine redundante Speicherung der Objekte in den Partitionen zu aktivieren, werden die Partitionen über die Lunacm synchronisiert.

4.2.2. Key Storage Provider und Cryptographic Service Provider

Da KSP SHA-2 unterstützt, CSP aber nur SHA-1, wird als Standard bei allen Zertifizierungsstellen auf KSP gesetzt und CSP nur für den NDES Dienst konfiguriert und verwendet. Der NDES Dienst läuft nur auf der Sub-MDM. Eine detaillierte Konfiguration der KSPs und CSPs befindet sich in Kapitel A.2.2 der Screenshot gestützten Dokumentation.

Für die Verwendung der Luna HSM wird zuerst beim Luna KSP die Luna Sicherheitsbibliothek und anschließend die HA-Partition registriert.

Falls der CSP eingesetzt wird, dann muss explizit der Luna CSP konfiguriert werden und die HA-Partition in der CSP registriert werden. Anschließend müssen alle Programme, die den CSP benutzen, konfiguriert und einmal ausgeführt werden, bevor die CSP Konfiguration abgeschlossen werden kann. Konkret bedeutet dies in dieser Implementierung, dass erst der NDES und CEP Dienst fertig konfiguriert werden müssen. Danach wird ein erhöhter Passwortschutz aktiviert, der es nur Windows Benutzern erlaubt den CSP zu benutzen, die bis zu diesem Zeitpunkt auf dem Computer angelegt worden sind.

4.3. Zertifizierungsstellen

Für das Aufsetzen der Zertifizierungsstellen wird der Microsoft Assistent zum Hinzufügen von Rollen und Features verwendet. Dieser wird durch Konfigurationsskripte, wie nachfolgend beschrieben, unterstützt.

4.3.1. Konfigurationsskripte für Windows Zertifizierungsstellen

Durch das optionale Verwenden von Skripten, welche im Vorfeld erstellt werden können, wird das Risiko möglicher Falscheingaben minimiert und die Konfiguration transparenter. Bei einer Neuaufsetzung einer CA kann diese leichter wieder identisch konfiguriert werden. Dabei setzen die Zertifizierungsstellenkonfigurationsskripte in der Windows Registrierungsdatenbank unter dem Pfad „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc“ verschiedene Konfigurationsparameter.

4.3.1.1. CAPolicy.inf

Die CAPolicy.inf ist eine Konfigurationsdatei für das Zertifizierungsstellenzertifikat und wird von dem Windows Server-Manager, der die Zertifikatdienste installiert und konfiguriert, verwendet. Aus diesem Grund muss die CAPolicy.inf vor der Installation der Zertifikatdienste

4. Umsetzung

in das Windows Installationsverzeichnis, meist „C:\Windows“, kopiert werden.

Jede CAPolicy.inf, eine Beispieldatei ist in Listing 4.1 zu sehen, fängt immer mit den Zeilen 1 bis 2 an, die die eingesetzte Version beschreiben und beinhaltet anschließend weitere Sektionen. Eine Sektion ist durch eine Bezeichnung in eckigen Klammern gekennzeichnet und beinhaltet alle Einträge bis zur nächsten Sektion. Die nachfolgenden Sektionen nach der Sektion „[Version]“ werden nach den individuellen Anforderungen an die CA gestaltet.

In der Beispieldatei wird in der Sektion [certsrv_server] die Schlüssellänge bei Erneuerung des Zertifizierungsstellenzertifikats auf 4096 Bit, die Gültigkeitsdauer auf 20 Jahre und die Gültigkeit der Sperrliste auf 5 Jahre festgelegt. Die Zeile 12, die als Gültigkeitswert der Delta Sperrliste null festlegt, bewirkt, dass keine Delta CRL benutzt wird. Die Einheit der Gültigkeitsdauer, also bei der Basissperrliste die CRLPeriodUnits, kann entweder „hours“, „days“, „weeks“, „months“ oder „years“ betragen. Bei der CRLDeltaPeriodUnits kommt zusätzlich noch „minutes“ dazu.

Der Eintrag „LoadDefaultTemplates=0“ in Zeile 14 bewirkt, dass nicht automatisch nach der Installation der CA einige Standardzertifikatvorlagen bei ihr veröffentlicht werden. Dies ermöglicht eine erweiterte Kontrolle der CA, da nun genau definiert werden kann, welche Zertifikatvorlagen bei dieser CA veröffentlicht werden. Die automatisch veröffentlichten Zertifikatvorlagen nach der Installation, wenn dieser Eintrag nicht in der CAPolicy.inf steht, kann in der Quellenangabe [Mic12a] nachgelesen werden.

Soll in einer mehrstufigen PKI das Root Zertifikat nicht auf Gültigkeit überprüft werden, dürfen die AIA und CDP Erweiterungen nicht im Root Zertifikat stehen. Stehen im Root Zertifikat keine CDP Erweiterungen, sondern nur die AIA Erweiterungen, kann es dennoch vorkommen, dass manche Programme den Gültigkeitsstatus des Root Zertifikats überprüfen wollen. Die Exkludierung der AIA und CDP Erweiterungen aus dem Zertifizierungsstellenzertifikat geschieht durch das Hinzufügen von Zeile 16 bis 20 in die CAPolicy.inf. In Windows Server Betriebssystemen 2008 und aufwärts müssen die beiden Zeilen mit den Einträgen Empty=True nicht explizit eingetragen werden, es genügt jeweils eine leere Zeile. Statt dem Eintrag Empty=True können hier allerdings auch die Pfade für den CDP oder die AIA angegeben werden.

In der Sektion [BasicConstraintsExtension] sind Beschränkungen aufgelistet. In diesem Fall ist die Pfadlänge auf 2 limitiert, d. h. wenn dies die Root CA wäre, könnte maximal eine dreistufige PKI aufgebaut werden. Der Eintrag Critical=True in dieser Sektion bedeutet, dass, wenn eine Überprüfung der Einträge dieser Sektion nicht möglich ist, das Zertifikat als ungültig behandelt werden soll.

Listing 4.1: Beispiel einer CAPolicy.inf

```

1 [Version]
2 Signature="$Windows NT$"
3
4 [certsrv_server]
5 renewkeylength=4096
6 RenewalValidityPeriodUnits=20
7 RenewalValidityPeriod=years
8
9 CRLPeriod=years
10 CRLPeriodUnits=5
11 CRLDeltaPeriod=days
12 CRLDeltaPeriodUnits=0
13
14 LoadDefaultTemplates=0
15
16 [CRLDistributionPoint]
17 Empty=True
18
19 [AuthorityInformationAccess]
20 Empty=True
21
22 [BasicConstraintsExtension]
23 PathLength=2
24 Critical=True

```

4.3.1.2. Zertifizierungsstellenkonfigurationsskript

Für das Ausführen dieses Skripts wird das Microsoft Kommandozeilenprogramm Certutil verwendet, welches standardmäßig auf allen Windows Server Betriebssystemen ab Windows Server 2003 installiert ist.

Der Distinguished Name (DN) ist eine Sequenz aus Relative Distinguished Names, zu welchen unter anderem der Common Name (CN), der Domain Component (DC) oder die Organizational Unit (OU) gehören und ein LDAP Objekt beschreiben.

Der Common Name ist der Objekt- oder AD-Ordnername, die Domain Components sind einzelne Abschnitte der Domäne und die Organizational Unit beschreibt z. B. die Abteilung, zu der das Objekt gehört.

Ein PC mit den Namen „Daniels-PC“ und der Abteilung „Heimtechnik“ in der Domäne „leimig.com“ hätte also z. B. den Distinguished Name CN=Daniels-PC, OU=Heimtechnik, DC=leimig, DC=com [Mictc].

Der Domain Name, der ebenfalls mit DN abgekürzt wird, aber Bestandteil des Domain Name Systems (DNS) und nicht des LDAP ist, wäre mit obigem Beispiel leimig.com. Der Fully Qualified Domain Name ist dann Daniels-PC.leimig.com.

Dieses Konfigurationsskript, ein Beispielskript ist in dem Listing 4.2 zu sehen, wird nach der Installation der Zertifizierungsdienste, des Zertifizierungsstellenzertifikats und der erst-

4. Umsetzung

maligen Inbetriebnahme ausgeführt.

In Zeile 2 des Listings 4.2 wird der Distinguished Name der CA festgelegt. In den Zeilen 5 bis 8 werden die CRL Veröffentlichungsintervalle und in Zeile 11 bis 14 der Überschneidungszeitraum, wie in Kapitel 2.2.1.2 erläutert, definiert.

Die CDP-Erweiterung wird in der Zeile 17 des Listings 4.2 definiert. Es wird zuerst der Ort, in dem die Sperrliste abgerufen werden kann, eingetragen und anschließend wird die Funktion des Ortes spezifiziert. Der Pfad bzw. die URL des Standorts kann dabei mit Hilfe von Variablen definiert werden, siehe Tabelle 4.3. Die Funktion des Ortes wird mit „\n<Parameter>“ spezifiziert, siehe Tabelle 4.1.

Tabelle 4.1.: Erklärung der Sperrlisten-Verteilungspunkt (CDP) Parameter

| Parameter | Bedeutung | Beschreibung |
|-----------|---|---|
| 1 | Sperrlisten an diesem Ort veröffentlichen | Veröffentlicht/speichert die Sperrliste an diesem Ort. |
| 2 | In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen | Fügt den angegebenen Ort in die CDP-Erweiterung der ausgestellten Zertifikate ein, von der die CRL heruntergeladen werden kann. |
| 4 | In Sperrlisten einbeziehen. Wird zur Suche von Deltasperrlisten verwendet | Definiert den Pfad in der Basissperrliste zum Abruf der Deltasperrliste. |
| 8 | In alle Sperrlisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll | Wird zur Angabe des LDAP-URL Pfads verwendet, in dem die Sperrlisten im AD gespeichert sind. |
| 64 | Deltasperrlisten an diesem Ort veröffentlichen | Veröffentlicht/speichert die Deltasperrliste an diesem Ort. |
| 128 | In die IDP-Erweiterung ausgestellter CRLs einbeziehen | Wird von nicht-Windows-Clients zur Bestimmung des Aufteilungsbereichs, also z. B. nur dem Auflisten von Zertifikaten mit dem Sperrgrund „abgelöst“, von partitionierten CRLs verwendet. |

In der Zeile 20 des Listings 4.2 werden die AIA-Erweiterungen definiert. Diese definieren die Orte, an denen das Zertifizierungsstellenzertifikat heruntergeladen und gegebenenfalls der OCSP-Server erreicht werden kann. Der Pfad bzw. die URL des Standorts kann dabei mit Hilfe von Variablen definiert werden, siehe Tabelle 4.3. Die Funktion des Ortes wird mit dem Parameter spezifiziert.

Tabelle 4.2.: Erklärung der Stelleninformationen (AIA) Parameter

| Parameter | Bedeutung | Beschreibung |
|-----------|--|---|
| 2 | In AIA-Erweiterung des ausgestellten Zertifikats einbeziehen | Fügt den angegebenen Ort in die AIA Erweiterungen des ausgegebenen Zertifikats ein, von dem das Zertifizierungsstellenzertifikat heruntergeladen werden kann. |
| 32 | In OCSP-Erweiterungen einbeziehen | Fügt eine HTTP-URL in die AIA Erweiterungen ein, von der der OCSP-Server aus erreicht werden kann. |

In Zeile 23 des Listings 4.2 wird die Überwachung der CA aktiviert. Jedes Ereignis, das überwacht werden kann, ist mit einer Zahl im Konfigurationsskript auswählbar. Dabei ist die Zahl, die dem AuditFilter im Konfigurationsskript als Parameter übergeben wird, die Summe der zu überwachenden Ereignisse, die aktiviert werden sollen. Siehe hierzu Abbildung 4.1. Die Zahl 127 in der Zeile 23 ergibt sich aus der Summe aller auswählbaren Ereignisse.

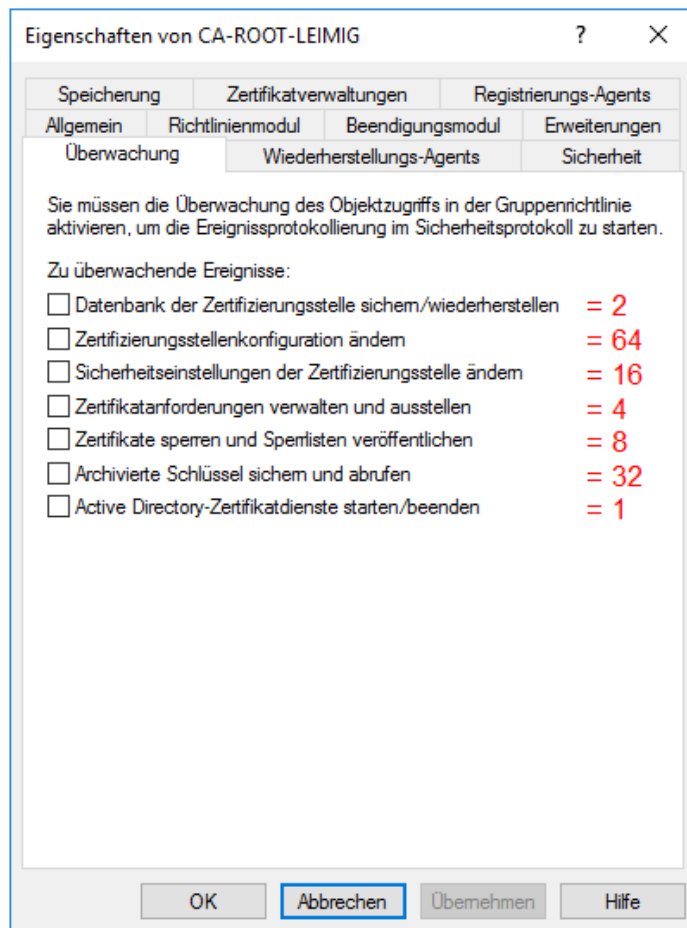


Abbildung 4.1.: Reiter „Überwachung“ mit Markierung für das Konfigurationsskript

4. Umsetzung

In Zeile 26 und 27 des Listings 4.2 wird die maximale Laufzeit der ausgegebenen Zertifikate festgelegt. Die Anzahl und die Einheit der Länge der maximalen Laufzeit wird, wie in Kapitel 2.2.1.2 erläutert, definiert. In Zeile 30 wird der Zertifizierungsstellendienst neu gestartet, um die Änderungen zu übernehmen und anschließend wird in Zeile 34 eine neue CRL generiert.

Listing 4.2: Beispiel Konfigurationsskript für eine Zertifizierungsstelle

```
1  :: Konfigurations DN festlegen
2  certutil -setreg CA\DSConfigDN CN=Configuration ,DC=ntmnet ,DC=m-net ,DC=
   de
3
4  ::CRL Veroeffentlichungsintervalle
5  certutil -setreg CA\CRLPeriodUnits 2
6  certutil -setreg CA\CRLPeriod "years"
7  certutil -setreg CA\CRLDeltaPeriodUnits 5
8  certutil -setreg CA\CRLDeltaPeriod "days"
9
10 :: CRL Overlap Intervall
11 certutil -setreg CA\CRLOverlapUnits 1
12 certutil -setreg CA\CRLOverlapPeriod "Months"
13 certutil -setreg CA\CRLDeltaOverlapUnits 3
14 certutil -setreg CA\CRLDeltaOverlapPeriod "Days"
15
16 ::CDP Extension URLs
17 certutil -setreg CA\CRLPublicationURLs "1:%windir%\system32\CertSrv\
   CertEnroll\%%3%%8%%9.crl\n14:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=
   Public Key Services ,CN=Services,%%6%%10\n2:http://pki.m-net.de
   /%%3%%8%%9.crl\n2:http://pki.m-online.net/%%3%%8%%9.crl"
18
19 ::AIA Extension URLs
20 certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\CertSrv
   \CertEnroll\%%1_%%3%%4.crt\n2:ldap:///CN=%%7,CN=AIA,CN=Public Key
   Services ,CN=Services,%%6%%11\n32:http://pki-intern.m-net.de/ocsp\
   n2:http://pki.m-net.de/%%1_%%3%%4.crt\n2:http://pki.m-online.net
   /%%1_%%3%%4.crt"
21
22 :: Auditing events aktivieren
23 certutil -setreg CA\AuditFilter 127
24
25 :: Maximale Laufzeit fuer ausgegebene Zertifikate
26 certutil -setreg CA\ValidityPeriodUnits 10
27 certutil -setreg CA\ValidityPeriod "Years"
28
29 :: Restart Certificate Services
30 net stop certsvc & net start certsvc
31 pause
32
33 :: Publish CRL
34 certutil -CRL
35 pause
```

Tabelle 4.3.: Erklärung der Variablen im Konfigurationsskript

| Variable | Bedeutung | Beschreibung |
|----------|--------------------------|--|
| %1 | <ServerDNSName> | DNS Name des Servers |
| %2 | <ServerShortName> | NetBIOS Name des Servers |
| %3 | <CaName> | Name der Zertifizierungsstelle |
| %4 | <CertificateName> | Fügt das Suffix „(<Zahl>)“ für die Zertifizierungsstellenzertifikatversion an den Dateinamen des Zertifikats an, nachdem das Zertifizierungsstellenzertifikat das erste Mal erneuert wird und zählt die Zahl dann bei jeder Erneuerung hoch [Kom12]. |
| %5 | <Domain DN > | Distinguished Name der Domäne; wird seit Windows Server 2003 nicht mehr verwendet |
| %6 | <ConfigurationContainer> | Speicherort des Konfigurationscontainers im AD |
| %7 | <CATruncatedName> | Der auf 32 Zeichen abgeschnittene Name der CA mit einem Hash Symbol am Ende |
| %8 | <CRLNameSuffix> | Fügt das Suffix „(<Zahl>)“ für die Zertifizierungsstellenzertifikatversion an den Dateinamen der CRL an, nachdem das Zertifizierungsstellenzertifikat das erste Mal erneuert wird und zählt die Zahl dann bei jeder Erneuerung hoch |
| %9 | <DeltaCRLAllowed> | Fügt das Suffix „+“ zu dem CRL Namen hinzu und bildet so den Namen der DeltaCRL |
| %10 | <CDPObjectClass> | Markiert das Objekt als CDP-Objekt im AD |
| %11 | <CAObjectClass> | Markiert das Objekt als CA-Zertifikatobjekt im AD |

Nach Abschluss der Installation und Konfiguration der Zertifizierungsstelle können in der Microsoft Management Console (MMC) die Eigenschaften der Zertifizierungsstelle geöffnet werden. Dort sieht man im Reiter „Erweiterungen“ die AIA- und CDP-Erweiterungen, die mit dem Konfigurationsskript konfiguriert werden. Dies ist in Abbildung 4.2 zu sehen. Die roten Zahlen stellen hierbei AIA- und CDP-Parameter dar, die in den Tabellen 4.1 und 4.2 erklärt werden.

4. Umsetzung

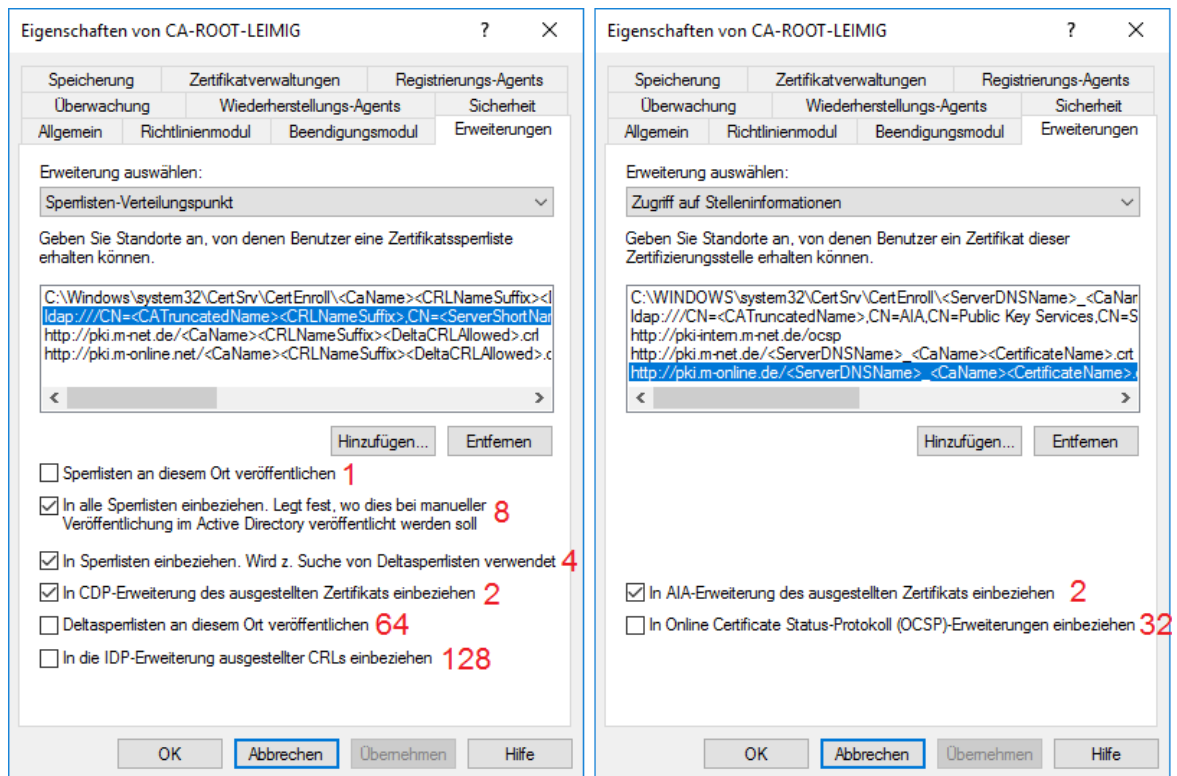


Abbildung 4.2.: AIA- und CDP-Erweiterungen mit Markierung für das Konfigurationsskript

4.3.2. Installation

Dieses Kapitel beschreibt die Installation und Konfiguration der Zertifizierungsstellen. Im Fall einer untergeordneten Zertifizierungsstelle wird zusätzlich die Signierung des untergeordneten Zertifizierungsstellenzertifikats beschrieben. Eine detailliertere Dokumentation für die Root CA befindet sich in Kapitel A.3 und für die Sub CA in Kapitel A.5.

Die vorbereitete CAPolicy.inf wird in das Windows Installationsverzeichnis kopiert. Im Server Manager wird der „Assistent zum Hinzufügen von Rollen und Features“ gestartet, bei den Serverrollen die „Active Directory-Zertifikatdienste“ ausgewählt und bei den Rollendiensten die Dienste ausgewählt, die installiert werden sollen. Bei der Root CA ist das nur die „Zertifizierungsstelle“. Bei der Sub-Intern wird die „Zertifizierungsstelle“ und die „Zertifizierungsstellen-Webregistrierung“, bei der Sub-CA-ServiceLan die „Zertifizierungsstelle“, die „Zertifizierungsstellen-Webregistrierung“ und der „Online-Responder“ ausgewählt. Bei der Sub-CA-MDM werden die „Zertifizierungsstelle“, die „Zertifizierungsstellen-Webregistrierung“ und der „Registrierungsdienst für Netzwerkgeräte“ angeklickt. Anschließend wird die Maschine neu gestartet.

Nun kann die Zertifizierungsstelle konfiguriert werden. Dazu wird im Server Manager der „Konfigurationsassistent“ aufgerufen. Die Anmeldeinformationen zur Konfiguration sind bei der Root CA das Standardkonto und bei den Sub CAs der adminpki, welcher der lokalen Administratorgruppe auf den Sub CAs angehört. Die Zertifizierungsstelle wird nun als zu

konfigurierender Rollendienst ausgewählt.

Im Fall der Root CA wird als Installationstyp „Eigenständige Zertifizierungsstelle“ ausgewählt, da sie kein Domänenmitglied ist. Bei den Sub CAs wird „Unternehmenszertifizierungsstelle“ ausgewählt, da alle Sub CAs Domänenmitglieder sind. Als Zertifizierungstyp wird bei der Root CA „Stammzertifizierungsstelle“ ausgewählt und bei den Sub CAs „Untergeordnete Zertifizierungsstelle“. Danach wird das Erstellen des privaten Schlüssels mit dem Luna KSP, SHA-256 und 4096 Bit konfiguriert, der Name der Zertifizierungsstelle wie in 3.2 definiert und eingegeben, sowie die Gültigkeit des Zertifikats auf 20 Jahre bei der Root CA bzw. auf 10 Jahre bei den Sub CAs festgelegt. Für die Root CA werden die Orte der Datenbank unverändert übernommen und die Konfiguration abgeschlossen. Bei den Sub CAs wird zusätzlich noch eine Zertifikatanforderung erstellt.

Auf der Root CA kann nach dem Hinzufügen des Zertifizierungsstellen Snap-Ins in der Microsoft Management Console der Zertifizierungsstellendienst gestartet und das vorbereitete Konfigurationsskript mit Administratorrechten ausgeführt werden. Im Verzeichnis „C:\Windows\System32\CertSrv\CertEnroll“ befinden sich nun das Zertifikat und die Sperrliste. Beide müssen nun noch veröffentlicht werden, siehe Kapitel 4.3.3.

Bei einer Sub CA muss die Zertifikatanforderung auf die Root CA kopiert und dort in dem Zertifizierungsstelle Snap-In der MMC eingereicht und ausgestellt werden. Mit dem Zertifikatexport-Assistenten wird das Zertifikat als PKCS#7 Datei exportiert, auf die Sub CA kopiert und dort in dem Zertifizierungsstellen Snap-In als Zertifizierungsstellenzertifikat eingereicht. Die Sub CA wird gestartet und das vorbereitete Konfigurationsskript ausgeführt.

Damit ist die Konfiguration der Root CA und die grundlegende Konfiguration der Sub CA abgeschlossen.

4.3.3. Veröffentlichung Root CA Zertifikat und Sperrliste

Das Zertifikat und die Sperrliste müssen an allen konfigurierten Orten des AIA und des CDP verfügbar gemacht werden. Im Fall der autarken Root CA muss dies manuell erfolgen. Für die Veröffentlichung in den jeweiligen Domänen werden beide Dateien auf ein Domänenmitglied kopiert und folgende Befehle als Administrator ausgeführt:

```
„certutil -f -dspublish <Zertifikatname>.crt RootCA“  
„certutil -f -dspublish <Sperrlistenname>.crl“
```

Der Webserver ist so eingerichtet, dass er die Sperrlisten, die von den Sub CAs auf den Fileshare abgelegt werden, selbständig kopiert und auf der in Kapitel 3.2.8 definierten URL <http://pki.m-net.de/> zur Verfügung stellt. Auf das Fileshare müssen alle Zertifikate der CAs und die CRL der Root CA kopiert werden.

Damit ist die Veröffentlichung des Zertifikats und der Sperrliste der Root CA abgeschlossen.

4.3.3.1. Überwachung Zertifizierungsdienste

In diesem Kapitel wird die Aktivierung, der in dem Konfigurationsskript der Sub CA konfigurierten Überwachung der Zertifizierungsdienste, durchgeführt. Dazu wird in den lokalen Sicherheitsrichtlinien die Überwachung der Zertifizierungsdienste aktiviert, siehe Implementierungsschritt Nummer 63. Zur Überwachung der Windows Maschine und den darauf laufenden Diensten wird die Netzwerk-Monitoring-Software op5 Monitor eingesetzt, deren Konfiguration in dieser Bachelorarbeit allerdings nicht behandelt wird.

4.3.3.2. Aktivierung der SANs

Die Aktivierung der SANs geschieht mit folgendem Befehl und einem Neustart der CA:
„Certutil -Setreg Policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2“

4.4. Zertifikatvorlagen

Diese Kapitel behandelt die Installation und Konfiguration der Zertifikatvorlagen.

Da die Sub CAs Domänenmitglieder sind, werden die Zertifikatvorlagen auf den Domänencontrollern gespeichert. Daher muss eine Zertifikatvorlage nur einmal pro Domäne angepasst werden und dann auf der/den gewünschten Zertifizierungsstellen veröffentlicht werden.

Die Sub CAs sind durch den CAPolicy.inf Eintrag „LoadDefaultTemplates=0“, siehe Implementierungsschritt 60, ohne veröffentlichte Standardvorlagen installiert worden. Durch Hinzufügen des Zertifikatvorlagen Snap-Ins in die Microsoft Management Console und dem anschließenden Bestätigen des Installationsfensters werden die Standardzertifikatvorlagen installiert.

Um eine bessere Übersicht und Kontrolle zu erhalten, wird jede Zertifikatvorlage dupliziert, umbenannt und konfiguriert, bevor sie veröffentlicht wird. Mit einem Rechtsklick auf eine Standardvorlage und anschließendem Klick auf „Vorlage duplizieren“ wird die Vorlage dupliziert und kann nun bearbeitet werden. Die bei M-net beschlossene Namenskonvention für die Zertifikatvorlagen beinhaltet eine Umbenennung der deutschen Zertifikatvorlagennamen ins englische und dem Hinzufügen des Präfixes „M-net_“, um eine schnelle Erkennung der angepassten Zertifikatvorlagen zu ermöglichen. Anschließend wird der Sicherheitsreiter der Zertifikatvorlagen bei der M-net so angepasst, dass mindestens diese Einträge enthalten sind:

- Authentifizierte Benutzer mit der Berechtigung „Lesen“
- groupadminpki mit den Berechtigungen „Lesen“ und „Schreiben“

Die Berechtigung „Schreiben“ erlaubt den Mitgliedern der Gruppe groupadminpki die Zertifikatvorlage anzupassen. Die Computer, Benutzer, Gruppen oder Dienste, die ein Zertifikat durch diese Zertifikatvorlage anfordern dürfen, werden mit der Berechtigung „Registrieren“ eingetragen. Wenn diese ein Zertifikat automatisch anfordern dürfen, bekommen sie die Berechtigung „Automatisch registrieren“.

Anschließend erfolgt die spezifische Konfiguration der Zertifikatvorlagen. Einige Konfigurationen der benötigten Zertifikatvorlagen sind in den Unterkapiteln der Implementierungsdokumentation 4.4.1, 4.4.2, 4.4.3 und 4.4.4 beschrieben.

Nach der Konfiguration der Zertifikatvorlage muss diese auf der CA, die damit Zertifikate ausstellen soll, veröffentlicht werden. Dies geschieht mit einem Rechtsklick auf die Zertifikatvorlagen der CA und einem Klick auf „Neu“ → „Auszustellende Zertifikatvorlage“. Nun öffnet sich ein Fenster in dem alle in dieser Domäne verfügbaren Zertifikatvorlagen aufgelistet sind. Die gewünschte Zertifikatvorlage wird nun ausgewählt und damit auf der CA veröffentlicht.

Damit ist die Konfiguration der Zertifikatvorlagen abgeschlossen und es können mit Hilfe der veröffentlichten Zertifikatvorlagen der CAs Zertifikate angefordert werden.

4.4.1. Zertifikatvorlage für SSL Zertifikate

Für die Erstellung einheitlicher SSL Zertifikate für die IIS wird eine Zertifikatvorlage konfiguriert. Dafür wird die Zertifikatvorlage „Webserver“ dupliziert und in „M-net_Domain-Webserver“ umbenannt. Der Reiter „Sicherheit“ wird nach dem M-net Standard konfiguriert und zusätzlich die Computerkonten aller Sub CAs mit den Rechten „Lesen“ und „Registrieren“ eingefügt. In dem Reiter „Antragstellername“ wird konfiguriert, dass der DNS-Name der Maschine aus dem Active Directory verwendet werden soll. Mit Hilfe dieses Zertifikats werden die SSL Zertifikate für die HTTPS Verbindung des IIS erstellt. Die CAs werden dabei nur mit der Berechtigung „Registrieren“ und nicht mit der Berechtigung „Automatisch registrieren“ eingetragen, da mehrere CAs in der gleichen Domäne sind und es für den IIS wichtig ist, ein Zertifikat der richtigen Zertifizierungsstelle zu erhalten. Der IIS auf der Sub-CA-Intern benötigt ein Zertifikat, das von der Sub-CA-Intern ausgestellt wird. Analog dazu verhalten sich die IIS der anderen Sub CAs. Bei Domänenmitgliedern werden Zertifikate, die durch eine Zertifikatvorlage ausgestellt werden, automatisch erneuert, wenn diese Zugriff auf die domänenintegrierte Sub CA haben, die die Zertifikatvorlage veröffentlicht hat. Im konkreten Fall eines ausgestellten Zertifikats von der Zertifikatvorlage M-net_Domain-Webserver der Sub-CA-Intern bedeutet dies, dass das ausgestellte Zertifikat auch wieder durch die Zertifikatvorlage M-net_Domain-Webserver der Sub-CA-Intern erneuert wird. Da diese Zertifikatvorlage in beiden Domänen benötigt wird, muss sie in beiden Domänen erstellt werden. Mit der Veröffentlichung dieser Zertifikatvorlage auf allen Sub CAs können nun SSL Zertifikate angefordert werden.

4.4.2. Zertifikatvorlagen für den NDES

Für den Betrieb des NDES Dienstes werden Zertifikate benötigt, wofür in diesem Kapitel die zwei zuständigen Zertifikatvorlagen eingerichtet werden.

Diese beiden Zertifikatvorlagen müssen auf der Sub-CA-MDM erstellt werden, da nur dort der Luna CSP eingerichtet wurde. Dies führt dazu, dass der Reiter „Kryptografie“ dieser Zertifikatvorlage auf anderen CAs nicht richtig angezeigt wird, da diese den Luna CSP nicht unterstützen und somit den Luna CSP als Kryptografieanbieter auch nicht anzeigen können. Statt dem Luna CSP wird auf diesen CAs dann ein anderer Kryptografieanbieter angezeigt.

4. Umsetzung

Für das Exchange Enrollment Zertifikat, welches für die Zertifikatanforderung an die CA benötigt wird, muss die Zertifikatvorlage Exchange Enrollment Agent (Offline Request) angepasst werden. Diese wird nun nach M-net_Exchange-Enrollment-Agent(offlinerequest) umbenannt und in dem Reiter „Kryptografie“ der Luna CSP mit 2048 Bit Schlüssellänge ausgewählt. In dem Reiter „Sicherheit“ werden die bei M-net standardmäßigen Einstellungen vorgenommen und zusätzlich das Computerkonto „CA-SUB03-X1“ mit den Rechten „Lesen“ und „Registrieren“ hinzugefügt.

Für die verschlüsselte Kommunikation zwischen NDES und dem Dienst, der die NDES Schnittstelle benutzt, wird die Zertifikatvorlage „CEP-Verschlüsselung“ angepasst. Diese wird dupliziert und in „M-net_CEP-Encryption“ umbenannt. Die Einstellungen im Reiter „Kryptografie“ und „Sicherheit“ sind analog zur M-net_Exchange-Enrollment-Agent(offlinerequest) Zertifikatvorlage.

Durch diese beiden Zertifikatvorlagen ist nun u. a. sichergestellt, dass die verwendeten Zertifikate für den Betrieb des NDES Dienstes den in Kapitel 3.2.6 definierten Schlüssellängen entsprechen. Nach dem Veröffentlichen der beiden Zertifikatvorlagen auf der Sub-CA-MDM sind die Zertifikatvorlagen für den NDES einsatzfähig.

4.4.3. Zertifikatvorlage für das MDM

In diesem Kapitel wird die zuständige Zertifikatvorlage für die Zertifikate konfiguriert, die für mobile Endgeräte, z. B. Handys, von MobileIron ausgestellt werden. Dafür wird die Zertifikatvorlage IPsec (Offlineanforderung) dupliziert und in „M-net_SCEP-MobileIron“ umbenannt. Die Gültigkeitsdauer wird auf ein Jahr festgelegt, der Reiter „Sicherheit“ wird nach dem M-net Standard angepasst und zusätzlich der Benutzer ndesuser mit den Rechten „Lesen“ und „Registrieren“ eingefügt. Im Reiter „Kryptografie“ wird die Schlüssellänge auf 2048 Bit definiert.

Mit der Veröffentlichung dieser Zertifikatvorlage ist die Konfiguration der Zertifikatvorlage für das Mobile Device Management abgeschlossen.

4.4.4. Zertifikatvorlage für den OCSP Responder

Damit der OCSP Responder seine Antwort an den Client signieren kann, braucht er ein Signaturzertifikat von der jeweiligen Zertifizierungsstelle, an die er angeschlossen ist. Für den OCSP Responder wird die Zertifikatvorlage OCSP-Antwortsignatur dupliziert und in dem Reiter „Kryptografie“ der Luna KSP in Verbindung mit RSA und 2048 Bit Schlüssellänge ausgewählt. In dem Reiter „Sicherheit“ wird der M-net Standard eingetragen und alle OCSP Responder mit den Berechtigungen „Lesen“ und „Registrieren“ hinzugefügt. Bei der Sub-CA-ServiceLan läuft der OCSP Responder direkt auf der CA, weshalb dort in dem Reiter „Sicherheit“ die Sub-CA-ServiceLan eingetragen wird. Durch das Beschränken auf „Registrieren“ und nicht auf „Automatisch registrieren“ wird es möglich, das Signaturzertifikat für den OCSP Responder bei einer manuellen Zertifikatregistrierung von einer bestimmten Zertifizierungsstelle zu erhalten. Dies ist notwendig, da sonst die Antwort des OCSP Responders eventuell mit dem Signaturzertifikat der falschen CA signiert und als ungültig behandelt

wird.

Diese Zertifikatvorlage muss in beiden Domänen erstellt und auf allen Sub CAs veröffentlicht werden. Damit ist die Konfiguration der Zertifikatvorlage für den OCSP Responder abgeschlossen.

4.5. Konfiguration Zertifizierungsdienste

Die erforderlichen Zertifizierungsdienste IIS, OCSP und NDES sind in Kapitel 4.3.2 installiert worden und müssen nun konfiguriert werden. Im Fall der Zertifizierungsstellen-Webregistrierung, die auf dem IIS läuft, ist die Konfiguration in Kapitel 4.3.2 zusammen mit der Zertifizierungsstelle abgeschlossen worden. Um die Anmeldedaten auf der Webseite verschlüsselt zu übertragen, muss der IIS noch per SSL abgesichert werden, was in Kapitel 4.5.1 durchgeführt wird.

4.5.1. Microsoft Internet Information Services (IIS)

Dieses Kapitel beschreibt die Absicherung des IIS per SSL. Eine Screenshot gestützte Dokumentation zur Absicherung des IIS per SSL kann in Kapitel A.5.6 nachgelesen werden.

Um die Kommunikation des IIS per HTTPS abzusichern, wird ein SSL Zertifikat benötigt. Dieses wird in dem Snap-In „Zertifikate (Lokaler Computer)“ der MMC durch die Zertifikatvorlage M-net.Domain-Webserver, welche in Kapitel 4.4.1 konfiguriert wurde, angefordert. In dem Internetinformationsdienste (IIS)-Manager wird anschließend für die „Default Web Site“ unter dem Menüpunkt „Bindungen“ die Sitebindung vom Typ „https“ auf den Port „443“ mit dem angeforderten SSL Zertifikat eingerichtet. In den SSL Einstellungen der Certsrv Webseite wird nun noch die Option „SSL erforderlich“ aktiviert, um den Zugriff nur per HTTPS zu erlauben.

Damit ist der IIS funktionstüchtig per SSL abgesichert und es können über die Webregistrierung Zertifikate angefordert werden.

4.5.2. OCSP Responder

Der OCSP Responder der Sub-CA-ServiceLan wird direkt auf der CA eingerichtet, während bei den anderen Sub CAs der OCSP Responder ausgelagert wird. Die Maschinen, die nur den OCSP Responder betreiben, müssen erst an die parocsp Partitionen der HSMs, wie in Kapitel 3.2.4 definiert und in Kapitel 4.2 beschrieben, angebunden werden. Anschließend wird der „Online-Responder Rollendienst“ über den Assistenten zum Hinzufügen von Rollen und Features installiert.

Die Konfiguration des Online-Responders ist für die Sub-CA-ServiceLan und die ausgelagerten OCSP Responder identisch. Über den Konfigurationsassistenten wird die Konfiguration des Online-Responders durchgeführt. Anschließend wird in den lokalen Diensten der Online-Responder-Dienst ausgewählt und dort im Reiter „Anmelden“ die Punkte „Anmelden als Lokales Systemkonto“ und „Datenaustausch zwischen Dienst und Desktop zulassen“ aktiviert. Die Aktivierung dieser beiden Punkte ist für das Luna HSM notwendig, um mit

4. Umsetzung

dem Online-Responder auf die HSM zugreifen zu können. In der MCC wird das Online-Responder Snap-In hinzugefügt und mit Rechtsklick auf „Sperrkonfiguration“ eine „Sperrkonfiguration hinzufügen“ ausgewählt. Dort gibt man einen beliebigen Namen für die Sperrkonfiguration ein, im Fall der M-net der Name des OCSP Responders. Danach „Zertifikat für eine vorhandene Unternehmenszertifizierungsstelle auswählen“ und „In Active Directory veröffentlichte Zertifizierungsstellenzertifikate suchen“ anklicken und die entsprechende Zertifizierungsstelle auswählen. Um die Konfiguration abzuschließen „Automatisch für ein OCSP-Signaturzertifikat registrieren“ anklicken und die entsprechende Zertifizierungsstelle auswählen. Mit Rechtsklick auf die „Sperrkonfiguration“ → „Eigenschaften“ werden im Reiter „Sperranbieter“ die „Sperranbiereigenschaften“ geöffnet und dort das Aktualisierungsintervall für die CRLs auf fünf Minuten gesetzt.

Damit ist der Online-Responder funktionstüchtig und im Dienstkonto des Computers befindet sich das entsprechende Signaturzertifikat.

4.5.3. Network Device Enrollment Service (NDES)

Für die Anbindung des MDM an die Sub-CA-MDM durch das Simple Certificate Enrollment Protocol, muss auf der Sub-CA-MDM der NDES Zertifizierungsdienst benutzt werden. Da dieser mittels IIS per HTTPS verfügbar gemacht wird, muss zuerst der IIS eingerichtet und so konfiguriert werden, dass er HTTPS Verbindungen unterstützt. Dies ist in Kapitel 4.5.1 beschrieben worden.

Für den NDES werden zwei Domänenaccounts eingerichtet. Der `ndesservice` benannte Account wird auf der Sub-CA-MDM den NDES betreiben. Der `ndesuser` benannte Account ist für den Zugriff von dem MobileIron Server, welcher das Mobile-Device-Management übernimmt, auf die CA notwendig, um die Zertifikate anzufordern. Der `ndesuser` ist normaler Domänenbenutzer. Der `ndesservice` ist Domänenadmin und wird in die lokale Administratorengruppe der Sub-CA-MDM und in die `IIS_IUSRS` Gruppe aufgenommen. Siehe hierzu den Dokumentationsschritt Nummer 93.

Für den NDES wird nun die Konfiguration des NDES über den Servermanager ausgeführt. Dabei wird das eben eingerichtete Dienstkonto `ndesservice` angegeben und der auf dieser Maschine eingerichtete Luna CSP als Kryptografieanbieter mit 2048 Bit Schlüssellänge verwendet. Nach der Konfiguration muss der NDES neu gestartet werden, was mit einem Neustart des IIS und somit des Befehls „`iisreset`“ möglich ist.

Damit von MobileIron aus Zertifikate angefordert werden können, muss in MobileIron folgendes konfiguriert werden:

- Microsoft SCEP als Protokoll angeben
- URL zur `mscep.dll` angeben:
„`https://<FQDN der Sub-CA-MDM>/CertSrv/mscep/mscep.dll`“
- Abfrage-URL des Netzwerk-Registrierungsdienstes angeben:
„`https://<FQDN der Sub-CA-MDM>/CertSrv/mscep_admin/`“
- Benutzerkonto `ndesuser` und Passwort eingeben

- Verschlüsselungsalgorithmus: RSA
- Schlüssellänge: 2048 Bit
- Signaturalgorithmus: SHA-256
- Zertifikatverwendungszwecke definieren

Damit ist die NDES Konfiguration und die Anbindung von MobileIron an die Sub-CA-MDM abgeschlossen .

4.6. Backup der Datenbank und der Konfiguration der Zertifizierungsstellen

Obwohl die Sub CAs alle drei Stunden automatisiert gesichert werden, wird zur Sicherheit nicht nur von der Root CA ein Backup angelegt, sondern auch einmalig eines der Sub CAs.

Ein Backup der Datenbank und der Konfiguration kann durch Abruf einer Batchdatei, wie in dem Listing 4.3 dargestellt, erfolgen.

Der „@echo off“ Befehl dient dazu, die Ausgabe auf der Kommandokonsole übersichtlicher zu präsentieren. Der Befehl „pause“ verhindert das automatische Schließen der Eingabeaufforderung, um den Status der Ausführung verfolgen zu können. Sollte das Skript automatisiert aufgerufen werden, so muss der „pause“ Befehl gelöscht oder auskommentiert werden. Mit dem Befehl „certutil -f -backupDB <Speicherort des Backups>“ wird die Datenbank exportiert. Durch den Befehl „reg export HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration <Speicherort des Backups>\<Dateiname>.reg“ wird die Konfiguration der CA exportiert. Durch das „/y“ wird die Datei, falls vorhanden, ohne Bestätigungsaufforderung überschrieben.

Diese Batchdatei wird auf jeder Zertifizierungsstelle ausgeführt. Das Backup der Datenbank und der Konfiguration werden in einem PGP verschlüsseltem Bereich abgelegt, von dem automatisiert Backups erstellt werden.

Listing 4.3: Batchdatei für das Backup der Datenbank und Konfiguration einer CA

```
1 @echo off
2 certutil -f -backupDB C:\pki_sources\Backup_CA
3 reg export HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
   CertSvc\Configuration C:\pki_sources\Backup_CA\pkiconfig.reg /y
4 pause
```

Das Backup der Datenbank und der Konfiguration der Zertifizierungsstellen ist damit abgeschlossen. Das Backup wird nun auf ein verschlüsseltes PGP Netzlaufwerk verschoben.

4.7. Offlinenehmen der Root CA

Um die Root CA offline zu nehmen, wird sie heruntergefahren. Im Anschluss daran muss die Verbindung zwischen den HSMs und der Root CA deaktiviert werden. Dazu meldet man sich analog zu Kapitel 4.9 an beiden HSMs an. Mit dem Befehl „client delete -client <Client-name>“ löscht man den Client von dem HSM. Dadurch kann die Root CA keine Verbindung mit den HSMs mehr herstellen.

Wenn die Root CA wieder benötigt wird, muss Folgendes auf der HSM durchgeführt werden:

- Übertragen des Clientzertifikats der Root CA
- Hinzufügen der Root CA als Client
- Neustart des NTLS Dienstes
- Zuweisen der zugehörigen Partition
- Speichern der IP-Adresse der Root CA

Dies sind die Schritte Nummer 6 bis 13 der Implementierungsdokumentation.

Zusätzlich könnte man noch die Konfiguration der HSM durch die KSPConfig.exe auf der Root CA löschen. Jedoch ist das Partitions Passwort verschlüsselt abgespeichert und ohne Konfiguration der Root CA als Client auf einer der HSMs kann keine Verbindung zum privaten Schlüssel hergestellt werden. Da die Root CA eine virtuelle Maschine ist, wird diese auf einen mit PGP verschlüsselten Dateiserver verschoben, auf den nur eine stark eingeschränkte Personengruppe Zugriff hat.

Somit ist die Root CA nun offline, verschlüsselt abgespeichert und von der HSM isoliert.

4.8. Erstellung des Schlüsselpaares der Backup Root CA

Das Erstellen des Backup Root CA Schlüsselpaares wird auf einem Laptop mit frisch installiertem Ubuntu 16.04 LTS und OpenSSL 1.0.2g durchgeführt. Für die Installation und Konfiguration des Luna Clients wird an dieser Stelle auf die Dokumentation von Gemalto [Gem15b] verwiesen. Es wird hierbei nur das HSM01 angebunden, da in Kapitel 4.9 ein Backup des HSM01 mit dem Backup HSM Modul erstellt wird, welches in Kapitel 5.1.3 zur Validierung auf der HSM02 wiederhergestellt wird.

Um das Schlüsselpaar erzeugen zu können, wird die in Listing 4.4 abgebildete Konfigurationsdatei „config.conf“ für OpenSSL erstellt. In Zeile 1 wird die Sektion „req“ definiert. In dieser Sektion wird nun in Zeile 2 der Signatur-Hash-Algorithmus festgelegt. Die Sektion „req.distinguished_name“, in Zeile 7 bis 13, wird in Zeile 3 dem Distinguished Name zugeordnet. Zeile 4 verhindert ein Eingabefenster und sorgt dafür, dass die Werte aus der Konfigurationsdatei übernommen werden. In Zeile 5 wird die Sektion für die Zertifikaterweiterungen definiert, in welcher das Zertifikat in Zeile 16 als Zertifizierungsstellenzertifikat festgelegt wird. Zusätzlich wird in Zeile 17 die Schlüsselverwendung als Digitale Signatur,

Zertifikatsignatur und Signieren der Sperrliste definiert, da die CA nur Zertifikate signieren, verifizieren und die CRL erstellen soll. Die Zertifikaterweiterung Schlüsselkennung des Antragstellers (subjectKeyIdentifier), wird in Zeile 18 definiert und bewirkt, dass der Hashwert des öffentlichen Schlüssels in das Zertifikat aufgenommen wird.

Listing 4.4: OpenSSL Konfigurationsdatei

```

1 [ req ]
2 default_md           = sha256
3 distinguished_name   = req_distinguished_name
4 prompt              = no
5 x509_extensions      = v3_ca
6
7 [ req_distinguished_name ]
8 C                   = DE
9 ST                  = Bavaria
10 L                  = Munich
11 O                   = M-net Telekommunikations GmbH
12 OU                  = IT
13 CN                  = M-net-Root-X2
14
15 [ v3_ca ]
16 basicConstraints    = critical , CA:true
17 keyUsage            = digitalSignature , keyCertSign , cRLSign
18 subjectKeyIdentifier = hash

```

Durch Ausführen des Befehls „openssl req -newkey rsa:4096 -x509 -keyout key.pem -out cert.pem -nodes -config config.conf -days 7305“ wird nun der private Schlüssel key.pem und das Zertifikat cert.pem generiert. In diesem Fall hat die Gültigkeitsdauer den Wert 7305. Mit dem Parameter „newkey“ und dem Argument „rsa:4096“ wird mit der Schlüssellänge 4096 Bit unter Verwendung von RSA ein neuer privater Schlüssel und eine Zertifikatsanforderung erzeugt. Der Parameter „x509“ bewirkt, dass statt dem CSR ein selbst signiertes Zertifikat erstellt wird. Der Dateiname des privaten Schlüssels wird mit dem Parameter „keyout“ und dem Argument „key.pem“ als „key.pem“ definiert. Der Dateiname des öffentlichen Schlüssels wird mit dem Parameter „out“ und dem Argument „cert.pem“ definiert. Mit dem Parameter „nodes“ wird die Verschlüsselung des privaten Schlüssels verhindert, da das HSM einen unverschlüsselten privaten Schlüssel benötigt. Der Parameter „config“ lädt mit seinem Argument die „config.conf“ Konfigurationsdatei. Mit dem Parameter „days“ wird die Gültigkeitsdauer des Zertifikats auf 7305 Tage festgelegt, was 20 Jahren entspricht und in Kapitel 3.2.6 für die Root CA definiert wurde.

Mit dem Befehl „openssl x509 -in cert.pem -noout -text“ lässt sich das Zertifikat im Editor anzeigen und überprüfen. Auf einem Windows Computer kann das „cert.pem“ in „cert.cer“ umbenannt werden und dann per Doppelklick geöffnet und angeschaut werden.

Da die HSM ein nicht verschlüsseltes PKCS#8 Format benötigt, wird folgender Befehl ausgeführt: „openssl pkcs8 -in key.pem -topk8 -out noenckey.pem -nocrypt“.

Die „noenckey.pem“ Datei wird nun in das Installationsverzeichnis des Luna Clients kopiert und dort ein Eingabefenster geöffnet. Um den privaten Schlüssel auf die HSM01 zu kopieren wird der Befehl „cmu importkey -PKCS8 -in key.pem -keyalg RSA“ eingegeben. Das Argument des Parameters „in“ ist der private Schlüssel und das Argument des Parame-

4. Umsetzung

ters „keyalg“ die Verschlüsselungsart, in diesem Fall RSA. Anschließend wird das Partitions-passwort des HSMs eingegeben, um das Hochladen auf die HSM zu starten. Das erfolgreiche Hochladen des Schlüssels lässt sich, wie in Kapitel 5.1.1 beschrieben, überprüfen. Der öffentliche Schlüssel wird analog zum öffentlichen Schlüssel der Root CA veröffentlicht, siehe Kapitel 4.3.3.

Da der Laptop nun nicht mehr benötigt wird, sollten die Daten auf der Festplatte vollständig gelöscht werden. Dies kann z. B. mit dem Programm Darik's Boot And Nuke, was das Bundesamt für Sicherheit in der Informationstechnik empfiehlt [datwn], getan werden.

4.9. Backup der Partitionen des Hardware-Sicherheitsmoduls

Beim Luna HSM Backup Modul gibt es zwei Arten den Inhalt der HSMs zu sichern:

- Das Backup HSM Modul wird per USB-Kabel an die Luna HSM angeschlossen und anschließend eine SSH Verbindung zur HSM aufgebaut, über die das Backup angestoßen wird.
- Das Backup Modul wird direkt an die Zertifizierungsstelle angeschlossen und über den Luna Client gesteuert. Dabei ist zu beachten, dass hierbei nur die Partitionen auf der HSM gesichert werden können, die auf der HSM konfiguriert sind.

Das HSM Backup Modul wird direkt an das HSM angeschlossen, da fünf Partitionen in Benutzung sind und es keine Maschine gibt, die mehr als eine Partition angebunden hat. Da nur auf der HSM01 der Schlüssel der Backup Root CA gespeichert ist, wird das HSM Backup Modul an die HSM01 angeschlossen und von dieser ein Backup gemacht. Sobald der Schlüssel der Backup Root CA in Kapitel 5.1.3 auf die HSM02 übertragen worden ist, ist die Wahl des HSMs, von welchem ein Backup erstellt werden soll, nicht mehr wichtig, da für alle anderen Partitionen beide HSMs zusammen in einem High Availability-Cluster eingerichtet sind und somit den gleichen synchronisierten Inhalt haben. Dadurch muss nur von einer der beiden HSMs ein Backup erstellt werden.

Mit einem SSH Programm, z. B. PuTTY, wird mit dem Befehl „ssh admin@<HSM-HostName>“ und der anschließenden Eingabe des Passworts die Anmeldung auf der HSM durchgeführt. Mit dem Befehl „token backup list“ wird die Seriennummer des HSM Backup Moduls angezeigt. Nun wird mit dem Befehl „partition backup -serial <Seriennummer> -partition <Partitionsname auf der HSM die gesichert werden soll> -tokenPar <Partitionsname auf dem Backup HSM> -tokenPW <HSM Backup Passwort> -password“ und der anschließenden Eingabe des Passworts der zu sichernden Partition, ein Backup durchgeführt. Mit „token backup show -serial <Seriennummer>“ kann nun die Erstellung des Backups angezeigt werden.

Das HSM Backup Modul wird in einem Tresor mit stark eingeschränktem Zugriff verwahrt.

4.10. Zusammenfassung

Die Implementierung des in Kapitel 3.2 ausgearbeiteten Konzepts wurde in diesem Kapitel durchgeführt und in der Implementierungsdokumentation in Anhang A mit Screenshots dokumentiert.

Dabei wurde zuerst das HSM initialisiert, die erforderlichen Partitionen erstellt und anschließend die zu den CAs zugeteilten Partitionen an diese angebunden. Danach wurden auf den CAs das HA-Cluster und die Kryptografieanbieter konfiguriert. Für eine erleichterte Installation und Konfiguration der Zertifizierungsstellen sind zwei Konfigurationsskripte erklärt und erstellt worden, die dann bei der Installation der CAs und ihrer jeweiligen Zertifizierungsdienste benutzt wurden. Nach der Installation wurde der private Schlüssel und das Zertifikat der Root CA auf dem HA-Cluster erzeugt, die Root CA in Betrieb genommen und eine Sperrliste veröffentlicht. Anschließend sind die Sperrliste und das Root CA Zertifikat in den in Kapitel 3.2.8 definierten CDPs verfügbar gemacht worden. Nun wurden die Sub CAs mit von der Root CA signierten Zertifizierungsstellenzertifikaten in Betrieb genommen und die benötigten Zertifikatvorlagen konfiguriert. Mit der Konfiguration der Zertifizierungsdienste, u. a. des OCSP Responders und des NDES, ist die Installation der PKI abgeschlossen worden.

Es wurde von jeder CA die Datenbank und Konfiguration gesichert und anschließend die Root CA offline genommen. Der private Schlüssel und das Zertifikat der Backup Root CA wurden erstellt und auf der HSM01 gespeichert, von der anschließend ein Backup mit dem Backup HSM Modul gemacht wurde.

In dem nun folgenden Kapitel findet eine Funktionsüberprüfung der PKI und eine Verifikation der Umsetzung der Anforderungen aus Kapitel 3.1 statt.

5. Verifikation

In diesem Kapitel wird die erfolgreiche Implementierung der Public Key Infrastruktur und die Umsetzung der Anforderungen aus Kapitel 3.1 durch Tests überprüft. Dabei wird Folgendes überprüft:

Tabelle 5.1.: Funktionsüberprüfung der PKI

| Test | Kapitel |
|---|---------|
| Schlüsselspeicherung in den HSM Partitionen | 5.1.1 |
| HSM HA-Cluster | 5.1.2 |
| Backup und Wiederherstellung eines Schlüssels des HSM | 5.1.3 |
| Manuelles Ausstellen eines Zertifikats über die MMC auf der CA | 5.2.1.1 |
| Manuelles Ausstellen eines Zertifikats über die MMC auf dem Zertifikatempfänger | 5.2.1.2 |
| Manuelles Ausstellen eines Zertifikats über Certreq auf der CA | 5.2.1.3 |
| Manuelles Ausstellen eines Zertifikats über die Zertifizierungsstellen-Webregistrierung | 5.2.1.4 |
| Automatisches Ausstellen eines Zertifikats über Gruppenrichtlinien | 5.2.1.5 |
| Testzertifikat über NDES ausstellen | 5.2.1.6 |
| Zertifikatgültigkeit über das AD | 5.2.2.1 |
| Zertifikatgültigkeit über den Webserver | 5.2.2.2 |
| Zertifikatgültigkeit über das OCSP | 5.2.2.3 |

Tabelle 5.2.: Anforderungsüberprüfung der PKI

| Anforderung | Kapitel |
|------------------------|---------------------------|
| Ausbaumöglichkeiten | 3.2.3, 3.2.10 |
| Betriebssysteme | 3.2.4 |
| Ausstellbarkeit | 5.2.1.1, 5.2.1.3, 5.2.1.4 |
| MDM | 5.2.1.6 |
| Zertifikattypen | 5.2.1.2, 5.2.1.3 5.2.1.4 |
| Netzwerkcompatibilität | 3.2.4 |
| Schlüssellänge | 3.2.6 |
| Zertifikatanforderung | 5.2.1.4 |
| Zertifikatstatus | 5.2.2.1, 5.2.2.2, 5.2.2.3 |
| Verfügbarkeit | 3.2.4, 3.2.8, 3.2.13 |
| Wiederherstellbarkeit | 3.2.12, 4.8 |
| AltCA | 5.2.1.2 |

5.1. Hardware-Sicherheitsmodul

Hier geht es um die Überprüfung des Hardware-Sicherheitsmoduls in Bezug auf das Wiederherstellen der Verbindung zum HSM High Availability-Cluster, dem Backup der Schlüssel auf den HSMs und dem Wiederherstellen der Schlüssel aus dem Backup.

5.1.1. Schlüssel in Hardware-Sicherheitsmodul Partitionen

Um die erfolgreiche Generierung des Schlüsselpaares in der HSM zu überprüfen, kann der Inhalt der Partition, in der das Schlüsselpaar erzeugt und gespeichert wurde, angeschaut werden.

Dazu wird mit einem SSH Programm, z. B. PuTTY, mit dem Befehl „admin@<HSM name>“ eine Verbindung zum HSM hergestellt. Anschließend wird mit dem Befehl „partition showContent -partition <Partitionsname>“ der Inhalt der Partition angezeigt. Dies ist in Abbildung 5.1 zu sehen. Da die Schlüssel durch das High Availability-Cluster auf beiden HSMs gespeichert werden, wird zusätzlich überprüft, ob die Inhalte der Partitionen auf beiden HSMs identisch sind. Dies ist, mit Ausnahme der Partition, in der der Schlüssel der Backup Root CA gespeichert wird, der Fall. Der Schlüssel der Backup Root CA wird erst in Kapitel 5.1.3 auf die HSM02 kopiert.

```

login as: <Benutzer>
Authenticating with public key "<Key Name>"
Passphrase for key "<Key Name>":
Last login: Sun Nov 19 11:34:37 2017 from <IP eines PCs>
-bash-4.2$ ssh <Anmeldename an HSM>@HSM01
<Anmeldename an HSM>@HSM01 's password:
Last login: Sun Nov 19 05:35:14 2017 from <IP eines PCs>

Luna SA 6.2.2-5 Command Line Shell - Copyright (c) 2001-2016 SafeNet, Inc. All rights reserved.

[HSM01] lunash:>partition showContents -partition parit

Please enter the user password for the partition:
> *****

Partition Name:                parit
Partition SN:                  <Seriennummer parit>
Partition Label:               parit
Storage (Bytes): Total=20480, Used=3664, Free=16816
Number objects: 2

Object Label: M-net-Root-X1
Object Type: Private Key
Object Handle: 47

Object Label: M-net-Root-X1
Object Type: Public Key
Object Handle: 46

Command Result : 0 (Success)
[HSM01] lunash:>
    
```

Abbildung 5.1.: Inhalt der carootx1 Partition auf der HSM

5.1.2. High Availability-Cluster

Da die beiden HSMs in zwei verschiedenen Rechenzentren aufgebaut und somit automatisch an zwei verschiedenen Switchen angeschlossen sind, wird zum Testen des High Availability-Clusters der Port des Switches, an dem eine der beiden HSMs angeschlossen ist, deaktiviert. Die Funktion der CA sollte danach weiterhin gegeben sein. Überprüfbar ist dies durch eine Erstellung einer neuen CRL. Kann diese erstellt werden, besteht noch weiter Zugriff auf den privaten Schlüssel in der HSM, da dieser zum Signieren der CRL verwendet wird. Schlägt die Erstellung der CRL fehl, ist das High Availability-Cluster nicht richtig konfiguriert worden.

Um mitzuverfolgen, wie die Verbindung abbricht und wieder aufgebaut wird, kann das Logging auf der CA aktiviert werden. Dazu wird mit der Eingabeaufforderung in das Installationsverzeichnis des Luna Clients navigiert, dort die Lunacm durch Eingabe von „lunacm“ gestartet und mit „ha halog -enable“ das Logging aktiviert. Die Ausgabe der Logdatei ist in Listing 5.1 zu sehen.

Listing 5.1: Ausgabe HALog nach Trennen der Verbindung zu einer HSM

```

1 Fri Nov 10 10:32:28 2017 : [276] HA group: <Seriennummer HA-Partition>
  Probing thread started
2 Fri Nov 10 10:34:25 2017 : [2088] HA group: <Seriennummer HA-Partition
  > unable to reach member: <Seriennummer Partition>. Manual Recover
  or Auto Recovery will be able to recover this member
3 Fri Nov 10 10:34:25 2017 : [2088] HA group: <Seriennummer HA-Partition
  > Probing thread started
4 Fri Nov 10 10:42:06 2017 : [2828] HA group: <Seriennummer HA-Partition
  > unable to reach member: <Seriennummer Partition>. Manual Recover
  or Auto Recovery will be able to recover this member
5 Fri Nov 10 10:42:06 2017 : [2828] HA group: <Seriennummer HA-Partition
  > Probing thread started
6 Fri Nov 10 10:42:56 2017 : [2828] HA group: <Seriennummer HA-Partition
  > recovery attempt #1 failed for member: <Seriennummer Partition>.
  Code: 0xC000050B : RC.REMOTE_PEER_OFFLINE
7 Fri Nov 10 10:43:26 2017 : [2828] HA group: <Seriennummer HA-Partition
  > recovery attempt #2 failed for member: <Seriennummer Partition>.
  Code: 0xC000050B : RC.REMOTE_PEER_OFFLINE
8 Fri Nov 10 10:44:36 2017 : [2828] HA group: <Seriennummer HA-Partition
  > recovery attempt #3 failed for member: <Seriennummer Partition>.
  Code: 0xC000050B : RC.REMOTE_PEER_OFFLINE
9 Fri Nov 10 10:45:46 2017 : [2828] HA group: <Seriennummer HA-Partition
  > recovery attempt #4 failed for member: <Seriennummer Partition>.
  Code: 0xC000050B : RC.REMOTE_PEER_OFFLINE
10 Fri Nov 10 10:46:56 2017 : [2828] HA group: <Seriennummer HA-Partition
  > recovery attempt #5 failed for member: <Seriennummer Partition>.
  Code: 0xC000050B : RC.REMOTE_PEER_OFFLINE
11 Fri Nov 10 10:48:07 2017 : [2828] HA group: <Seriennummer HA-Partition
  > recovery attempt #6 failed for member: <Seriennummer Partition>.
  Code: 0xC000050B : RC.REMOTE_PEER_OFFLINE
12 Fri Nov 10 10:49:07 2017 : [2828] HA group: <Seriennummer HA-Partition
  > recovery attempt #7 failed for member: <Seriennummer Partition>.
  Code: 0xC000050B : RC.REMOTE_PEER_OFFLINE
13 Fri Nov 10 10:50:17 2017 : [2828] HA group: <Seriennummer HA-Partition
  > recovery attempt #8 failed for member: <Seriennummer Partition>.
  Code: 0xC000050B : RC.REMOTE_PEER_OFFLINE
14 Fri Nov 10 10:51:27 2017 : [2828] HA group: <Seriennummer HA-Partition
  > recovery attempt #9 failed for member: <Seriennummer Partition>.

```

5. Verifikation

```
Code: 0xC000050B : RC_REMOTE_PEER_OFFLINE
15 Fri Nov 10 10:52:37 2017 : [2828] HA group: <Seriennummer HA-Partition
   > recovery attempt #10 failed for member: <Seriennummer Partition
   >. Code: 0xC000050B : RC_REMOTE_PEER_OFFLINE
16 Fri Nov 10 10:53:47 2017 : [2828] HA group: <Seriennummer HA-Partition
   > recovery attempt #11 failed for member: <Seriennummer Partition
   >. Code: 0xC000050B : RC_REMOTE_PEER_OFFLINE
17 Fri Nov 10 10:54:57 2017 : [2828] HA group: <Seriennummer HA-Partition
   > recovery attempt #12 failed for member: <Seriennummer Partition
   >. Code: 0xC000050B : RC_REMOTE_PEER_OFFLINE
18 Fri Nov 10 10:56:08 2017 : [2828] HA group: <Seriennummer HA-Partition
   > recovery attempt #13 failed for member: <Seriennummer Partition
   >. Code: 0xC000050B : RC_REMOTE_PEER_OFFLINE
19 Fri Nov 10 10:57:08 2017 : [2828] HA group: <Seriennummer HA-Partition
   > recovery attempt #14 failed for member: <Seriennummer Partition
   >. Code: 0xC000050B : RC_REMOTE_PEER_OFFLINE
20 Fri Nov 10 10:58:18 2017 : [2828] HA group: <Seriennummer HA-Partition
   > recovery attempt #15 failed for member: <Seriennummer Partition
   >. Code: 0xC000050B : RC_REMOTE_PEER_OFFLINE
21 Fri Nov 10 10:59:28 2017 : [2828] HA group: <Seriennummer HA-Partition
   > recovery attempt #16 failed for member: <Seriennummer Partition
   >. Code: 0xC000050B : RC_REMOTE_PEER_OFFLINE
22 Fri Nov 10 11:00:38 2017 : [2828] HA group: <Seriennummer HA-Partition
   > recovery attempt #17 failed for member: <Seriennummer Partition
   >. Code: 0xC000050B : RC_REMOTE_PEER_OFFLINE
23 Fri Nov 10 11:01:48 2017 : [2828] HA group: <Seriennummer HA-Partition
   > recovery attempt #18 failed for member: <Seriennummer Partition
   >. Code: 0xC000050B : RC_REMOTE_PEER_OFFLINE
24 Fri Nov 10 11:02:49 2017 : [2828] HA group: <Seriennummer HA-Partition
   > recovery attempt #19 succeeded for member: <Seriennummer
   Partition>
25 Fri Nov 10 11:40:46 2017 : [2828] HA group: <Seriennummer HA-Partition
   > Probing thread terminated
26 Fri Nov 10 12:09:47 2017 : [3096] HA group: <Seriennummer HA-Partition
   > Probing thread started
```

Somit ist die Umsetzung der Anforderung Verfügbarkeit in Bezug auf die HSMs durch das erfolgreiche Testen des High Availability-Clusters umgesetzt.

5.1.3. Backup und Wiederherstellung der Schlüssel der Hardware-Sicherheitsmodule

Die Verifikation des erfolgreich verlaufenen Backups wurde in Kapitel 4.9 durchgeführt.

Um zu testen, ob das Backup wieder eingespielt werden kann, wird der private Schlüssel der Backup Root CA, der auf dem Backup HSM gesichert ist, auf der HSM02 wiederhergestellt. Dafür wird das Backup HSM an das HSM angeschlossen und folgender Befehl nach der Anmeldung auf der HSM über ssh ausgeführt: „partition restore -serial <Seriennummer des Backup HSMs> tokenPar <Partitionsname auf dem Backup HSM die wiederhergestellt werden soll> -partition <Partitionsname auf der HSM, in der das Backup wiederhergestellt werden soll> -replace -tokenPW <Passwort des Backup HSMs>-password“. Anschließend wird das Partitionspassword auf der HSM, in das das Backup wiederhergestellt werden soll, abgefragt. Mit dem Befehl „partition showContents -partition -password“ und der anschließenden

Eingabe des Partitionspasswords lässt sich der Inhalt der wiederhergestellten Partition überprüfen.

5.2. Zertifikate

In diesem Kapitel werden die verschiedenen Arten, wie ein Zertifikat angefordert werden kann, validiert. Ebenfalls werden zur Funktionsüberprüfung der CDPs Zertifikate gesperrt.

5.2.1. Ausstellung Zertifikate

Die verschiedenen Arten Zertifikate anzufordern, die durch die Anforderungen Ausstellbarkeit, MDM, Zertifikattypen und Zertifikatanforderung umgesetzt werden müssen, werden in diesem Kapitel verifiziert.

5.2.1.1. Manuelles Ausstellen über die Microsoft Management Console auf der Zertifizierungsstelle

Um ein Zertifikat manuell direkt auf der Zertifizierungsstelle auszustellen, wird eine Zertifikatanforderung benötigt. Mit dem Programm OpenSSL kann z. B. ein privater Schlüssel und ein CSR mit nachfolgendem Befehl erstellt werden:

```
„openssl req -new -newkey rsa:2048 -sha256 -nodes -out PCMUC363.csr -keyout PCMUC363.key -subj „/C=DE/ST=Bavaria/L=Munich/O=M-net Telekommunikations GmbH/OU=IT/CN=PCMUC363““
```

Der nun erstellte PCMUC363.key ist der private Schlüssel und der PCMUC363.csr die Zertifikatanforderung, welche beide in Base64 codiert sind.

Die Datei „PCMUC363.csr“ wird nun auf die CA kopiert und dort die Microsoft Management Console geöffnet. Dort wird das Snap-In „Lokale Zertifizierungsstelle“ zur Konsole hinzugefügt und mit Rechtsklick auf den Namen der Zertifizierungsstelle unter „Alle Aufgaben“ → „Neue Anforderung einreichen“ die Zertifikatanforderung ausgewählt und somit auf der CA eingereicht. Unter „Ausstehende Anforderungen“ ist diese nun zu finden und wird mit Rechtsklick „Alle Aufgaben“ → „Ausstellen“ ausgestellt, woraufhin sich dieses unter den ausgestellten Zertifikaten befindet. Mit dem Zertifikatexport-Assistenten lässt sich das Zertifikat exportieren. Dies ist in der Screenshot gestützten Implementierungsdokumentation in den Schritten Nummer 55 bis 58 abgebildet.

5.2.1.2. Manuelles Ausstellen über die Microsoft Management Console auf dem Zertifikatempfänger

Eine manuelle Zertifikatanforderung für eine domänenintegrierte Windows Maschine über die Microsoft Management Console garantiert eine höhere Kontrolle und erlaubt u. a. die Angabe von SANs, was bei der automatischen Zertifikatregistrierung, wie sie in Kapitel 5.2.1.5 beschrieben ist, nicht möglich ist.

Zuerst muss man sich auf der Sub CA, die das Zertifikat ausstellen soll, anmelden, um dort die gewünschte Zertifikatvorlage zu konfigurieren und zu veröffentlichen. Die Duplizierung

5. Verifikation

und die M-net spezifische Konfiguration wird, wie in Kapitel 4.4 beschrieben, durchgeführt. Anschließend muss im Reiter „Sicherheit“ der Zertifikatvorlage der Computer aufgenommen und ihm das Recht „Registrieren“ gegeben werden. Zusätzlich wird im Reiter „Antragstellername“ die Option „Antragstellerinformationen aus vorhandenen Zertifikaten für Erneuerungsanforderungen für die automatische Registrierung verwenden“, wie in Abbildung 5.2 zu sehen, ausgewählt. Die Zertifikatvorlage wird nun, wie in Kapitel 4.4 erläutert, veröffentlicht.

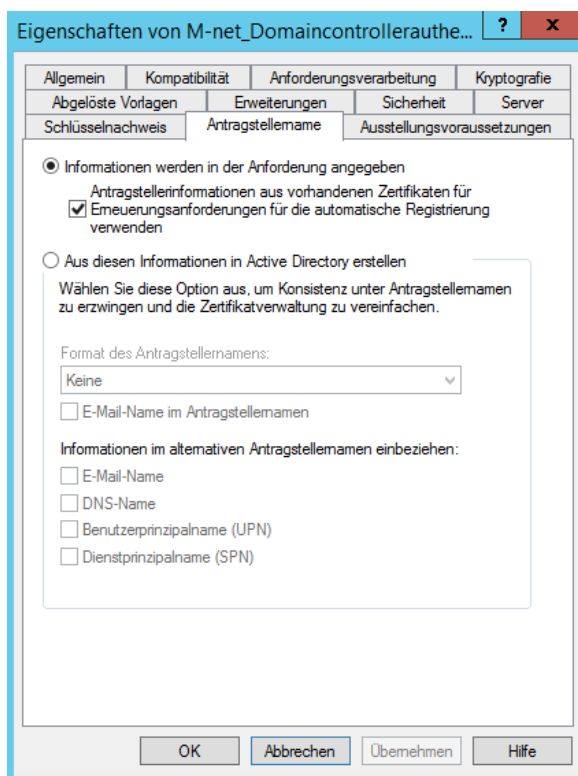


Abbildung 5.2.: Anpassen der Informationen über den Antragstellername für das manuelle Ausstellen eines Zertifikates über die MMC

Nun öffnet man auf der Maschine, die das Zertifikat bekommen soll, die MMC Konsole mit Domänenadminrechten und bindet das Snap-In „Zertifikate (Lokaler Computer)“ ein. Anschließend führt man einen Rechtsklick auf „Eigene Zertifikate“ aus und wählt „Alle Aufgaben“ → „Neues Zertifikat anfordern“ aus. Nun wird in dem sich öffnenden Fenster die gewünschte Zertifikatvorlage ausgewählt, welche mit Klick auf die Eigenschaften nun konfiguriert werden kann, um beispielsweise individuelle SANs für diese Maschine, wie z. B. die IP-Adresse, anzugeben. Nach einem Klick auf „Übernehmen“ und „Registrieren“ befindet sich im Ordner „Eigene Zertifikate“ das ausgestellte Zertifikat. Ein so ausgestelltes Zertifikat mit angegebenen SANs ist in Abbildung 2.9 zu sehen. In Kapitel A.5.6 wird auf diese Weise ein SSL Zertifikat angefordert, wobei ein Teil der Schritte mit Screenshots dokumentiert ist.

5.2.1.3. Manuelles Ausstellen mit dem Programm Certreq auf der Zertifizierungsstelle

Das Microsoft Kommandokonsolenprogramm Certreq ist seit Windows Server 2003 und Windows XP verfügbar und seit Windows Vista bzw. Server 2008 vorinstalliert. Certreq

ermöglicht das Ausstellen, Verwalten, Erstellen und Akzeptieren von Zertifikatanforderungen [Mic17].

Es wird eine Zertifikatanforderung „request.csr“ auf die CA kopiert, die das Zertifikat ausstellen soll. In diesem Ordner wird nun ein Eingabefenster geöffnet und nachfolgender Befehl eingegeben, um in diesem Ordner das Zertifikat „cert.crt“ zu erstellen:

```
„certreq -submit -attrib „CertificateTemplate:<Zertifikatvorlage>“ -config „<Maschinenname der CA>\<CA name>“ request.csr cert.crt“
```

Für das Hinzufügen von SANs muss der Parameter hinter -attrib mit Folgendem ersetzt werden: „CertificateTemplate:<Zertifikatvorlage> \nSAN:DNS=<FQDN der Maschine, die das Zertifikat bekommen soll>& IP-Address=<IP-Adresse der Maschine, die das Zertifikat bekommen soll>“. Anschließend kann das erzeugte Zertifikat „cert.crt“ per Doppelklick geöffnet und überprüft werden. Das ausgestellte Zertifikat ist nun auch unter den ausgestellten Zertifikaten in der CA sichtbar.

Zur Verifizierung wird ein Zertifikat für die Maschine „PCMUC363“ auf der Sub CA M-net-Sub-Intern-01 mit der Zertifikatvorlage „M-net_SSLservices“ ausgestellt, siehe Abbildung 5.3.

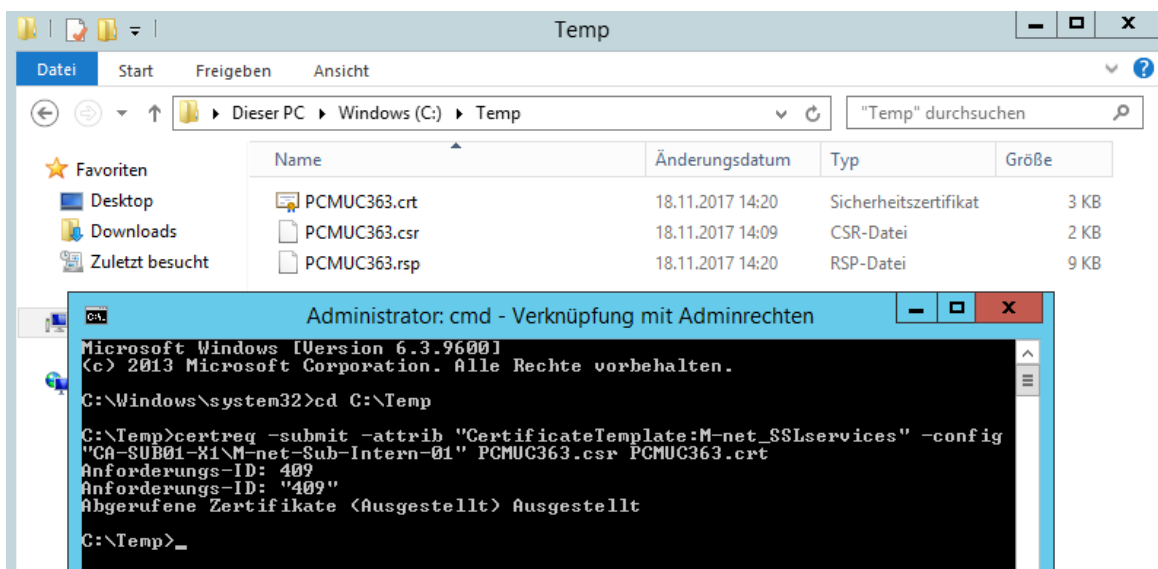


Abbildung 5.3.: Manuelles Ausstellen eines Zertifikats mit dem Programm Certreq

5.2.1.4. Manuelles Ausstellen über die Zertifizierungsstellen-Webregistrierung

Dieses Kapitel behandelt die Verifizierung der Ausstellbarkeit eines Zertifikats über die Zertifizierungsstellen-Webregistrierung, welche auf dem IIS Webserver läuft.

Die Zertifizierungsstellen-Webregistrierung wird in einem Browser unter dem Pfad „https://<FQDN der CA>/certsrv/“ geöffnet, auf der man zur Eingabe seiner Anmeldedaten aufgefordert wird und die anschließend die Zertifizierungsstellen-Webregistrierung der CA anzeigt. Siehe Abbildung 5.4.

5. Verifikation



Abbildung 5.4.: Zertifizierungsstellen-Webregistrierung

Dort wird „Ein Zertifikat anfordern“ ausgewählt und anschließend auf die Option zum Einreichen einer Zertifikatanforderung geklickt. Es öffnet sich die in Abbildung 5.5 dargestellte Webseite. Eine Base64 codierte Zertifikatanforderung, die man z. B. mit dem Programm OpenSSL, wie in Kapitel 5.2.1.1 beschrieben, erstellen kann, öffnet man mit einem Editor und kopiert den Text aus dieser Datei in das Textfeld der Webseite. Danach wird die gewünschte Zertifikatvorlage ausgewählt und ggf. in dem Textfeld „Attribute“ noch zusätzliche SANs eingetragen. Mit Klick auf „Einsenden“ kann anschließend das Zertifikat heruntergeladen werden. Auf der CA kann dieses nun auch unter den ausgestellten Zertifikaten eingesehen werden.

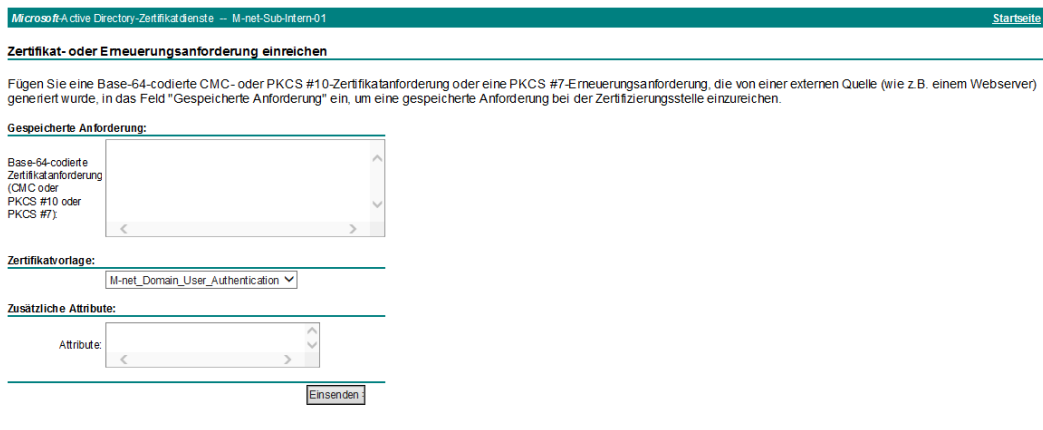


Abbildung 5.5.: Zertifikatanforderung über den IIS einreichen

5.2.1.5. Automatische Verteilung der Zertifikate durch Gruppenrichtlinien

Das Recht zur automatischen Verteilung der Zertifikate muss per Gruppenrichtlinie konfiguriert und anschließend eine Aktualisierung der Gruppenrichtlinien auf den Maschinen angestoßen werden. Eine manuelle Aktualisierung der Gruppenrichtlinie auf einer Windowsmaschine erfolgt mit dem Befehl „gpupdate /force“. Anschließend wird in der Microsoft Management Console auf dem Computer in dem eingebundenen Snap-in „Eigene Zertifikate - Lokaler Computer“ bzw. „Eigene Zertifikate - Benutzerkonto“ das erstellte Zertifikat angezeigt. Das ausgestellte Zertifikat wird zudem auch in der CA unter den ausgestellten Zertifikaten aufgelistet.

5.2.2. Zertifikatsperrung und Gültigkeitsüberprüfung

Dieses Kapitel behandelt die Überprüfung der Sperrung eines Zertifikats und des Sperrstatus der einzelnen CDPs.

Wird ein Zertifikat gesperrt und nicht sofort eine neue Sperrliste ausgestellt, wird der aktuelle Zertifikatsstatus erst mit dem regulären Sperrlistenenerneuerungsintervall übermittelt. Wird jedoch die Sperrliste nach der Sperrung sofort ausgestellt, kommt es je nach CDP zu unterschiedlichen Verzögerungen. Die dabei auftretenden Verzögerungen werden in den folgenden Unterkapiteln 5.2.2.1, 5.2.2.2 und 5.2.2.3 für diese PKI erläutert.

Läuft die Gültigkeitsdauer eines Zertifikats aus, muss dafür keine CRL durchsucht werden, da die Clients die Gültigkeitsdauer anhand ihrer Uhrzeit überprüfen können.

5.2.2.1. Active Directory

Das AD braucht bei M-net ca. 15 Minuten, bis sich alle Domänencontroller synchronisiert haben. Ab diesem Zeitpunkt ist die Anfrage eines Zertifikatsstatus eines gesperrten Zertifikats über LDAP spätestens mit ungültig beantwortet.

Um dies zu testen, wird ein Zertifikat gesperrt, die Sperrliste manuell veröffentlicht, das gesperrte Zertifikat exportiert und auf dem Desktop gespeichert. Es werden 20 Minuten abgewartet und anschließend auf dem Desktop eine Kommandokonsole geöffnet, wobei Folgendes eingetippt wird: „certutil -url „<Zertifikatsname>.cer““. Es öffnet sich die Certutil GUI, siehe Abbildung 5.8. In diesem Programm können alle Zertifikate und Sperrlisten aus den eingetragenen AIAs und CDPs des Zertifikats heruntergeladen werden. Für die Überprüfung der Sperrliste über LDAP wird auf den LDAP CDP ein Doppelklick ausgeführt, woraufhin die aktuelle Sperrliste, mit dem soeben gesperrten Zertifikat, angezeigt wird.

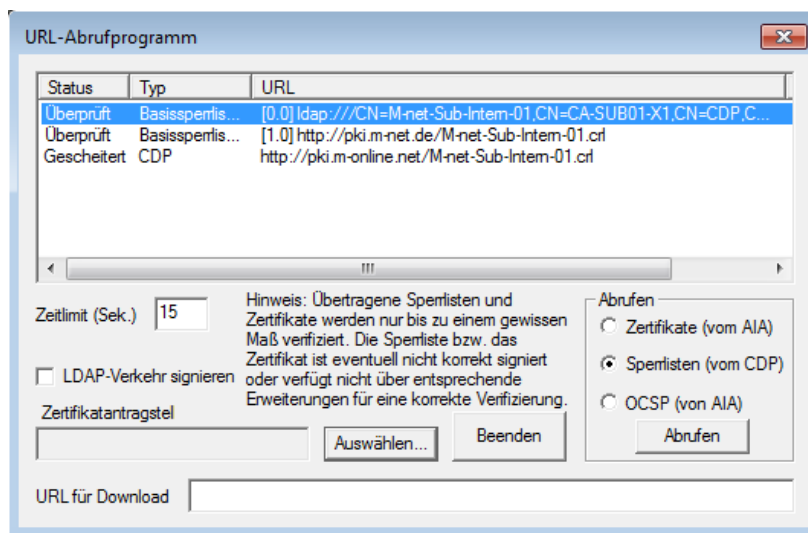


Abbildung 5.8.: Certutil GUI

Die Überprüfung einer Zertifikatsperrung mit der Sperrliste, die über das Active Directory

bezogen wird, ist damit erfolgreich getestet worden.

5.2.2.2. Webserver

Die Webserver greifen auf den Netzwerkspeicher zu, in dem die Zertifizierungsstellen ihre CRLs ablegen und stellen die CRLs dann auf *http://pki.m-net.de* zum Abruf bereit. Der Zugriff auf den Netzwerkspeicher findet alle fünf Minuten statt.

Das Überprüfen des Webservers geht zum Beispiel direkt mit einem Aufruf der Webseite über einen Browser. Dort können alle Zertifikate und Sperrlisten heruntergeladen werden. Eine Überprüfung mit dem Certutil Programm, wie in Kapitel 5.2.2.1 beschrieben, ist ebenfalls möglich. Dazu ist hier ein Doppelklick auf den HTTP CDP notwendig.

Um dies zu testen, wird ein Zertifikat gesperrt, die Sperrliste manuell veröffentlicht und sieben Minuten später die CRL von *itemithttp://pki.m-net.de* heruntergeladen. Auch dieser Test verlief erfolgreich.

5.2.2.3. Online Certificate Status Protocol (OCSP)

Um den OCSP Responder einer CA zu testen, kann ein von ihr ausgestelltes und gesperrtes Zertifikat verwendet und mit folgendem Befehl die Certutil GUI geöffnet und dort überprüft werden: „certutil -url „<Zertifikatname>.cer““

Bei einem gesperrten Zertifikat kommt die Antwort „gesperrt“, ansonsten „überprüft“.

Zu Beachten ist, dass der OCSP Responder die Gültigkeitsdauer nicht kontrolliert und bei einem zeitlich abgelaufenem Zertifikat trotzdem den Status „Überprüft“ zurückliefert. Da der OCSP Responder kürzlich erfolgte Zertifikatstatusanfragen in einem Cache speichert, darf der Zertifikatstatus vor der Sperrung nicht über den OCSP Responder überprüft werden.

Da das Aktualisierungsintervall des OCSP Responders in Kapitel 4.5.2 auf fünf Minuten festgelegt wurde, wird zum Test des OCSP Responders ein Zertifikat gesperrt, die Sperrliste manuell veröffentlicht und sieben Minuten später der Sperrstatus mit der Certutil GUI überprüft. Dieser Test ist erfolgreich verlaufen, siehe Abbildung 5.9.

5. Verifikation

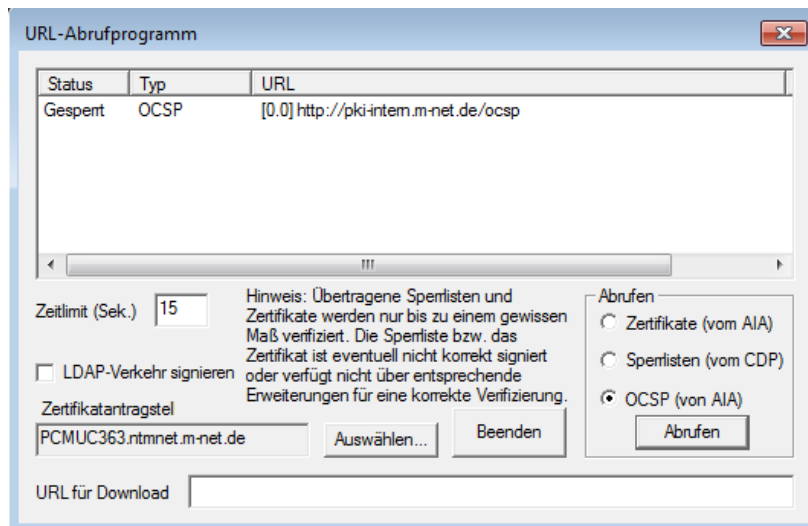


Abbildung 5.9.: Certutil GUI OCSP

Somit ist die Umsetzung der Anforderung Zertifikatstatus, die verschiedene CDPs fordert, verifiziert.

5.3. Ergebnis der Verifikation

Alle Tests der Kapitel 5.1 und 5.2 sind positiv abgeschlossen worden.

Tabelle 5.3.: Ergebnis der Funktionsüberprüfung der PKI

| Test | Ergebnis |
|---|----------|
| Schlüsselspeicherung in den HSM Partitionen | ✓ |
| Verbindungstest HSM HA-Cluster | ✓ |
| Backup und Wiederherstellung eines Schlüssels des HSM | ✓ |
| Manuelles Ausstellen eines Zertifikats über die MMC auf der CA | ✓ |
| Manuelles Ausstellen eines Zertifikats über die MMC auf dem Zertifikatempfänger | ✓ |
| Manuelles Ausstellen eines Zertifikats über Certreq auf der CA | ✓ |
| Manuelles Ausstellen eines Zertifikats über die Zertifizierungsstellen-Webregistrierung | ✓ |
| Automatisches Ausstellen eines Zertifikats über Gruppenrichtlinien | ✓ |
| Testzertifikat über NDES ausstellen | ✓ |
| Zertifikatgültigkeit über das AD | ✓ |
| Zertifikatgültigkeit über den Webserver | ✓ |
| Zertifikatgültigkeit über das OCSP | ✓ |

Mit der Implementierung einer zweistufigen PKI, keinen Einschränkungen bei der Ausstellung von Zertifikaten und den individuell konfigurierbaren Zertifikatvorlagen mit Unterstützung der Schemaversion 4, ist die Anforderung Ausbaumöglichkeiten umgesetzt. Die

Verwendung der Gemalto Luna HSMs und den verschiedenen Konfigurationsskripten für die Root CA, erfüllt die Anforderung Betriebssysteme. Durch die individuell konfigurierbaren Zertifikatvorlagen und der manuellen Zertifikatanforderung auf dem Zertifikatempfänger konnten kritische Systeme, z. B. die Domänencontroller, einzeln mit neuen Zertifikaten ausgestattet werden, die die vorherigen Zertifikate abgelöst haben. Dies setzt die Anforderungen Ausstellbarkeit und AltCA um. In Kapitel 5.2.1.6 ist die Anforderung MDM positiv überprüft worden. Die Anforderung Zertifikattypen wird durch die verschiedenen Zertifikatvorlagen und die konfigurierten SANs in Kapitel 4.3.3.2 realisiert. Die Umsetzung der in Kapitel 3.2.6 festgelegten Schlüssellängen erfüllt die Anforderung Schlüssellänge. Mit dem Kapitel 5.2 ist die Anforderung Zertifikatanforderung positiv getestet worden. Die Verwendung virtueller Maschinen, dreier Webserver, der OCSP Responder, des Active Directory und des HSM HA-Clusters setzen die Anforderungen Zertifikatstatus und Verfügbarkeit um. Die Erzeugung des Backup Root CA Schlüsselpaares, die Einrichtung des automatischen Backups der virtuellen Maschinen und des Backup HSMs erfüllen die Anforderung Wiederherstellbarkeit.

Tabelle 5.4.: Ergebnis der Anforderungsüberprüfung der PKI

| Anforderung | Ergebnis |
|------------------------|----------|
| Ausbaumöglichkeiten | ✓ |
| Betriebssysteme | ✓ |
| Ausstellbarkeit | ✓ |
| MDM | ✓ |
| Zertifikattypen | ✓ |
| Netzwerkcompatibilität | ✓ |
| Schlüssellänge | ✓ |
| Zertifikatanforderung | ✓ |
| Zertifikatstatus | ✓ |
| Verfügbarkeit | ✓ |
| Wiederherstellbarkeit | ✓ |
| AltCA | ✓ |

6. Fazit und Ausblick auf weitere Einsatzmöglichkeiten

In dieser Bachelorarbeit wurde das Prinzip einer Public Key Infrastruktur erläutert, Anforderungen an die aufzubauende PKI bei der M-net Telekommunikations GmbH erstellt, ein Integrationskonzept entwickelt und dieses anschließend umgesetzt.

Dabei wurde zuerst die grundlegende Methodik der Verschlüsselung, anschließend die Funktionsweise einer PKI und einzelner Dienste, z. B. dem Network Device Enrollment Service erklärt.

In den Anforderungen an die PKI in Kapitel 3.1 wurden Ausbaumöglichkeiten für u. a. WLAN Authentifizierung, der Unterstützung für Zertifizierungsstellen mit verschiedenen Betriebssystemen, der Ausstellbarkeit von Zertifikaten für das Mobile Device Management und für Computer mit unterschiedlichen Betriebssystemen und unterschiedlichen Domänenzugehörigkeiten gefordert. Zusätzlich wurde die Unterstützung für verschiedene Zertifikattypen und SANs, die Kompatibilität zur bestehenden Netzwerkstruktur, eine hohe Kompatibilität zur sehr heterogenen Client-Landschaft, die vor allem die Schlüssellänge betrifft und mehrere Möglichkeiten der Zertifikatanforderung und Zertifikatstatusüberprüfung gefordert. Eine Verfügbarkeit von 99,5 % für die Zertifizierungsstellen und 99,9 % für die Sperrlisten, eine Wiederherstellbarkeit möglichst innerhalb von zwei Arbeitstagen und die Berücksichtigung einer vorhandenen Root CA, die abgelöst wurde, waren ebenfalls Teil der Anforderung.

Das ausgearbeitete Konzept enthält eine offline Root CA, sechs Sub CAs und zwei ausgelagerte OCSP Responder, die sich in verschiedenen Netzwerken, VLANs und Domänen befinden. Dabei laufen alle Zertifizierungsstellen und OCSP Responder auf eigenen virtuellen Maschinen. Für das Ausstellen von Zertifikaten für das Mobile Device Management kommt der Network Device Enrollment Service zum Einsatz, der ebenfalls seine Schlüssel auf den HSMs generiert und speichert. Als Sperrlisten-Verteilungspunkt werden zusätzlich zu den OCSP Respondern drei Webserver und das Active Directory genutzt. Um die Sicherheit der PKI zu erhöhen, werden die Schlüssel der Zertifizierungsstellen, der OCSP Responder und des Network Device Enrollment Services auf zwei Gemalto Luna SA 1700 Hardware-Sicherheitsmodulen generiert und gespeichert.

In der Umsetzung wurden die Implementierungsschritte mit Screenshots dokumentiert. Dabei sind die zwei Hardware-Sicherheitsmodule als ein High Availability-Cluster und mit mehreren Partitionen für die einzelnen Zertifizierungsstellen und OCSP Responder konfiguriert worden.

Die Verifikation der Funktionsfähigkeit des HSM High Availability-Clusters wurde durch eine Überprüfung der Schlüssel in den HSM Partitionen und einem Verbindungstest bestätigt.

6. Fazit und Ausblick auf weitere Einsatzmöglichkeiten

Ebenso wurde ein Schlüssel mit dem Backup HSM gesichert und wiederhergestellt. Auf der CA wurden erfolgreich manuell mit der Microsoft Management Console und dem Kommandokonsolenprogramm Certreq Zertifikate ausgestellt. Auf einem Zertifikatempfänger konnten über die Zertifizierungsstellen-Webregistrierung Zertifikate angefordert werden, im Fall eines Windowscomputers zusätzlich noch über die Microsoft Management Console. Das automatische Ausstellen der Zertifikate über Gruppenrichtlinien wurde ebenfalls erfolgreich getestet, genauso wie die Zertifikate für das Mobile Device Management über den Network Device Enrollment Service. Die einzelnen Sperrlisten-Verteilungspunkte LDAP, HTTP und OCSP wurden hinsichtlich ihrer Aktualisierungszeit nach dem Veröffentlichen einer CRL erfolgreich überprüft.

Die PKI hat sich inzwischen mit über 1000 ausgestellten Zertifikaten im produktiven Einsatz bewährt. Durch die Erfüllung aller Anforderungen wurden die Zertifikate der vorhandenen Root CA durch Zertifikate dieser PKI ersetzt. Die WLAN Sicherheit wurde durch die Clientauthentifizierung über die neu ausgestellten Zertifikate erhöht und somit das Arbeiten an einem mobilen Arbeitsplatz mit den gleichen Zugriffsrechten wie an einem stationärem ermöglicht.

Ausblickend kann gesagt werden, dass die PKI für die Anforderungen eines weiteren Ausbaus vorbereitet ist. Dies kann z.B. die Unterstützung einer externen VPN Anbindung an das Unternehmensnetzwerk oder eine sichere E-Mail-Kommunikation mittels Secure/Multi-purpose Internet Mail Extensions sein.

A. Screenshot gestützte Implementierungsdokumentation

A.1. Einrichtung Hardware-Sicherheitsmodul (HSM)

Die Einrichtung und Initialisierung der HSM ist nicht mit Screenshots dokumentiert, daher wird hier auf Kapitel 4.1 verwiesen.

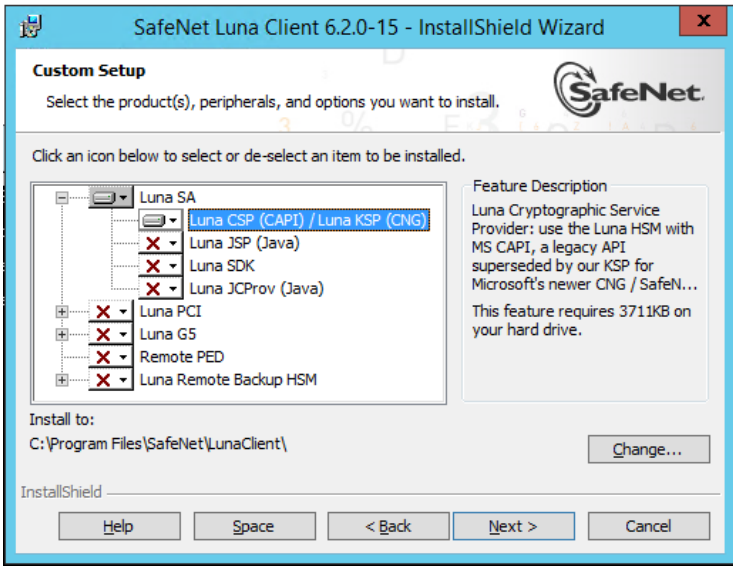
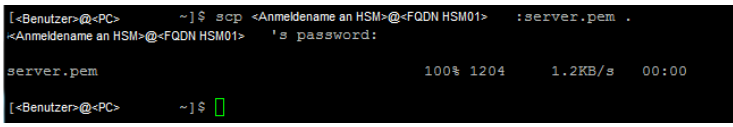
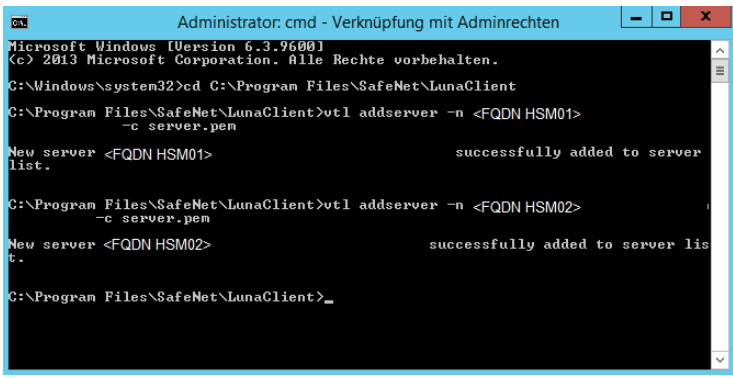
A.2. Anbindung Zertifizierungsstelle an das Hardware-Sicherheitsmodul High Availability-Cluster

In diesem Kapitel wird die Einrichtung des HSM HA-Clusters an die Zertifizierungsstellen beschrieben und mit Screenshots veranschaulicht.

A.2.1. Installation und Konfiguration des Safenet Luna Clients

| Nr. | Beschreibung | Abbildung |
|-----|--|--|
| 1 | Die Installation des Luna Clients setzt .Net Framework 3.5 voraus. Dies kann z. B. über den Assistenten zum Hinzufügen von Rollen und Features installiert werden. |  |

A. Screenshot gestützte Implementierungsdokumentation

| | | |
|----------|--|--|
| <p>2</p> | <p>Der Luna CSP und KSP wird ausgewählt</p> |  |
| <p>3</p> | <p>Mit z. B. PuTTY den Befehl „scp admin@<HSM-Host-Name>:server.pem .“ ausführen, um das Server Zertifikat von dem HSM herunterzuladen. Dieses muss anschließend im Installationsverzeichnis des Luna Clients abgelegt werden.</p> |  |
| <p>4</p> | <p>Per Windows Eingabeaufforderung wird in das Installationsverzeichnis des Luna Clients navigiert und dort mit „vtl addserver -n <FQDN-HSM> -c server.pem“ das HSM auf der Windows Maschine registriert.</p> |  |

A.2. Anbindung Zertifizierungsstelle an das Hardware-Sicherheitsmodul High Availability-Cluster

| | | |
|---|---|---|
| 5 | <p>Nun muss die Windows Maschine noch im HSM registriert werden. Dazu wird zuerst ein Maschinenzertifikat mit dem Befehl „vtl createCert -n <FQDN MaschinenName>“ erzeugt.</p> |  <pre>C:\Program Files\SafeNet\LunaClient>vtl createCert -n ca-sub03-x1.ntmnet.m-net.de Private Key created and written to: C:\Program Files\SafeNet\LunaClient\cert\cli ent\ca-sub03-x1.ntmnet.m-net.de\key.pem Certificate created and written to: C:\Program Files\SafeNet\LunaClient\cert\cli ent\ca-sub03-x1.ntmnet.m-net.de.pem C:\Program Files\SafeNet\LunaClient>_</pre> |
| 6 | <p>In PuTTY wird mit dem Befehl „scp <FQDN MaschinenName>.pem admin@<HSM-HostName>:“ das Clientzertifikat auf das HSM kopiert. Da zwei HSMs zum Einsatz kommen, muss dies bei der zweiten HSM ebenfalls gemacht werden.</p> |  <pre>-bash-4.2\$ scp ca-sub03-x1.ntmnet.m-net.de.pem <Anmeldename an HSM>@HSM01 : <Anmeldename an HSM>@HSM01 's password: ca-sub03-x1.ntmnet.m-net.de.pem 100% 1208 1.2KB/s 00:00 -bash-4.2\$</pre> |
| 7 | <p>Mit dem Befehl „ssh admin@<HSM-HostName>“ muss man sich nun auf der HSM anmelden und dort „client register -client <FQDN MaschinenName> -hostname <FQDN MaschinenName>“ ausführen. Analoge Ausführung auf der zweiten HSM.</p> |  <pre>-bash-4.2\$ ssh <Anmeldename an HSM>@HSM01 <Anmeldename an HSM>@HSM01 's password: Last login: Thu Aug 17 08:44:03 2017 from <IP eines PCs> Luna SA 6.2.2-5 Command Line Shell - Copyright (c) 2001-2016 SafeNet, Inc. All rights reserved. [HSM01] lunash:>client register -client ca-sub03-x1.ntmnet.m-net.de -hostname ca-sub03-x1.ntmnet. m-net.de 'client register' successful. Command Result : 0 (Success) [HSM01] lunash:></pre> |
| 8 | <p>Mit „service restart ntl“ muss der NTLS Dienst auf beiden HSMs neu gestartet werden.</p> |  <pre>[HSM01] lunash:>service restart ntl Checking for connected clients before stopping NTLS service: WARNING !! There are 7 client(s) connected to this Luna SA appliance. It is recommended that you disconnect all clients before stopping or restarting the NTLS service. If you wish to proceed, type 'proceed', otherwise type 'quit' > proceed Proceeding... Stopping ntl:OK Starting ntl:OK Command Result : 0 (Success) [HSM01] lunash:>exit</pre> |
| 9 | <p>Durch Eingabe des Befehls „client list“ auf beiden HSMs kann überprüft werden, ob die Windows Maschine ordnungsgemäß in den HSMs registriert wurde.</p> |  <pre>[HSM01] lunash:>client list registered client 1: ca-sub01-x1.ntmnet.m-net.de registered client 2: ca-root-x1.intern.m-net.de registered client 3: ca-sub02-x1.service.m-net.de registered client 4: <Backbone CA 1> registered client 5: <Backbone CA 2> registered client 6: <Backbone CA 3> registered client 7: ca-sub04-x1.ntmnet.m-net.de registered client 8: <FQDN OCSF-MDM> registered client 9: ca-sub03-x1.ntmnet.m-net.de registered client 10: <FQDN OCSF-Item> Command Result : 0 (Success) [HSM01] lunash:></pre> |

A. Screenshot gestützte Implementierungsdokumentation

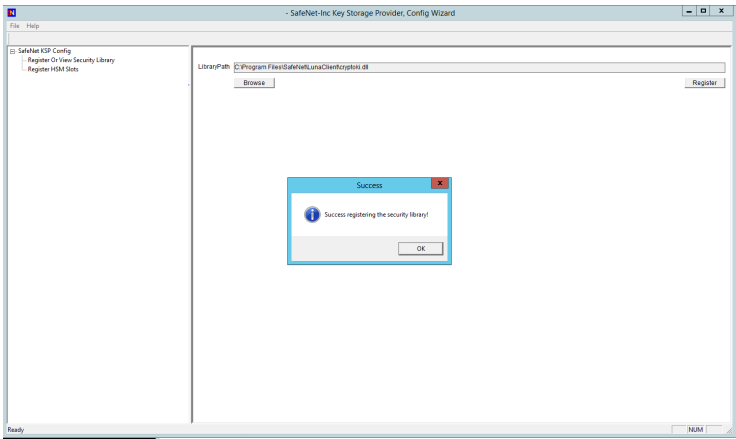
| | | |
|----|---|--|
| 10 | <p>Auf der HSM wird nun der Windows Maschine ihre zugehörige Partition zugewiesen. Dies geschieht mit dem Befehl „client assignpartition -client <FQDN MaschinenName> -partition <Partitions Name>“ und erfolgt analog auf der zweiten HSM.</p> | <pre>[-Benutzer@PC ~] \$ ssh <Anmeldename an HSM>@HSM01 <Anmeldename an HSM>@HSM01 ~'s password: Last login: Mon May 22 14:39:48 2017 from <IP eines PCs> Luna SA 6.2.2-5 Command Line Shell - Copyright (c) 2001-2016 SafeNet, Inc. All rights reserved. [HSM01 ~] lunash:>client assignpartition -client ca-sub03-x1.ntmnet.m-net.de -partition part 'client assignPartition' successful. Command Result : 0 (Success)</pre> |
| 11 | <p>Überprüfung erfolgt mit dem Befehl „client show -client <FQDN MaschinenName>“.</p> | <pre>[HSM01 ~] lunash:>client show -client ca-sub03-x1.ntmnet.m-net.de ClientID: ca-sub03-x1.ntmnet.m-net.de Username: ca-sub03-x1.ntmnet.m-net.de HTL Required: no OTL Expiry: n/a Partitions: "part"</pre> |
| 12 | <p>Für den Fall eines Ausfalls des DNS Servers wird noch die IP der Windows Maschine auf beiden HSMs eingetragen „client hostip map -client <FQDN MaschinenName> -ip <IP der Windows Maschine>“.</p> | <pre>[HSM01 ~] lunash:>Client hostip map -client ca-sub03-x1.ntmnet.m-net.de -ip <IP der CA></pre> |
| 13 | <p>„client hostip show“ überprüft die Einstellung.</p> | <pre>[HSM01 ~] lunash:>client hostip show Client Name Host Name Host IP ----- ca-sub03-x1.ntmnet.m-net.de.ca-sub03-x1.ntmnet.m-net.de <IP der CA></pre> |
| 14 | <p>Ein Ausführen des Befehls „vtl verify“ auf der Windows Maschine zeigt nun nach erfolgreicher Konfiguration den Partitions slot, die Seriennummer und den Partitionsnamen an.</p> | <pre>C:\Program Files\SafeNet\LunaClient>vtl verify The following Luna SA Slots/Partitions were found: Slot Serial # Label ---- - 0 <Seriennummer der Partition> part 1 <Seriennummer der Partition> part</pre> |

| | | |
|--|--|---|
| <p>15</p> <p>Die Konfiguration der HA erfolgt durch Ausführen der luna-cm.exe über das Eingabefenster und dem Befehl „hagroup creategroup -slot 0 -label <Partitionsname der HA-Partition> -password“.</p> | | <pre> lunacm:> hagroup creategroup -slot 0 -label haparit -password Enter the password: ***** Warning: There are objects currently on the new member. Do you wish to propagate these objects within the HA group, or remove them? Type 'copy' to keep and propagate the existing objects, 'remove' to remove them before continuing, or 'quit' to stop adding this new group member. > copy New group with label "haparit" created with group number <Seriennummer der HA-Partition> Group configuration is: HA Group Label: haparit HA Group Number: <Seriennummer der HA-Partition> HA Group Slot ID: Not Available Synchronization: enabled Group Members: <Seriennummer der part Partition von slot 0> Needs sync: no Standby Members: <none> Slot # Member S/N Member Label Status ===== 0 <Seriennummer der part Partition von slot 0> part alive Command Result : No Error LunaCM v6.2.0-15. Copyright (c) 2006-2015 SafeNet, Inc. Available HSMs: Slot Id -> 0 Label -> part Serial Number -> <Seriennummer der part Partition von slot 0> Model -> LunaSA 6.2.2 Firmware Version -> 6.24.3 Configuration -> Luna User Partition, No SO (PW) Signing With Cloning Mode Slot Id -> 1 Label -> part Serial Number -> <Seriennummer der part Partition von slot 1> Model -> LunaSA 6.2.2 Firmware Version -> 6.24.3 Configuration -> Luna User Partition, No SO (PW) Signing With Cloning Mode Slot Id -> 5 HSM Label -> haparit HSM Serial Number -> <Seriennummer der HA-Partition> HSM Model -> LunaVirtual HSM Firmware Version -> 6.24.3 HSM Configuration -> Luna Virtual HSM (PW) Signing With Cloning Mode HSM Status -> N/A - HA Group Current Slot Id: 0 </pre> |
| <p>16</p> <p>Die zweite HSM wird durch „hagroup add-member -slot 1 -group <Partitionsname der HA-Partition> -password“ der HA-Gruppe hinzugefügt.</p> | | <pre> lunacm:> hagroup addmember -slot 1 -group haparit -password Enter the password: ***** Warning: There are objects currently on the new member. Do you wish to propagate these objects within the HA group, or remove them? Type 'copy' to keep and propagate the existing objects, 'remove' to remove them before continuing, or 'quit' to stop adding this new group member. > copy Member <Seriennr part slot 1> successfully added to group haparit . New group configuration is: HA Group Label: haparit HA Group Number: <Seriennummer der HA-Partition> HA Group Slot ID: 5 Synchronization: enabled Group Members: <Seriennummer part slot 0>, <Seriennummer part slot 1> Needs sync: no Standby Members: <none> Slot # Member S/N Member Label Status ===== 0 <Seriennummer part slot 0> part alive 1 <Seriennummer part slot 1> part alive Please use the command "ha synchronize" when you are ready to replicate data between all members of the HA group. <If you have additional members to add, you may wish to wait until you have added them before synchronizing to save time by avoiding multiple synchronizations.> Command Result : No Error </pre> |

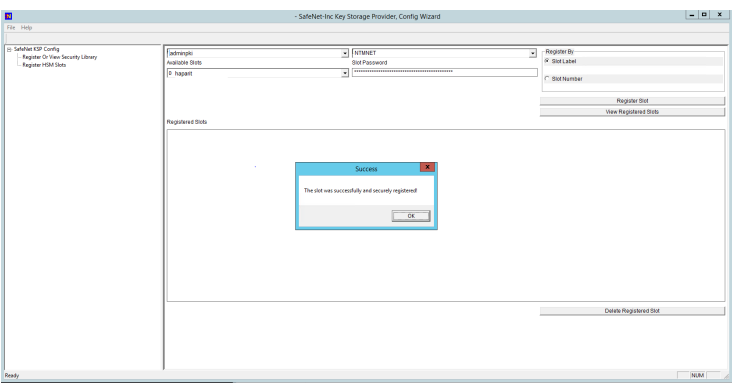
| | | |
|----|--|---|
| 17 | Im Installationsverzeichnis des Luna Clients wird nun überprüft, ob in der crystoki.ini die Konfiguration eingetragen wurde. | <pre>[VirtualToken] VirtualToken00Label=haparit VirtualToken00SN=<Seriennummer HA-Partition> VirtualToken00Members=<Snr parit slot 0>, <Snr parit slot 1></pre> |
| 18 | Nun synchronisiert man die beiden Partitionen, um die Objekte auf beiden HSMs redundant verfügbar zu machen: „hagroup synchronize -group <Partitionsname der HA-Partition> -password <Partitions-passwort> -enable“. | <pre>lunac:> hagroup synchronize -group haparit -password <Partitionspasswort> -enable_ HA Synchronization is already enabled No synchronization performed/needed. Command Result : No Error</pre> |

A.2.2. Key Storage Provider (KSP) und Cryptographic Service Provider (CSP)

Da KSP SHA-2 unterstützt, CSP aber nur SHA-1, wird als Standard bei allen Zertifizierungsstellen der KSP eingesetzt. CSP wird nur für den NDES Dienst konfiguriert und verwendet, welcher nur auf der Sub-MDM läuft. Für den KSP muss zuerst die Sicherheitsbibliothek eingerichtet und anschließend die Partition registriert werden.

| | | |
|----|---|--|
| 19 | Im Unterordner KSP des Luna Clients Installationsverzeichnisses öffnet man nun die KSPConfig.exe und führt dort einen Doppelklick auf „Register or View Security Library“ aus. Dort wird der „LibraryPath“ angegeben, indem zum Installationsverzeichnis des Luna Clients navigiert, dort die cryptoki.dll ausgewählt und auf „Register“ geklickt wird. |  |
|----|---|--|

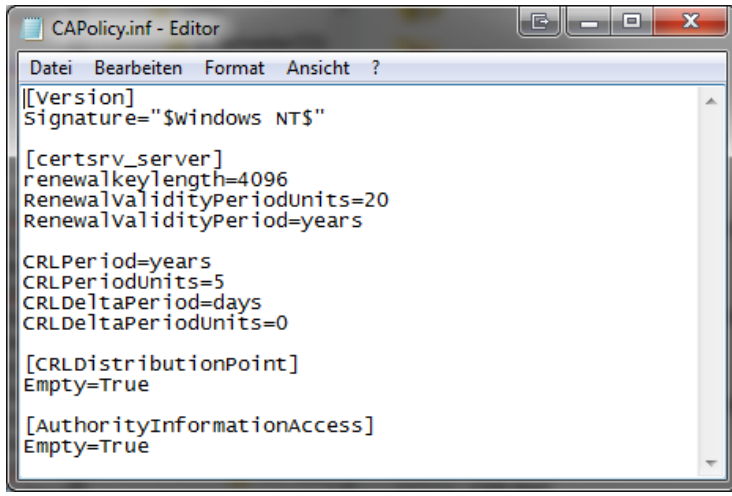
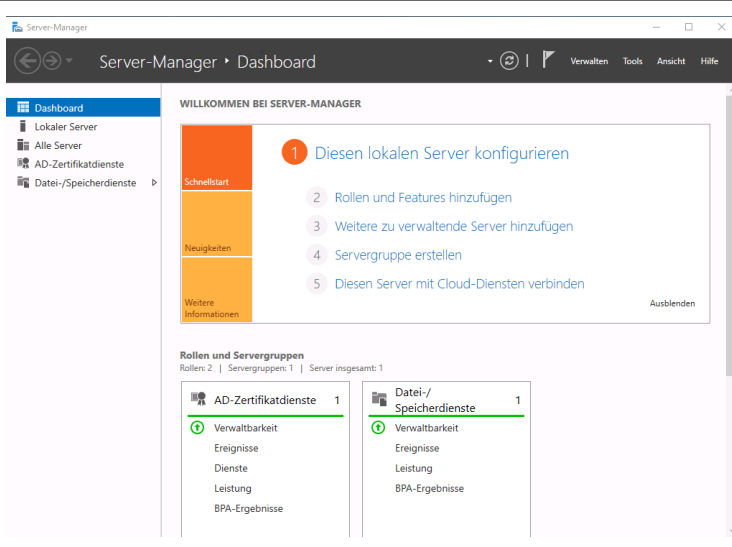
A.2. Anbindung Zertifizierungsstelle an das Hardware-Sicherheitsmodul High Availability-Cluster

| | | |
|-----------|--|--|
| <p>20</p> | <p>Doppelklick auf „Registrieren HSM Slots“. Dort das angemeldete Administratorkonto, die Domäne und den haslot auswählen, das Partitions Passwort eingeben und registrieren.</p> |  |
| <p>21</p> | <p>Per Eingabeaufforderung wird nun in den Ordner KSP navigiert und dort „kspcmd password /s <Name der HA-Partition>/u SYSTEM /d NT-AUTORITÄT“ ausgeführt. Sollte es sich um ein englisches Betriebssystem handeln, so muss „NT AUTHORITY“ statt „NT-AUTORITÄT“ verwendet werden. Das nun abgefragte Passwort ist das Partitions Passwort.</p> | <pre> C:\Program Files\SafeNet\LunaClient>cd ksp C:\Program Files\SafeNet\LunaClient\KSP>kspcmd password /s haparit /u SYSTEM /d NT-AUTORITÄT This Servers Host Name is: CA-SUB03-X1.ntmnet.n-net.de and the logged on user is adminpk Enter challenge for slot '0' <Just hit Enter when using PED>:***** ***** The slot haparit was successfully and securely registered for user SYSTEM at domain NT-AUTORITÄT! </pre> |

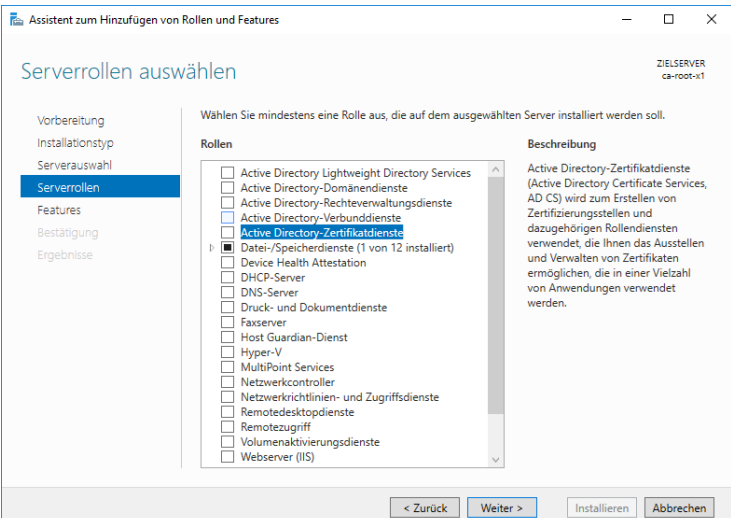
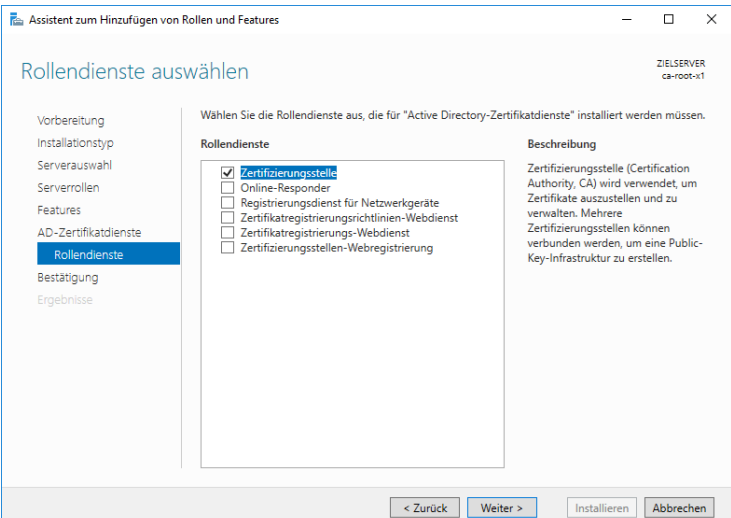
A. Screenshot gestützte Implementierungsdokumentation

| | | |
|-----------|--|--|
| <p>22</p> | <p>Für die Einrichtung des CSPs mit HA wird per Eingabeaufforderung in den Unterordner CSP des Luna Client Installationsverzeichnisses gewechselt und „register /highavail“ ausgeführt.</p> <p>Anschließend müssen alle Programme, die den CSP benutzen, konfiguriert und einmal ausgeführt werden. In dieser Implementierung bedeutet das, dass erst NDES und CEP konfiguriert und getestet werden müssen, bevor mit Schritt 23 fortgefahren werden kann.</p> |  <pre> Administrator: cmd - Verknüpfung mit Adminrechten Microsoft Windows [Version 6.3.9600] (c) 2013 Microsoft Corporation. Alle Rechte vorbehalten. C:\Windows\system32>cd C:\Program Files\SafeNet\LunaClient\CSP C:\Program Files\SafeNet\LunaClient\CSP>register /highavail register v1.0.1 ***** * * * Safenet Inc. LunaCSP, Partition Registration * * Protect the HSM's challenge for the selected partitions. * NOTE: * This is a WEAK protection of the challenge!! * After you have configured all applications that will use * the LunaCSP, and ran them once, you MUST run: * register /partition /strongprotect * to strongly protect the registered challenges!! ***** This procedure is a destructive procedure and will completely replace any previous settings!! Do you wish to continue?: [y/n] Do you want to register the partition named 'haparocsp' ?[y/n]: y Enter challenge for partition 'haparocsp' :***** ***** Success registering the ENCRYPTED challenge for partition 'haparocsp' :0'. Only the LunaCSP will be able to use this data! Do you want to register the partition named 'haparocsp' ?[y/n]: y Enter challenge for partition 'haparocsp' :***** ***** Success registering the ENCRYPTED challenge for partition 'haparocsp' :0'. Only the LunaCSP will be able to use this data! Registered 2 partition(s) for use by the LunaCSP! C:\Program Files\SafeNet\LunaClient\CSP>_ </pre> |
| <p>23</p> | <p>„register /partition /strongprotect“ ausführen, um den Passwortschutz zu erhöhen.</p> |  <pre> Administrator: cmd - Verknüpfung mit Adminrechten Microsoft Windows [Version 6.3.9600] (c) 2013 Microsoft Corporation. Alle Rechte vorbehalten. C:\Windows\system32>cd C:\Program Files\SafeNet\LunaClient\CSP C:\Program Files\SafeNet\LunaClient\CSP>register /partition /strongprotect register v1.0.1 </pre> |
| <p>24</p> | <p>„register library“ verbindet nun die Luna CSP Bibliotheken</p> |  <pre> C:\Program Files\SafeNet\LunaClient\CSP>register /library register v1.0.1 Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna enhanced BSA and AES provider for Microsoft Windows ! Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna Cryptographic Services for Microsoft Windows ! Success registering SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Luna SChannel Cryptographic Services for Microsoft Windows ! C:\Program Files\SafeNet\LunaClient\CSP>_ </pre> |

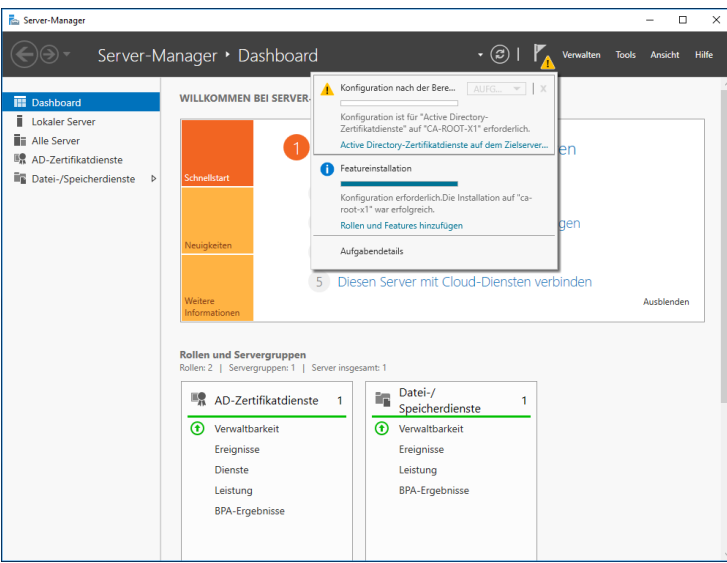
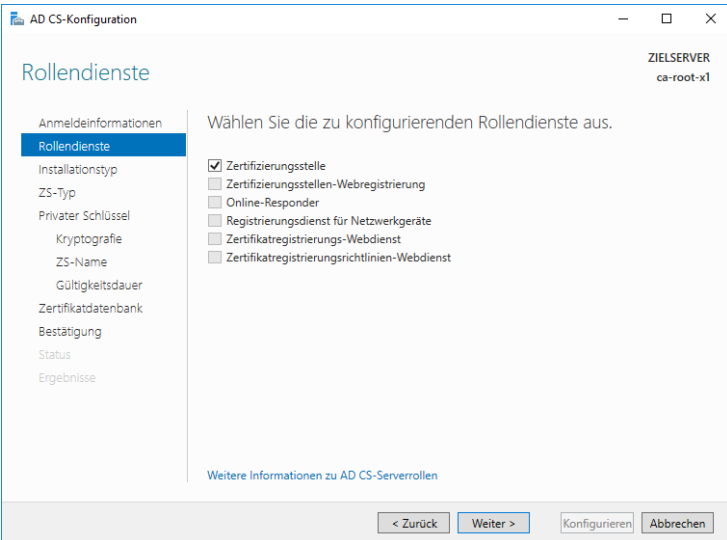
A.3. Einrichtung Active Directory-Zertifikatdienste der Root CA

| | | |
|-----------|--|---|
| <p>25</p> | <p>Die vorbereitete capolicy.inf wird nach C:\Windows kopiert.</p> |  <pre> CAPolicy.inf - Editor Datei Bearbeiten Format Ansicht ? [[version] Signature="\$windows NT\$" [certsrv_server] renewalkeylength=4096 RenewalValidityPeriodUnits=20 RenewalValidityPeriod=years CRLPeriod=years CRLPeriodUnits=5 CRLDeltaPeriod=days CRLDeltaPeriodUnits=0 [CRLDistributionPoint] Empty=True [AuthorityInformationAccess] Empty=True </pre> |
| <p>26</p> | <p>Über den Server-Manager wird der „Assistent zum Hinzufügen von Rollen und Features“ ausgeführt.</p> |  |

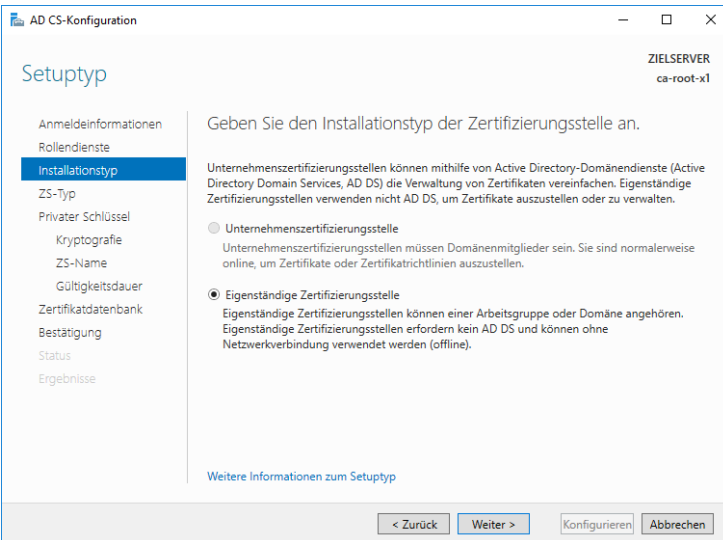
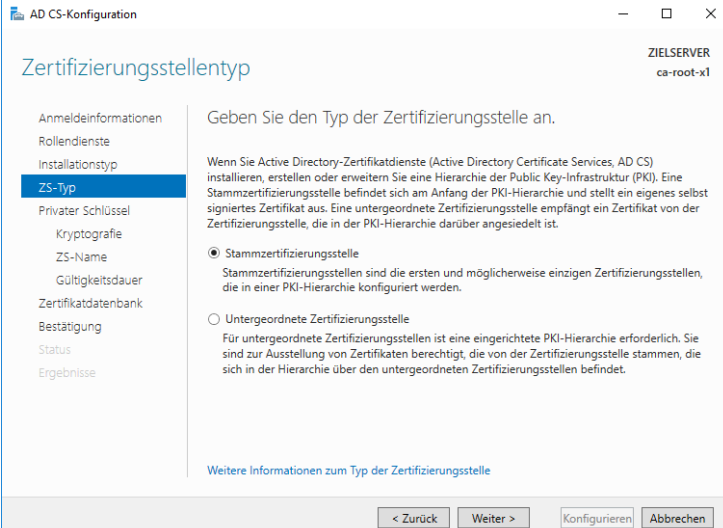
A. Screenshot gestützte Implementierungsdokumentation

| | |
|--|---|
| <p>27</p> <p>Die „Active Directory-Zertifikatdienste“ werden ausgewählt.</p> |  <p>Assistent zum Hinzufügen von Rollen und Features</p> <p>ZIELSERVER ca-root-11</p> <h3>Serverrollen auswählen</h3> <p>Vorbereitung Installationstyp Serverauswahl Serverrollen Features Bestätigung Ergebnisse</p> <p>Wählen Sie mindestens eine Rolle aus, die auf dem ausgewählten Server installiert werden soll.</p> <p>Rollen</p> <ul style="list-style-type: none"> <input type="checkbox"/> Active Directory Lightweight Directory Services <input type="checkbox"/> Active Directory-Domänendienste <input type="checkbox"/> Active Directory-Rechteverwaltungsdienste <input type="checkbox"/> Active Directory-Verbunddienste <input checked="" type="checkbox"/> Active Directory-Zertifikatdienste <input type="checkbox"/> Datei-/Speicherdienste (1 von 12 installiert) <input type="checkbox"/> Device Health Attestation <input type="checkbox"/> DHCP-Server <input type="checkbox"/> DNS-Server <input type="checkbox"/> Druck- und Dokumentdienste <input type="checkbox"/> Faxserver <input type="checkbox"/> Host Guardian-Dienst <input type="checkbox"/> Hyper-V <input type="checkbox"/> MultiPoint Services <input type="checkbox"/> Netzwerkcontroller <input type="checkbox"/> Netzwerkrichtlinien- und Zugriffsdienste <input type="checkbox"/> Remotedesktopdienste <input type="checkbox"/> Remotezugriff <input type="checkbox"/> Volumenaktivierungsdienste <input type="checkbox"/> Webserver (IIS) <p>Beschreibung</p> <p>Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) wird zum Erstellen von Zertifizierungsstellen und dazugehörigen Rollendiensten verwendet, die Ihnen das Ausstellen und Verwalten von Zertifikaten ermöglichen, die in einer Vielzahl von Anwendungen verwendet werden.</p> <p>< Zurück Weiter > Installieren Abbrechen</p> |
| <p>28</p> <p>Bei den Rollendiensten wird die Zertifizierungsstelle ausgewählt und installiert.</p> |  <p>Assistent zum Hinzufügen von Rollen und Features</p> <p>ZIELSERVER ca-root-11</p> <h3>Rollendienste auswählen</h3> <p>Vorbereitung Installationstyp Serverauswahl Serverrollen Features AD-Zertifikatdienste Rollendienste Bestätigung Ergebnisse</p> <p>Wählen Sie die Rollendienste aus, die für "Active Directory-Zertifikatdienste" installiert werden müssen.</p> <p>Rollendienste</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Zertifizierungsstelle <input type="checkbox"/> Online-Responder <input type="checkbox"/> Registrierungsdienst für Netzwerkgeräte <input type="checkbox"/> Zertifikatregistrierungsrichtlinien-Webdienst <input type="checkbox"/> Zertifikatregistrierungs-Webdienst <input type="checkbox"/> Zertifizierungsstellen-Webregistrierung <p>Beschreibung</p> <p>Zertifizierungsstelle (Certification Authority, CA) wird verwendet, um Zertifikate auszustellen und zu verwalten. Mehrere Zertifizierungsstellen können verbunden werden, um eine Public-Key-Infrastruktur zu erstellen.</p> <p>< Zurück Weiter > Installieren Abbrechen</p> |

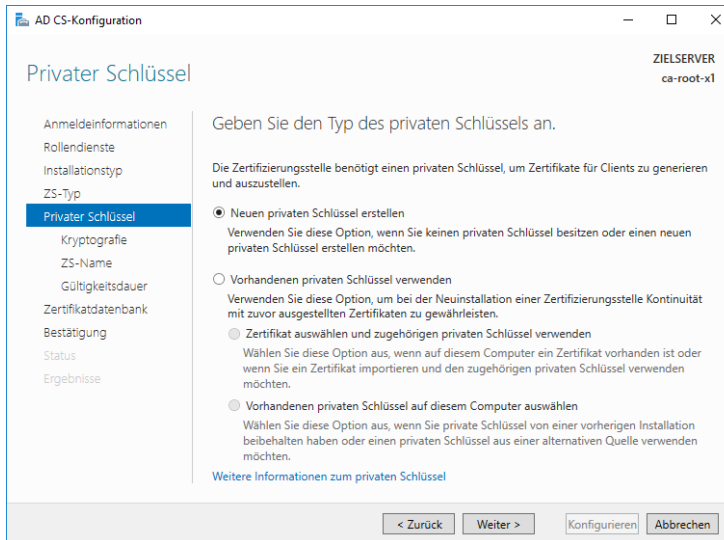
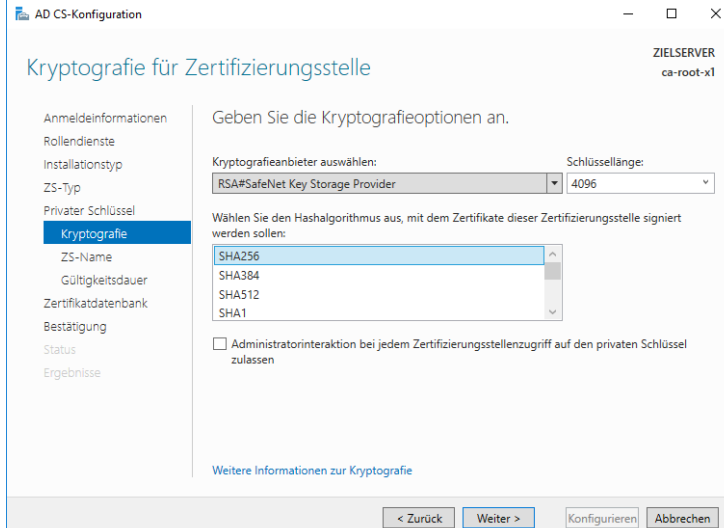
A.3. Einrichtung Active Directory-Zertifikatdienste der Root CA

| | |
|---|--|
| <p>29</p> <p>Nach Abschluss der Installation erfolgt die Konfiguration.</p> |  <p>The screenshot shows the Server Manager interface. A warning dialog box is open, stating: 'Konfiguration nach der Bere... Konfiguration ist für "Active Directory-Zertifikatdienste" auf "ca-root-x1" erforderlich, Active Directory-Zertifikatdienste auf dem Zielserver...'. Below the dialog, the 'Rollen und Servergruppen' section shows 'AD-Zertifikatdienste' and 'Datei-/Speicherdienste' installed on the server.</p> |
| <p>30</p> <p>Der Punkt „Zertifizierungsstelle“ wird ausgewählt und die erforderlichen Features hinzugefügt.</p> |  <p>The screenshot shows the 'AD CS-Konfiguration' wizard at the 'Rollendienste' step. The title bar says 'ZIELSERVER ca-root-x1'. The instruction is 'Wählen Sie die zu konfigurierenden Rollendienste aus.' The 'Zertifizierungsstelle' checkbox is checked, while others are unchecked. At the bottom, there are buttons for '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.</p> |

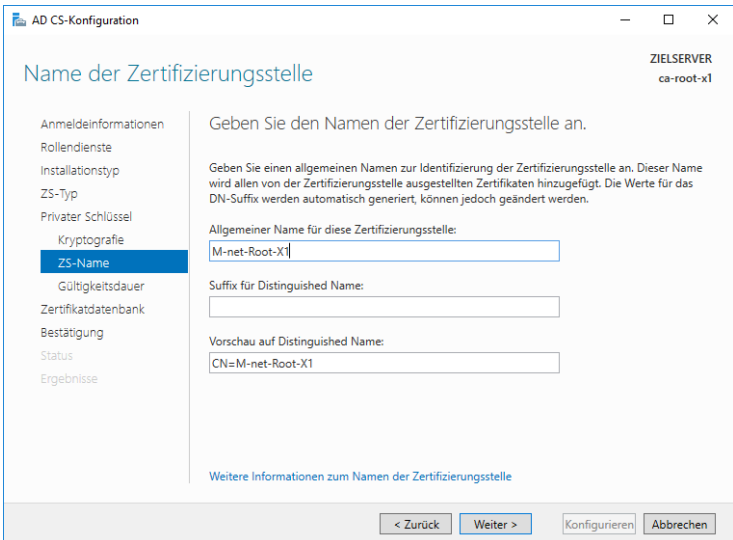
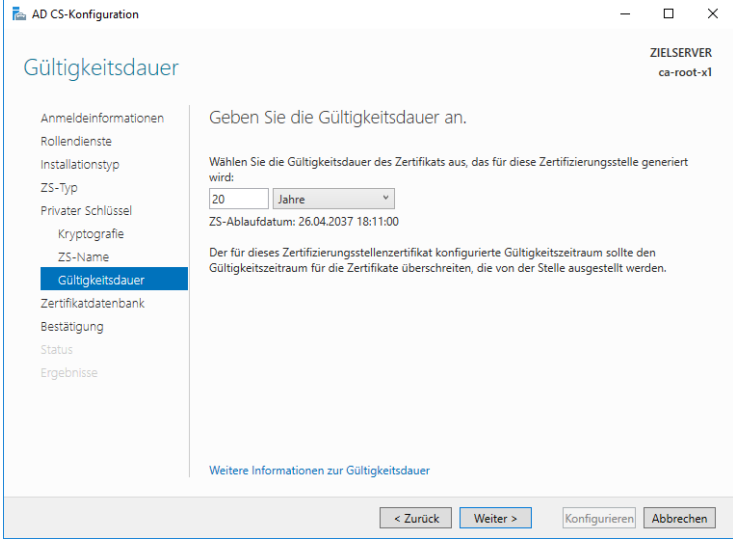
A. Screenshot gestützte Implementierungsdokumentation

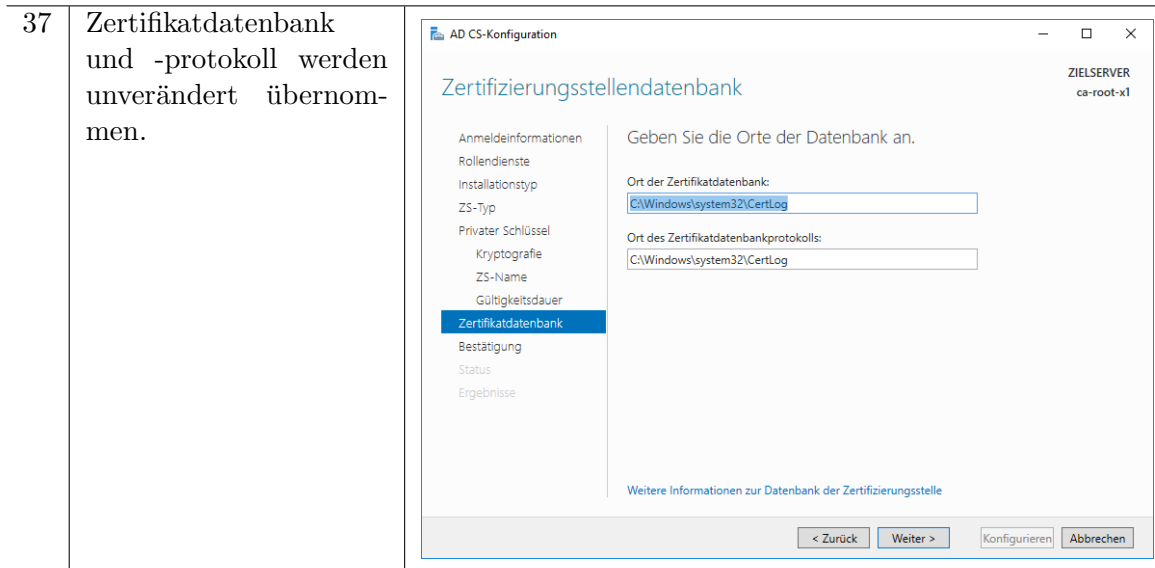
| | | |
|-----------|--|---|
| <p>31</p> | <p>Da die Root CA kein Mitglied einer Domäne ist, wird der Punkt „Eigenständige Zertifizierungsstelle“ ausgewählt.</p> |  <p>The screenshot shows the 'AD CS-Konfiguration' window with the 'Setuptyp' (Setup Type) step selected in the left-hand navigation pane. The main content area displays the question: 'Geben Sie den Installationstyp der Zertifizierungsstelle an.' (Specify the installation type of the certification authority). Two options are listed: 'Unternehmenszertifizierungsstelle' (Enterprise Certification Authority) and 'Eigenständige Zertifizierungsstelle' (Standalone Certification Authority). The 'Eigenständige Zertifizierungsstelle' option is selected with a radio button. Below the options, there is a link for 'Weitere Informationen zum Setuptyp' (More information about the setup type). At the bottom, there are navigation buttons: '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.</p> |
| <p>32</p> | <p>Da dies die Root CA ist, wird der Punkt „Stammzertifizierungsstelle“ ausgewählt.</p> |  <p>The screenshot shows the 'AD CS-Konfiguration' window with the 'Zertifizierungsstellentyp' (Certification Authority Type) step selected in the left-hand navigation pane. The main content area displays the question: 'Geben Sie den Typ der Zertifizierungsstelle an.' (Specify the type of certification authority). Two options are listed: 'Stammzertifizierungsstelle' (Standalone Certification Authority) and 'Untergeordnete Zertifizierungsstelle' (Subordinate Certification Authority). The 'Stammzertifizierungsstelle' option is selected with a radio button. Below the options, there is a link for 'Weitere Informationen zum Typ der Zertifizierungsstelle' (More information about the type of certification authority). At the bottom, there are navigation buttons: '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.</p> |

A.3. Einrichtung Active Directory-Zertifikatdienste der Root CA

| | | |
|----|---|---|
| 33 | <p>„Neuen Schlüssel auswählen.“</p> <p>privaten erstellen“</p> |  |
| 34 | <p>Hier wird nun „RSA#SafeNet Key Storage Provider“, „SHA256“ und 4096 Bit Schlüssellänge ausgewählt.</p> |  |

A. Screenshot gestützte Implementierungsdokumentation

| | | |
|----|--|---|
| 35 | Der Name der Root CA wird eingetragen |  <p>The screenshot shows the 'Name der Zertifizierungsstelle' (Name of the Certification Authority) step in the AD CS Configuration wizard. The left sidebar lists various configuration options, with 'ZS-Name' selected. The main area contains instructions and input fields: 'Allgemeiner Name für diese Zertifizierungsstelle:' with the value 'M-net-Root-X1', 'Suffix für Distinguished Name:' (empty), and 'Vorschau auf Distinguished Name:' showing 'CN=M-net-Root-X1'. Navigation buttons at the bottom include '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.</p> |
| 36 | Die Gültigkeit wird auf 20 Jahre festgelegt. |  <p>The screenshot shows the 'Gültigkeitsdauer' (Validity Period) step in the AD CS Configuration wizard. The left sidebar has 'Gültigkeitsdauer' selected. The main area shows instructions and a dropdown menu for the validity period, which is set to '20 Jahre'. Below the dropdown, the expiration date is shown as 'ZS-Ablaufdatum: 26.04.2037 18:11:00'. A warning message states: 'Der für dieses Zertifizierungsstellenzertifikat konfigurierte Gültigkeitszeitraum sollte den Gültigkeitszeitraum für die Zertifikate überschreiten, die von der Stelle ausgestellt werden.' Navigation buttons at the bottom include '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.</p> |



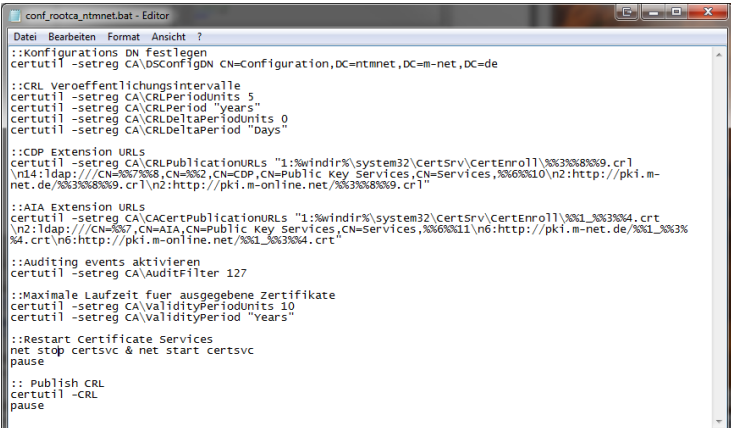
Auf der Root CA wird nun eine Konsole per mmc.exe Aufruf geöffnet und das Snap-In „Lokales Computerkonto“ hinzugefügt. Unter dem Reiter „Eigene Zertifikate“ wird nun der private Schlüssel angezeigt. Ein Nachschauen auf der HSM mit dem Befehl „par showC - par <Partitionsname> -pas <Passwort der Partition>“ zeigt nun zwei Elemente an, wenn die Partition zuvor leer war: Den privaten und den öffentlichen Schlüssel. Siehe Abbildung 5.1.

A.4. Veröffentlichung des Zertifikats und der Sperrliste der Root CA

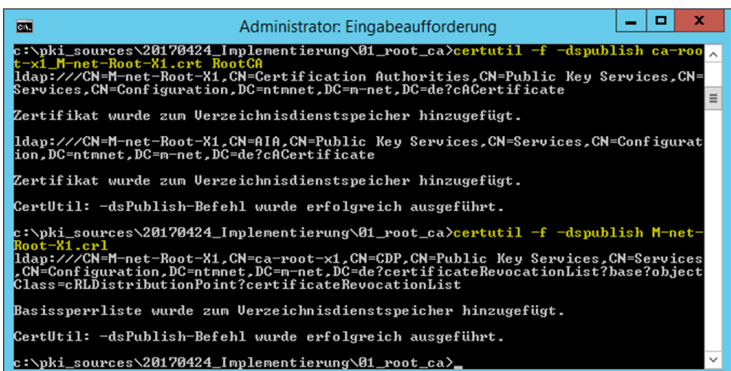
Da die Root CA für zwei verschiedene Domänen und eine domänenlose Umgebung als Stammzertifizierungsstelle benutzt wird, muss diese immer für die jeweilige Umgebung richtig konfiguriert werden.

A.4.1. Konfiguration Root CA und Veröffentlichung Zertifikat und Sperrliste der Root CA in der NTMNET Domäne

Auf der Root CA wird die vorbereitete conf_rootca_ntmnet.bat ausgeführt.

| | |
|--|---|
| <p>38 Ausführen des Konfigurationsskripts für die Root CA mit der Konfiguration für die ntmnet Domäne.</p> |  <pre> conf_rootca_ntmnet.bat - Editor Datei Bearbeiten Format Ansicht ? ::Konfigurations DN festlegen certutil -setreg CA\DSConfigDN CN=Configuration,DC=ntmnet,DC=m-net,DC=de ::CRL Veröffentlichungsintervalle certutil -setreg CA\CRLPeriodunits 5 certutil -setreg CA\CRLPeriod "years" certutil -setreg CA\CRLDeltaPeriodunits 0 certutil -setreg CA\CRLDeltaPeriod "days" ::CDP Extension URLs certutil -setreg CA\CRLPublicationURLs "1:%windir%\system32\certsrv\certenroll\%*%*.cr1 \n14:ldap://CN=%*%*%8,CN=%*%2,CN=CDP,CN=Public Key Services,CN=Services,%*%10\n2:http://pki.m- net.de/%*%3%8%9.cr1\n2:http://pki.m-online.net/%*%3%8%9.cr1" ::AIA Extension URLs certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\certsrv\certenroll\%*1_%*3%4.crt \n2:ldap://CN=%*7,CN=AIA,CN=Public Key Services,CN=Services,%*6%11\n6:http://pki.m-net.de/%*1_%*3% %4.crt\n6:http://pki.m-online.net/%*1_%*3%4.crt" ::Auditing events aktivieren certutil -setreg CA\AuditFilter 127 ::Maximale Laufzeit fuer ausgegebene Zertifikate certutil -setreg CA\ValidityPeriodunits 10 certutil -setreg CA\ValidityPeriod "Years" ::Restart Certificate Services net stop certsvc & net start certsvc pause :: Publish CRL certutil -crl pause </pre> |
|--|---|

Anschließend muss das erstellte Zertifikat und die Sperrliste an den Orten, die in den CDP Erweiterungen festgelegt wurden, veröffentlicht werden. In unserer Konfiguration bedeutet dies das Kopieren der beiden Dateien auf die beiden Webserver, um diese unter der URL verfügbar zu machen sowie das Veröffentlichen der Sperrliste und des Zertifikats der Root CA im Active Directory durch eine der Sub CAs der Domäne ntmnet.

| | |
|--|---|
| <p>39 Kopieren des ca-root-x1_M-net-Root-X1.crt und der M-net-Root-X1.crl nach „C:\Windows\System32\Cert-Srv\CertEnroll“ auf einen der Windows Server in der ntmnet Domäne, auf dem später eine untergeordnete Zertifizierungsstelle laufen soll. Anschließend in diesem Ordner folgende Befehle mit der Eingabeaufforderung ausführen: „certutil -f -dspublish ca-root-x1_M-net-Root-X1.crt RootCA“ und „certutil -f -dspublish M-net-Root-X1.crl“.</p> |  <pre> Administrator: Eingabeaufforderung c:\pki_sources\20170424_Implementierung\01_root_ca>certutil -f -dspublish ca-root-x1_M-net-Root-X1.crt RootCA ldap://CN=M-net-Root-X1,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=ntmnet,DC=m-net,DC=de?caCertificate Zertifikat wurde zum Verzeichnisdienstspeicher hinzugefügt. ldap://CN=M-net-Root-X1,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=ntmnet,DC=m-net,DC=de?caCertificate Zertifikat wurde zum Verzeichnisdienstspeicher hinzugefügt. CertUtil: -dsPublish-Befehl wurde erfolgreich ausgeführt. c:\pki_sources\20170424_Implementierung\01_root_ca>certutil -f -dspublish M-net-Root-X1.crl ldap://CN=M-net-Root-X1,CN=ca-root-x1,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=ntmnet,DC=m-net,DC=de?certificateRevocationList?base?objectClass=cRLDistributionPoint?certificateRevocationList Basisperrliste wurde zum Verzeichnisdienstspeicher hinzugefügt. CertUtil: -dsPublish-Befehl wurde erfolgreich ausgeführt. c:\pki_sources\20170424_Implementierung\01_root_ca> </pre> |
|--|---|

A.4.2. Konfiguration Root CA und Veröffentlichung Zertifikat und Sperrliste der Root CA in der ACI Domäne

Dies verläuft analog zu Kapitel A.4.1, abgesehen von der Verwendung des conf_rootca_serviceLan.bat Skripts und der Veröffentlichung auf einer CA der ServiceLan Domäne.

| | |
|---|--|
| <p>40 Das conf_rootca_serviceLan.bat Skript passt die Einträge zur Domäne der ServiceLan Domäne an und konfiguriert die CDP und AIA Erweiterungen entsprechend.</p> | <pre> conf_rootca_serviceLan.bat - Editor Datei Bearbeiten Format Ansicht ? ::Konfigurations DN festlegen certutil -setreg CA\dsconfigDN CN=Configuration,DC=mnet,DC=aci ::CRL veroeffentlichungsintervalle certutil -setreg CA\CRLPeriodunits 5 certutil -setreg CA\CRLPeriod "years" certutil -setreg CA\CRLDeltaPeriodunits 0 certutil -setreg CA\CRLDeltaPeriod "Days" ::CDP Extension URLs certutil -setreg CA\CRLPublicationURLs "1:%windir%\system32\CertSrv\CertEnroll\%3%8% %9_serviceLan.cr1\n14:ldap://CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6% %10\n2:http://pk1.m-net.de/%3%8%9_serviceLan.cr1\n2:http://pk1.m-online.net/%3%8% %9_serviceLan.cr1" ::AIA Extension URLs certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\CertSrv\CertEnroll\%1_%3%4.cr t\n2:ldap://CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n6:http://pk1.m-net.de/%1_%3% %4.crt\n6:http://pk1.m-online.net/%1_%3%4.crt" ::Auditing events aktivieren certutil -setreg CA\auditfilter 127 ::Maximale Laufzeit fuer ausgegebene Zertifikate certutil -setreg CA\ValidityPeriodunits 10 certutil -setreg CA\ValidityPeriod "years" ::Restart Certificate Services net stop certsvc & net start certsvc pause :: Publish CRL certutil -CRL pause </pre> |
|---|--|

A.4.3. Konfiguration Root CA und Veröffentlichung Zertifikat und Sperrliste der Root CA für eine domänenlose Umgebung

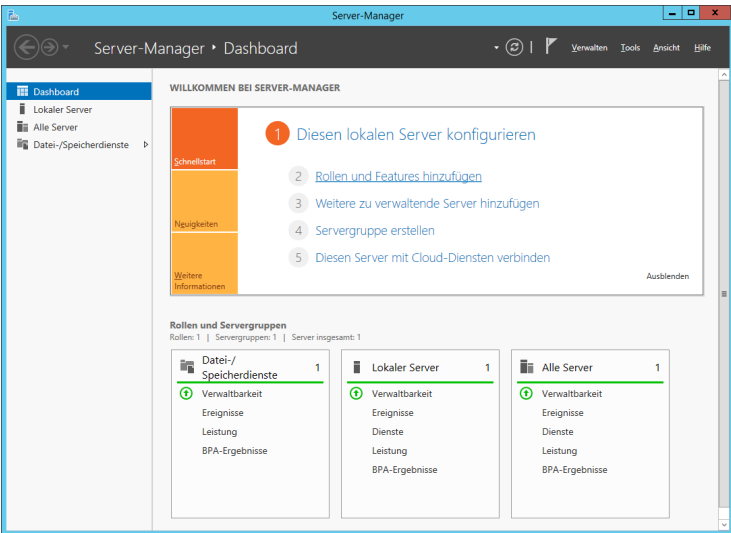
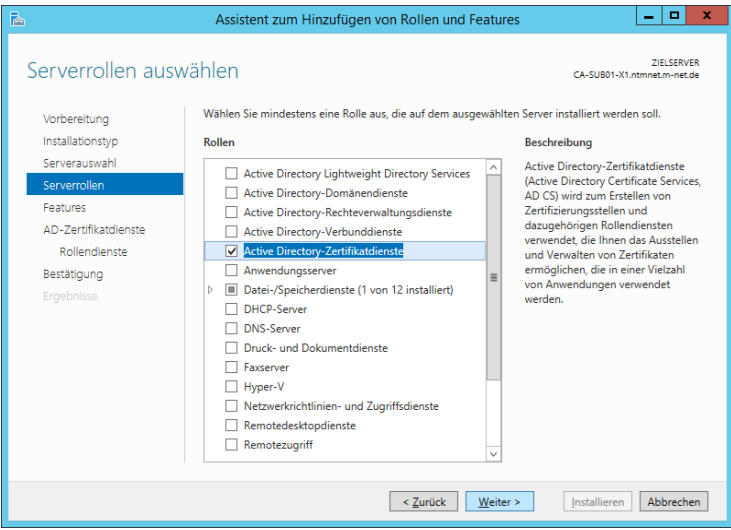
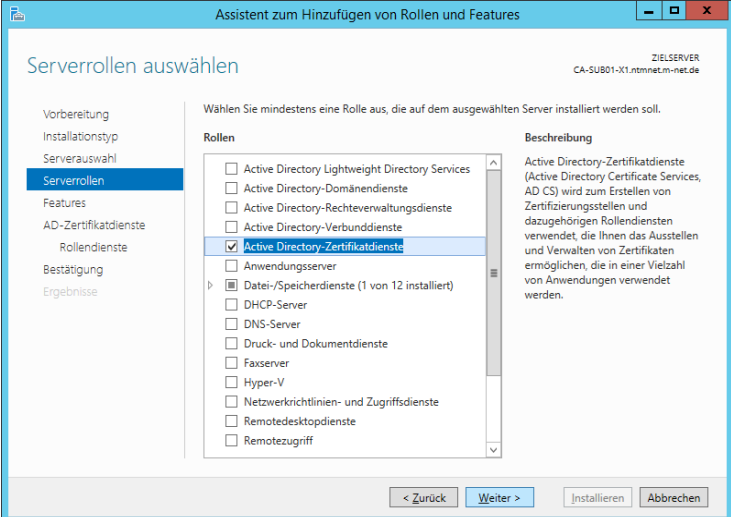
Dies verläuft analog zu Kapitel A.4.1, abgesehen von der Verwendung des conf_rootca_nonDomain.bat Skripts und der Veröffentlichung auf einer CA der ServiceLan Domäne.

| | |
|--|--|
| <p>41 Das conf_rootca_nonDomain.bat Skript löscht aus der CA die Einträge zur Domäne und konfiguriert die CDP und AIA Erweiterungen ohne ldap Pfade.</p> | <pre> conf_rootca_nonDomain.bat - Editor Datei Bearbeiten Format Ansicht ? ::Konfigurations DN festlegen certutil -delreg CA\dsconfigDN ::CRL veroeffentlichungsintervalle certutil -setreg CA\CRLPeriodunits 5 certutil -setreg CA\CRLPeriod "years" certutil -setreg CA\CRLDeltaPeriodunits 0 certutil -setreg CA\CRLDeltaPeriod "Days" ::CDP Extension URLs certutil -setreg CA\CRLPublicationURLs "1:%windir%\system32\CertSrv\CertEnroll\%3%8% %9_nondomain.cr1\n2:http://pk1.m-net.de/%3%8%9_nondomain.cr1\n2:http://pk1.m- online.net/%3%8%9_nondomain.cr1" ::AIA Extension URLs certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\CertSrv\CertEnroll\%1_%3%4.cr t\n6:http://pk1.m-net.de/%1_%3%4.crt\n6:http://pk1.m-online.net/%1_%3%4.crt" ::Auditing events aktivieren certutil -setreg CA\auditfilter 127 ::Maximale Laufzeit fuer ausgegebene Zertifikate certutil -setreg CA\ValidityPeriodunits 10 certutil -setreg CA\ValidityPeriod "years" ::Restart Certificate Services net stop certsvc & net start certsvc pause :: Publish CRL certutil -CRL pause </pre> |
|--|--|

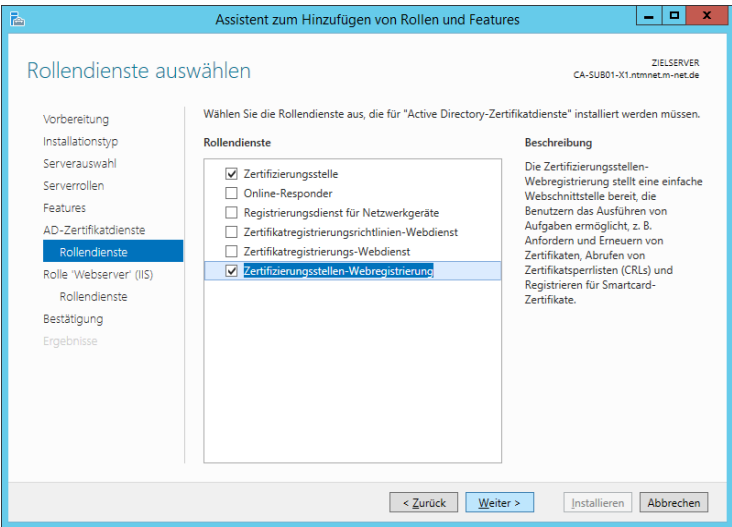
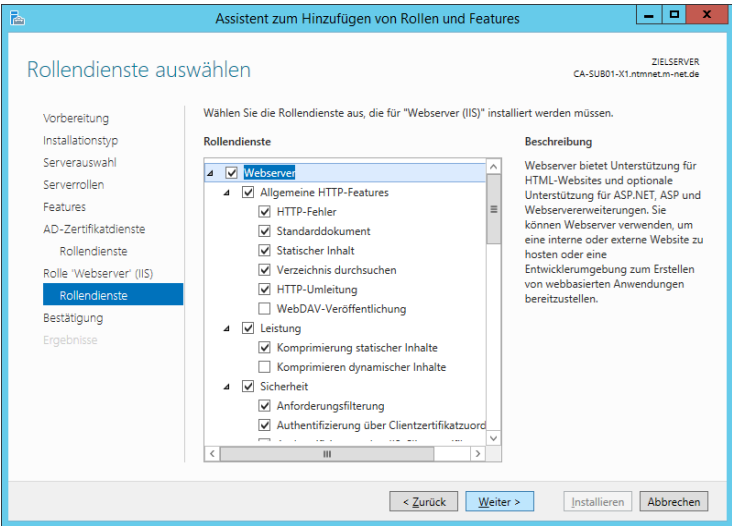
A.5. Einrichtung Active Directory-Zertifikatsdienste der Sub CAs

In diesem Kapitel wird die Installation und Konfiguration der AD-Zertifikatsdienste beschrieben, in deren Verlauf der CSR zur Signierung des Zertifizierungsstellenzertifikats generiert wird. Dieser muss im Anschluss an die Root CA geschickt werden.

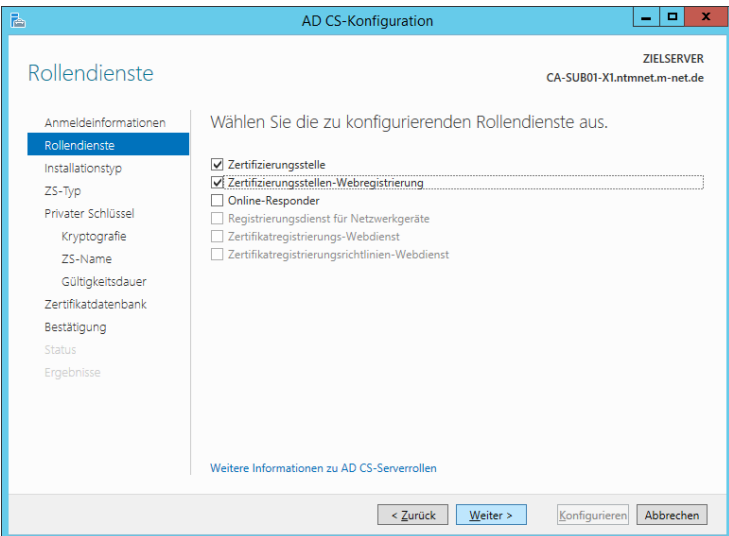
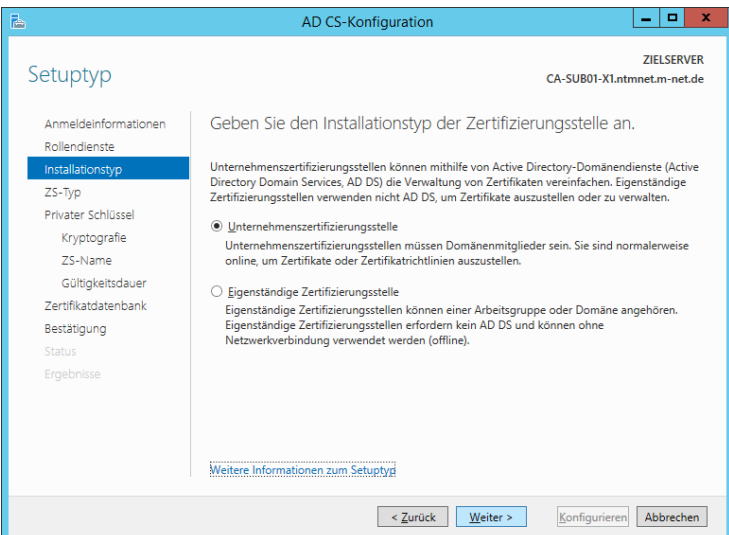
A. Screenshot gestützte Implementierungsdokumentation

| | |
|--|--|
| <p>42 Die vorbereitete capolicy.inf wird nach „C:\Windows“ kopiert. Über den Server-Manager wird anschließend der „Assistent zum Hinzufügen von Rollen und Features“ ausgeführt.</p> |  |
| <p>43 Die „Active Directory-Zertifikatdienste“ werden ausgewählt.</p> |  |
| <p>44 Bei den Rollendiensten wird der Punkt „Active Directory-Zertifikatdienste“ ausgewählt und installiert.</p> |  |

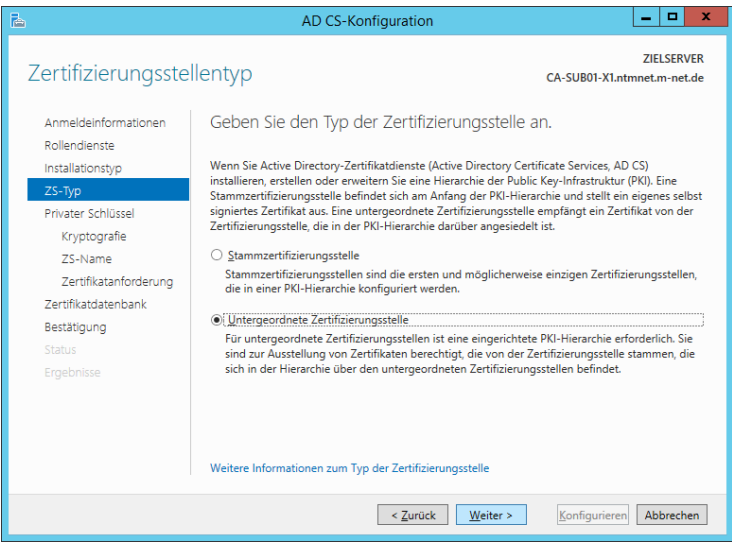
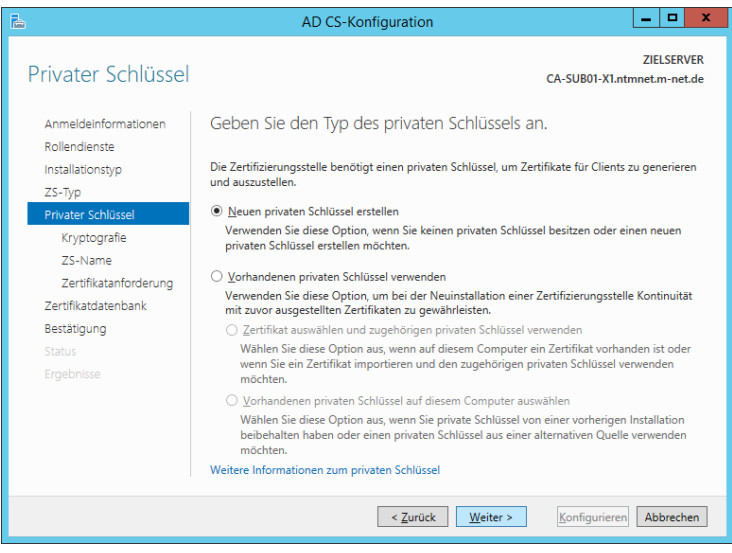
A.5. Einrichtung Active Directory-Zertifikatsdienste der Sub CAs

| | |
|--|---|
| <p>45</p> <p>Die Punkte „Zertifizierungsstelle“ und „Zertifizierungsstellen-Webregistrierung“ werden ausgewählt und die erforderlichen Features hinzugefügt.</p> <p>Bei der M-net-Sub-ServiceLan-01 wird zusätzlich der „Online-Responder“ ausgewählt, da dieser im Gegensatz zu den anderen Sub CAs hier nicht ausgelagert wird.</p> <p>Bei der M-net-Sub-MDM-01 wird zusätzlich für NDES der „Registrierungsdienst für Netzwerkgeräte“ ausgewählt.</p> |  <p>The screenshot shows the 'Assistent zum Hinzufügen von Rollen und Features' window for 'Active Directory-Zertifikatsdienste'. The 'Rollendienste' list includes 'Zertifizierungsstelle', 'Online-Responder', 'Registrierungsdienst für Netzwerkgeräte', 'Zertifikatregistrierungsrichtlinien-Webdienst', and 'Zertifizierungsstellen-Webregistrierung'. The 'Zertifizierungsstellen-Webregistrierung' role is selected. The 'Beschreibung' section explains that the 'Zertifizierungsstellen-Webregistrierung' role provides a simple web interface for users to perform tasks such as requesting, renewing, and revoking certificates, and for registering smartcard certificates.</p> |
| <p>46</p> <p>Der Webserver wird als Rollendienst hinzugefügt.</p> |  <p>The screenshot shows the 'Assistent zum Hinzufügen von Rollen und Features' window for 'Webserver (IIS)'. The 'Rollendienste' list includes 'Webserver', 'Allgemeine HTTP-Features', 'Leistung', and 'Sicherheit'. The 'Webserver' role is selected. The 'Beschreibung' section explains that the 'Webserver' role provides support for HTML websites and optional support for ASP.NET, ASP, and WebServer extensions. It allows the WebServer to be used to host an internal or external website or to create a web-based development environment for creating web-based applications.</p> |

A. Screenshot gestützte Implementierungsdokumentation

| | | |
|-----------|--|---|
| <p>47</p> | <p>Nach Abschluss der Installation erfolgt die Konfiguration, indem die Zertifizierungsstelle und die Zertifizierungsstellen-Webregistrierung ausgewählt werden.</p> |  <p>The screenshot shows the 'AD CS-Konfiguration' window for 'ZIELSERVER' on 'CA-SUB01-X1.ntmnet.m-net.de'. The 'Rollendienste' (Roles) section is active. A list of roles is shown on the left, with 'Rollendienste' selected. The main area contains the instruction 'Wählen Sie die zu konfigurierenden Rollendienste aus.' (Select the roles to configure). The following roles are listed with their selection status: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Zertifizierungsstelle (Certificate Authority) <input checked="" type="checkbox"/> Zertifizierungsstellen-Webregistrierung (Certificate Authority Web Enrollment) <input type="checkbox"/> Online-Responder <input type="checkbox"/> Registrierungsdienst für Netzwerkgeräte (Registration Service for Network Devices) <input type="checkbox"/> Zertifikatregistrierungs-Webdienst (Certificate Registration Web Service) <input type="checkbox"/> Zertifikatregistrierungsrichtlinien-Webdienst (Certificate Registration Policy Web Service) At the bottom, there are navigation buttons: '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'. </p> |
| <p>48</p> | <p>Wenn die Sub CA ein Mitglied einer Domäne ist, was bei unserer Konfiguration der Fall ist, wird der Punkt „Unternehmenszertifizierungsstelle“ ausgewählt.</p> |  <p>The screenshot shows the 'AD CS-Konfiguration' window for 'ZIELSERVER' on 'CA-SUB01-X1.ntmnet.m-net.de'. The 'Setuptyp' (Setup Type) section is active. The main area contains the instruction 'Geben Sie den Installationstyp der Zertifizierungsstelle an.' (Specify the installation type of the certificate authority). The following options are listed: <ul style="list-style-type: none"> <input checked="" type="radio"/> Unternehmenszertifizierungsstelle (Enterprise Certificate Authority): Unternehmenszertifizierungsstellen können mithilfe von Active Directory-Domänendienste (Active Directory Domain Services, AD DS) die Verwaltung von Zertifikaten vereinfachen. Eigenständige Zertifizierungsstellen verwenden nicht AD DS, um Zertifikate auszustellen oder zu verwalten. Unternehmenszertifizierungsstellen müssen Domänenmitglieder sein. Sie sind normalerweise online, um Zertifikate oder Zertifikatrichtlinien auszustellen. <input type="radio"/> Eigenständige Zertifizierungsstelle (Standalone Certificate Authority): Eigenständige Zertifizierungsstellen können einer Arbeitsgruppe oder Domäne angehören. Eigenständige Zertifizierungsstellen erfordern kein AD DS und können ohne Netzwerkverbindung verwendet werden (offline). At the bottom, there are navigation buttons: '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'. </p> |

A.5. Einrichtung Active Directory-Zertifikatsdienste der Sub CAs

| | | |
|-----------|---|---|
| <p>49</p> | <p>Hier wird der Punkt „Untergeordnete Zertifizierungsstelle“ ausgewählt.</p> |  <p>The screenshot shows the 'Zertifizierungsstellentyp' (Certificate Authority Type) configuration window. The left-hand navigation pane has 'ZS-Typ' selected. The main area contains instructions and two radio button options: 'Stammzertifizierungsstelle' (unselected) and 'Untergeordnete Zertifizierungsstelle' (selected). Below the selected option, there is explanatory text about subordinate CAs and a link for further information. At the bottom, there are buttons for '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.</p> |
| <p>50</p> | <p>„Neuen privaten Schlüssel auswählen.“</p> |  <p>The screenshot shows the 'Privater Schlüssel' (Private Key) configuration window. The left-hand navigation pane has 'Privater Schlüssel' selected. The main area contains instructions and three radio button options: 'Neuen privaten Schlüssel erstellen' (selected), 'Vorhandenen privaten Schlüssel verwenden' (unselected), and 'Zertifikat auswählen und zugehörigen privaten Schlüssel verwenden' (unselected). Below the selected option, there is explanatory text about creating a new key. At the bottom, there are buttons for '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.</p> |

A. Screenshot gestützte Implementierungsdokumentation

| | | |
|-----------|---|--|
| <p>51</p> | <p>Hier wird nun „RSA#SafeNet Key Storage Provider“, „SHA256“ und 4096 Bit Schlüssellänge ausgewählt.</p> | |
| <p>52</p> | <p>Der Name der Sub CA und der Domäne wird eingetragen</p> | |

| | | |
|-----------|---|--|
| <p>53</p> | <p>Der Pfad für die Speicherung der Zertifikatanforderung wird angegeben.</p> | |
| <p>54</p> | <p>Zertifikatdatenbank und -protokoll werden unverändert übernommen.</p> | |

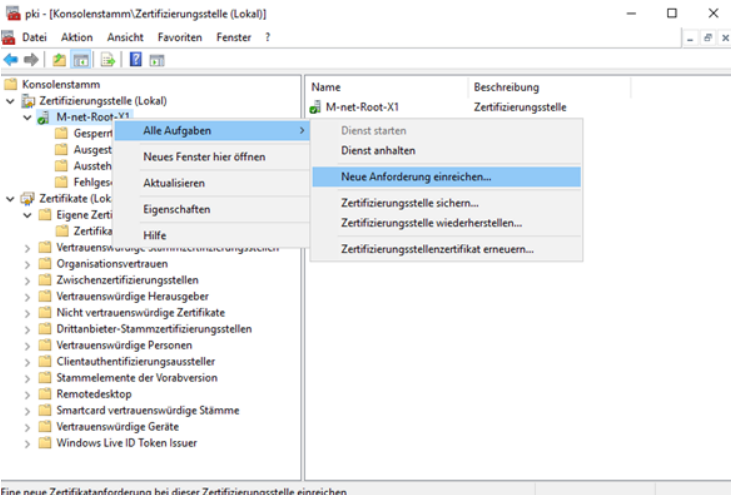
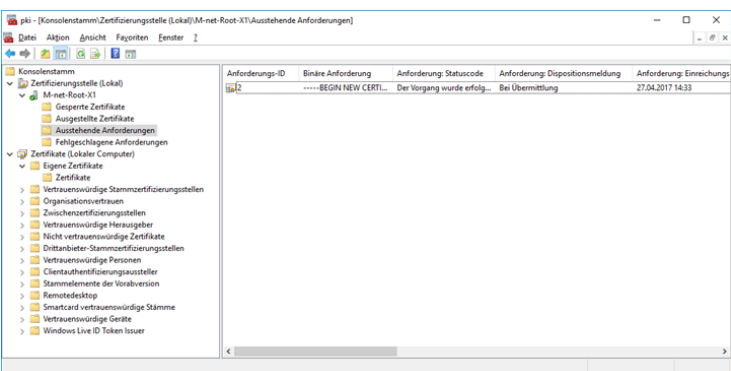
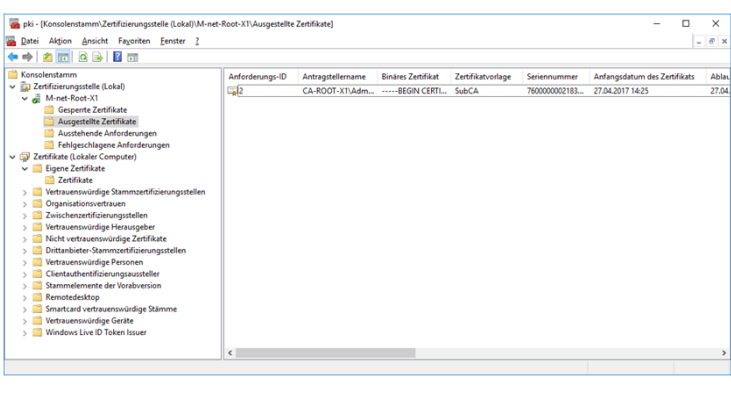
Die Überprüfung, ob die Zertifikate auf der HSM liegen, erfolgt wie in Kapitel 5.1.1. Damit ist eine Zertifikatanforderung erstellt, die nun zur Root CA transportiert und dort ausgestellt werden muss.

A.5.1. Signieren des Sub CA Zertifikats und Konfiguration Sub CA

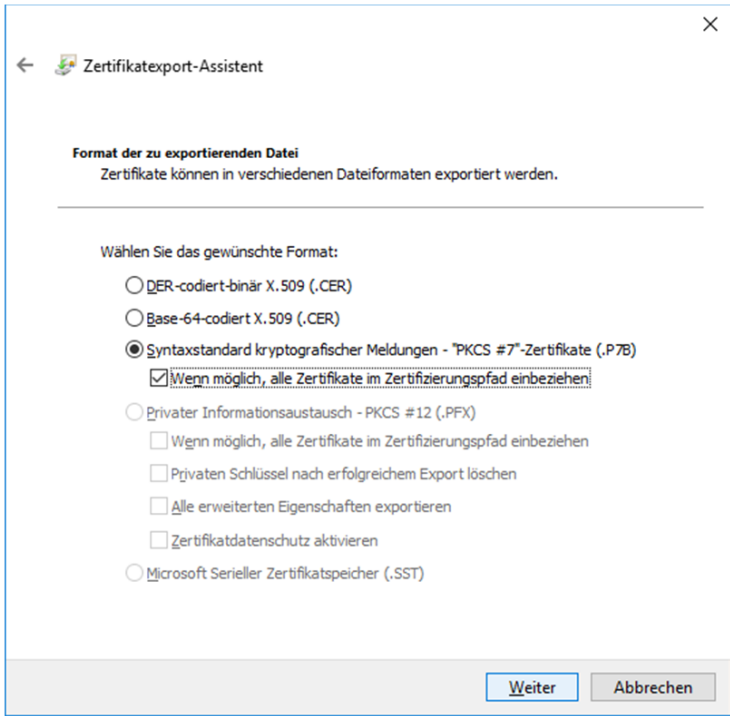
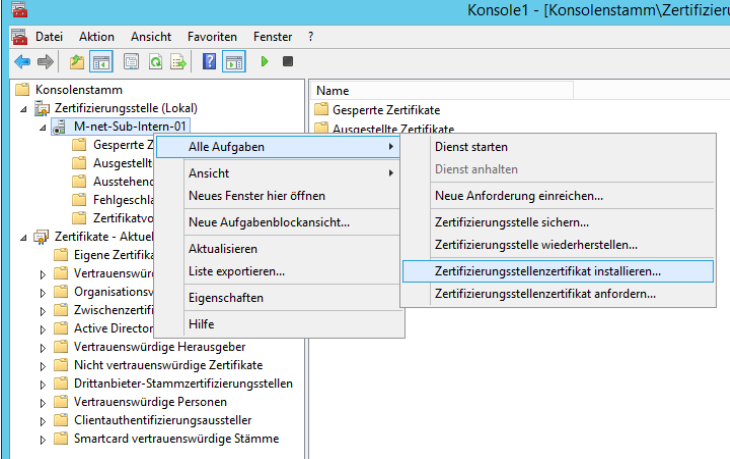
In diesem Kapitel wird die Zertifikatanforderung der Sub CA auf der Root CA eingereicht und signiert. Anschließend wird die Konfiguration der Sub CA durchgeführt.

Die auf der Sub CA erzeugte Zertifikatanforderung muss nun auf die Root CA kopiert werden. Sollte die Root CA nicht für die richtige Domäne konfiguriert sein, muss dies zuvor geändert werden. Es wird die MMC geöffnet und das Snap-In „Lokale Zertifizierungsstelle“ zur Konsole hinzugefügt.

A. Screenshot gestützte Implementierungsdokumentation

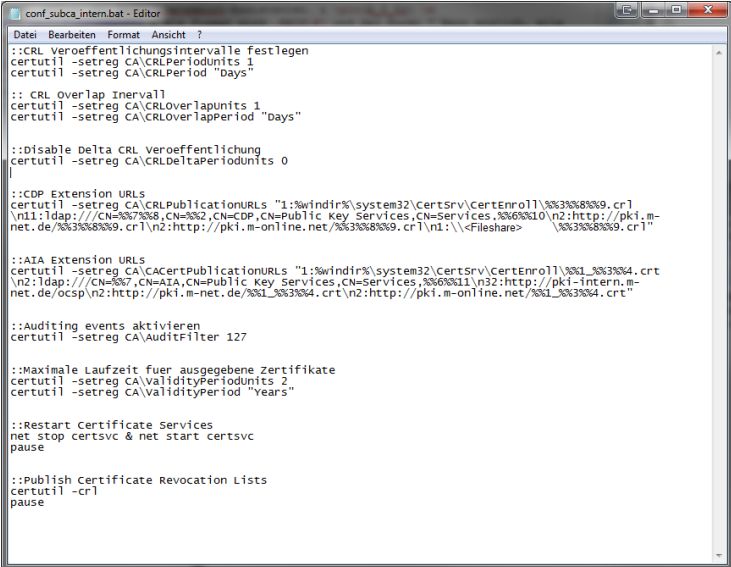
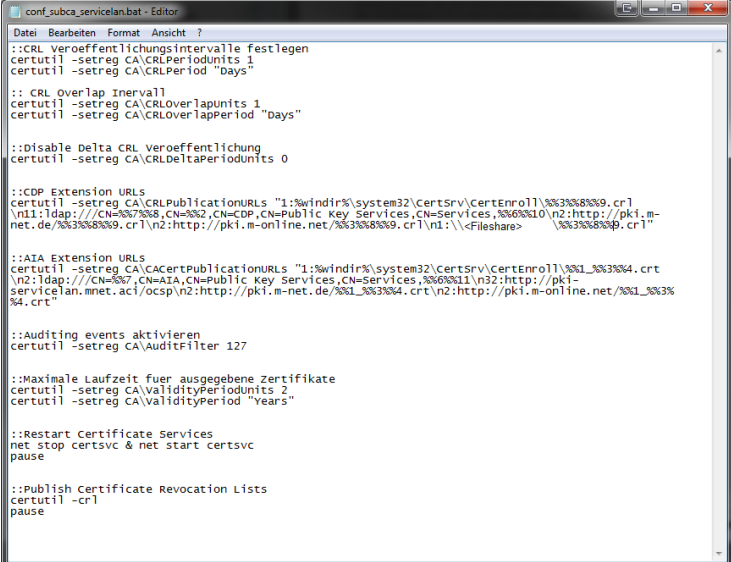
| | | |
|-----------|--|--|
| <p>55</p> | <p>Mit Rechtsklick auf den Namen der Root CA, wird unter „Alle Aufgaben“ → „Neue Anforderung einreichen“ die Zertifikatanforderung ausgewählt.</p> |  |
| <p>56</p> | <p>Diese ist anschließend unter „Ausstehende Anforderungen“ zu finden und wird mit Rechtsklick „Alle Aufgaben“ → „Ausstellen“ ausgestellt.</p> |  |
| <p>57</p> | <p>Unter „Ausgestellte Zertifikate“ ist nun das fertige Zertifikat aufgelistet. Zum Öffnen des Zertifikatexport-Assistenten wird ein Doppelklick auf das Zertifikat ausgeführt, zu dem Reiter „Details“ gewechselt und „In Datei kopieren“ angeklickt.</p> |  |

A.5. Einrichtung Active Directory-Zertifikatsdienste der Sub CAs

| | | |
|-----------|--|---|
| <p>58</p> | <p>Als Format wird PKCS#7 und der Punkt „Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen“ ausgewählt und anschließend das Zertifikat auf die Sub CA kopiert.</p> |  |
| <p>59</p> | <p>Dort Zertifizierungsstellenzertifikat installieren anklicken und das Zertifikat auswählen.</p> |  |

Nun wird die Zertifizierungsstelle mit Rechtsklick auf die CA ->Alle Aufgaben ->Dienst starten gestartet und anschließend das entsprechende Konfigurationsskript für die CA ausgeführt. Im Fall der CA-Sub-Intern ist es das conf.subca.intern.bat Skript, siehe Schritt Nummer 60.

A. Screenshot gestützte Implementierungsdokumentation

| | |
|--|--|
| <p>60</p> <p>Abbildung der conf_-subca.intern.bat.</p> |  <pre> conf_subca_intern.bat - Editor Datei Bearbeiten Format Ansicht ? ::CRL Veröffentlichungsintervalle festlegen certutil -setreg CA\CRLPeriodunits 1 certutil -setreg CA\CRLPeriod "days" :: CRL Overlap Intervall certutil -setreg CA\CRLOverlapunits 1 certutil -setreg CA\CRLOverlapPeriod "days" ::Disable Delta CRL Veröffentlichung certutil -setreg CA\CRLDeltaPeriodunits 0 ::CDP Extension URLs certutil -setreg CA\CRLPublicationURLs "1:%windir%\system32\certsrv\CertEnroll\%1_%3%8%9.cr1 \n1:ldap://CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%10\n2:http://pki.m- net.de/%3%8%9.cr1\n2:http://pki.m-online.net/%3%8%9.cr1\n1:\<Fileshare> \\\%3%8%9.cr1" ::AIA Extension URLs certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\certsrv\CertEnroll\%1_%3%8%4.crt \n2:ldap://CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n3:http://pki- net.de/ocsp\n2:http://pki.m-net.de/%1_%3%8%4.crt\n2:http://pki.m-online.net/%1_%3%8%4.crt" ::Auditing events aktivieren certutil -setreg CA\AuditFilter 127 ::Maximale Laufzeit fuer ausgegebene zertifikate certutil -setreg CA\ValidityPeriodunits 2 certutil -setreg CA\ValidityPeriod "years" ::Restart Certificate Services net stop certsvc & net start certsvc pause ::Publish Certificate Revocation Lists certutil -cr1 pause </pre> |
| <p>61</p> <p>Abbildung der conf_-subca.servicelan.bat.</p> |  <pre> conf_subca_servicelan.bat - Editor Datei Bearbeiten Format Ansicht ? ::CRL Veröffentlichungsintervalle festlegen certutil -setreg CA\CRLPeriodunits 1 certutil -setreg CA\CRLPeriod "days" :: CRL Overlap Intervall certutil -setreg CA\CRLOverlapunits 1 certutil -setreg CA\CRLOverlapPeriod "days" ::Disable Delta CRL Veröffentlichung certutil -setreg CA\CRLDeltaPeriodunits 0 ::CDP Extension URLs certutil -setreg CA\CRLPublicationURLs "1:%windir%\system32\certsrv\CertEnroll\%1_%3%8%9.cr1 \n1:ldap://CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%10\n2:http://pki.m- net.de/%3%8%9.cr1\n2:http://pki.m-online.net/%3%8%9.cr1\n1:\<Fileshare> \\\%3%8%9.cr1" ::AIA Extension URLs certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\certsrv\CertEnroll\%1_%3%8%4.crt \n2:ldap://CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n3:http://pki- servicelan.mnet.ac1/ocsp\n2:http://pki.m-net.de/%1_%3%8%4.crt\n2:http://pki.m-online.net/%1_%3%8% 4.crt" ::Auditing events aktivieren certutil -setreg CA\AuditFilter 127 ::Maximale Laufzeit fuer ausgegebene zertifikate certutil -setreg CA\ValidityPeriodunits 2 certutil -setreg CA\ValidityPeriod "years" ::Restart Certificate Services net stop certsvc & net start certsvc pause ::Publish Certificate Revocation Lists certutil -cr1 pause </pre> |

62 Abbildung der conf_subca_mdm.bat.

```

conf_subca_mdm.bat - Editor
Datei Bearbeiten Format Ansicht ?
::CRL Veröffentlichungsintervalle festlegen
certutil -setreg CA\CRLPeriodUnits 1
certutil -setreg CA\CRLPeriod "Days"

:: CRL Overlap Intervall (CRL 1st nach Ablauf noch diese zeitspanne gültig; optional; Default: 10%)
certutil -setreg CA\CRLOverlapUnits 1
certutil -setreg CA\CRLOverlapPeriod "Days"

::Disable Delta CRL Veröffentlichung
certutil -setreg CA\CRLDeltaPeriodUnits 0

::CDP Extension URLs
certutil -setreg CA\CRLPublicationURLs "1:%windir%\system32\Certsrv\CertEnroll\%33%8%9.cr1
\n2:https://pki.m-net.de/%33%8%9.cr1\n2:https://pki.m-online.net/%33%8%9.cr1\n1:ldap://CN=%7%
%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10\n1:\<Fileshare> \\\%3%8%9.cr1"

::AIA Extension URLs
certutil -setreg CA\CertPublicationURLs "1:%windir%\system32\Certsrv\CertEnroll\%31_%3%4.cr1
\n2:https://pki.m-net.de/%33%8%9.cr1\n2:https://pki.m-online.net/%33%8%9.cr1\n1:ldap://CN=%7%
%8,CN=%2,CN=AIA,CN=Public Key Services,CN=Services,%6%11"

::Auditing events aktivieren
certutil -setreg CA\AuditFilter 127

::Maximale Laufzeit fuer ausgegebene Zertifikate
certutil -setreg CA\ValidityPeriodUnits 2,
certutil -setreg CA\ValidityPeriod "Years"

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

::Publish Certificate Revocation Lists
certutil -cr1
pause
    
```

Anschließend müssen die erstellte Sperrliste und das erstellte Zertifikat auf den Webserver kopiert werden.

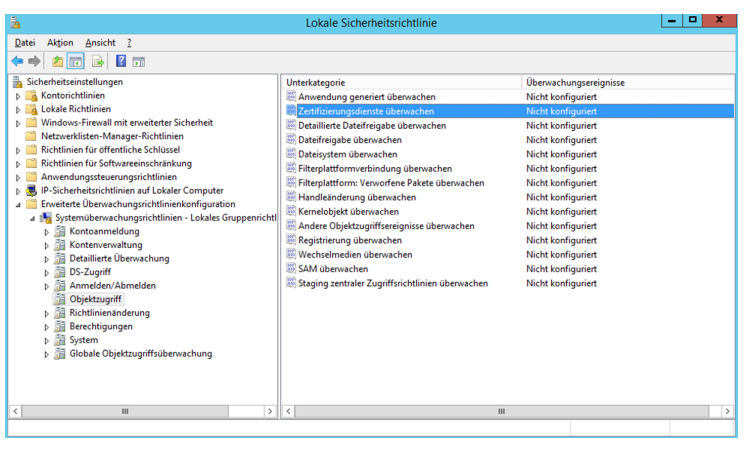
Damit ist die grundlegende Konfiguration der Sub CA abgeschlossen und es können spezifische Einstellungen, z. B. die Unterstützung für SANs vorgenommen werden.

A.5.2. Aktivierung der Systemüberwachungsrichtlinien auf den Sub CAs

In diesem Kapitel wird die Überwachung der Sub CA, die in dem Konfigurationsskript von Schritt Nummer 60 konfiguriert wurde, aktiviert.

Um eine Überwachung der CA zu ermöglichen, muss diese in der lokalen Sicherheitsrichtlinie aktiviert werden.

63 Auf der Sub CA wird die lokale Sicherheitsrichtlinie geöffnet, zum Punkt „Zertifizierungsdienste überwachen“ navigiert, diese geöffnet und dort bei „Erfolg“ und „Fehler“ jeweils ein Haken gesetzt.



A.5.3. Aktivierung der Subject Alternative Names (SANs) in Zertifikaten

Damit auf einer CA ein Zertifikat mit einem „Subject Alternative Name“ ausgestellt werden kann, um z. B. zusätzliche DNS Namen oder eine IP einzutragen, muss dies erst aktiviert werden. Dafür wird in der Eingabeaufforderung auf der CA folgender Befehl ausgeführt:

```
„Certutil -Setreg Policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2“
```

Anschließend muss der Zertifizierungsdienst neu gestartet werden. Dies kann in der Microsoft Management Console erfolgen oder per Eingabeaufforderung und den Befehlen „net stop certsvc“ und anschließend „net start certsvc“.

A.5.4. Installation der Zertifikatvorlagen

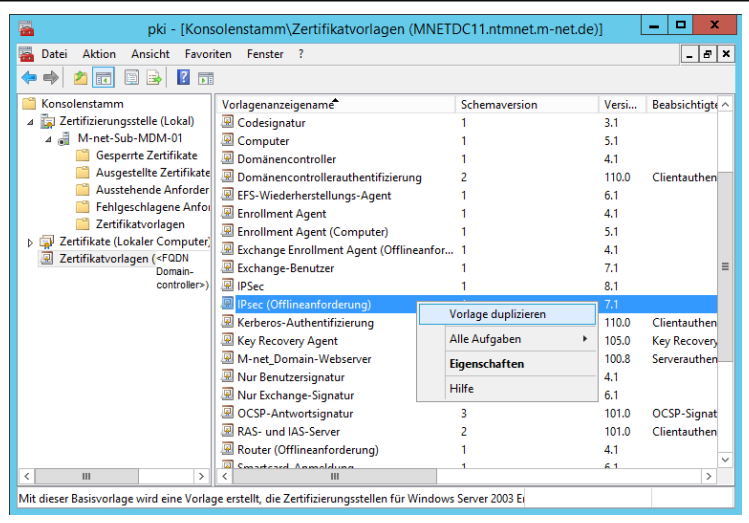
In der MMC muss das Snap-In „Zertifikatvorlagen“ hinzugefügt werden. Anschließend erscheint ein Fenster, das einen zur Installation auffordert, was bestätigt werden muss. Nun sind die Standard Zertifikatvorlagen sichtbar und benutzbar. Dies muss einmal in jeder Domäne gemacht werden.

A.5.5. Konfiguration der Zertifikatvorlagen

In diesem Kapitel werden die Konfigurationen einiger der benötigten Zertifikatvorlagen dokumentiert.

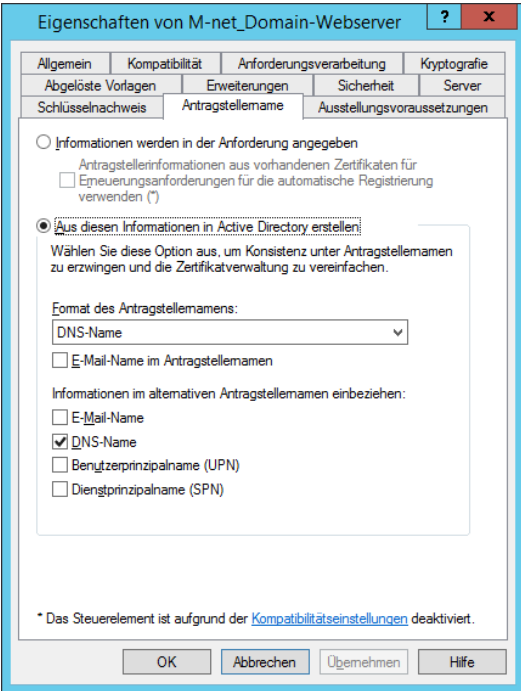
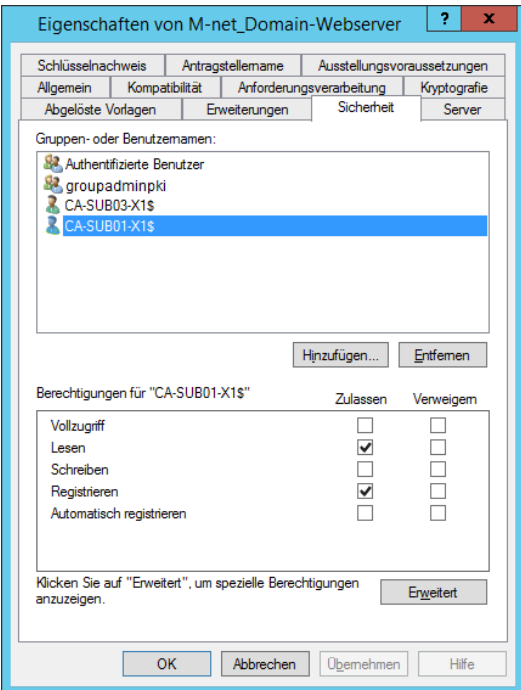
Nach Abschluss der Konfiguration der Zertifikatvorlagen müssen diese auf den CAs veröffentlicht werden, die mit Hilfe dieser Zertifikatvorlagen Zertifikate ausstellen sollen.

Um eine bessere Übersicht über die Zertifikatvorlagen zu erhalten, wird jede verwendete Zertifikatvorlage dupliziert und umbenannt. Dabei geschieht die Umbenennung durch Hinzufügen des Präfixes „M-net_“ vor den englischen Namen der Zertifikatvorlage. Das Duplizieren ist im Implementierungsschritt Nummer 64 beschrieben. Anschließend wird auf jede Vorlage die Standard Sicherheitskonfiguration, wie in Kapitel 4.4 veranschaulicht, konfiguriert.

| | |
|---|--|
| <p>64 Eine Vorlage wird dupliziert, indem man in das MMC Snap-In „Zertifikatvorlagen“ wechselt und dort einen Rechtsklick auf eine Standardvorlage ausführt und „Vorlage duplizieren“ auswählt.</p> <p>In diesem Beispielbild wird dies auf die Vorlage „IPSec (Offlineanforderung)“ angewandt.</p> |  |
|---|--|

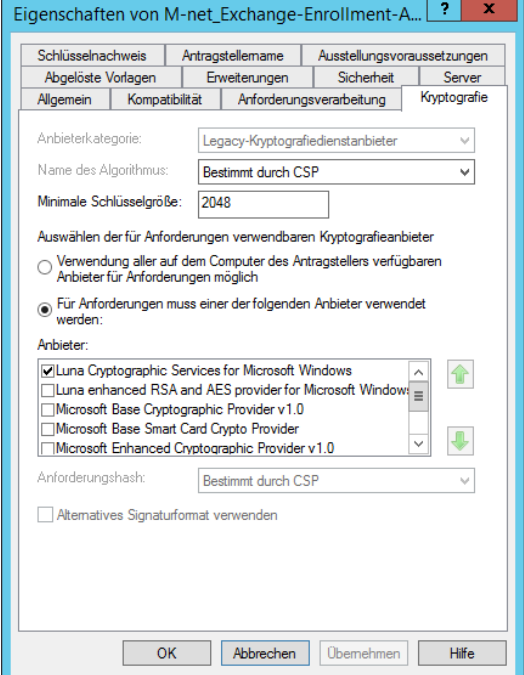
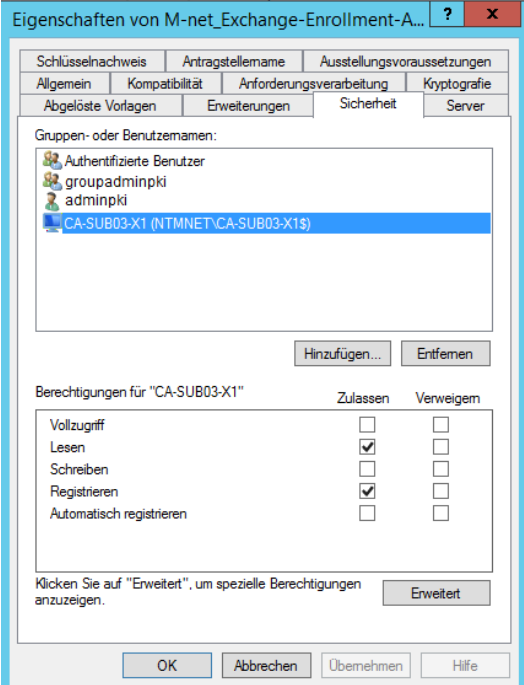
A.5.5.1. M-net_Domain-Webserver

Diese Zertifikatvorlage dient zur Erstellung von SSL Zertifikaten. Da jede CA eine Zertifizierungsstellen-Webregistrierung über einen selbst gehosteten IIS bereitstellt, braucht der IIS ein SSL Zertifikat, das von seiner CA signiert ist. Dies bedeutet, dass diese Zertifikatvorlage in der ServiceLan und in der ntmnet Domäne erstellt und von jeder CA veröffentlicht werden muss.

| | | |
|-----------|--|--|
| <p>65</p> | <p>Der DNS-Name wird als Antragstellernamen konfiguriert und in den SAN einbezogen.</p> |  |
| <p>66</p> | <p>Die Sub CAs werden mit den Rechten „Lesen“ und „Registrieren“ im Sicherheitsreiter konfiguriert. In der ntmnet Domäne sind dies die Sub-CA-Intern und die Sub-CA-MDM, in der ServiceLan Domäne die Sub-CA-ServiceLan.</p> |  |

A.5.5.2. M-net_Exchange-Enrollment-Agent(offlinerequest)

In diesem Kapitel wird die Konfiguration der Zertifikatvorlage für das Exchange Enrollment Zertifikat beschrieben, welche für die Zertifikatanforderung an die CA benötigt wird. Diese Zertifikatvorlage muss auf der Sub-CA-MDM erstellt werden, da nur diese den Luna CSP als Kryptografieanbieter eingerichtet hat.

| | | |
|-----------|---|--|
| <p>67</p> | <p>Der Luna CSP wird als Kryptografieanbieter mit 2048 Bit Schlüssellänge ausgewählt.</p> |  |
| <p>68</p> | <p>Die Sub-CA-MDM wird im Sicherheitsreiter mit den Rechten „Lesen“ und „Registrieren“ hinzugefügt.</p> |  |

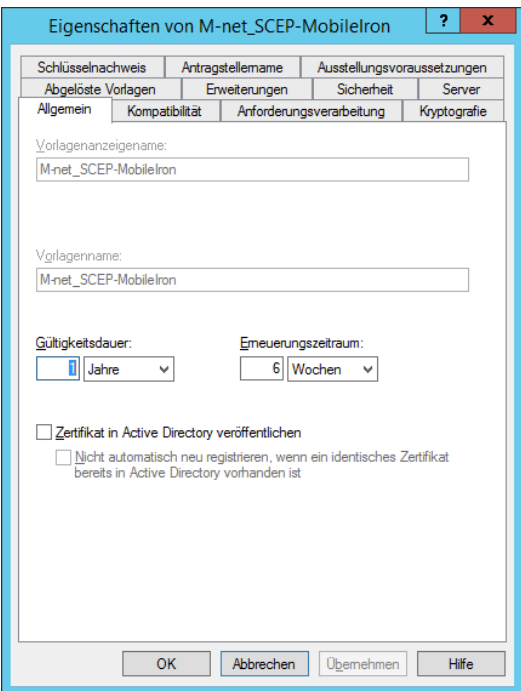
Anschließend wird diese Zertifikatvorlage auf der Sub-CA-MDM veröffentlicht.

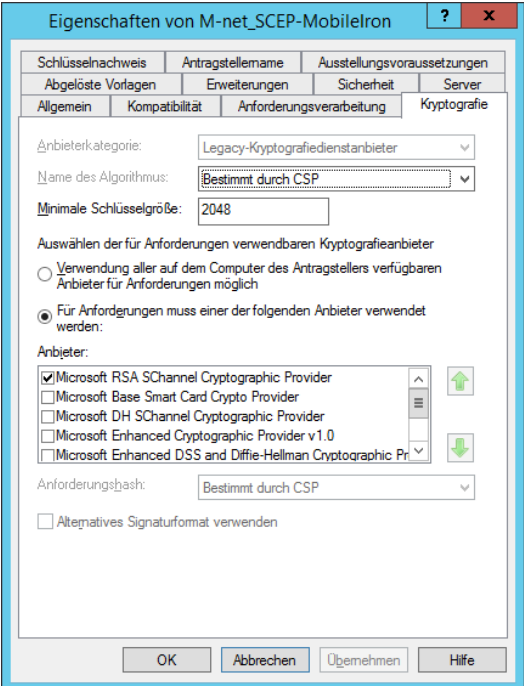
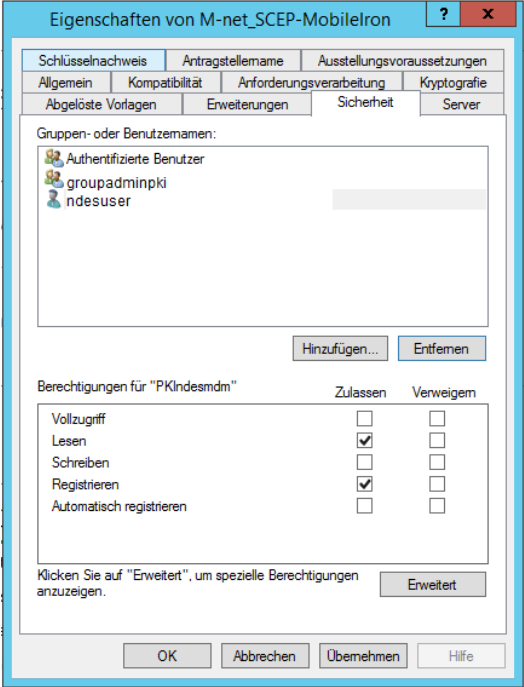
A.5.5.3. M-net_CEP-Encryption

Für die verschlüsselte Kommunikation zwischen dem NDES Dienst und MobileIron wird die Zertifikatvorlage M-net_CEP-Encryption verwendet. Dazu wird die Zertifikatvorlage „CEP-Verschlüsselung“ dupliziert und in „M-net_CEP-Encryption“ umbenannt. Die Einstellungen im Reiter „Kryptografie“ und „Sicherheit“ sind analog zur M-net_Exchange-Enrollment-Agent(offlinerequest) Zertifikatvorlage. Diese wird nach Abschluss der Konfiguration auf der Sub-CA-MDM veröffentlicht.

A.5.5.4. M-net_SCEP-MobileIron

Die Zertifikatvorlage M-net_SCEP-MobileIron wird nur für MobileIron verwendet, um von MobileIron aus Zertifikate anzufordern. Daher wird diese Zertifikatvorlage nur auf der Sub-CA-MDM veröffentlicht. Dazu wird die Standardvorlage „IPSec (Offlineanforderung)“ dupliziert und in „M-net_SCEP-MobileIron“ umbenannt.

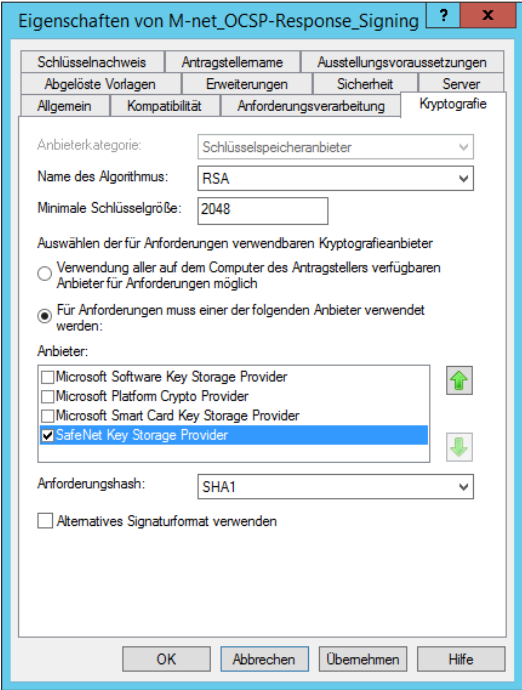
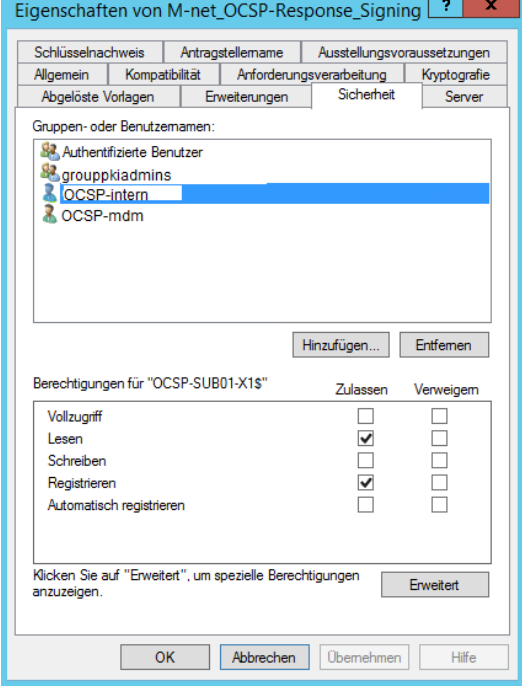
| | | |
|-----------|---|--|
| <p>69</p> | <p>Die Gültigkeitsdauer wird auf ein Jahr festgelegt.</p> |  <p>The screenshot shows a dialog box titled "Eigenschaften von M-net_SCEP-MobileIron". It has several tabs: "Schlüsselnachweis", "Antragstellename", "Ausstellungsvoraussetzungen", "Abgelöste Vorlagen", "Erweiterungen", "Sicherheit", and "Server". The "Allgemein" tab is selected. The "Vorlagenanzeigename" and "Vorlagenname" fields both contain "M-net_SCEP-MobileIron". The "Gültigkeitsdauer" is set to "1" year, and the "Erneuerungszeitraum" is set to "6" weeks. There are two checkboxes: "Zertifikat in Active Directory veröffentlichen" (unchecked) and "Nicht automatisch neu registrieren, wenn ein identisches Zertifikat bereits in Active Directory vorhanden ist" (unchecked). At the bottom, there are buttons for "OK", "Abbrechen", "Übernehmen", and "Hilfe".</p> |
|-----------|---|--|

| <p>70</p> | <p>Die Schlüssellänge wird mit 2048 Bit angegeben.</p> |  | | | | | | | | | | | | | | | | | | |
|---------------------------------|--|--|---------------------------------|----------|------------|-------------|--------------------------|--------------------------|-------|-------------------------------------|--------------------------|-----------|--------------------------|--------------------------|--------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| <p>71</p> | <p>Der Benutzer ndesuser wird im Sicherheitsreiter mit den Rechten „Lesen“ und „Registrieren“ hinzugefügt.</p> |  <table border="1" data-bbox="710 1310 1173 1489"> <thead> <tr> <th>Berechtigungen für "PKIndesmdm"</th> <th>Zulassen</th> <th>Verweigern</th> </tr> </thead> <tbody> <tr> <td>Vollzugriff</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Lesen</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Schreiben</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Registrieren</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Automatisch registrieren</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> | Berechtigungen für "PKIndesmdm" | 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"/> |
| Berechtigungen für "PKIndesmdm" | 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"/> | | | | | | | | | | | | | | | | | | |

Nach Abschluss der Konfiguration wird die Zertifikatvorlage auf der Sub-CA-MDM veröffentlicht.

A.5.5.5. M-net_OCSP-Response_Signing

Für die Signatur der Nachrichten der OCSP Responder wird die Zertifikatvorlage „OCSP-Antwortsignatur“ verwendet, dupliziert und in „M-net_OCSP-Response_Signing“ umbenannt.

| | | |
|-----------|---|--|
| <p>72</p> | <p>Der Luna KSP wird als Kryptografieanbieter ausgewählt.</p> |  |
| <p>73</p> | <p>In der Domäne ntmnet werden die beiden OCSP Responder mit den Rechten „Lesen“ und „Registrieren“ eingetragen. In der Domäne ServiceLan wird statt dem OCSP Responder die Sub-CA-ServiceLan im Sicherheitsreiter eingetragen, da dort der OCSP Dienst auf der Sub CA läuft und nicht ausgegliedert wurde.</p> |  |

Diese Zertifikatvorlage wird nun auf allen Sub CAs veröffentlicht, da jede Sub CA einen OCSP Responder benutzt.

A.5.6. Konfiguration des Microsoft Internet Information Services (IIS)

In diesem Kapitel wird die Konfiguration des IIS für die Zertifizierungsstellen-Webregistrierung durchgeführt.

Die Microsoft Internet Information Services erlauben einen Zertifikatanforderungsprozess über eine gehostete Webseite der CAs. Dafür muss die Zertifizierungsstellen-Webregistrierung installiert und anschließend die AD CS-Konfiguration durchgeführt werden. Dies ist in Kapitel A.5 geschehen.

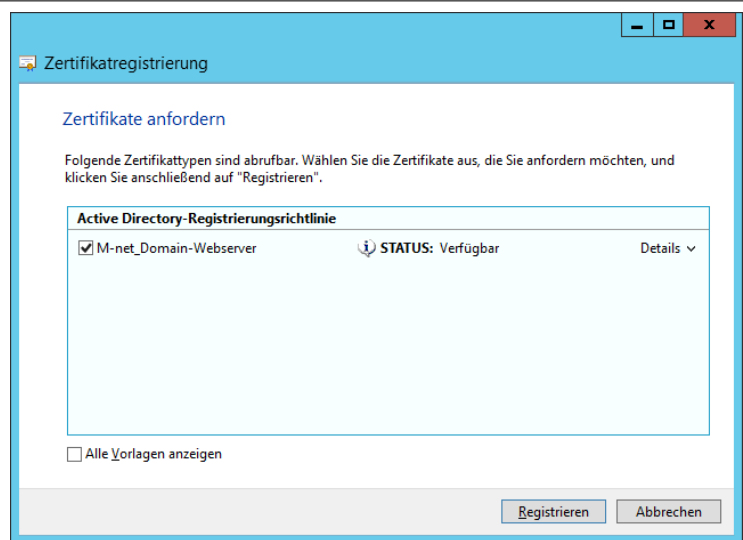
Für die Zertifikatanforderung über diese Webseite sind Anmeldedaten erforderlich, weshalb die Verbindung per SSL abgesichert werden muss, was den Einsatz eines SSL-Zertifikats erforderlich macht. Deshalb wird in beiden Domänen eine Zertifikatvorlage erstellt, die ein automatisches Registrieren eines SSL-Zertifikats für den IIS ermöglicht. Dies ist in Kapitel A.5.5.1 beschrieben.

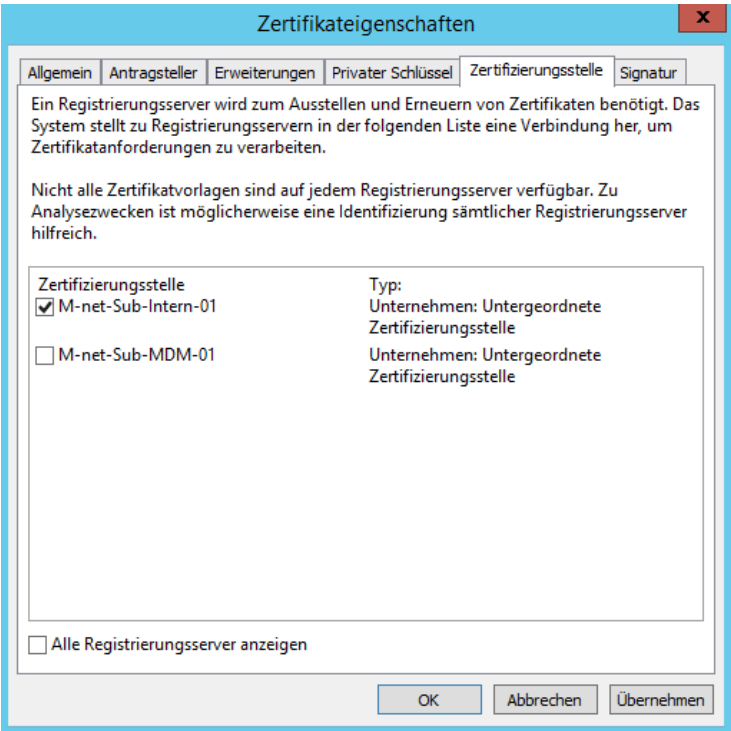
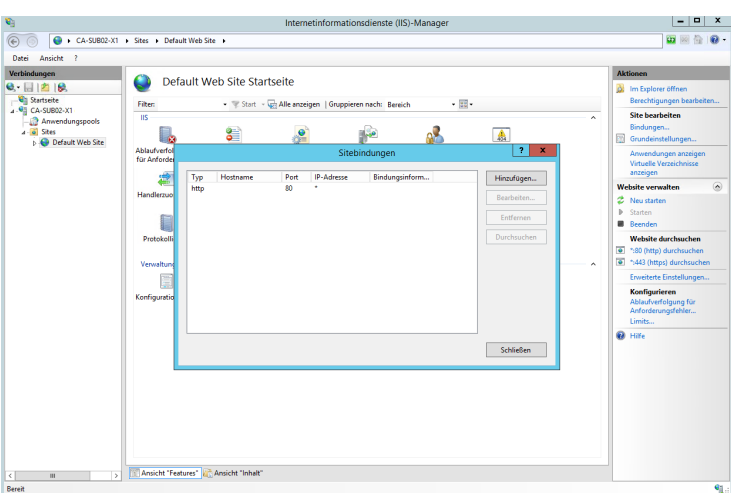
| | |
|--|--|
| <p>74 In der MMC wird das Snap-In „Eigene Zertifikate (Lokaler Computer)“ eingebunden. Anschließend wird mit Rechtsklick auf die eigenen Zertifikate und mit einem Klick auf „Alle Aufgaben“ → „Neues Zertifikat anfordern...“ das Zertifikatregistrierungsfenster geöffnet.</p> | |
|--|--|

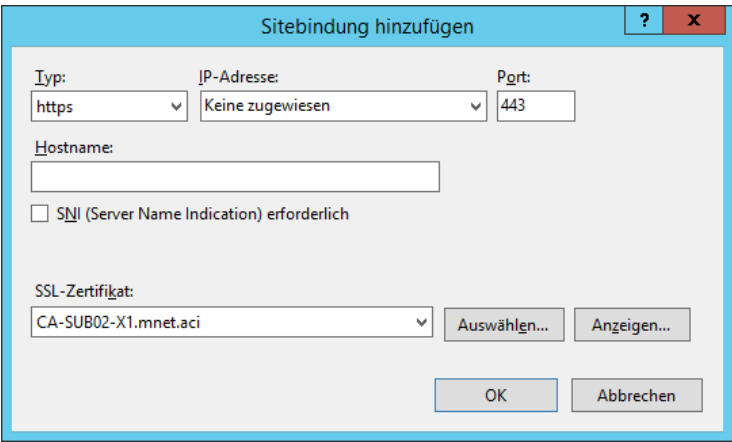
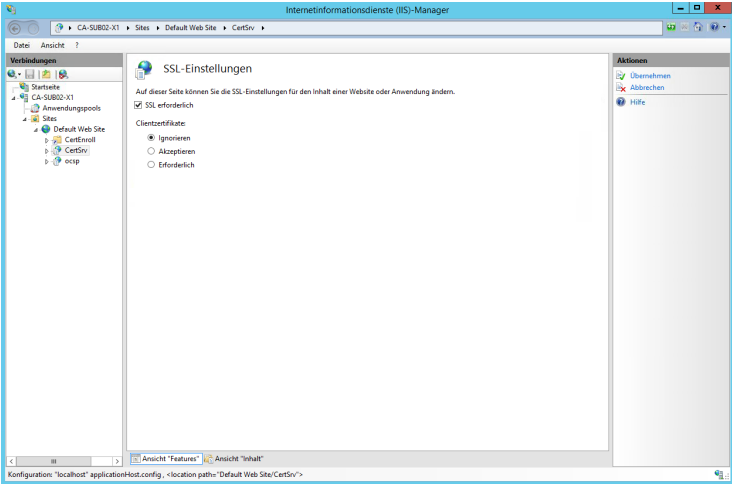
75

In dem Zertifikatregistrierungsfenster wird die Zertifikatvorlage „M-net_Domain-Webserver“ ausgewählt.

Wenn mehrere gleichnamige Zertifikatvorlagen von verschiedenen CAs in der gleichen Domäne verfügbar sind, muss mit Klick auf „Details“ und dann „Eigenschaften“ die CA definiert werden, von der die Zertifikatvorlage benutzt werden soll. Ist dies der Fall, muss Schritt Nummer 76 ausgeführt werden. Ansonsten kann dieser Schritt übersprungen werden und das SSL Zertifikat mit Klick auf „Registrieren“ angefordert werden.



| | | |
|-----------|---|---|
| <p>76</p> | <p>Im Reiter „Zertifizierungsstelle“ wird nun die CA ausgewählt, von der das Zertifikat ausgestellt werden soll. Mit Klick auf „Übernehmen“ und anschließend „Registrieren“ wird das SSL Zertifikat dann angefordert.</p> |  <p>The screenshot shows the 'Zertifikateigenschaften' dialog box with the 'Zertifizierungsstelle' tab selected. The text reads: 'Ein Registrierungsserver wird zum Ausstellen und Erneuern von Zertifikaten benötigt. Das System stellt zu Registrierungsservern in der folgenden Liste eine Verbindung her, um Zertifikatanforderungen zu verarbeiten.' Below this, it states: 'Nicht alle Zertifikatvorlagen sind auf jedem Registrierungsserver verfügbar. Zu Analyse Zwecken ist möglicherweise eine Identifizierung sämtlicher Registrierungsserver hilfreich.' A table lists two registration servers: 'M-net-Sub-Intern-01' (checked) and 'M-net-Sub-MDM-01' (unchecked). The 'Typ' for both is 'Unternehmen: Untergeordnete Zertifizierungsstelle'. At the bottom, there is a checkbox for 'Alle Registrierungsserver anzeigen' and buttons for 'OK', 'Abbrechen', and 'Übernehmen'.</p> |
| <p>77</p> | <p>Nun wird der IIS-Manager geöffnet, die „Default Web Site“ ausgewählt, auf „Bindungen...“ geklickt und das nebenstehende Fenster öffnet sich. Dort wird nun auf Hinzufügen geklickt, woraufhin sich das Fenster von Schritt Nummer 78 öffnet.</p> |  <p>The screenshot shows the IIS Manager interface for the 'Default Web Site Startseite'. The 'Sitebindungen' dialog box is open, displaying a table with the following columns: 'Typ', 'Hostname', 'Port', and 'Bindungsform...'. The table contains one entry: 'http', 'http', '80', and '-'. To the right of the table are buttons for 'Hinzufügen...', 'Bearbeiten...', 'Entfernen', and 'Durchsuchen'. At the bottom of the dialog is a 'Schließen' button. The background shows the IIS Manager interface with the 'Default Web Site' selected in the tree view.</p> |

| | |
|---|---|
| <p>78 Der Typ „https“ und der Port „443“ wird definiert. Als SSL-Zertifikat wird das ausgestellte SSL Zertifikat ausgewählt.</p> |  |
| <p>79 Da die Verbindung über die Zertifizierungsstellen-Webregistrierung nur verschlüsselt erfolgen soll, werden die „SSL-Einstellungen“ des „CertSrv“ geöffnet und dort der Punkt „SSL erforderlich“ ausgewählt.</p> |  |

Damit ist der IIS und die darauf laufende Zertifizierungsstellen-Webregistrierung fertig eingerichtet.

A.5.7. Konfiguration des OCSP Responders

In diesem Kapitel wird die Implementierung des OCSP Responders beschrieben.

Dabei wird der OCSP Responder für die Sub-CA-Intern und die Sub-CA-MDM ausgelagert, während bei der Sub-CA-ServiceLan dieser auf der Sub CA direkt läuft. Die Installation über den Assistenten zum Hinzufügen von Rollen und Features wurde für den OCSP Responder der Sub-CA-ServiceLan bereits in Kapitel A.5 durchgeführt. Deswegen müssen die Installationsschritte Nummer 81 und 82 nur für die ausgelagerten OCSP Responder durchgeführt werden. Die Konfiguration des OCSP Responders erfolgt bei beiden Varianten gleich.

Für den OCSP Responder Dienst muss eine Zertifikatvorlage für die OCSP Antwortsignatur veröffentlicht werden, was in Kapitel A.5.5.5 durchgeführt wurde. Mit Hilfe dieser Zertifikatvorlage fordert der OCSP-Dienst ein Zertifikat von der Zertifizierungsstelle an, an die er angebunden ist. Mit diesem Zertifikat signiert der OCSP Responder seine Antwort-

A. Screenshot gestützte Implementierungsdokumentation

nachricht an das zertifikatstatusanfragende Gerät.

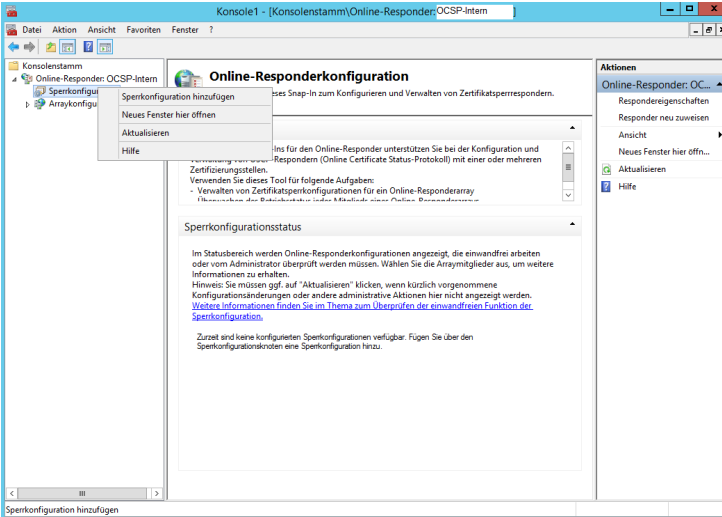
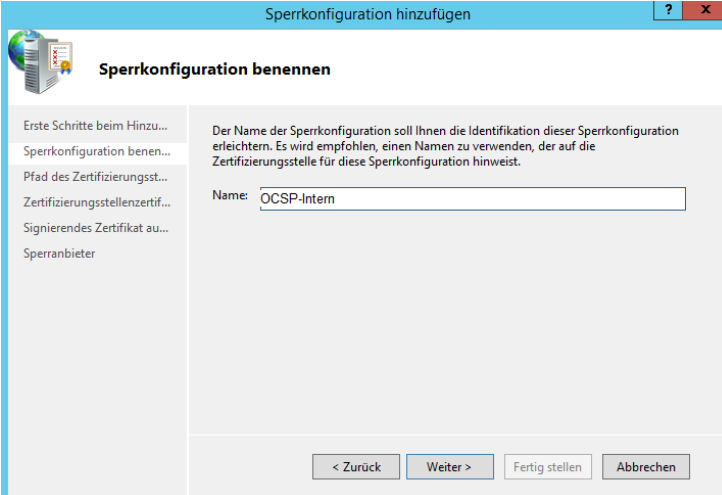
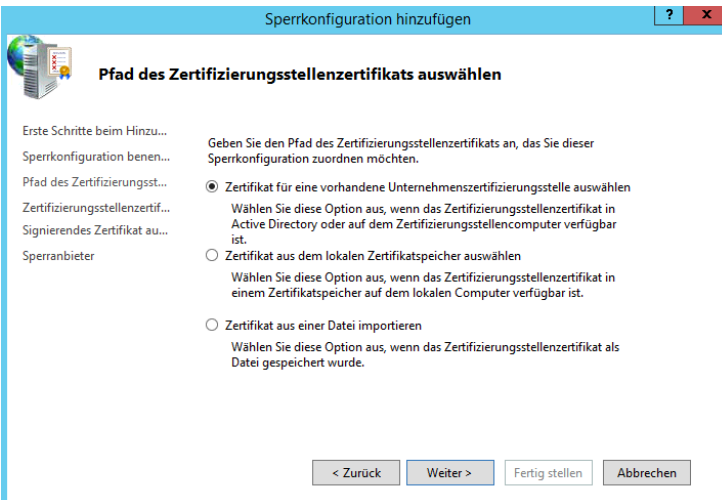
| | |
|--|--|
| <p>80</p> <p>Der Pfad des OCSP Responders muss in den AIA Erweiterungen konfiguriert und der Punkt „In OCSP-Erweiterungen einbeziehen“ ausgewählt sein.</p> <p>Dies ist durch das Verwenden des conf_subca_intern.bat Skriptes in Schritt Nummer 60 bereits geschehen.</p> | |
| <p>81</p> <p>Auswahl der „Active Directory-Zertifikatdienste“ als Serverrolle zur Installation.</p> | |

A.5. Einrichtung Active Directory-Zertifikatsdienste der Sub CAs

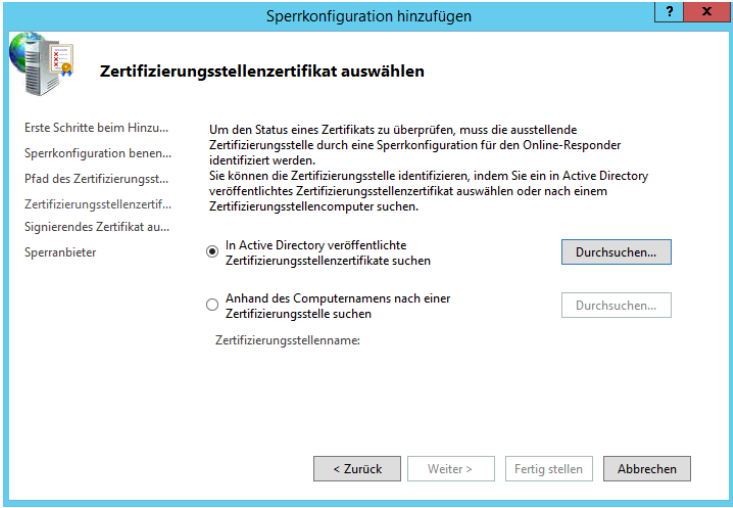
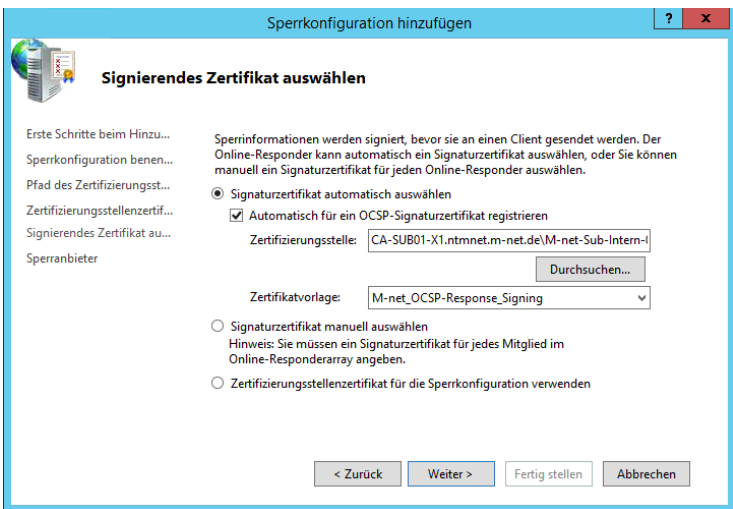
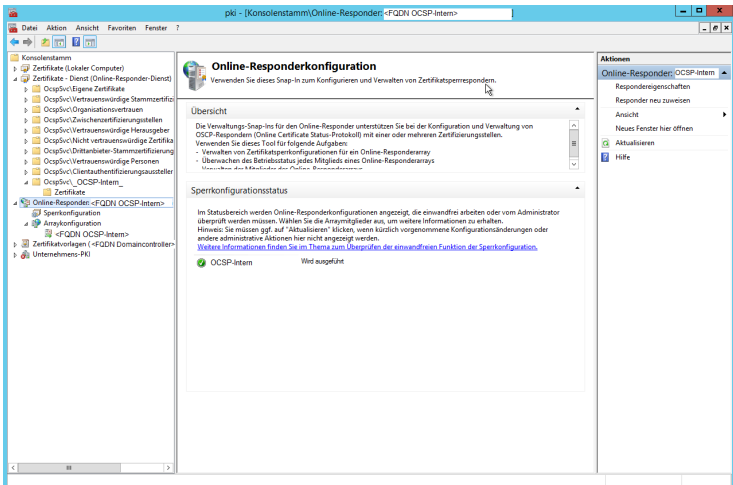
| | | |
|-----------|--|--|
| <p>82</p> | <p>Den „Online-Responder“ bei den Rollendiensten auswählen, die weiteren Dialogfenster mit „weiter“ bestätigen und die Installation abschließen.</p> | |
| <p>83</p> | <p>Nach Abschluss der Installation muss nun der Online-Responder konfiguriert werden.</p> | |

| | | |
|-----------|---|--|
| <p>84</p> | <p>Den „Online-Responder“ auswählen, die Bestätigungsfenster mit „weiter“ bestätigen und die Konfiguration abschließen.</p> | |
| <p>85</p> | <p>Die in Kapitel A.5.5.5 konfigurierte Zertifikatvorlage bedingt die Verwendung der HSMs für das Signaturzertifikat der Online Responder.</p> <p>Dadurch muss in den lokalen Diensten für den Online-Responder-Dienst die Anmeldung so konfiguriert werden, dass diese mit dem lokalen Systemkonto erfolgt und ein Datenaustausch zwischen Dienst und Desktop zugelassen wird.</p> | |

A.5. Einrichtung Active Directory-Zertifikatsdienste der Sub CAs

| | | |
|-----------|---|--|
| <p>86</p> | <p>Nun muss in der Microsoft Management Console das Snap-In „Online-Responder“ hinzugefügt und mit Rechtsklick auf „Sperrkonfiguration“ eine neue Sperrkonfiguration hinzugefügt werden.</p> |  |
| <p>87</p> | <p>Dieser vergibt man einen Namen, wobei bei dieser PKI Implementierung der Name des OCSF Responders verwendet wird.</p> |  |
| <p>88</p> | <p>Da der OCSF Responder Mitglied der gleichen Domäne wie die CA ist, wird der Punkt „Zertifikat für eine vorhandene Unternehmenszertifizierungsstelle auswählen“ mit Klick auf „weiter“ bestätigt.</p> |  |

A. Screenshot gestützte Implementierungsdokumentation

| | | |
|----|--|--|
| 89 | <p>Das Zertifizierungsstellenzertifikat von der CA, an die der OCSP Responder angebunden wird, wird mit Klick auf „durchsuchen“ ausgewählt.</p> |  <p>The screenshot shows a dialog box titled 'Sperrkonfiguration hinzufügen' with a sub-header 'Zertifizierungsstellenzertifikat auswählen'. It contains instructions on how to select a certificate and two radio button options: 'In Active Directory veröffentlichte Zertifizierungsstellenzertifikate suchen' (selected) and 'Anhand des Computernamens nach einer Zertifizierungsstelle suchen'. There are 'Durchsuchen...' buttons for each option and navigation buttons at the bottom.</p> |
| 90 | <p>Es wird die automatische Signaturzertifikatregistrierung, die entsprechende CA und die Zertifikatvorlage für den OCSP Responder ausgewählt und somit die Konfiguration der Sperrkonfiguration abgeschlossen.</p> |  <p>The screenshot shows the same dialog box but at the 'Signierendes Zertifikat auswählen' step. It includes instructions on signing and a checked option 'Automatisch für ein OCSP-Signaturzertifikat registrieren'. A dropdown menu for 'Zertifikatvorlage' is set to 'M-net_OCSP-Response_Signing'. There are also options for manual selection or using the CA certificate.</p> |
| 91 | <p>Die soeben konfigurierte Sperrkonfiguration erscheint nun bei dem Punkt „Sperrkonfiguration“, auf der HSM wird ein Schlüsselpaar für den OCSP Responder generiert und das Zertifikat der Sperrkonfiguration zugewiesen. Daraufhin ändert sich der Sperrkonfigurationsstatus auf „Wird ausgeführt“, womit der OCSP Responder funktionsfähig ist.</p> |  <p>The screenshot shows the 'Online-Responderkonfiguration' window in a console environment. The left sidebar shows a tree view with 'Sperrkonfiguration' selected. The main area shows an overview of the configuration and its status, which is 'Wird ausgeführt' (Running). A right-hand pane shows actions like 'Responder neu zuweisen'.</p> |

| | |
|--|--|
| <p>92 In den Eigenschaften der „Sperrkonfiguration“ werden die „Sperranbieterereigenschaften“ geöffnet und das Aktualisierungsintervall auf fünf Minuten festgelegt.</p> | |
|--|--|

Damit ist die Einrichtung des OCSP Responders abgeschlossen.

A.5.8. Konfiguration des Network Device Enrollment Services (NDES)

Dieses Kapitel behandelt die Einrichtung des NDES Dienstes, welcher SCEP bereitstellt und zur Anbindung an den MobileIron Server benutzt wird.

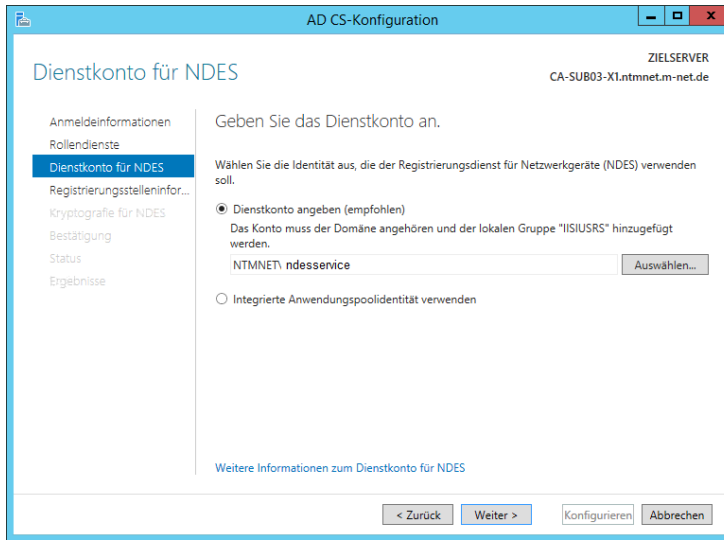
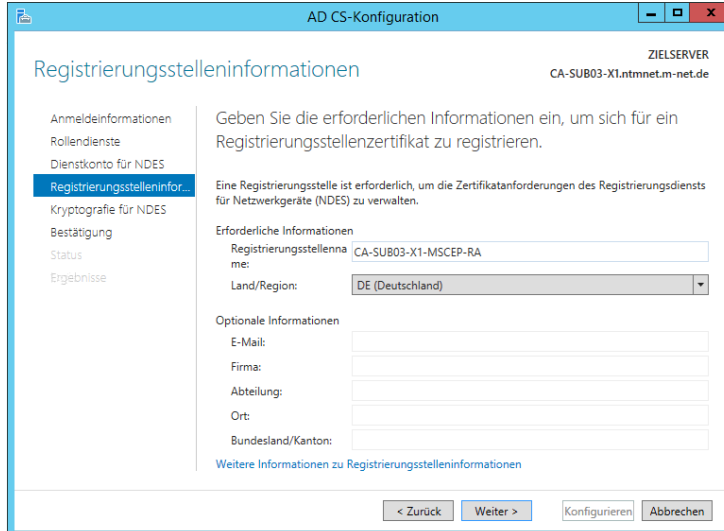
Dafür müssen zwei Domänenaccounts eingerichtet werden. Der Domänenadministrator ndesservice betreibt den NDES Dienst, während der Domänenbenutzer ndesuser die Zertifikate für das Mobile-Device-Management anfordert.

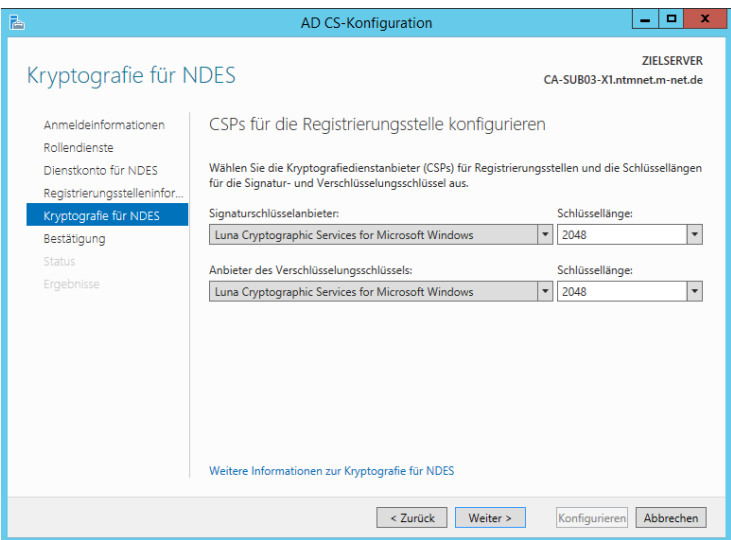
| | |
|--|--|
| <p>93 Der Domänenadministrator ndesservice muss der lokalen Benutzergruppe „IIS_IUSRS“ und den lokalen Administratoren hinzugefügt werden.</p> | |
|--|--|

A. Screenshot gestützte Implementierungsdokumentation

| | | |
|-----------|---|--|
| <p>94</p> | <p>Die Konfiguration des NDES wird über den Servermanager gestartet und der Benutzer ndesservice wird als Anmeldekonto angegeben.</p> | |
| <p>95</p> | <p>Bei den Rollendiensten wird der „Registrierungsdienst für Netzwerkgeräte“ ausgewählt.</p> | |

A.5. Einrichtung Active Directory-Zertifikatsdienste der Sub CAs

| | | |
|-----------|---|--|
| <p>96</p> | <p>Als Dienstkonto wird der ndesservice ausgewählt.</p> |  <p>The screenshot shows the 'AD CS-Konfiguration' window with the 'Dienstkonto für NDES' step selected. The left sidebar lists steps: Anmeldeinformationen, Rollendienste, Dienstkonto für NDES (highlighted), Registrierungsstelleninfor..., Kryptografie für NDES, Bestätigung, Status, and Ergebnisse. The main content area asks to provide service account information. The 'Dienstkonto angeben (empfohlen)' radio button is selected. Below it, the text states: 'Das Konto muss der Domäne angehören und der lokalen Gruppe "IISUSRS" hinzugefügt werden.' A text box contains 'NTMNET\ndesservice' and an 'Auswählen...' button is to its right. The 'Integrierte Anwendungspoolidentität verwenden' radio button is unselected. At the bottom, there are buttons for '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.</p> |
| <p>97</p> | <p>Der Registrierungsstellenname „<CA Maschinenname>-MSCEP-RA“ wird ohne Änderung übernommen.</p> |  <p>The screenshot shows the 'AD CS-Konfiguration' window with the 'Registrierungsstelleninformationen' step selected. The left sidebar lists steps: Anmeldeinformationen, Rollendienste, Dienstkonto für NDES, Registrierungsstelleninfor... (highlighted), Kryptografie für NDES, Bestätigung, Status, and Ergebnisse. The main content area asks for information to register for a certificate. It states: 'Eine Registrierungsstelle ist erforderlich, um die Zertifikatanforderungen des Registrierungsdiensts für Netzwerkgeräte (NDES) zu verwalten.' Under 'Erforderliche Informationen', the 'Registrierungsstellenname:' text box contains 'CA-SUB03-X1-MSCEP-RA'. The 'Land/Region:' dropdown menu is set to 'DE (Deutschland)'. Under 'Optionale Informationen', there are empty text boxes for 'E-Mail:', 'Firma:', 'Abteilung:', 'Ort:', and 'Bundesland/Kanton:'. At the bottom, there are buttons for '< Zurück', 'Weiter >', 'Konfigurieren', and 'Abbrechen'.</p> |

| | | |
|----|--|--|
| 98 | Als CSP wird der Luna CSP mit einer 2048 Bit Schlüssellänge definiert und die Konfiguration abgeschlossen. |  |
|----|--|--|

Mit dem Ausführen des Befehls „iisreset“ in der Eingabeaufforderung wird der IIS neu gestartet und somit auch der NDES. Damit ist die Konfiguration des NDES seitens der Zertifizierungsstelle und die Screenshot gestützte Implementierungsdokumentation abgeschlossen.

Die Konfiguration für einen Dienst, der die NDES Schnittstelle zur CA nutzt, ist mit MobileIron in Kapitel 4.5.3 beschrieben.

Abkürzungsverzeichnis

| | |
|-----------|--|
| AD | Active Directory |
| AIA | Authority Information Access |
| ASCII | American Standard Code for Information Interchange |
| CA | Certificate Authority |
| CDP | CRL Distribution Point |
| CEP | Certificate Enrollment Protocol |
| CER | Canonical Encoding Rules |
| CIFS | Common Internet File System |
| CN | Common Name |
| CNG | Cryptography API: Next Generation |
| CSP | Cryptographic Service Provider |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| DC | Domain Component |
| DER | Distinguished Encoding Rules |
| DN (LDAP) | Distinguished Name |
| DN (DNS) | Domain Name |
| DNS | Domain Name System |
| DMZ | Demilitarized Zone |
| FTP | File Transfer Protocol |
| FQDN | Fully Qualified Domain Name |
| HA | High Availability |
| HSM | Hardware Security Module |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| IDP | Issuing Distribution Point |
| IIS | Internet Information Services |
| IP | Internet Protocol |
| KSP | Key Storage Provider |
| LDAP | Lightweight Directory Access Protocol |
| MDM | Mobile Device Management |
| MMC | Microsoft Management Console |
| NDES | Network Device Enrollment Service |
| NTL | Network Trust Link |
| NTLS | Network Trust Link Service |
| NTP | Network Time Protocol |
| OCSP | Online Certificate Status Protocol |
| OU | Organizational Unit |
| PEM | Privacy-enhanced Electronic Mail |

Abkürzungsverzeichnis

| | |
|--------|--|
| PGP | Pretty Good Privacy |
| PKCS | Public-Key Cryptography Standards |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| RNS | Relative Distinguished Names |
| RSA | Rivest, Shamir und Adleman |
| SAN | Subject Alternative Name |
| SANs | Subject Alternative Names |
| SCEP | Simple Certificate Enrollment Protocol |
| SHA | Secure Hash Algorithm |
| SMB | Server Message Block |
| SSL | Secure Sockets Layer |
| S/MIME | Secure / Multipurpose Internet Mail Extensions |
| TCP | Transmission Control Protocol |
| VA | Validation Authority |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| VTL | Virtual Token Library |

Abbildungsverzeichnis

| | |
|--|----|
| 2.1. Symmetrische Verschlüsselung | 3 |
| 2.2. Asymmetrische Verschlüsselung | 4 |
| 2.3. Anwendung des Signatur-Algorithmus | 6 |
| 2.4. Anwendung des Signatur-Hash-Algorithmus | 6 |
| 2.5. Zertifikatanforderung | 8 |
| 2.6. Zertifikatvalidierung | 8 |
| 2.7. Beispiel einer Zertifikatvorlage von Schemaversion 4 | 13 |
| 2.8. Veröffentlichung der Deltasperrliste | 17 |
| 2.9. Zertifikat mit angegebenen SANs | 20 |
| 2.10. NDES Administratorseite | 22 |
| 2.11. Zertifikatanforderung über NDES | 22 |
| 2.12. HSM mit vier Partitionen, auf die jeweils eine CA zugreift | 24 |
| 2.13. Zertifizierungsstelle mit zwei angebundenen HSMs als HA-Cluster konfiguriert | 25 |
| 2.14. Zertifikatkette | 26 |
| 2.15. Mehrstufige PKI; links eine zweistufige PKI, rechts eine dreistufige PKI | 26 |
| 2.16. Kreuzzertifizierung | 27 |
| | |
| 3.1. Teilübersicht der PKI | 36 |
| 3.2. Teilübersicht der PKI mit den HSMs | 38 |
| 3.3. Übersicht der PKI | 42 |
| | |
| 4.1. Reiter „Überwachung“ mit Markierung für das Konfigurationsskript | 49 |
| 4.2. AIA- und CDP-Erweiterungen mit Markierung für das Konfigurationsskript | 52 |
| | |
| 5.1. Inhalt der carootx1 Partition auf der HSM | 66 |
| 5.2. Anpassen der Informationen über den Antragstellernamen für das manuelle Ausstellen eines Zertifikates über die MMC | 70 |
| 5.3. Manuelles Ausstellen eines Zertifikats mit dem Programm Certreq | 71 |
| 5.4. Zertifizierungsstellen-Webregistrierung | 72 |
| 5.5. Zertifikatanforderung über den IIS einreichen | 72 |
| 5.6. Meldung über ein erfolgreich angefordertes Testzertifikat in MobileIron | 73 |
| 5.7. Meldung über ein erfolgreich angefordertes Testzertifikat (Anforderungs-ID 209) für MobileIron | 73 |
| 5.8. Certutil GUI | 74 |
| 5.9. Certutil GUI OCSP | 76 |

Listingsverzeichnis

| | |
|---|----|
| 2.1. Ausführen des OpenSSL Speed Befehls für RSA 512 Bit, 1024 Bit, 2048 Bit und 4096 Bit auf einem AMD Phenom II X6 1090T mit 3,2 Ghz | 4 |
| 2.2. Selbst-signiertes Zertifizierungsstellenzertifikat | 10 |
| 2.3. Selbst-signiertes Zertifizierungsstellenzertifikat Base64 codiert | 11 |
| 4.1. Beispiel einer CAPolicy.inf | 47 |
| 4.2. Beispiel Konfigurationsskript für eine Zertifizierungsstelle | 50 |
| 4.3. Batchdatei für das Backup der Datenbank und Konfiguration einer CA | 59 |
| 4.4. OpenSSL Konfigurationsdatei | 61 |
| 5.1. Ausgabe HALog nach Trennen der Verbindung zu einer HSM | 67 |

Tabellenverzeichnis

| | | |
|------|--|----|
| 2.1. | Beispiel zweier Hashwerte mit SHA-256 | 5 |
| 2.2. | Zertifikatdetails der X.509 Version 1 | 9 |
| 2.3. | Zusätzliche Zertifikatdetails der X.509 Version 2 | 9 |
| 2.4. | Kurzbeschreibung der Reiter der Zertifikatvorlagen von Schemaversion 4 | 14 |
| 2.5. | Sperrgründe | 16 |
| 3.1. | HSM Partitionen und deren zugriffsberechtigte Clients | 37 |
| 3.2. | Gültigkeitsdauer Zertifikate bzw. Sperrlisten | 39 |
| 4.1. | Erklärung der Sperrlisten-Verteilungspunkt (CDP) Parameter | 48 |
| 4.2. | Erklärung der Stelleninformationen (AIA) Parameter | 49 |
| 4.3. | Erklärung der Variablen im Konfigurationsskript | 51 |
| 5.1. | Funktionsüberprüfung der PKI | 65 |
| 5.2. | Anforderungsüberprüfung der PKI | 65 |
| 5.3. | Ergebnis der Funktionsüberprüfung der PKI | 76 |
| 5.4. | Ergebnis der Anforderungsüberprüfung der PKI | 77 |

Literaturverzeichnis

- [Bod13] BODDENBERG, ULRICH B.: *Windows Server 2012 R2*. Rheinwerk Computing, Bonn, 4. Auflage, 2013. ISBN: 978-3-8362-2013-2.
- [Bun14] BUNDESNETZAGENTUR FÜR ELEKTRIZITÄT, GAS, TELEKOMMUNIKATION, POST UND EISENBAHNEN: *Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)*, BAnz AT 20.02.2014 B4 Auflage, Februar 2014. [https://www.bundesanzeiger.de/ebanzwww/wexsservlet?genericsearch_param.fulltext=BAnz+AT+20.02.2014+B4&genericsearch_param.part_id=&\(page.navid%3Dto_quicksearchlist\)=Suchen](https://www.bundesanzeiger.de/ebanzwww/wexsservlet?genericsearch_param.fulltext=BAnz+AT+20.02.2014+B4&genericsearch_param.part_id=&(page.navid%3Dto_quicksearchlist)=Suchen).
- [Bunwn] *Das Trusted Platform Module (TPM)*, unknown. <https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/TrustedComputing/TrustedPlatformModuleTPM/TrustedPlatformModuleTPM/aufbaustruktur.html>.
- [CA/14] CA/BROWSER FORUM: *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.2.3*, Version 1.2.3 Auflage, Oktober 2014. <https://cabforum.org/wp-content/uploads/BRv1.2.3.pdf>.
- [cab17] *Members*, 2017. <https://cabforum.org/members/>.
- [Cavwn] *LiquidSecurity® Hardware Security Module Family*, unknown. <http://cavium.com/product-liquidsecurity.html>.
- [ct08] *Silberne Erinnerungen*. c't, 16:116–123, 2008.
- [datwn] *Daten auf Festplatten richtig löschen*, unknown. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html.
- [DC04] DE CLERCQ, JAN: *Windows Server 2003 Security Infrastructures: Core Security Features*. Elsevier Digital Press, Burlington, 2004. ISBN: 1-55558-283-4.
- [Fujwn] *LTO Ultrium Technology*, unknown. https://www.fujifilmusa.com/shared/bin/LTO_Data_Tape_Seminar_2012.pdf.
- [Gem15a] GEMALTO: *Safenet Network HSM 6.2 Product Documentation*, 007-011136-010 Rev. A Auflage, Dezember 2015. HSM Administration Guide, How long does Data last?
- [Gem15b] GEMALTO: *Safenet Network HSM 6.2 Product Documentation*, 007-011136-010 Rev. A Auflage, Dezember 2015. Linux SafeNet HSM Client Installation.

- [Gemwn] *SafeNet Luna Network HSMs*, unknown. <https://safenet.gemalto.com/data-encryption/hardware-security-modules-hsms/safenet-network-hsm/>.
- [Kom04] KOMAR, BRIAN UND DAS MICROSOFT PKI-TEAM: *Microsoft Windows Server 2003 PKI und Zertifikatsicherheit*. Microsoft Press, Unterschleißheim, 2004. ISBN: 3-86063-973-0.
- [Kom08] KOMAR, BRIAN: *Windows Server 2008 PKI and Certificate Security*. Microsoft Press, Redmond, 2008. ISBN: 978-0735625167.
- [Kom12] KOMAR, BRIAN: *CDP Variable <CRLNameSuffix>*, Februar 2012. <https://social.technet.microsoft.com/Forums/office/en-US/b3bee083-a069-40cd-b9e4-a3af6433548a/cdp-variable-crlnamesuffix?forum=winserversecurity>.
- [Med17] MEDLEY, JOSEPH: *Deprecations and Removals in Chrome 58; Remove support for commonName matching in certificates*, März 2017. <https://developers.google.com/web/updates/2017/03/chrome-58-deprecations>.
- [Mic09a] MICROSOFT DOCS: *Certificate Template Versions*, November 2009. [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc725838\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc725838(v=ws.11)).
- [Mic09b] MICROSOFT DOCS: *Configuring a Certificate Template*, November 2009. [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731511\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731511(v=ws.11)).
- [Mic09c] MICROSOFT DOCS: *How Online Responders Work*, November 2009. [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731001\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731001(v=ws.11)).
- [Mic12a] MICROSOFT DOCS: *Certificate Templates Overview*, Juli 2012. [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc730826\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc730826(v=ws.10)).
- [Mic12b] MICROSOFT DOCS: *Request Handling*, November 2012. [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732007\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732007(v=ws.11)).
- [Mic13a] MICROSOFT DOCS: *Online Responder Installation, Configuration, and Troubleshooting Guide*, Mai 2013. [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770413\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770413(v=ws.10)).
- [Mic13b] MICROSOFT DOCS: *Schedule Publication of Certificate Revocation Lists*, Februar 2013. [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732174\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732174(v=ws.11)).
- [Mic13c] MICROSOFT TECHNET: *Windows Server 2012: Certificate Template Versions and Options*, November 2013. <https://social.technet.microsoft.com/wiki/contents/articles/13303.windows-server-2012-certificate-template-versions-and-options.aspx>.

- [Mic15] MICROSOFT TECHNET: *Active Directory Certificate Services (AD CS) Clustering*, November 2015. <https://social.technet.microsoft.com/wiki/contents/articles/9256.active-directory-certificate-services-ad-cs-clustering.aspx>.
- [Mic16a] MICROSOFT DEVELOPER NETWORK: *Leitdaten für Zertifizierungsstellen*, September 2016. [https://msdn.microsoft.com/de-de/library/hh831574\(v=ws.11\).aspx](https://msdn.microsoft.com/de-de/library/hh831574(v=ws.11).aspx).
- [Mic16b] MICROSOFT DEVELOPER NETWORK: *Leitfaden für den Registrierungsdienst für Netzwerkgeräte*, September 2016. [https://msdn.microsoft.com/de-de/library/hh831498\(v=ws.11\).aspx](https://msdn.microsoft.com/de-de/library/hh831498(v=ws.11).aspx).
- [Mic16c] MICROSOFT DOCS: *TPM Key Attestation*, August 2016. [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn581921\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn581921(v=ws.11)).
- [Mic17] MICROSOFT IT PRO CENTER: *certreq_1*, Oktober 2017. https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certreq_1.
- [Mic18] MICROSOFT TECHNET: *Active Directory Certificate Services (AD CS): Network Device Enrollment Service (NDES)*, Februar 2018. <https://social.technet.microsoft.com/wiki/contents/articles/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes.aspx>.
- [Micnta] MICROSOFT DEV CENTER: *CNG Key Storage Providers*, unbekannt. [https://msdn.microsoft.com/en-us/library/windows/desktop/bb931355\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/bb931355(v=vs.85).aspx).
- [Micntb] MICROSOFT DEV CENTER: *Cryptography API: Next Generation*, unbekannt. [https://msdn.microsoft.com/en-us/library/windows/desktop/aa376210\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa376210(v=vs.85).aspx).
- [Micntc] MICROSOFT DEVELOPER NETWORK: *Distinguished Names*, unbekannt. [https://msdn.microsoft.com/en-us/library/aa366101\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa366101(v=vs.85).aspx).
- [San11] SANDISK PRESS RELEASES: *SANDISK MEMORY VAULT PRESERVES PHOTOS FOR UP TO 100 YEARS*, September 2011. <https://www.sandisk.de/about/media-center/press-releases/2011/2011-09-14-sandisk-memory-vault-preserves-photos-for-up-to-100-years>.
- [Verwna] *Archival Grade Gold CD-R*, unknown. <http://www.verbatim.com/subcat/optical-media/cd/archival-grade-gold-cd-r/>.
- [Verwnb] *Archival Grade Gold DVD-R*, unknown. <http://www.verbatim.com/subcat/optical-media/dvd/archival-grade-gold-dvd-r/>.
- [Verwnc] *Verbatim MDISC*, unknown. <http://www.verbatim.de/de/cat/mdisc-archival-media/>.

Literaturverzeichnis

- [Wik17] *Secure Hash Algorithm*, Dezember 2017. https://de.wikipedia.org/wiki/Secure_Hash_Algorithm.
- [Wik18] *Magnetband*, Januar 2018. <https://de.wikipedia.org/wiki/Magnetband>.