Kapitel 2 Aufbau einer Windows-CA-Infrastruktur

In diesem Kapitel lernen Sie, wie Sie die für den geplanten Einsatz benötigten Zertifizierungsstellen installieren und anschließend die erfolgreiche Installation prüfen.

Zu Beginn dieses Kapitels gehe ich kurz auf die Neuerungen in den Zertifikatdiensten seit Windows Server 2012 R2 ein. Administratoren, die bereits PKI-Erfahrung besitzen, erfahren so, was sich im Vergleich zu früheren Windows-Versionen geändert hat.

Neuerungen in Windows Server 2012 R2:

- Unterstützung von Richtlinien-Modulen für den Registrierungsdienst für Netzwerkgeräte – Dadurch kann die Sicherheit erhöht werden, wenn Benutzer oder Geräte Zertifikate über den Network Device Enrollment Service (NDES) beziehen wollen. NDES ist die Microsoft-Implementierung des Simple Certificate Enrollment Protocol (SCEP).
- Der TPM-Schlüsselnachweis kann eingesetzt werden. Mit ihm kann die CA prüfen, ob verwendete private Schlüssel in einem *Trusted Platform Module* (TPM) sicher gespeichert sind.
- Windows PowerShell-Modul f
 ür die Zertifikatdienste Es wurden neue Power-Shell-Cmdlets f
 ür die Verwaltung der Zertifizierungsstelle hinzugef
 ügt, insbesondere f
 ür die Sicherung und die Wiederherstellung.

Neuerungen in Windows Server 2016:

- Mit Windows Server 2016 können Smartcard-Zertifikate zum Schlüsselnachweis verwendet werden. In früheren Versionen musste hier ein TPM-Chip verwendet werden. Dadurch können virtuelle Smartcards mit einem Schlüsselnachweis ausgerollt werden, der auf einer physischen Smartcard basiert.
- Bei Verwendung des Registrierungsdienstes f
 ür Netzwerkger
 äte kann mit Windows Server 2016 der Schl
 üsselnachweis verwendet werden.

Neuerungen in Windows Server 2019:

▶ In Windows Server 2019 sind keine Neuerungen für die Zertifikatdienste enthalten.

2.1 Notwendige Parameter und Rahmenbedingungen für eine CA-Installation

Bevor Sie mit der eigentlichen Installation der ersten Zertifizierungsstelle beginnen können, müssen noch ein paar Rahmenbedingungen und Parameter geklärt werden, die in der folgenden Liste definiert werden:

Sicherheitsanforderungen – Bei den Sicherheitsanforderungen, die an eine Zertifizierungsstelle gestellt werden, geht es primär darum, zu definieren, welche »Art« von Zertifikaten durch die Zertifizierungsstelle ausgestellt wird. Dies können Maschinenzertifikate sein, die von Clients oder Netzwerkgeräten zur Authentifizierung verwendet werden. Andererseits können aber auch Benutzerzertifikate ausgestellt werden, mit denen zum Beispiel Zahlungsverkehr autorisiert wird.

Damit wird klar, dass an eine *Maschinenzertifikat-Zertifizierungsstelle* geringere Sicherheitsanforderungen gestellt werden als an eine Zertifizierungsstelle, mit deren Zertifikaten man Zahlungsverkehr autorisieren kann. Muss zum Beispiel eine Zahlungsanweisung mit einem Zertifikat eines berechtigten Benutzers autorisiert werden, könnte ein Angreifer ebenfalls Zahlungen autorisieren, sobald er es schafft, an den privaten Schlüssel des Zertifikats zu gelangen oder ein anderes, vergleichbares Zertifikat unberechtigterweise zu erstellen.

Eine Zertifizierungsstelle wird üblicherweise im Tier-O platziert. Das Tier-Modell (*https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material*) dient dazu, schützenswerte Systeme vor nicht berechtigtem Zugriff zu schützen. So können sich an Systemen eines bestimmten Tiers nur die Administratoren anmelden, die zum gleichen Tier gehören.

Anzahl der Ebenen – In der Praxis findet man Zertifizierungsstellen-Infrastrukturen mit 1 bis 3 Ebenen. Die häufigste Variante ist eine zweistufige CA-Infrastruktur. Die Gründe für den Einsatz mehrerer Ebenen ergeben sich aus den Sicherheitsanforderungen. Durch den Einsatz einer Offline RootCA in der obersten Ebene haben Sie die Möglichkeit, die untergeordnete Zertifizierungsstelle zu sperren und können so Clients die Information zukommen lassen, dass die Zertifizierungsstelle (und alle von ihr ausgestellten Zertifikate) kompromittiert wurden. Bei einer einstufigen Zertifizierungsstelle können Sie die Zertifizierungsstelle nicht auf eine Sperrliste setzen, da Sie für das RootCA-Zertifikat keine Sperrlisteninformationen konfigurieren und keine Sperrlisten veröffentlichen können.

Setzt man eine zweistufige Zertifizierungsstellen-Infrastruktur ein, wird in aller Regel die RootCA offline betrieben und die untergeordnete SubCA mit dem Netzwerk verbunden.

Dreistufige Infrastrukturen beinhalten zusätzlich eine Richtlinien-Zertifizierungsstelle (PolicyCA). Sie werden dann eingesetzt, wenn es mehrere untergeordnete Zertifizierungsstellen gibt, an die ähnliche Sicherheitsanforderungen gestellt werden, die aber untereinander unterschiedliche Anforderungen haben, die jeweils von der PolicyCA vorgegeben werden.

- Hardware Security Modules (HSM, teilweise auch als Hardware Storage Module bezeichnet) – sind Speichergeräte, auf denen Schlüsselmaterial abgelegt werden kann und kryptografische Operationen durchgeführt werden können (Erstellen von Schlüsseln und Signaturoperationen, wie das Signieren einer Sperrliste). Es gibt diese Geräte als »Einbauversion«, als Netzwerkversion oder als USB-Version zum Anstecken an den Server. Eine Beschreibung zu HSM finden Sie in Abschnitt 2.8.1.
- ► Administrationspersonal für die CA Eine der wichtigsten Fragen rund um die Zertifizierungsstelle ist die, wer sie administrieren soll. Abhängig vom Einsatzzweck der Zertifikate muss Ihnen bewusst sein, dass der Administrator der Zertifizierungsstelle die volle Kontrolle über die Zertifizierungsstelle und damit auch über die Zertifikate hat, die ausgestellt wurden. Dadurch könnte die Möglichkeit entstehen, dass der CA-Administrator sich über ein Zertifikat Domänenadministratorrechte oder Organisationsadministrator-Rechte beschaffen kann.

Es stellt sich nun die Frage, ob die Administratoren der Umgebung (Active Directory) die gleichen Personen sind, die auch die Zertifizierungsstelle betreuen. Ist dies der Fall, kann es sein, dass eine Rollentrennung nicht sinnvoll ist, da hierbei die Komplexität erhöht wird, jedoch der Sicherheitsgewinn überschaubar ist.

Werden jedoch Personen mit der Administration der Zertifizierungsstelle betraut, die nicht auch mit der Verwaltung des Active Directory beauftragt sind, ist die Trennung in weitere Rollen sinnvoll, um einen Missbrauch der Rechte zu erschweren.

 Rollentrennung – Eine Windows-Zertifizierungsstelle kennt die Verwaltungsrollen aus Tabelle 2.1, die an die PKI-Rollen der Common Criteria (*https://www.commoncriteriaportal.org/pps/*) angelehnt sind.

Lokale Rechte auf der Zertifizierungsstelle

Ein Konto mit lokalen Rechten auf der Zertifizierungsstelle kann die Rollentrennung wieder aufheben.

Rolle	Berechtigung	Verwendungszweck
CA-Administrator	Verwaltung der Zertifizierungsstelle	Hauptverwalter der CA mit der Berechtigung, die Rollen zu defi- nieren. Besitzt das Recht, das CA-Zertifikat zu erneuern.

Tabelle 2.1 Berechtigungsrollen in einer Windows-CA

2

[%]

Rolle	Berechtigung	Verwendungszweck
Zertifikatverwaltung	Ausstellen und Verwal- ten von Zertifikaten	Durchführen von Sperrungen und das Genehmigen von Zertifi- katanforderungen, die nicht automatisch genehmigt wurden
Sicherungs-Operator	Sichern und Wiederher- stellen von Dateien und Ordnern	Dieses Konto darf das System sichern und wiederherstellen.
Auditor	Verwaltung der Überwa- chungs- und Sicherheits- protokolle	Konfiguration, Auswertung der Überwachungsprotokolle (Ereig- nisanzeige)
Registrierende	Lesen- und Registrieren- Recht auf Zertifikat- vorlagen	Benutzer, Computer oder Dienste, die das Recht haben, Zertifikate anzufordern

Tabelle 2.1 Berechtigungsrollen in einer Windows-CA (Forts.)

- Maximale Laufzeit eines Nutzerzertifikats Die maximale Laufzeit eines Nutzerzertifikats (Benutzer, Dienst oder Computerkonto) definiert indirekt die maximale Laufzeit der Zertifizierungsstellen. Eine Zertifizierungsstelle kann keine Zertifikate ausstellen, die länger gültig sind als ihr eigenes Zertifizierungsstellenzertifikat.
- Maximale Laufzeit der Zertifizierungsstelle Beispiel: Die Zertifikate für die Clientcomputer sollen 3 Jahre lang gültig sein. (3 Jahre sind der Zyklus, in dem Clientcomputer in Firmen für gewöhnlich ausgetauscht werden.) Ist aber die Laufzeit der Zertifizierungsstelle auf 5 Jahre begrenzt, müssten Sie nun bereits nach 2 Jahren das CA-Zertifikat erneuern, um die maximale Laufzeit für die Client-Zertifikate gewährleisten zu können.

Eine Faustformel für die maximale Laufzeit einer untergeordneten Zertifizierungsstelle lautet:

(Maximale Laufzeit eines Nutzerzertifikats × 2) + Reservezeit

In unserem Beispiel wären das 3 Jahre × 2 + 1 = 7 Jahre. Für eine Stammzertifizierungsstelle verwenden Sie als Faustformel:

(2 × Laufzeit der untergeordneten Zertifizierungsstelle) + Reservezeit

In unserem Beispiel sind das $2 \times 7 + 1 = 15$ Jahre.

 Schlüssellänge und Algorithmen des CA-Zertifikats – Bei der Schlüssellänge gilt grundsätzlich: je größer, desto sicherer. Es ist jedoch Vorsicht geboten: Manche Clients (besonders Telefone oder andere Netzwerkgeräte) haben unter Umständen Probleme mit bestimmten Schlüssellängen bzw. bestimmten Algorithmen. Dabei kann es auch zu dem Problem kommen, dass Clients CA-Zertifikate nicht akzeptieren, wenn eine bestimmte Schlüssellänge überschritten wird. Die maximale Schlüssellänge bei einer Windows-Zertifizierungsstelle hängt von dem verwendeten Algorithmus ab.

Zu beachten ist aber: Es gibt Algorithmen, die mit geringerer Schlüssellänge eine deutlich höhere Sicherheit gewährleisten als veraltete Algorithmen (z. B. RSA) mit großer Schlüssellänge.

- ► Speicherort des CA-Zertifikats und der Sperrlisten Damit Clients die Gültigkeit von Zertifikaten prüfen können, muss der Client auf die Sperrliste der CA zugreifen können. Mögliche Speicherorte für Sperrlisten sind:
 - Webserver
 - LDAP (Active Directory)
 - File-Server
 - FTP

Die Speicherorte der Sperrlisten hängen davon ab, von »wo« Sie die Zertifikate verwenden wollen. Werden Zertifikate nur innerhalb des lokalen Netzwerks eingesetzt, wird vermutlich das Speichern innerhalb des Active Directory (LDAP) die einfachste Implementierung sein, da – beim Einsatz mehrerer Domänencontroller – automatisch eine Hochverfügbarkeit der Sperrliste gewährleistet wird. Sollen jedoch Clients von außerhalb des Netzwerks Sperrlisten abrufen können (oder Netzwerkkomponenten und Clients, die nicht der Domäne angehören), ist der Einsatz von HTTP zweckmäßig. Hierbei bietet es sich an, auch für die interne Verwendung den öffentlichen Namensraum zu nutzen, da durch diese Maßnahme die Einträge der Sperrlisten-Verteilungspunkte in den Zertifikaten reduziert werden können und damit die Prüfung schneller erfolgen kann. Die HTTP-Veröffentlichungspunkte müssen Sie dann über einen Netzwerklastenausgleich hochverfügbar bereitstellen.

- Aktualisierungsintervall der Sperrlisten Mithilfe der Sperrlisten kann die Gültigkeit eines Zertifikats geprüft werden. Je länger die Laufzeit (und damit die Gültigkeit) einer Sperrliste ist, desto länger dauert es, bis gewährleistet werden kann, dass alle Clients die Informationen über das Sperren eines Zertifikats erhalten. Für jede Zertifizierungsstelle der Infrastruktur kann eine eigene Sperrlistenlaufzeit konfiguriert werden. Die Laufzeit einer Sperrliste kann ohne größeren Aufwand im laufenden Betrieb geändert werden. Zu beachten ist aber, dass eventuell Clients Sperrlisten mit der alten Laufzeit heruntergeladen haben und die Änderung erst nach Ablauf der alten Gültigkeitsdauer wirksam wird.
- ► Einsatz eines Online-Responders Möchten Sie die Verzögerung beim Herunterladen und Aktualisieren von Sperrlisten reduzieren oder möchten Sie die Daten-

menge reduzieren, die Clients von den Sperrlisten-Verteilungspunkten herunterladen, dann sollten Sie über den Einsatz eines Online-Responders nachdenken. Dabei werden die Sperrinformationen für jeweils ein angefragtes Zertifikat unter Verwendung der Seriennummer des Zertifikats bei einer zentralen Stelle abgefragt, und der Online-Responder liefert dann die entsprechende Antwort, ob das Zertifikat gesperrt wurde oder nicht. Ein Online-Responder verwendet das *Online Certificate Status Protocol* (OCSP), das von Windows-Clients ab Vista unterstützt wird. Bei Clients mit Nicht-Microsoft-Betriebssystem muss geprüft werden, ob sie OCSP unterstützen.

Schlüsselarchivierung – Bei der Schlüsselarchivierung wird der private Schlüssel, der zu einem Zertifikat gehört, in die Datenbank der Zertifizierungsstelle gesichert. Üblicherweise verbleibt der private Schlüssel beim Client – oder bei der Komponente, die das Schlüsselpaar generiert – und wird nicht übertragen. Werden nun aber Zertifikate für eine (dauerhafte) Verschlüsselung von Daten verwendet, kann es notwendig sein, eine Sicherung des privaten Schlüssels vorzuhalten, sollte der »originale« verloren gehen, weil zum Beispiel das Profil des Benutzers oder die Festplatte des Computers gelöscht wurde.

Werden Zertifikate mit dem Zweck *Verschlüsselung* verwendet, sollte die Zertifizierungsstelle so konfiguriert werden, dass sie die Schlüssel archiviert. Dabei werden Schlüsselwiederherstellungsagenten eingerichtet, die in der Lage sind, im Notfall private Schlüssel wiederherzustellen.

Name der Zertifizierungsstelle – Immer wieder spannend ist die Namensfindung für Zertifizierungsstellen. Bedenken Sie, dass der Name einer Zertifizierungsstelle nachträglich nicht mehr geändert werden kann. Möchten Sie den Namen nachträglich ändern, müssen Sie die Zertifizierungsstelle deinstallieren oder eine neue Zertifizierungsstelle mit dem neuen Namen installieren.

Bei der Namensfindung sollten Sie auch betrachten, wer in Kontakt mit Zertifikaten der Zertifizierungsstelle kommt, denn der Name der Zertifizierungsstelle (der nicht der Hostname des CA-Computers sein sollte) ist damit eventuell von »außen« sichtbar.

Der Name der Zertifizierungsstelle kann nicht mehr als 64 Zeichen lang sein. Sie können Probleme bekommen, wenn Sie Sonderzeichen verwenden. Ein »_« zum Beispiel kann von einigen Routern nicht ausgewertet werden, wenn diese auf die CA zugreifen oder Zertifikate verwenden sollen, die von einer Zertifizierungsstelle stammen, die Unicode-Zeichen verwendet.

Physische CA oder virtuelle CA – Grundsätzlich ist es unerheblich, ob die Zertifizierungsstelle als physischer Computer oder als virtuelle Maschine betrieben wird. Sie sollten aber daran denken, dass eine physische Maschine eventuell einfacher vor nicht berechtigtem Zugriff geschützt werden kann als eine virtuelle Maschine, bei der zum Beispiel die Virtualisierungsadministratoren Zugriff auf die virtuelle Maschine (per Snapshot) oder auf die virtuellen Festplatten besitzen. In diesem Zusammenhang empfiehlt sich unter Windows Server 2016 der Einsatz von *geschützten virtuellen Maschinen (Shielded-VMs)*.

Der Vorteil einer virtuellen Maschine ist die Entkopplung von der Hardware, sodass eine Wiederherstellung der kompletten Maschine einfacher ist.

- Server Core oder Installation mit grafischer Oberfläche Eine Windows-Zertifizierungsstelle kann auf einem Windows Server mit grafischer Oberfläche oder auf einem Windows Server Core installiert werden. Ein Server Core bietet eine geringere Angriffsfläche, da ein Großteil der Binärdateien nicht mitinstalliert und damit nicht geladen wird. Die Verwaltung des Server Core erfolgt lokal über die Kommandozeile und die PowerShell oder remote über die gewohnten Verwaltungstools. Bei einem Server Core kann es zu Funktionseinschränkungen bei den Exit-Modulen kommen, da die notwendigen Binärdateien nicht vorhanden sind.
- Verwendungszwecke der Zertifikate Im Vorfeld sollten Sie sich überlegen, wozu die Zertifikate, die von den Zertifizierungsstellen ausgestellt werden, verwendet werden sollen.

Durch das Auflisten und Dokumentieren der verschiedenen Zertifikatsverwendungen werden zusätzliche Anforderungen an die Zertifizierungsstellen sichtbar und können definiert werden.

Beispiele für mögliche Einsatzwecke für Zertifikate sind:

- CA-Zertifikate
- Benutzerauthentifizierung
- Computerauthentifizierung
- IPSec
- Serverauthentifizierung
- Webserver
- Dateiverschlüsselung
- E-Mail-Signatur
- E-Mail-Verschlüsselung

Zu den verschiedenen Einsatzszenarien gehören entsprechende Schlüsselverwendungen:

- digitale Signatur
- Schlüsselverschlüsselung
- Datenverschlüsselung
- Zertifikatsignatur
- Zertifikatregistrierungsrichtlinien-Webdienst (*Certificate Enrollment Policy*, CEP) und Zertifikatregistrierungs-Webdienst (*Certificate Enrollment Web Ser*vices, CES)

Standardmäßig kontaktiert ein Client einer Active Directory-Umgebung, der ein Zertifikat bekommen möchte, die Zertifizierungsstelle mittels DCOM (*Distributed Component Object Model*), das einen RPC-Aufruf (*Remote Procedure Call*) an die Zertifizierungsstelle sendet.

Eine RPC-Verbindung besteht aus mehreren Kommunikationsverbindungen. Die erste Verbindung wird zum Zielport 135 (RPC-Endpoint-Mapper) aufgebaut, über den der Server dem Client einen dynamischen Highport zuweist (ab Windows Server 2008 ist der Port-Bereich 49152 bis 65535). Die folgende Kommunikation erfolgt dann über diesen sogenannten Highport.

Möchten Sie nun die Kommunikation zu einem Zielsystem schützen, das RPC verwendet, können Sie entweder die Anzahl der dynamischen Highports einschränken (was jedoch die Anzahl der gleichzeitigen Verbindungen beschränkt), oder Sie müssen den dynamischen Port-Bereich in der Firewall freigeben.

Damit nun Clients aus unsicheren Netzwerken Zugriff auf eine Zertifikatregistrierungsstelle bekommen können, wurden mit Windows Server 2008 R2 zwei neue Rollendienste für die Zertifizierungsstelle bereitgestellt. Diese können auch dann eingesetzt werden, wenn Netzwerkregeln existieren, die eine Kommunikation über Highports zwischen bestimmten Netzwerksegmenten untersagen.

Ein Client baut zu den beiden Diensten eine Verbindung mittels HTTPS auf, und die beiden Server verwenden dann die entsprechenden Protokolle (RPC bzw. LDAP), um auf die Zielsysteme zuzugreifen. Dadurch kann die Kommunikation zur Zertifizierungsstelle eingeschränkt werden, wodurch die Angriffsfläche in Richtung Zertifizierungsstelle reduziert wird. Der Zertifikatregistrierungsrichtlinien-Webdienst stellt eine Verbindung zu einem Domänencontroller per LDAP auf, und der Zertifikatregistrierungs-Webdienst verbindet sich per RPC mit der Zertifizierungsstelle. Sie sollten prüfen, ob Sie diese Funktion benötigen und einsetzen wollen.

- Zertifikatrichtlinie (Certificate Policy) Eine Zertifikatrichtlinie ist ein Dokument, das regelt, wie ein Client ein Zertifikat bekommt. Dabei wird definiert, wie sich der Client authentifizieren muss und ob weitere Schutzmechanismen etabliert werden, um z. B. die Identität des Antragstellers zu überprüfen (Firmenausweis). Dabei werden in der Zertifikatrichtlinie üblicherweise für verschiedene Zertifikatverwendungen auch verschieden starke Authentifizierungen gefordert. Die Richtlinie regelt dabei auch, wo die privaten Schlüssel der Zertifikate gespeichert werden dürfen und welche Gründe zu einer Sperrung des Zertifikats führen. Häufig werden in Zertifikatrichtlinien verschiedene Klassen definiert, die dann beschreiben, welche »Hürden« ein Client nehmen muss, um ein entsprechendes Zertifikat zu erhalten.
- Zertifikatverwendungsrichtlinie (Certificate Practice Statement) Ein Certificate Practice Statement (CPS) definiert, wie die Zertifizierungsstelle betrieben und

geschützt wird. Ein CPS wird dabei häufig anhand von RFC 3647 erstellt und besteht aus einem Standardformat, das folgende Abschnitte beinhalten kann:

- Einführung: Sie enthält eine kurze Information über das Ziel der Zertifizierungsstelle und ihren Einsatz – also darüber, wer als Client Zertifikate von der Zertifizierungsstelle bezieht.
- **Verantwortlichkeiten:** Wer ist Ansprechpartner für die Zertifizierungsstelle und wer ist verantwortlich?
- Identifizierung und Authentifizierung: Hier wird definiert, wie Clients identifiziert werden und ob weitere Authentifizierungen zum Anfordern eines Zertifikats notwendig sind.
- Zertifikate, Sperrlisten und OCSP-Profile: Hier wird beschrieben, welche Zertifikat-Typen ausgestellt werden und welche Gründe für eine Sperrung infrage kommen. Zusätzlich werden die Informationen über die Sperrprüfung (Sperrlisten/OCSP) hinterlegt.



Abbildung 2.1 Option mit Informationen zur Ausstellererklärung (CPS)

Eine Zertifikatverwendungsrichtlinie wird üblicherweise veröffentlicht und für Clients erreichbar hinterlegt. Ein Link zu dem Dokument wird im Zertifikat hinterlegt, sodass ein Client, der Kontakt zu einem Zertifikat hat, direkt diese Informationen (manuell) abrufen kann.

In Abbildung 2.1 sehen Sie das Zertifikat des Webservers des Rheinwerk-Verlages. Bei diesem Zertifikat wurde durch die ausstellende Zertifizierungsstelle ein Link hinterlegt (siehe Abbildung 2.2), unter dem das CPS oder auch weitere Dokumente der Zertifizierungsstelle abgerufen werden können.

Verzichtserklärung		×
https://www.thawte.com/repository	,	
	Schließen	Weitere Informationen

Abbildung 2.2 Link zum CPS der Zertifizierungsstelle

2.1.1 Festlegen der Zertifikate, die ausgestellt werden

Um den notwendigen Funktionsumfang der Zertifizierungsstelle(n) zu definieren, kann es hilfreich sein, zuerst eine Übersicht zu erstellen, die aufschlüsselt, welche Zertifikate ausgestellt werden sollen und welche Anforderungen an die einzelnen Zertifikate bestehen.

Tabelle 2.2 und Tabelle 2.3 zeigen eine mögliche Übersicht der Informationen, die Sie sammeln können, um die notwendigen Entscheidungen treffen zu können. Die Tabelle wurde zweigeteilt. Tabelle 2.3 muss hinter Tabelle 2.2 angefügt werden (anhand der Zeilennummer)

Zeile	Computer/ Benutzer	Zielgruppe	Laufzeit	Automatisch registrieren
1	Computer	Domänencontroller	1 Jahr	Ja
2	Computer	Webserver (ichkanngarnix\ CertWebserver)	3 Jahre	Nein
3	Benutzer	Buchhaltungsbenutzer	1 Jahr	Ja
4	Benutzer	Buchhaltungsbenutzer	5 Jahre	Ja

Tabelle 2.2 Dokumentation der Anforderungen an die Zertifikatvorlagen (Teil 1)

Zeile	Computer/ Benutzer	Schlüssel- export	Schüssel- archivierung	Einschrän- kungen bekannt	Bemerkungen
1	Computer	Nein	Nein	Keine	
2	Computer	Nein	Nein	Keine	

 Tabelle 2.3 Dokumentation der Anforderungen an die Zertifikatvorlagen (Teil 2)

Zeile	Computer/ Benutzer	Schlüssel- export	Schüssel- archivierung	Einschrän- kungen bekannt	Bemerkungen
3	Benutzer	Nein	Nein	Keine	Veröffentlichung im AD, um dop- pelte Ausstellung zu verhindern
4	Benutzer	Nein	Ja	Keine	Veröffentlichung im AD

Tabelle 2.3 Dokumentation der Anforderungen an die Zertifikatvorlagen (Teil 2) (Forts.)

2.2 Installationsvoraussetzungen für eine CA

Soll eine Online-Zertifizierungsstelle installiert werden, muss sichergestellt sein, dass das Betriebssystem einen aktuellen Patch-Stand (über *Windows Update* oder besser einen *Windows Server Update Service*, WSUS) besitzt und dass ein Virenscanner installiert ist. Eine Online-CA muss auch während des Betriebs mit Updates und Virensignaturen versorgt werden.

Bei einer Offline-CA ist dies nicht unbedingt notwendig, da eine Offline-Zertifizierungsstelle nie an ein produktives Firmennetzwerk angeschlossen wird. Updates werden dort nur aufgespielt,

- wenn dies aus Betriebssicht notwendig ist, da zum Beispiel Fehler in einem Update behoben wurden oder durch ein Update benötigte Funktionen erweitert oder hinzugefügt werden, oder
- ► wenn der Lifecycle es erfordert, damit die Umgebung weiter unterstützt und im Fehlerfall mit einem Hotfix des Herstellers versorgt wird, falls es zu einem technischen Ausfall kommt, der z. B. auf einem Softwarefehler basiert.

Jede Zertifizierungsstelle sollte gehärtet werden. Dazu gibt es entsprechende Beschreibungen und Anleitungen auf der Microsoft-Website. Ich stelle im Folgenden die Tools *Security Compliance Manager* (SCM) und *Security Compliance Toolkit* vor.

2.2.1 Security Compliance Manager

Aktuell gibt es noch ein Tool, mit dem zusätzliche Informationen und Vorlagen für Konfigurationsempfehlungen von Microsoft geprüft und definiert werden: der *Security Compliance Manager* (SCM, siehe Abbildung 2.3).



Abbildung 2.3 Der Startbildschirm des Security Compliance Managers

Der Security Compliance Manager ist bei Microsoft als kostenloser Download unter *www.aka.ms/scm* verfügbar.

Microsoft hat das Tool jedoch abgekündigt und wird es vermutlich nicht weiterentwickeln. Es gibt aber aktuell darin Informationen bis zu Windows Server 2016 mit verschiedenen Rollen, die installiert werden können.

Der SCM kann auf einem Betriebssystem ab Windows 7 installiert werden. Die notwendige SQL-Express-Installation kann von dem Installationsassistenten mit übernommen werden.

Über die Menüleiste (siehe Abbildung 2.4) können Sie mithilfe des Menüpunktes FILE nach Aktualisierungen und neuen Vorlagen (z. B. für neue Betriebssysteme) suchen und diese herunterladen.

SCM ist abgekündigt

Noch einmal der Hinweis: Das Tool ist abgekündigt, und es gibt nach Windows Server 2016 keine Aktualisierungen mehr. Trotzdem kann sich das Tool zum Nachschlagen von Informationen bzw. zum Lernen als sehr nützlich erweisen!



Abbildung 2.4 Suche nach Updates

Nachdem das System Kontakt zum Microsoft-Server aufgenommen hat, wird die aktuelle Liste der Programm-Updates und Vorlagen-Updates angezeigt (siehe Abbildung 2.5) und Sie können auswählen, welche Vorlagen Sie herunterladen wollen.

ij	Dow	nload Updates	23
	1		
		Microsoft Security Compliance Manager v4.0 4.0.0.1 Th, Jul 28 2016 Application Update	
		Windows 10 version 1511 Security Baseline 1.0 Fri, February 19 2016 The security and compliance baselines package for Microsoft Windows 10 version 1511 provides setti	Ξ
		Windows 10 version 1511 Baseline Attachments 1.0 Fri, February 19 2016 This collection includes all attachments and guidance associated with the Microsoft Windows 10 version and the second se	
	7	Windows Server 2012 R2 Security Baseline 1.0 Fr, August 15 2014 The security and compliance baselines package for Microsoft Windows Server 2012 R2 provides setting	,
	V	Windows Server 2012 R2 Baseline Attachments 1.0 Fr, August 15 2014 This collection includes all attachments and guidance associated with the Microsoft Windows Server 2	
	7	Windows 8.1 Security Baseline 1.0 Fr, August 15 2014 The security and compliance baselines package for Microsoft Windows 8.1 provides setting-specific d	ł
	×	Windows 8.1 Baseline Attachments 1.0 Fr, August 15 2014 This collection includes all attachments and ouidance associated with the Microsoft Windows 8.1 pro	-
	Filt	er All Cancel Cancel	

Abbildung 2.5 Liste der verfügbaren Updates für den SCM

Da die Software für die Aktualisierungen eine Internetverbindung benötigt, ist es ratsam, die Software auf einem Desktop-Client zu installieren, der über eine Internetverbindung verfügt. Von diesem Client aus können Sie dann die Konfigurationseinstellungen exportieren und auf die Serverbetriebssysteme, die vielleicht keinen Internetzugang haben, übertragen bzw. per Gruppenrichtlinie anwenden.

Es kann sinnvoll sein, mehrfach nach Updates zu suchen. Vorhandene *Application Updates* schalten neue Funktionen frei, und damit sind eventuell neue Update-Funktionen vorhanden.

Nach dem Ende des Downloads startet ein Installationsassistent, der Sie durch die Installation des Programm-Updates bzw. durch den Import der Vorlagen führt (siehe Abbildung 2.6).

🐨 Import Baselines Wizard		×
Re	sults	
C	This wizard helps you import baselines into the Microsoft Security Compliance Manager tool.	
Select package files Baseline details Results	 Windows-10-1607-Security-Compliance-Baseline.cab Win10-1607 BitLocker Security was imported successfully. Win10-1607 Credential Guard Security was imported successfully. Win10-1607 Domain Security Compliance was imported successfully. Windows-10-1607-Security-Compliance-Baseline_Attachments.cab Win10-1607 Baseline Attachments was imported successfully. Windows-Server-2016-Security-Compliance-Baseline.cab WS2016 Domain Controller Security Compliance was imported successfully. WS2016 Member Server Security Compliance was imported successfully. Windows-Server-2016-Security-Compliance-Baseline.cab WS2016 Member Server Security Compliance was imported successfully. Windows-Server-2016-Security-Compliance-Baseline_Attachments.cab WS2016 Baseline Attachments was imported successfully. Windows-10-1511-Security-Compliance-Baseline_Cab Win10-1511 Computer Security Compliance was imported successfully. Win10-1511 Computer Security Compliance was imported successfully. Win10-1511 Domain Security Compliance was imported successfully. Win10-1511 Domain Security Compliance was imported successfully. Win10-1511 Domain Security Compliance was imported successfully. Win10-1511 Baseline Attachments was imported successfully. Win10-1511 Baseline Attachments was imported successfully. Win10-1511 Baseline Attachments was imported successfully. Windows-Server-2012-R2-Security-Compliance-Baseline_Attachments.cab Windows-Server-2012-R2-Security-Compliance-Baseline.cab Windows-Server-2012-R2	* *

Abbildung 2.6 Ergebnis der Aktualisierung

Nachdem die Updates eingespielt sind, stehen neue Einträge zur Verfügung (u. a. für Windows Server 2016). Für Windows Server 2012 gibt es für die Rolle *Zertifikatdienste* auch eine Liste der verfügbaren Systemdienste auf einem Windows Server und die Konfigurationsempfehlung für eine Zertifizierungsstelle. In der Auflistung der Dienste (siehe Abbildung 2.7) sehen Sie, wie die Standardeinstellung eines Dienstes auf dem ausgewählten Betriebssystem konfiguriert ist (Spalte DEFAULT) und wie die Microsoft-Empfehlung für die Startart des Dienstes lautet (Spalte MICROSOFT). Ist eine Vorlage manuell angepasst worden, stehen diese Werte in der Spalte CUSTO-MIZED.

Der SCM bietet zusätzliche Informationen zur Funktion des Dienstes und dazu, welche Auswirkungen es hat, wenn der Dienst deaktiviert wird.

Für Windows Server 2016 werden auch Auflistungen angeboten, die erläutern, wie die Server-Härtung mithilfe der Sicherheitsoptionen konfiguriert werden kann.

Wicrosoft Security Compliance Manager						- J ×
File View Help						Global setting search
Custom Baselines	WS2012 AD Certificate Services Ser	ver Security 1.0	203 unique	e setting(s)		Import <u>GPO Backup (folde</u> SCM (cph)
Internet Explorer 10 Internet Explorer 8 Internet Explorer 8 Microsoft Office 2007 SP2 Microsoft Office 2010 SP1 Windows 7 SP1	Name System Services 203 Setting(s) KDC Proxy Server service (KPS) Windows Driver Foundation - User-n	Default Not Defined Manual	Microsoft Manual Manual	Customized Manual Manual	Se Or Or	Export Excel (xism) GPO Backup (folde SCAP v1 0 (cab)
Viindows 8 Viindows Server 2003 SP2 Viindows Server 2008 R2 SP1 Viindows Server 2008 SP2 Viindows Server 2012 Ottachwarts / Guider	Link-Layer Topology Discovery Mapp Windows Event Collector IKE and AuthIP IPsec Keying Module: Special Administration Console Help	Manual Manual Not Defined Manual	Manual Manual Manual Manual	Manual Manual Manual Manual	OF OF OF	SCCM DCM 2007 (SCM (.cab) Baseline
WS2012 AD Certificate Services Server Security 1.0 WS2012 DHC9 Server Security 1.0 WS2012 DNS Server Security 1.0 WS2012 Domain Controller Security Compliance 1 WS2012 Domain Security Compliance 1.0 WS2012 File Server Security 1.0	Windows Modules Installer Windows Internal Database VSS Writ Remote Desktop Configuration DFS Namespace	Manual Not Defined Manual Not Defined	Manual Not Defined Manual Not Defined	Manual Not Defined Manual Not Defined	Ok Ok Ok Ok	Delete Duplicate Properties
WS2012 Hyper-V Security 1.0 WS2012 Member Server Security Compliance 1.0 WS2012 Network Policy and Access Services Secur WS2012 Print Server Security 1.0 WS2012 Remote Access Services Security 1.0 WS2012 Remote Pactor Services Security 1.0	Network Euclaton Awareness Net.Tcp Listener Adapter Network Policy Server Portable Device Enumerator Service Shell Hardware Detection	Not Defined Not Defined Manual Automatic	Not Defined Not Defined Manual Automatic	Not Defined Not Defined Manual Automatic	Ot Ot Ot	Setting Group Help About Help Topics
Wiscola remove besido pervices security 1.0 Windows Vista SP2 Windows XP SP3 Windows 10 version 1607 Windows Server 2016	AD RMS Logging Service Remote Access Quarantine Agent Network Access Protection Agent	Not Defined Not Defined Manual	Not Defined Not Defined Manual	Not Defined Not Defined Manual	Ok Ok Ok	<u>Release Notes</u> <u>Send Feedback</u> <u>Privacy Statement</u>
 Windows 10 version 1511 Windows Server 2012 R2 Windows 8.1 Internet Explorer 11 Microsoft Office 2013 	Server WMI Performance Adapter Distributed Scan Server service Windows Font Cache Service	Automatic Manual Not Defined Automatic	Automatic Manual Not Defined Automatic	Automatic Manual Not Defined Automatic	Ok Ok Ok	
 SQL Server 2012 Other Baselines 	Microsoft iSNS Server	Not Defined	Not Defined	Not Defined	° aO ⇒	

Abbildung 2.7 Anzeige der Vorlagen

In Abbildung 2.8 erkennen Sie, dass der SCM eine Liste mit über 1000 Einstellungen für Windows Server 2016 bereitstellt. Hier werden – wie bei den Diensten – die Default-Einstellungen des Betriebssystems und die Empfehlung von Microsoft angezeigt. Diese Empfehlung kann durchaus von der Default-Einstellung abweichen, da eine Einstellung aus Sicherheitssicht vielleicht anders konfiguriert sein sollte oder sich die Empfehlung mit der Zeit geändert hat. Bei der Entwicklung eines Betriebssystems ist schließlich immer ein Spagat zwischen Funktionalität (Kompatibilität) und Sicherheit notwendig.

Der Security Compliance Manager kann die Einstellungen über die Export-Optionen speichern, sodass diese auf anderen Systemen angewendet bzw. per Gruppenrichtlinie verteilt werden können.

Zusätzlich können Sie eigene Einstellungen importieren und dann mithilfe des Tools analysieren und dokumentieren.

Möchten Sie eine Gruppenrichtlinie, die mithilfe des SCM gesichert wurde, in das Active Directory importieren, bietet es sich an, dies mithilfe der PowerShell zu tun, da die grafischen Optionen in der Gruppenrichtlinienverwaltungskonsole nicht immer zuverlässig arbeiten und die Erfahrung zeigt, dass häufig die gesicherten Informationen nicht als Sicherung erkannt werden. Dieser Umstand kann durch die PowerShell kompensiert werden.

victoson security compliance Manager							
View Help					G	iloba	I setting search
WS200872 DNS Server Security Compliance 1.0 WS20085P2 DNS Server Security Compliance 1.0 WS20085P2 Domain Security Compliance 1.0 WS20085P2 Domain Security Compliance 1.0	WS2016 Member Server Se	ecurity Compliance 1.0	1011 uniqu	e setting(s)			Import GPO Backup (fold SCM (.cab)
WS2008572 Hyper-V Security Compliance 10 WS2008572 Hyper-V Security Compliance 10 WS2008572 Network Access Services Server Secu WS2008572 Print Server Security Compliance 10 WS2008572 Print Server Security Compliance 10 WS2008572 Terminal Services Security Compliance 10 Windows Server 2012 Attachments \ Guides WS2012 AD Certificate Services Server Security 1 WS2012 DHCP Server Security 10	Name Authentication Types Interactive logon: Number of Network security: LAN Manu <u>Collapse</u> Value must be equal to Se Customize setting value	Default 21 Setting(s) If previou ager auth Send NTLMv2 R nd NTLMv2 response only Send NTLMv2 response only	Microsoft Not Defined es Send NTLMv2 . Refuse LM & NT	Customized Not Defined res; Send NTLMv2 TLM. Comm	Se Op resi Cr erity: ents:	 	Export Excel (.xlsm) GPO Backup (fold SCAP v1.0 (.cab) SCCM DCM 2007 SCM (.cab) Baseline
WS2012 DNS Server Security 1.0 WS2012 Domain Controller Security Compliance WS2012 Domain Security Compliance 1.0 WS2012 File Server Security 1.0 WS2012 Hyper-V Security 1.0 WS2012 Member Server Security Compliance 1.0	Setting Details UI Path: Computer Configuration\\ Description:	Vindows Settings\Security	Settings\Local Po	olicies\Security Opti Vulnerability:	ons	(*)	Delete Duplicate Properties Setting
WS2012 Network Policy and Access Services Secu WS2012 Print Server Security 1.0 WS2012 Remote Desktop Services Security 1.0 WS2012 Web Server Security 1.0 Windows Vista SP2 Windows Version 1607 4 Windows Server 2016 Attachments \Guides WS2016 Domain Controller Security Compliance 1.0 Windows 10 Version 1511 Windows Server 2012 R2 Windows 8.1 Internet Explorer 11 Microsof Chrifice 2013 \$ SII Server 2017	LAN Manager (LM) is a far software that allows users single network. Network C. default autork. Network C. default authentication pro- not negotiated for some r or NTLMv2. LAN Manager authenticat version 2 (NTLMv2) varian authenticate all Windows operations: - Join a domain - Authenticate to down-le - Authenticate to comput Vindows Server 2003, or - Authenticate to comput	nily of early Microsoft clier to link personal computer apabilities include transpa features, and network ad omains, the Kerberos prot coci. However, if the Kert eason, Active Directory wil on includes the LM, NTLM is, and is the protocol that clients when they perform two Directory forests vel domains rs that do not run Window Xindows XP) we that are not in the dom	ht/server s together on a rent file and ministration ocol is the veros protocol is I use LM, NTLM, , and NTLM is used to the following vs 2000, ain	In Windows Vista, 2000, Windows S- by default to senc (Windows 95-bas) The default settin servers and use th responses —the ve sent over the neth sniff that traffic to The Windows 95, cannot use the Ke this reason, in a 9 authenticate by dhetwork authenti authentication pr NT by using NTIL channel to protec MTIM:0 for earlie	this se erver 2 § LM ai ed and g on si eir res veakes work, a more windc riberos findow efault ration. botocol /v2. Fc t the a section		Setting Group Help About Help Topics Release Notes Send Feedback Privacy Statement

Abbildung 2.8 Sicherheitsoptionen für Windows Server 2016

Auf einem System, auf dem die Gruppenrichtlinienverwaltungskonsole installiert ist, steht das PowerShell-Modul für Gruppenrichtlinien zur Verfügung.

Mithilfe der folgenden Befehle können Sie eine neue Gruppenrichtlinie (auch als GPO, Gruppenrichtlinienobjekt, bezeichnet) erstellen und die Einstellungen aus dem Backup importieren:

New-GPO -Name "Name der neuen GPO"

Import-GPO -Path 'Pfad zum Backup' -BackupId <ID im Backup-Ordner> -TargetName "Name der neuen GPO"

Die BackupId entspricht dem Ordnernamen (siehe Abbildung 2.9) ohne die geschweiften Klammern.

Dieser PC > Lokaler Datenträger (C:) > GPOBackup > {460d286c-3208-4063-a1b5-2b030c7467f9} >					
	Name	Änderungsdatum	Тур	Größe	
	DomainSysvol	31.08.2017 19:16	Dateiordner		
7	📄 Backup	31.08.2017 19:15	XML-Dokument	6 KB	
R	📄 bkupInfo	31.08.2017 19:15	XML-Dokument	1 KB	

Abbildung 2.9 Inhalt des Backup-Ordners

Nachdem der Import durchgeführt wurde (siehe Abbildung 2.10), können Sie das Gruppenrichtlinienobjekt wie gewohnt in der Verwaltungskonsole bearbeiten (siehe Abbildung 2.11) und bei Bedarf die Sicherheitseinstellungen anpassen.

PS C:\Users\Admin Import-GPO -Path	istrator≻ New-GPO -Name "W52012-CA" 'C:\GPOBackup\' -BackupId '460d286c-3208-4063-a1b5-2b030c7467f9' -TargetName "W52012-CA"
DisplayName DomainName Owner Id GpoStatus Description CreationTime ModificationTime UserVersion ComputerVersion WmiFilter	: WS2012-CA : training.corp.ichkanngarnix.de : TRAINING/Domänen-Admins : 7e0b899e-4c70-4d5d-8019-83c17227aaec : AllSettingsEnabled : : 31.08.2017 19:44:17 : 31.08.2017 19:44:18 : AD Version: 0, SysVol Version: 0 : AD Version: 0, SysVol Version: 0 :
DisplayName DomainName Owner Id Description CreationTime UserVersion ComputerVersion WmiFilter	: WS2012-CA : training.corp.ichkanngarnix.de : TRAINING\Domänen-Admins : 7e0b899e-4c70-4d5d-8019-83c17227aaec : UserSettingsDisabled : : 31.08.2017 19:44:17 : 31.08.2017 19:44:18 : AD Version: 1, SysVol Version: 1 : AD Version: 1, SysVol Version: 1 :

Abbildung 2.10 Import der Gruppenrichtlinie

VS2012-	CA						
Bereich [Details	Einstellungen	Delegierung	S	Status		
WS2	012-0	CA					
Daten e	ermittelt	am: 31.08.2017	19:45:06			Alle ausblenden	
Comput	terkon	figuration (Ak	tiviert)			Ausblenden	
Richt	linien					<u>Ausblenden</u>	
Win	ndows-	Einstellunger	1			<u>Ausblenden</u>	
Si	icherh	eitseinstellun	gen			Ausblenden	1
	Syste	mdienste				Ausblenden	1
	Ae	LookupSvc (S	Startmodus:	Ma	anuell)	Ausblenden	
	B	erechtigunge eine Berechtigu	:n ngen angegeb	en	1		
	C K	berwachung eine Überwacht	ung angegeber	n			
	Ga	tewaydienst a	auf Anwendu	Jing	gsebene (Startmodus: Manuell)	Ausblenden	
	E K	erechtigunge eine Berechtigu	:n ngen angegeb	en	1		
	Ŭ K	berwachung eine Überwacht	ung angegeber	n			
	All	UserInstallAg	ent (Startmo	du	us: Manuell)	Ausblenden	
	B	erechtigunge eine Berechtigu	n ngen angegeb	en	1		

Abbildung 2.11 Anzeige der Einstellungen der importierten Gruppenrichtlinie

2.2.2 Security Compliance Toolkit

Als Nachfolger des Security Compliance Managers ist das Security Compliance Toolkit unter https://www.microsoft.com/en-us/download/details.aspx?id=55319 verfügbar.

Version:	Date Published
1.0	9/24/2019
File Name:	File Size:
Windows 10 Version 1903 and Windows Server Version 1903 Security Bas	1.3 MB
eline.zip	797 KB
LGPO.zip	538 KB
Office365-ProPlus-Sept2019-FINAL.zip	1.6 MB
PolicyAnalyzer.zip	904 KB
Windows 10 Version 1507 Security Baseline.zip	1.5 MB
Windows 10 Version 1607 and Windows Server 2016 Security Baseline.zip	1.0 MB
Windows 10 Version 1709 Security Baseline.zip	1.1 MB
Windows 10 Version 1803 Security Baseline.zip	1.3 MB
Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip	699 KB
Windows Server 2012 R2 Security Baseline.zip	

Abbildung 2.12 Inhalte des Security Compliance Toolkits

Das Toolkit besteht aus folgenden Komponenten (siehe Abbildung 2.12):

- ► Local GPO Tool (LGPO)
- ► Policy Analyzer
- ► Vorlagen

Mithilfe des *Local GPO Tools* können Sie lokale Richtlinien verwalten. Der *Policy Analyzer* (siehe Abbildung 2.13) liefert Informationen rund um die Konfigurationsempfehlungen von Microsoft – ähnlich wie der Security Compliance Manager.

Jdt Policy Anmelden/Abmelden Abmelden überwachen Success Success Success and Fail	Judit Policy Anmelden/Abmelden Abmelden überwachen Success	Policy Type	Policy Group or Registry Key	Policy Setting	MSFT-Win10-TH1-	MSFT-Win10-TH2-	MSFT-Win1
udit Policy Anmelden/Abmelden Anmelden überwachen Success and Fail	udit Policy Anmelden/Abmelden Anmelden überwachen Success and Fail Success and Fail Success and Valle Policy Anmelden/Abmelden Kortosperung überwachen Success Success Success Success udit Policy Berechtigungen Sersible Verwendung von Rechte Success and Fail Success and fai	udit Policy	Anmelden/Abmelden	Abmelden überwachen	Success	Success	Success
udit Policy Anmelden/Abmelden Kontosperrung überwachen Success Success Success and didt Policy Armelden/Abmelden Spezielle Armeldung überwachen Success and Fall	udit Policy Anmelden/Abmelden Kontosperung überwachen Success Success Success Success und Policy Anmelden/Abmelden Spezielle Anmeldung überwachen Success Success Success Success und Policy Berechtigungen Sensible Verwendung von Rechte Success and Fail Success and Fail Success Success und Policy Detailerte Überwachung Prozesserstellung überwachen Success Success Success und Policy DS-Zugriff Verzeichnisdienständerungen über Success Success Success and Policy Success and Policy US-Zugriff Verzeichnisdienstanderungen über Success and Fail Success and Bail Success and Policy Success and Policy US-Zugriff Verzeichnisdienstanderungen über Success and Fail Success and Bail Success and Policy Kontenverwaltung Andere Kontoverwaltung überwa Success and Fail Success and Holicy Kontenverwaltung Computerkontoverwaltung überwa Success and Fail Success and Fail Success and fail Success and the Policy Kontenverwaltung Sicherheitsgruppenverwaltung überwa Success and Fail Suc	udit Policy	Anmelden/Abmelden	Anmelden überwachen	Success and Fail	Success and Fail	Success and
dit Policy Anmelden/Abmelden Spezielle Anmeldung überwachen Success Success Success did Policy Berechtigungen Sensible Verwendung von Rechte Success and Fal Success and Fal Success and Fal Success and Policy Detailed Tracking Plug and Play Events Success Success Success under Policy Detailed Tracking Prozesserstellung überwachen Success Success Success and Policy D5-Zugriff Verzeichnisdienständerungen über Success and Fal Success and Fal Success and Fal Success and Policy D5-Zugriff Verzeichnisdienständerungen über Success Success Success and Policy D5-Zugriff Verzeichnisdienstanderungen über Success and Fal Success a	udit Policy Anmelden/Abmelden Spezielle Anmeldung überwachen Success Success Success Success and Jahr Policy Berechtigungen Sensible Verwendung von Rechte Success and Fail Success and Fail Success and Fail Success and Folicy Detaillete Überwachung Prozesserstellung überwachen Success Success Success udit Policy D5-Zugriff Verzeichnisdienständerungen über Success and Fail Success and Jahr Policy D5-Zugriff Verzeichnisdienständerungen über Success and Fail Success and Jahr Policy Kontenverwaltung Andere Kontoverwaltung überwa Success and Fail Success and Fail Success and Jahr Policy Kontenverwaltung Benutzerkontenverwaltung überwa Success and Fail Success and Fail Success and Fail Success and Jahr Policy Kontenverwaltung Sicherheitsgrupperverwaltung überwa udit Policy Kontenverwaltung Überprüfen der Anmeldeinformatio Success and Fail Success and Jahr Policy Kontenverwaltung Überprüfen der Anmeldeinformatio Success and Fail Success and Jahr Policy Kontenverwaltung Überprüfen der Anmeldeinformatio Success and Fail Success and Jahr Policy Kontenverwaltung Überprüfen der Anmeldeinformatio Success and Fail Success and Jahr Policy Kontenverwaltung Uberprüfen der Anmeldeinformatio Success and Fail Success and Jahr Policy Logon/Logoff Group Membership Success Success Success Success Success Membership Success Audit Policy Configuration Audit Policy Kontenverwalten Amelden Abmelden Uberwachen Bahr Success Audit Policy Configuration Audit Poli	udit Policy	Anmelden/Abmelden	Kontosperrung überwachen	Success	Success	Success and
udit Policy Berechtigungen Sensible Verwendung von Rechte Success and Fail	udit Policy Berechtigungen Sensible Verwendung von Rechte Success and Fail Success and Fail Success and Verzeichnisdienständerungen übervachen Success Success Success udit Policy Detaillet Uberwachung Prozessenstellung überwachen Success Success Success Success and Verzeichnisdienständerungen über Judit Policy DS-Zugriff Verzeichnisdienständerungen über Judit Policy DS-Zugriff Verzeichnisdienständerungen über Judit Policy DS-Zugriff Verzeichnisdienständerungen über Judit Policy Kontenverwaltung Andere Kontoverwaltung überwachen Success and Fail Success and Fail Success and Fail Success and Fail	udit Policy	Anmelden/Abmelden	Spezielle Anmeldung überwachen	Success	Success	Success
udit Policy Detailled Tracking Plug and Play Events Success Success Success Success Judt Policy Detailliette Überwachung Prozesserstellung überwachen Success Success Success Judt Policy DS-Zugriff Verzeichnisdienständerungen über Judt Policy DS-Zugriff Verzeichnisdienständerungen über Judt Policy Kontenverwaltung Andere Kontoverwaltung überwachen Success and Fail Success and Pail Success and Pail Success and Fail Suc	udit Policy Detaillet Tracking Plug and Play Events Success Success Success Success Under Policy Detailliete Überwachung Prozessenstellung überwachen Success Success Success Success udit Policy DS-Zugriff Verzeichnisdienständerungen über Mit Policy DS-Zugriff Verzeichnisdienstugriff Überwachen Success and Fail Success	udit Policy	Berechtigungen	Sensible Verwendung von Rechte	Success and Fail	Success and Fail	Success and
udit Policy Detaillierte Überwachung Prozesserstellung überwachen Success Success Success Success and Jahr Policy DS-Zugriff Verzeichnisdienständerungen über Success and Success and Pall Success and Fall Success and	udit Policy Detaillierte Überwachung Prozesserstellung überwachen Success Success Success udit Policy D5-Zugriff Verzeichnisdienständerungen über Success an Success an udit Policy D5-Zugriff Verzeichnisdienständerungen über Success an Success an udit Policy Kontenverwaltung Andere Kontoverwaltung überwa Success and Fail	udit Policy	Detailed Tracking	Plug and Play Events	Success	Success	Success
udit Policy DS-Zugriff Verzeichnisdienständerungen über Judit Policy DS-Zugriff Verzeichnisdienständerungen über Judit Policy Kontenverwaltung Andere Kontoverwaltungsreigniss Judit Policy Kontenverwaltung Benutzerkontenverwaltung überw Judit Policy Kontenverwaltung Computerkontoverwaltung überw Judit Policy Kontenverwaltung Sicherheitsgrupperverwaltung überwa Judit Policy Kontenverwaltung Obeprüfen der Anmeldeinformatio Judit Policy Logon/Logoff Group Membership Success and Fail Success and Fail Juccess and Fail Success and Fail.	udit Policy DS-Zuqriff Verzeichnisdienständerungen über Success an Judit Policy DS-Zuqriff Verzeichnisdienstzugriff überwachen Udit Policy Kontenverwaltung Andere Kontoverwaltungsereigniss Success and Fail Success and	udit Policy	Detaillierte Überwachung	Prozesserstellung überwachen	Success	Success	Success
udit Policy DS-Zugriff Verzeichnisdienstzugriff überwachen Success and dit Policy Kontenverwaltung Andere Kontoverwaltungsereigniss Success and Fail Success and Fail Success and dit Policy Kontenverwaltung Computerkontoverwaltung überwa dit Policy Kontenverwaltung Computerkontoverwaltung überwa success and Fail Success and Fail Success and Fail Success and Fail Success and Jourgen Success and Fail Success and Fail Success and Fail Success and Jourgen Success and Fail Success and Fail Success and Fail Success and Jourgen Success and Fail Success and Fail Success and Jourgen Jourgen Jourgen Success and Fail Success and Fail Success and Jourgen Jourgen J	Judt Policy DS-Zugriff Verzeichnisdienstzugriff überwachen Success and Jahr Policy Kontenverwaltung Andere Kontoverwaltung überwa. Judt Policy Kontenverwaltung Computerkonterverwaltung überwa. Judt Policy Kontenverwaltung Computerkontoverwaltung überwa. Judt Policy Kontenverwaltung Sicherheitsgruppenverwaltung überwa. Judt Policy Kontenverwaltung Oberpüffen der Anmeldeinformatio. Judt Policy Kontoanmeldung Oberpüffen der Anmeldeinformatio. Judt Policy Kontoanmelden Abmelden Abmelden Abmelden Ander Policy Konteger Aberlander Abmelden Abmelden Derick Aberlander Abmelden Abmel	udit Policy	DS-Zugriff	Verzeichnisdienständerungen über			Success and
udit Policy Kontenverwaltung Andere Kontoverwaltungsereigniss Success and Fail Success and Fail Success and Jail. Success and Jail. Success and Fail Succ	udit Policy Kontenverwaltung Andere Kontoverwaltungsereigniss Success and Fail S	udit Policy	DS-Zugriff	Verzeichnisdienstzugriff überwachen			Success and
udit Policy Kontenverwaltung Benutzerkontenverwaltung überw Success and Fail Success and Fail Success and Jail Policy Kontenverwaltung Computerkontoverwaltung überw Success and Fail Success	udit Policy Kontenverwaltung Benutzerkontenverwaltung überw Success and Fail Success and Fail Success and Add Policy Kontenverwaltung Computerkontoverwaltung überw Success and Fail Success a	udit Policy	Kontenverwaltung	Andere Kontoverwaltungsereigniss	Success and Fail	Success and Fail	Success and
dit Policy Kontenverwaltung Computerkontoverwaltung überwa Success and Fail Success and Fail Success and Kail Success and Fail S	dit Policy Kontenverwaltung Computerkontoverwaltung überwa Success and Fail Su	udit Policy	Kontenverwaltung	Benutzerkontenverwaltung überw	Success and Fail	Success and Fail	Success and
udit Policy Kontenverwaltung Sicherheitsgruppenverwaltung üb Success and Fail	udit Policy Kontenverwaltung Sicherheitsgruppenverwaltung üb Success and Fail Success and	udit Policy	Kontenverwaltung	Computerkontoverwaltung überwa			Success
udt Policy Kontoanmeldung Überprüfen der Anmeldeinformatio… Success and Fail… Success and Fail Success	udit Policy Kontoanmeldung Überprüfen der Anmeldeinformatio Success and Fail Suc	udit Policy	Kontenverwaltung	Sicherheitsgruppenverwaltung üb	Success and Fail	Success and Fail	Success and
udit Policy Logon/Logoff Group Membership Success Success Success III → → → → → → → → → → → → → → → → → →	udit Policy Logon/Logoff Group Membership Success Success Success III olicy Path: Advanced Audit Policy Configuration Audit Policy/Annelden/Abmelden Abmelden überwachen	udit Policy	Kontoanmeldung	Überprüfen der Anmeldeinformatio	Success and Fail	Success and Fail	Success and
III III Dicy Path: Advanced Audit Policy Configuration Audit Policy/Anmelden/Abmelden	III	udit Policy	Logon/Logoff	Group Membership	Success	Success	Success
plicy Path: Advanced Audit Policy Configuration Audit Policy/Anmelden/Abmelden	Dicy Path: Advanced Audit Policy Configuration Audit Policy Vanmelden /Abmelden Abmelden überwachen						P.
	Abmelden überwachen	olicy Path: Advanced Aud Audit Policy\Ar	it Policy Configuration imelden/Abmelden	III			
Abmelden		Mithilfe dies	er Richtlinieneinstellung können Sie E Ereignisse treten auf dem Computer	reignisse überwachen, die durch das Sc auf, auf den zugegriffen wurde. Bei eine	hließen einer Anmelde rinteraktiven Abmeld	esitzung generiert wu ung wird das	rden. Diese

Abbildung 2.13 Informationen zu den empfohlenen Einstellungen

Mithilfe des Policy Analyzers können Sie die Einstellungen nach Excel exportieren und damit einfach dokumentieren.

2.3 Installation der AD CS-Rolle

Die Installation einer Windows-Zertifizierungsstelle erfolgt in drei Schritten:

- 1. Installation der Rollen (Binärdateien)
- 2. Konfiguration der Rollen (Installations-/Konfigurationsassistent)
- 3. Konfigurationen nach der Installation (Anpassungen)

Die Binärdateien können am einfachsten über den Server-Manager installiert werden. Der Server-Manager ist ein Verwaltungstool, das automatisch gestartet wird, wenn Sie sich mit Administratorrechten an einem Server anmelden (siehe Abbildung 2.14). In ihm können Sie dann sowohl den lokalen Server verwalten als auch weitere Server (z. B. auch Server Core-Installationen) zusammenfassen und zentral verwalten bzw. überwachen.



Abbildung 2.14 Der Server-Manager unter Windows Server 2016

Für die Installation der Rolle gibt es keine Unterschiede zwischen Windows Server 2012 R2, Windows Server 2016 und Windows Server 2019. Zur Installation der Binärdateien benötigen Sie ein Konto mit lokalen Administratorrechten.

Nachdem Sie im Server-Manager die Option ROLLEN UND FEATURES HINZUFÜGEN angeklickt haben, wird der Assistent zum Hinzufügen von Rollen und Features gestartet, der Sie durch die Installation von Rollen und Features leiten wird (siehe Abbildung 2.15). Alternativ können Sie den Assistenten über den Menüpunkt VERWALTEN in der Menüleiste starten. Hier befindet sich auch die Option zum Entfernen von Rollen und Features.

🚘 Assistent zum Hinzufüg	en von Rollen und Features —		×
Vorbemerkun	gen	ZIELSER\ PKI-Root	/ER tCA
Vorbereitung Installationstyp Serverauswahl Serverrollen Features	Dieser Assistent unterstützt Sie beim Installieren von Rollen, Rollendiensten oder Featur bestimmen anhand der Anforderungen Ihrer Organisation, z. B. Freigabe von Dokument einer Website, welche Rollen, Rollendienste oder Features installiert werden sollen. Gehen Sie zum Entfernen von Rollen, Rollendiensten oder Features wie folgt vor: Starten Sie den Assistenten zum Entfernen von Rollen und Features. Stellen Sie sicher, dass die folgenden Aufgaben abgeschlossen wurden, bevor Sie den Versender	es, Sie en oder H organg	łosten
Bestatigung Ergebnisse	 Das Administratorkonto hat ein sicheres Kennwort. Die Netzwerkeinstellungen (z. B. statische IP-Adressen) sind konfiguriert. Die neuesten Sicherheitsupdates von Windows Update sind installiert. Wenn Sie überprüfen müssen, ob eine der vorhergehenden Voraussetzungen erfüllt wur den Assistenten, führen Sie die Schritte aus, und führen Sie den Assistenten dann erneut 	de, schliel t aus.	ßen Sie
	Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.		
	< Zurück Weiter > Installieren	Abbrech	ien

Abbildung 2.15 Der Installationsassistent gibt Empfehlungen.

Der Assistent weist Sie darauf hin, dass ein sicheres Administratorkennwort vergeben sein sollte und dass der Server über eine statische IP-Adresse verfügen sollte. Zusätzlich sollte das System einen aktuellen Patch-Stand aufweisen.

Nach einem Klick auf WEITER können Sie den Installationstyp auswählen. Hier stehen Rollen und Features zur Verfügung (Rollenbasierte oder featurebasierte Installation) oder die Installation von Remotedesktopdiensten, die in früheren Versionen *Terminaldienste* hießen (siehe Abbildung 2.16).

Nach der Auswahl der rollenbasierten Installation legen Sie fest, ob der lokale Server bearbeitet werden soll oder ob die Aufgaben auf einem verwalteten (Remote-)Server ausgeführt werden. Zusätzlich zu der Auswahl eines Servers können Sie hier auch eine virtuelle Festplatte auswählen und dort offline die Rollen und Features verwalten (siehe Abbildung 2.17).

Nachdem Sie die Festplatte ausgewählt haben, wird sie vom Assistenten analysiert. Er zeigt dann die bereits installierten Rollen und Features an.

Starten Sie anschließend die virtuelle Maschine, die diese virtuelle Festplatte verwendet, stehen die Rollen und Features dort zur Verfügung.

🚔 Assistent zum Hinzuf	ügen von Rollen und Features	-		Х
Installationst	yp auswählen		ZIELSERV PKI-Rooti	'ER CA
Vorbereitung Installationstyp	Wählen Sie den Installationstyp aus. Sie können Rollen und Features auf einem au Computer oder auf einem virtuellen Computer oder auch auf einer virtuellen Fest Disk, VHD) im Offlinemodus installieren.	sgeführ platte (V	ten physi ′irtual Ha	schen rd
Serverauswahl Serverrollen Features Bestätigung Ergebnisse	 Rollenbasierte oder featurebasierte Installation Konfigurieren Sie einen einzelnen Server, indem Sie Rollen, Rollendienste und F Installation von Remotedesktopdiensten Bei der Installation waren Rollendienste für die virtuelle Desktopinfrastruktur (V Infrastructure, VDI) erforderlich, um eine Desktopbereitstellung auf Basis eines oder einer Sitzung zu erstellen. 	eatures /irtual D virtuelle	hinzufüg esktop en Compu	jen. Jters
	< Zurück Weiter > Installie	ren	Abbrech	en



🖕 Assistent zum Hinzufü	igen von Rollen und Fea	atures		-		Х
Zielserver au	ıswählen				ZIELSER PKI-Roo	VER tCA
Vorbereitung Installationstyp Serverauswahl Serverrollen Features Bestätigung	Wählen Sie einen S installiert werden s © Einen Server au O Virtuelle Festpl Serverpool Filter:	Server oder eine virtuelle Fe sollen. Js dem Serverpool auswähle atte auswählen	stplatte aus, auf dem bzw.	der Rollen un	d Feature	s
	Name	IP-Adresse	Betriebssystem			
	PKI-RootCA 1 Computer gefun Auf dieser Seite we von Windows Serv Manager hinzugef noch nicht abgesch	172.16.90.100 den erden Server angezeigt, die er ausgeführt werden und r ügt wurden. Offlineserver u hlossen ist, werden nicht an	Microsoft Windows Sen unter Windows Server 201 nithilfe des Befehls "Server ad neu hinzugefügte Serve gezeigt.	ver 2016 Datad 2 oder einer n ⁻ hinzufügen" i er, für die die [eueren V im Server Datensam	érsion - imlung
		< Zurück	Weiter >	Installieren	Abbreck	hen

Abbildung 2.17 Auswahl des Servers oder einer virtuellen Festplatte

Nach der Auswahl der Online- oder Offline-Installation werden die verschiedenen Serverrollen aufgelistet. Die bereits installierten Rollen werden in der Checkbox entsprechend angezeigt (siehe Abbildung 2.18). Im Assistenten zur Installation von Rollen und Features können Sie keine Rollen und Features entfernen.



Abbildung 2.18 Auflistung der verfügbaren Rollen auf einem Windows Server

Einige Rollen (zum Beispiel Datei-/Speicherdienste) haben mehrere Rollendienste, die Sie auch einzeln auswählen können.

Die Liste der verfügbaren Rollen und Features sieht je nach Betriebssystemversion anders aus, da die verschiedenen Betriebssysteme unterschiedliche Funktionssets haben. In Bezug auf die Zertifikatdienste gibt es aber keine Unterschiede.

Die Zertifikatdienste sind unter der Option ACTIVE DIRECTORY-ZERTIFIKATDIENSTE verfügbar. Auch wenn die Zertifizierungsstelle und/oder der CA-Computer nicht Teil eines Active Directory sind, heißt die Rolle »mit Vornamen« Active Directory.

Zu der Active Directory-Zertifikatdienste-Rolle gehören Verwaltungstools. Setzen Sie im Popup-Fenster aus Abbildung 2.19, das nach der Auswahl der Rolle angezeigt wird, ein Häkchen in das Kästchen VERWALTUNGSTOOLS EINSCHLIESSEN, und klicken Sie dann auf FEATURES HINZUFÜGEN, um die Tools automatisch mitzuinstallieren.

Durch die Auswahl der Rolle werden neue Menüpunkte in den Ablauf des Installationsassistenten integriert.



Abbildung 2.19 Installation der Verwaltungstools

Werden die Zertifikatdienste (siehe Abbildung 2.20) auf einem Server installiert, können Sie den Computernamen und die Domänenmitgliedschaft anschließend nicht mehr ändern. Möchten Sie den Hostnamen oder die Domänenmitgliedschaft dennoch ändern, müssen Sie die Zertifikatdienste-Rolle vorher deinstallieren.



Abbildung 2.20 Informationen zu den Zertifikatdiensten

Vorsicht bei SConfig

Wenn Sie einen Server Core einsetzen (siehe Abschnitt 2.7) und dort das Verwaltungstool *SConfig* verwenden, kann der Server trotz installierter Zertifikatdienste umbenannt werden. Dies kann zu erheblichen Funktionsstörungen führen.

Die Zertifikatdienste bestehen aus mehreren Rollendiensten (siehe Abbildung 2.21):

 ZERTIFIZIERUNGSSTELLE – Dieser Rollendienst stellt die Zertifizierungsstellenfunktionalität zur Verfügung. Darin enthalten sind unter anderem die CA-Datenbank und die Dienste zum Bereitstellen von Sperrlisten und zum Ausstellen von Zertifikaten.

- ONLINE-RESPONDER Der Online-Responder stellt Sperrinformationen über das Online Certificate Status Protocol (OCSP) bereit. Er sollte nicht auf der Zertifizierungsstelle installiert werden, sofern die Zugriffe auf die Zertifizierungsstelle eingeschränkt werden sollen.
- REGISTRIERUNGSDIENST FÜR NETZWERKGERÄTE Dieser Dienst stellt einen Registrierungsdienst für Netzwerkgeräte bereit, die das Simple Certificate Enrollment Protocol (SCEP) verwenden. Diese Rolle sollte auf einem Server installiert werden, der nicht die Zertifikatdienste ausführt.
- ZERTIFIKATREGISTRIERUNGSRICHTLINIEN-WEBDIENST Dieser Dienst gestattet es Benutzern und Computern, Richtlinieninformationen abzurufen, auch wenn sie nicht Mitglied der Domäne sind oder sich außerhalb des Netzwerks befinden.
- ZERTIFIKATREGISTRIERUNGS-WEBDIENST Dieser Dienst gestattet es Benutzern und Computern, Zertifikate anzufordern, auch wenn sie nicht Mitglied der Domäne sind oder sich außerhalb des Netzwerks befinden.
- ZERTIFIZIERUNGSSTELLEN-WEBREGISTRIERUNG Dieser Dienst stellt eine Website bereit, auf der Benutzer Zertifikate anfordern können und das Zertifizierungsstellenzertifikat und die Sperrlisten abrufen können. Dieser Dienst ist ein »altes« Feature, das aus Kompatibilitätsgründen weiterhin verfügbar ist. Sie sollten die Webregistrierung nur installieren, wenn Sie sie unbedingt benötigen. Zum Einreichen von Zertifikatanforderungen von Nicht-Windows-Systemen gibt es vielleicht alternative – bessere – Wege, um die Zertifikate anzufordern (siehe Kapitel 4, »Eine Windows-CA-Infrastruktur verwenden«).



Abbildung 2.21 Rollendienste der Zertifikatdienste

Vorsicht

Nicht alle Zertifikate können über die Website bereitgestellt werden. Zertifikatvorlagen, deren Funktionsebene Windows Server 2008 oder höher ist, werden nicht angezeigt! Diese Vorlagen sind Vorlagen der Version 3. Wählen Sie die Rollen aus, die Sie installieren möchten, und starten Sie die Installation durch einen Klick auf INSTALLIEREN (siehe Abbildung 2.22).

🖕 Assistent zum Hinzufügen v	on Rollen und Features	-		Х
Installationsausv	vahl bestätigen		ZIELSERV PKI-Root	/ER :CA
Vorbereitung Installationstyp Serverauswahl	Klicken Sie auf "Installieren", um die folgenden Rollen, Rollendienste und Feature ausgewählten Server zu installieren. Zielserver bei Bedarf automatisch neu starten	s auf	dem	
Serveralen Serverrollen Features	Optionale Features (z. B. Verwaltungstools) können auf dieser Seite angezeigt w automatisch ausgewählt wurden. Wenn Sie diese optionalen Features nicht auto möchten, klicken Sie auf "Zurück", um die entsprechenden Kontrollkästchen zu o	erden, matiso leaktiv	da sie ch installi /ieren.	eren
AD-Zertifikatdienste Rollendienste Bestätigung Ergebnisse	Active Directory-Zertifikatdienste Zertifizierungsstelle Remoteserver-Verwaltungstools Rollenverwaltungstools Tools für Active Directory-Zertifikatdienste Tools für die Zertifizierungsstellenverwaltung			
	Konfigurationseinstellungen exportieren Alternativen Quellpfad angeben			
	< Zurück Weiter > Installiere	n	Abbrech	ien

Abbildung 2.22 Bestätigung der Installationsauswahl

Der Fortschritt der Installation wird im Assistenten angezeigt (siehe Abbildung 2.23).

Installationsstat	US ZIELSERVER PKI-RootCA	ł
Vorbereitung Installationstyp Serverauswahl Serverrollen	Installationsstatus anzeigen Featureinstallation Installation wurde gestartet auf "PKI-RootCA"	
Features AD-Zertifikatdienste Rollendienste Bestätigung Ergebnisse	Active Directory-Zertifikatdienste Zertifizierungsstelle Remoteserver-Verwaltungstools Rollenverwaltungstools Tools für Active Directory-Zertifikatdienste Tools für die Zertifizierungsstellenverwaltung	
	Sie können diesen Assistenten schließen, ohne die ausgeführten Aufgaben zu unterbrechen Zeigen Sie den Aufgabenstatus an, oder öffnen Sie diese Seite erneut, indem Sie auf der Befehlsleiste auf "Benachrichtigungen" klicken. Konfigurationseinstellungen exportieren	n.

Abbildung 2.23 Anzeige des Fortschritts der Installation

Ist die Installation abgeschlossen, wird eine Zusammenfassung wie in Abbildung 2.24 angezeigt.



Abbildung 2.24 Zusammenfassung der Installation

Sie können nun von hier direkt den Assistenten zum Konfigurieren der Active Directory-Zertifikatdienste starten. Zusätzlich können Sie die Konfigurationseinstellungen exportieren. Dabei wird eine XML-Datei erstellt, mit deren Hilfe die im Assistenten ausgewählten Optionen auf einem anderen Server oder auf mehreren anderen Servern angewendet werden (siehe Abbildung 2.25).

```
<?xml version="1.0"?>
<Objs xmlns="http://schemas.microsoft.com/powershell/2004/04" Version="1.1.0.1">
  <Obj RefId="0">
     <TN RefId="0">
         <T>System.Collections.ObjectModel.Collection `1
            [[System.Management.Automation.PSObject, System.Management.Automation,
            Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35]]</T>
         <T>System.Object</T
      </TN>
    - <LST>
        <Obj RefId="1">
            <TN RefId="1">
               <T>Microsoft.Management.Infrastructure.CimInstance#ROOT/Microsoft/Windows/Serv
              <T>Microsoft.Management.Infrastructure.CimInstance#ROOT/Microsoft/Windows/Serv
               <T>Microsoft.Management.Infrastructure.CimInstance#MSFT_ServerManagerServerCor
              <T>Microsoft.Management.Infrastructure.CimInstance</T>
               <T>System.Object</T>
            </TN>
           <ToString>ServerComponent_AD_Certificate</ToString>
          - <Props>
               <S N="PSComputerName">PKI-RootCA
            </Props>
           <MS>
              <I32 N="NumericId">16</I32>
             - <Obj RefId="2" N="__ClassMetadata">
                 <TN RefId="2">
                    <T>System.Collections.ArrayList</T>
```

Abbildung 2.25 Die vom Assistenten erstellte XML-Datei

Die exportierte XML-Datei können Sie mithilfe der PowerShell entweder auf einem einzelnen Server oder auf mehreren anderen Servern installieren:

Install-WindowsFeature -ConfigurationFilePath "D:\ Vorlage für die Bereitstellungskonfiguration.xml"

Listing 2.1 Installation auf einem Server

Install-WindowsFeature -ConfigurationFilePath "D:\ Vorlage für die Bereitstellungskonfiguration.xml" -ComputerName \$servername

Listing 2.2 Installation auf mehreren Servern

2.3.1 Installation der Rolle mithilfe der PowerShell

Die Rolle mit den entsprechenden Diensten können Sie auch ohne Antwortdatei mithilfe der PowerShell installieren. Dazu verwenden Sie das PowerShell-Cmdlet Install-WindowsFeature.

[] Active Directory-Verbunddienste	ADFS-Federation	Available
[X] Active Directory-Zertifikatdienste	AD-Certificate	Installed
[X] Zertifizierungsstelle	ADCS-Cert-Authority	Installed
[] Online-Responder	ADCS-Online-Cert	Available
[] Registrierungsdienst für Netzwerkgeräte	ADCS-Device-Enrollment	Available
[] Zertifikatregistrierungsrichtlinien-Webdienst	ADCS-Enroll-Web-Pol	Available
[] Zertifikatregistrierungs-Webdienst	ADCS-Enroll-Web-Svc	Available
[] Zertifizierungsstellen-Webregistrierung	ADCS-Web-Enrollment	Available
[X] Datei-/Speicherdienste	FileAndStorage-Services	Installed

Abbildung 2.26 Auflisten der installierten und verfügbaren Rollen und Features mit »Get-WindowsFeature«

Möchten Sie Rollen und Features mithilfe der PowerShell installieren, müssen Sie den internen Namen bzw. die Bezeichnung des Dienstes kennen. In Abbildung 2.26 können Sie den Anzeigenamen ACTIVE DIRECTORY-ZERTIFIKATDIENSTE und den Kurznamen AD-CERTIFICATE erkennen. Eine Auflistung der sechs verschiedenen Rollendienste können Sie sich mit dem PowerShell-Befehl (Get-WindowsFeature AD-Certificate).subfeatures anzeigen lassen (siehe Abbildung 2.27).



Abbildung 2.27 Anzeigen der Rollendienste mithilfe der PowerShell

Bei der Installation mithilfe der PowerShell tritt häufig der Fehler auf, den Sie in Abbildung 2.28 sehen. Er besagt, dass Sie nicht über die notwendigen Rechte verfügen, um die Änderung (Installation der Rolle) vorzunehmen, obwohl Sie zur Gruppe der lokalen Administratoren gehören, was Sie mit einem Whoami /Groups verifizieren können.

PS C:\Users\pkadmin> Install-WindowsFe	eature AD-Certificiate,ADCS-Online-Cert -IncludeAllSubFeature
Install-WindowsFeature : ArgumentNotVa	alid: Die Rolle, der Rollendienst oder der Featurename ist ungültig:
"AD-Certificiate". Der Name wurde nich	nt gefunden.
In Zeile:1 Zeichen:1	
+ Install-WindowsFeature AD-Certificia	ate,ADCS-Online-Cert -IncludeAllSu
+	
+ CategoryInfo : InvalidA + FullyQualifiedErrorId : NameDoes	<pre>\rgument: (AD-Certificiate:String) [Install-WindowsFeature], Exception NotExist,Microsoft.Windows.ServerManager.Commands.AddWindowsFeatureCommand</pre>
Success Restart Needed Exit Code	Feature Result
False No Invalidáros	n
Parse no invariangs	U.

Abbildung 2.28 Fehlermeldung, wenn die PowerShell nicht als Administrator ausgeführt wird

Ist auf dem Server die Benutzerkontensteuerung – wie empfohlen – aktiviert und verwenden Sie nicht das vordefinierte Administratorkonto, dann werden Power-Shell-Konsolen nicht automatisch mit Administratorrechten ausgeführt. Dies führt dazu, dass Sie – obwohl Sie zur Gruppe der Administratoren gehören – nur mit »nor-malen« Benutzerrechten an dem System angemeldet sind. Um das zu ändern, müssen Sie sich die erhöhten Rechte durch die Option ALS ADMINISTRATOR AUSFÜHREN zuweisen (siehe Abbildung 2.29).

Höchste Übere	instimmung
Windo	Demoschell ICE
Deskto	Als Administrator ausführen
Apps	Als anderer Benutzer ausführen
Windows	Speicherort öffnen
	Von "Start" lösen
	An Taskleiste anheften

Abbildung 2.29 Ausführen der »PowerShell ISE« als Administrator

Wenn Sie die Konfiguration der Benutzerkontensteuerung (siehe Abbildung 2.30) anpassen wollen, können Sie dies entweder in der lokalen Sicherheitsrichtlinie oder zentral über eine Gruppenrichtlinie steuern.

In der Standardkonfiguration ist die Benutzerkontensteuerung für alle Konten aktiviert – außer für das Administrator-Konto. Die Benutzerkontensteuerung sollte nicht deaktiviert werden!

Die Einstellungen in den Richtlinien finden Sie unter Computerkonfiguration • WINDOWS-EINSTELLUNGEN • SICHERHEITSEINSTELLUNGEN • LOKALE RICHTLINIEN • SICHERHEITSOPTIONEN bzw. bei den Gruppenrichtlinien der Domäne unter Computerkonfiguration • Richtlinien • WINDOWS-EINSTELLUNGEN • SICHERHEITS-EINSTELLUNGEN • LOKALE RICHTLINIEN • SICHERHEITSOPTIONEN.

Nach der Installation der Rolle wird die Zertifikatdienste-Rolle in den Server-Manager integriert. Dort stehen dann neue Verwaltungsmöglichkeiten zur Verfügung.

nuc.	
10 ° 010	Benutzerkontensteuerung: Administratorgenehmigungsmodus für das integrierte Administratorkonto
10 h 010	Benutzerkontensteuerung: Alle Administratoren im Administratorgenehmigungsmodus ausführen
10 ° 010	Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern
10 ⁰ 010	Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln
10 ° 010	Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren
10 ⁰ 010	Benutzerkontensteuerung: Erhöhte Rechte nur für UlAccess-Anwendungen, die an sicheren Orten installiert sind
10 ⁰ 010	Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind
10 ⁰ 010	Benutzerkontensteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desktop anfordern
10 ° 010	Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorgenehmigungsmodu
10 ° 010	Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer

Abbildung 2.30 Konfiguration der Benutzerkontensteuerung mithilfe von Richtlinien

Standardmäßig werden im Bereich EREIGNISSE (siehe Abbildung 2.31) Meldungen der letzten 24 Stunden angezeigt, die als KRITISCH, FEHLER oder WARNUNG gekennzeichnet werden. Diese Anzeige ist ein Filter, der die Daten aus der Ereignisanzeige liest. INFORMATIONEN und ältere Ereignisse können über die Ereignisanzeige-Konsole abgerufen werden.

Server-	Manager 🕨 AD-Zertifikatdienste 🕞 🛛 🖡	Verwalten Tools Ansicht Hilfe
Dashboard Lokaler Server Alle Server AD-Zertifikatdienste	EREIGNISSE Alle Ereignisse 2 insgesamt Filter Image: Comparison of the second secon	AUFGABEN 💌 Ereignisdaten konfigurieren Aktualisieren
■ Datei-/Speicherdienste ▷	Servername ID Schweregrad Quelle PKI-ENTCA 80 Warnung Microsoft-Windows-CertificationAuthority PKI-ENTCA 103 Warnung Microsoft-Windows-CertificationAuthority	Protokoll Datum und Uhrzeit Anwendung 02.09.2017 02:35:57 Anwendung 01.09.2017 20:41:01

Abbildung 2.31 Der Bereich »Ereignisse« zeigt Meldungen aus der Ereignisanzeige des Dienstes an.

Der Bereich DIENSTE (siehe Abbildung 2.32) listet den Status der Dienste auf, die zu der ausgewählten Rolle gehören. Hier können Sie durch einen Rechtsklick auf den jeweiligen Dienst die notwendigen Dienste starten bzw. stoppen.

DIENSTE Alle Dienste 1	1 insgesamt			AUFGABEN	-
Filter	٩	∎ • ®	•	Aktuali	isieren
Servername	Anzeigename	Dienstname	Status	Starttyp	
PKI-ENTCA	Active Directory-Zertifikatdienste	CertSvc	Wird ausgeführt	Automatisch	



Der BEST PRACTICES ANALYZER (BPA) des Server-Managers gleicht die Konfiguration der installierten Rolle mit den Konfigurationsempfehlungen von Microsoft ab (siehe Abbildung 2.33). Von Zeit zu Zeit werden die Regelwerke, die hinter dem BPA stecken, über Windows Update aktualisiert. Mit dem Menüpunkt BPA-ÜBERPRÜFUNG STAR-TEN lassen Sie den ausgewählten Dienst überprüfen. Anschließend werden die Ergebnisse angezeigt.

Filter		-		0	BPA-Überprüfung starter			
		Q	•••	•	Aktualisieren	Aktualisieren		
Filter wurde angewendet. × Alle löschen								

Abbildung 2.33 Der »Best Practices Analyzer« kann eine Rolle überprüfen.

Die *Leistungsanalyse* ist nach der Installation und Konfiguration des Servers nicht aktiv. Sie können sie durch einen Rechtsklick auf den Server • LEISTUNGSINDIKATO-REN STARTEN aktivieren. Die Leistungsanalyse sammelt dann Leistungsdaten des Servers (siehe Abbildung 2.34).

.rU-	Auslast	ung																	-	Leistu	ingswar	nungen	i konfigur
																				AKtua	lisieren		
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	00	01	02	03	04	05	06	07	08
erfü	igbarer	Arbeits	speiche	r																			
ilter					Q	(11	•																۲
		7-11			CDULIN			and L Ca	aichan		aon E	retor Au	ftraton	Lotate	or Auftr	oton							

Abbildung 2.34 Abfrage der Leistungsdaten des Servers

Die vom System gesammelten Daten werden im Ordner *C:\PerfLogs* abgelegt (sofern Laufwerk *C:* das Systemlaufwerk ist).

Im AUFGABEN-Menü gibt es die Möglichkeit, Warnschwellen für die CPU-Auslastung und den verfügbaren Arbeitsspeicher zu konfigurieren.

Wird eine konfigurierte Warnschwelle erreicht bzw. überschritten, werden die relevanten Daten (CPU und Speichernutzung des Systems) gespeichert und können über den Server-Manager abgerufen werden, sodass Sie feststellen können, welcher Dienst oder welcher Prozess beim Erreichen des Schwellenwertes Ressourcen auf dem System belegt hat. In der *Rollenansicht* im Server-Manager ist eine Option integriert, mit der Sie Rollen und Features hinzufügen oder entfernen können (siehe Abbildung 2.35). Hier startet der normale Assistent zum Hinzufügen oder der Assistent zum Entfernen von Rollen.

Filter		• •	•	Rollen und Features hinzufüge Rollen und Features entfernen
Servername	Name	Тур	Pfad	Aktualisieren
PKI-ENTCA	Active Directory-Zertifikatdienste	Rolle	Active Directory-Zertif	ikatdienste
PKI-ENTCA	Zertifizierungsstelle	Rollendienst	Active Directory-Zertif	ikatdienste\Zertifizierungsstelle

Abbildung 2.35 Hinzufügen und Entfernen von Rollen und Features

2.3.2 Installation der Rolle über das Windows Admin Center

Die Rollendienste können Sie auch mithilfe des Windows Admin Centers installieren.

Windows Admin Center	Server	-Manager \smallsetminus		1icrosoft	≻_	Q	÷	?
pki-subca02.corp.ichkanngarnix.de								
Tools	<	Rollen und	l Funktionen					
Tools suchen	ρ	+ Installierer	— Entfernen	270 Element	te 1 ausgewäh	n/t imes	Ö	
	~	Name		Status	Тур			
💀 Prozesse		Active	Directory-Verbunddienste	Verfügbar	Role			^
∰ Registrierung		 ✓ Active 	Directory-Zertifikatdienste	0 von 6 installiert	Role			- 1
		Onl	ine-Responder	Verfügbar	Role Service			
y nemotedesktop		Reg	istrierungsdienst für Netzwe	rkge Verfügbar	Role Service			
→ Rollen und Funktionen		Zerf	tifikatregistrierungs-Webdier	st Verfügbar	Role Service			
🖄 Sichern		Zerl	tifikatregistrierungsrichtlinier	-W Verfügbar	Role Service			
Speicher		√ Zerf	tifizierungsstelle	Verfügbar	Role Service			
		Zert	tifizierungsstellen-Webregist	rieru Verfügbar	Role Service			
비녜 Speicherreplikat		\ D-4-1	Cusishandisusha	4	D-I-			\sim
धुत्त Storage Migration Service		Details - Z	ertifizierungsste	lle (1 Ausgewählt)				\sim
📶 Systemdaten		Beschreibung						
Updates		Zertifizierung zu verwalten.	sstelle (Certification Au Mehrere Zertifizierung	thority, CA) wird verwende sstellen können verbunder	t, um Zertifikate a werden, um eine	iuszust Publi¢	tellen u c-Key-	und
🖓 Zertifikate	~	Infrastruktur 2	zu erstellen.					

Abbildung 2.36 Installation der Rollendienste mithilfe des Windows Admin Centers

Bei der Installation stehen alle Rollendienste zur Verfügung. Den Fortschritt der Installation können Sie über das Benachrichtigungsfeld prüfen. Nach der erfolgreichen Installation muss die Konfiguration entweder über die PowerShell oder über eine Verbindung (Remotedesktop) zum Zielsystem erfolgen.

2.3.3 Remoteserver-Verwaltungstools

Sollten Sie feststellen, dass die Verwaltungstools für die Zertifizierungsstelle auf Ihrem Server nicht verfügbar sind, oder sollten Sie die Verwaltungstools auf einem anderen Server installieren wollen, dann können Sie die Remoteserver-Verwaltungstools für die Zertifikatdienste installieren. Diese finden Sie auf einem Server-Betriebssystem unter den FEATURES (siehe Abbildung 2.37).



Abbildung 2.37 Remoteserver-Verwaltungstools für die Zertifizierungsstelle

Über die PowerShell können Sie diese Tools mit dem Befehl Add-WindowsFeature RSAT-ADCS-Mgmt installieren.

Es stehen zwei Verwaltungstools für die Zertifikatdienste zur Verfügung:

- ein Tool für die Zertifizierungsstellenverwaltung
- ► ein Online-Respondertool



Abbildung 2.38 RSAT-Tools in der PowerShell

Die Remoteserver-Verwaltungstools (*Remote Server Administration Tools* (RSAT), siehe Abbildung 2.38) stehen auch für die Client-Betriebssysteme zur Verfügung. Hierbei ist zu beachten, dass die Version des Clientbetriebssystems der Server-Betriebssystem-Version entsprechen sollte. Dadurch kann gewährleistet werden, dass alle Funktionen, die der Server bereitstellt, auf dem Client verwaltet und konfiguriert werden können. Setzen Sie einen Windows Server 2012 R2 ein, sollten Sie als Client mindestens Windows 8.1 einsetzen. Verwenden Sie Windows Server 2016 oder Windows Server 2019, sollten Sie als Client Windows 10 in der entsprechenden Version nutzen.

Um die Tools auf einem Client zu installieren, müssen Sie zuerst die Binärdateien in Form eines Installationspakets auf dem Client installieren. Die Download-Dateien der Remoteserver-Verwaltungstools stehen auf der Microsoft-Website zur Verfügung:

- Windows 8.1 https://www.microsoft.com/de-de/download/details.aspx?id=39296
- Windows 10 vor 1809 https://www.microsoft.com/de-DE/download/ details.aspx?id=45520
- Windows 10 nach 1809 Alternative Verteilmethode (siehe weiter unten im Kapitel)

Nach der Installation des Update-Paketes (siehe Abbildung 2.39) sollten Sie prüfen, ob die Verwaltungstools verfügbar sind. In früheren Versionen von Windows-Betriebssystemen mussten die einzelnen Tools separat installiert werden.



Abbildung 2.39 Installation der RSAT unter Windows 10 (vor 1809)

Aktuell werden alle Tools auf einmal mit der Installation des Update-Pakets bereitgestellt und stehen damit zur Verfügung.

Die einzelnen Konsolen werden in der Systemsteuerung über den Menüpunkt PRO-GRAMME UND FEATURES verwaltet. Möchten Sie dieses Tool (Systemsteuerung • PROGRAMME • PROGRAMME UND FEATURES, siehe Abbildung 2.40) über die Kommandozeile öffnen, können Sie mit dem Befehl appwiz.cpl den *Application Wizard* direkt starten.

0	Programme und Features	
<	→ 🗠 🛧 🗖 > Systemster	uerung > Programme > Programme und Features
•	Startseite der Systemsteuerung Installierte Updates anzeigen Windows-Features aktivieren oder deaktivieren	Programm deinstallieren oder ändern Wählen Sie ein Programm aus der Liste aus, und klicken Sie auf "E
		Organisieren 🔻

Abbildung 2.40 Sie können die Systemsteuerung verwenden, um die RSAT-Tools auf einem Client zu installieren.

Ein Klick auf WINDOWS-FEATURES AKTIVIEREN ODER DEAKTIVIEREN öffnet die Liste der verfügbaren Optionen auf dem Client-Betriebssystem. Durch das Update wurden die Role Administration Tools (auch als RSAT-Tools bezeichnet) hinzugefügt (siehe Abbildung 2.41).



Abbildung 2.41 Übersicht der RSAT-Konsolen, die installiert sind

Seit Windows 10 Version 1809 stehen die Verwaltungstools nicht mehr als separater Download zur Verfügung. Sie müssen nun auf einem Client entweder über den »Features-on-Demand«-Datenträger installiert werden oder in der Systemsteuerung über den Punkt APPS & FEATURES (siehe Abbildung 2.42).

Unter dem Menüpunkt OPTIONALE FEATURES können Sie nun RSAT-Tools (*Remote Server Administration Tools*) für die Zertifikatdienste auswählen und installieren lassen. Der Vorteil dieser Installationsoption ist die Möglichkeit, Aktualisierungen automatisch über den Microsoft-Store verteilen zu lassen und damit die Anwendung zu aktualisieren.

← Einstellungen	
命 Startseite	Apps & Features
Einstellung suchen	Quellen für das Abrufen von Apps auswählen
Apps	Wenn Sie ausschließlich Apps aus dem Microsoft Store installieren, tragen Sie zum Schutz Ihres Geräts bei.
Ē Apps & Features	Überall \checkmark
Standard-Apps	Apps & Features
印 <u></u> Offline-Karten	Optionale Features
Apps f ür Websites	Aliase für die App-Ausführung
□ Videowiedergabe	Sie können nach Laufwerken suchen, sortieren und filtern. Wenn Sie eine App deinstallieren oder verschieben möchten, wählen Sie sie
☐ Autostart	aus der Liste aus.
	Diese Liste durchsuchen

Abbildung 2.42 Option zum Installieren der »Optionalen Features«



Abbildung 2.43 Auswahl des gewünschten Features

Nach der Installation des Features sind die Verwaltungstools über das Startmenü verfügbar.

2.3.4 CAPolicy.inf

Nachdem Sie die Rolle installiert haben, müssen Sie die installierten Rollendienste konfigurieren. Zu diesem Zweck können Sie eine Art Antwortdatei verwenden. Diese Textdatei muss sich im Windows-Ordner (*%Windir%*) befinden und den Namen *CAPolicy.inf* besitzen.

Darin können Sie Einstellungen vornehmen, die der Konfigurationsassistent ausliest und konfiguriert. Die Einstellungen werden bei der Konfiguration der Rolle sowie beim Erneuern des Zertifizierungsstellenzertifikats angewendet.

Die Datei befindet sich in einem Ordner, in dem nur Mitglieder der lokalen Administratorgruppe Schreibrechte haben. Wenn Sie also einen Texteditor verwenden und die Datei direkt in dem Ordner speichern wollen, vergewissern Sie sich, dass Sie den Texteditor als Administrator öffnen und die Datei in der ANSI-Codierung speichern.

Die Datei besteht aus verschiedenen Bereichen. Sie beginnt immer mit:

[Version] Signature="\$Windows NT\$"

Der [Version]-Abschnitt muss in der Datei vorhanden sein und muss am Anfang der Datei stehen.

Die einzelnen Abschnitte der *CAPolicy.inf* sind optional und können – je nach Bedarf – in die Datei eingefügt werden.

Achtung!

Diese Datei wird nur bei der Konfiguration der Rolle angewendet oder wenn das CA-Zertifikat erneuert wird. Das Erneuern eines CA-Zertifikats erstellt quasi eine neue Instanz der Zertifizierungsstelle. Eine Installation und Konfiguration der Zertifizierungsstelle ist auch ohne Konfiguration der *CAPolicy.inf* möglich.

[PolicyStatementExtension]
Policies=Policy1, Policy2

Mithilfe der PolicyStatementExtension können Sie Richtlinien (CPS/CP) definieren und in das CA-Zertifikat übernehmen. Die definierten Policies müssen in der Datei ebenfalls definiert werden. Dazu konfigurieren Sie pro Policy einen eigenen Abschnitt mit den Daten:

[Policy1] OID=1.1.1.1.1.1 Notice="Text der Policy" [Policy2] OID=1.1.1.1.1.1.2 URL=http://crl.ichkanngarnix.de/Policy2.aspx Ein *Object Identifier* (OID) kann entweder ein selbst definierter Wert sein oder ein bei der IANA registrierter öffentlicher Wert.

[CRLDistributionPoint]
URL=http://crl.ichkanngarnix.de/RootCA.crl

Der Abschnitt CRLDistributionPoint legt die Veröffentlichungspunkte für die Sperrlisten fest.

[AuthorityInformationAccess] URL=http://crl.ichkanngarnix.de/RootCA.crt

Im Abschnitt AuthorityInformationAccess legen Sie die Veröffentlichungspunkte für das CA-Zertifikat fest, wenn Clients das Zertifikat herunterladen können müssen, um die Zertifikatkette zu bilden.

Wichtig!

Bei der Verwendung der *CAPolicy.inf* zur Konfiguration von Sperrlisten-Verteilungspunkten oder zum Zugriff auf Stelleninformationen müssen Sie auch darauf achten, dass Sie Variablen verwenden, sofern Sie eine automatische Anpassung beim Erneuern des CA-Zertifikats erreichen möchten. Hier können Sie entweder mit den Variablen (%3 %8 %9) arbeiten, oder die Texte aus der Konsole verwenden (<CaName>).

Die Einstellungen, die Sie in den Bereichen AuthorityInformationAccess und CRLDistributionPoint vornehmen, wirken sich ausschließlich auf die Ausstellung des CA-Zertifikats aus, sofern es sich um eine Stammzertifizierungsstelle handelt. Diese Einstellungen werden nicht in die Konfiguration der Zertifizierungsstelle übernommen.

[CertSrv_Server] RenewalKeyLength=4096 RenewalValidityPeriod=Years RenewalValidityPeriodUnits=5 CRLPeriod=Days CRLPeriodUnits=2 CRLDeltaPeriod=Hours CRLDeltaPeriodUnits=4 LoadDefaultTemplates=False

Im Abschnitt CertSrv_Server konfigurieren Sie Server-Einstellungen, die in der Registry abgelegt werden und nach der Installation auch manuell konfiguriert werden können.

In RenewalKeyLength legen Sie dann die Schlüssellänge beim Erneuern des CA-Zertifikats fest.

In RenewalValidityPeriod und RenewalValidityPeriodUnits habe ich in diesem Beispiel die Laufzeit des CA-Zertifikats bei einer RootCA auf 5 Jahre festgelegt.

Die CRL-Werte definieren hier, dass die Basissperrlisten 2 Tage und die Deltasperrlisten 4 Stunden gültig sind.

Im Punkt LoadDefaultTemplates legen Sie fest, ob die Unternehmenszertifizierungsstelle automatisch die Standard-Zertifikatvorlagen lädt und damit sofort Zertifikate verteilen kann. False bedeutet, dass die Templates nicht geladen werden; True bedeutet, dass die Vorlagen bereitgestellt werden und abgerufen werden können.

Capolicy - Editor X	🗚 Zertifikat 🛛 🗡
Datei Bearbeiten Format Ansicht Hilfe	
[Version]	
Signature="\$Windows NT\$"	Anzeigen: <alle> ~</alle>
[CRLDistributionPoint]	
UKL=http://pki.icnkanngarnix.de/rootca.cri	Feld Wert ^
URL=http://pki_ichkappgarpix_de/rootca_crt	Schlüsselverwendung Digitale Signatur, Zertifikatsign
[certsry server]	Schlüsselkennung des Antra ca67a3c374a24417690245ef3
RenewalKeyLength=4096	Sperilisten-Verteilungspunkte [1]Sperilisten-Verteilungspunk
RenewalValidityPeriod=Years	Zugriff auf Stelleninformatio [1]Stelleninformationszugriff:
RenewalValidityPeriodUnits=30	Basiseinschränkungen Typ des Antragstellers=Zertifi
CRLPeriod=Months	Fingerabdruck 480987d8824f63b54b24855ef
CRLPeriodUnits=6	*
Eigenschaften von Gesperte Zertifikate ? ×	[1]Sperrlisten-Verteilungspunkt
	Name des Verteilungspunktes: Vollst. Name:
Parameter fur Spentistenveroff Intlichung Zertifikatspentiste anzeigen	URL=http://pki.ichkanngarnix.de/rootca.crl
Eine Zertfikatssperfiste beschre bt Zertfikate, die Clients als ungültig betrachten sollen.	
Veröffentlichungsintervall der 👩 Monate 🗸	
Nächste Aktualisierung: 29.03.2020 08:25	Eigenschaften bearbeiten In Datei kopieren
Deltasperfisten veröffentlichen	
Veröffentlichungsintervall: 1 Tagen	OK

Abbildung 2.44 Der Zusammenhang zwischen der »CAPolicy.inf« und der Konfiguration in der Zertifizierungsstelle

In Abbildung 2.44 können Sie die Auswirkungen der *CAPolicy.inf* auf die Konfiguration in der Zertifizierungsstelle nachvollziehen. Die Einstellungen unter [CRLDistributionPoint] und [AuthorityInformationAccess] wirken sich auf die Eigenschaften des Zertifizierungsstellenzertifikats aus. Die Einstellungen CRLPeriod und CRLPeriod-Units werden für die Einstellungen der Sperrliste in der Konfiguration der Zertifizierungsstelle übernommen.

Für ein Stammzertifizierungsstellenzertifikat ist es nicht zweckmäßig, einen Sperrlisten-Verteilungspunkt »für sich selbst« einzutragen oder einen Verweis, wo das gleiche Zertifikat heruntergeladen werden kann. Daher sollten Sie die Einträge in der *CAPolicy.inf* auf der RootCA nicht konfigurieren. Eine Speicherung des Zertifikats unter %window%\system32\Certsrv\Certenroll ist fest im Betriebssystem hinterlegt und kann auch nicht geändert werden. Mithilfe von Parametern in der *CAPolicy.inf* können Sie Einfluss auf die Zertifikate nehmen, die eine Zertifizierungsstelle (auch eine untergeordnete Zertifizierungsstelle) ausstellen kann. Über die Parameter

[BasicConstraintsExtension] PathLength=1 Critical=Yes

legen Sie zum Beispiel fest, wie viele Zertifizierungsstellen-Ebenen erstellt werden können.

g Zertifikat			X				
Allgemein D	etails Zertifizierungspf	fad					
Anzeigen: <alle> ~</alle>							
Feld		Wert	^				
Parame Schlüss Schlüss Version	eter für öffentlichen elverwendung elkennung des Antra der Zertifizierungsst	05 00 Digitale Signatur, Zertifikatsign e47c23e3ad25605b128a9419 V0.0					
Zertifik	atrichtlinien	[1]Zertifikatrichtlinie:Richtlinie					
Basiseir	nschränkungen Ibdruck	Typ des Antragstellers=Zertifi bc728f21617eb785add389cb1					
			~				
Typ des An Einschränku	tragstellers=Zertifizierur Ing der Pfadlänge=1	ngsstelle					

Abbildung 2.45 Auswirkung der konfigurierten Basiseinschränkung

Im Zertifikat der Zertifizierungsstelle wird eine Basiseinschränkung für die Pfadlänge definiert (siehe Abbildung 2.45). Ist der Wert 1, kann nur noch eine Ebene verwendet werden. Wird auf dieser Zertifizierungsstelle nun ein Zertifikat ausgestellt, wird die EINSCHRÄNKUNG DER PFADLÄNGE auf 0 gesetzt, wie Sie in Abbildung 2.46 sehen. Wenn die Pfadlänge 0 ist, können mit diesem Zertifikat – das ein CA-Zertifikat sein könnte – keine weiteren (untergeordneten) Zertifikate ausgestellt werden.

Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=0

Abbildung 2.46 Auswirkung der Pfadlänge auf ausgestellte Zertifikate

Auf diese Weise können Sie zum Beispiel verhindern, dass unterhalb einer SubCA weitere SubCAs installiert werden, über die Sie vielleicht keine Kontrolle haben, oder dafür sorgen, dass diese Option in einer Zertifikatverwendungsrichtlinie ausgeschlossen ist.



Abbildung 2.47 Anforderung eines Zertifikats auf einer Zertifizierungsstelle mit einer Pfadlänge von 0

Wird nun auf einer Zertifizierungsstelle mit verbleibender Pfadlänge O ein Zertifikat angefordert, wird die Anfrage abgelehnt (siehe Abbildung 2.47) und ein Fehler in der Ereignisanzeige protokolliert. Zusätzlich wird ein Eintrag unter FEHLGESCHLAGENE ANFORDERUNGEN erstellt.

Eine weitere interessante Einschränkung ist die Verwendung der Namenseinschränkung. Damit können Sie konfigurieren, welche Namen zugelassen bzw. verweigert werden. Mit dieser Option können Sie zum Beispiel Wildcard-Zertifikate verweigern.

Wenn Sie in der *CAPolicy.inf* folgende Zeilen ergängen, wird eine Namenseinschränkung hinterlegt:

[Strings]
szOID_NAME_CONSTRAINTS = "2.5.29.30"

[Extensions] Critical = %szOID_NAME_CONSTRAINTS% %szOID_NAME_CONSTRAINTS% = "{text}" _continue_ = "SubTree=Include&" _continue_ = "DNS = .rheinwerk-verlag.de&" _continue_ = "DIRECTORYNAME = CN=rheinwerk-verlag.de&"

continue = "SubTree=Exclude&"
continue = "DNS = *.rheinwerk-verlag.de&"

Listing 2.3 Definition der Namenseinschränkung für eine Zertifizierungsstelle

Diese Einschränkung wird im CA-Zertifikat hinterlegt und kann dort unter den DETAILS abgerufen werden (siehe Abbildung 2.48).

Sie können hier mit Whitelisting und Blacklisting arbeiten. "SubTree=Include&" und "SubTree=Exclude&" können Sie verwenden, um Namen zu erlauben bzw. zu verweigern. Sie müssen dabei auf die Syntax der hinterlegten Werte achten:

DirectoryName = "DC=contoso,DC=com" – gestattet jeden Namen unterhalb der Stammdomäne.

- DNS = contoso.com gestattet *.contoso.com, zum Beispiel www.contoso.com, aber keine Subdomänen darunter (www.intranet.contoso.com).
- DNS = .contoso.com gestattet Subdomänen wie www.intranet.contoso.com.
- ► Email = @contoso.com gestattet benutzer@contoso.com.
- Email = .contoso.com gestattet benutzer@intranet.contoso.com.
- IPAddress = 192.168.0.0, 255.255.0 gestattet IP-Adressen aus dem angegebenen Subnetz. Das Format ist: {IP-Netzwerkadresse }, {Subnetzmaske}



Abbildung 2.48 Im CA-Zertifikat hinterlegte Namenseinschränkungen

Wird nun ein Zertifikat angefordert, das gemäß der Namenseinschränkung nicht gestattet ist, wird die Anforderung mit einem Fehler abgelehnt wie in Abbildung 2.49.

Active Directory-Registrierungsrichtlinie	^
✓ Rheinwerk-Webserver-V1.0 ★ STATUS: Anfrage abgelehnt Details ▼ Das Zertifikat hat einen ungültigen Namen. Der Name ist nicht in der Liste der zulässigen Namen enthalten, oder er ist explizit ausgeschlossen. Rheinwerk-SubCA.intranet.rheinwerk-verlag.de\intranet-RHEINWERK-SUBCA-CA Fehler beim Erstellen bzw. Veröffentlichen des Zertifikats Keine zugelassenen	
Namenseinschränkungen für <dns-name=rheinwerk-dc> Keine zugelassenen Namenseinschränkungen für <verzeichnisadresse:cn=rheinwerk-dc></verzeichnisadresse:cn=rheinwerk-dc></dns-name=rheinwerk-dc>	

Abbildung 2.49 Verweigern eines Zertifikatrequests aufgrund falscher Namensinformationen

Namenseinschränkungen sollten nur von erfahrenen Administratoren verwendet werden und nur für Einsatzzwecke, bei denen wenig dynamische Namen und Unterdomänen verwendet werden müssen. Alternativ können Sie – nach dem Ausstellen von den Zertifikaten – diese prüfen und bei Bedarf sperren.

2.4 Konfiguration einer einfachen CA-Infrastruktur

In diesem Abschnitt werden wir eine »einfache« CA-Infrastruktur konfigurieren, wie sie beispielweise in Test-Umgebungen ausreichen kann. Dazu habe ich die Vorgaben, die ich in Abschnitt 2.1 erörtert habe, in Tabelle 2.4 zusammengefasst:

	Konfiguration
Anzahl der Ebenen	1
Sicherheitsanforderungen	Keine
Administrative Trennung	Nicht notwendig
Maximale Laufzeit eines Nutzer- zertifikats	5 Jahre
Maximale Laufzeit der Zertifizierungs- stelle	12 Jahre
Schlüssellänge	2048 Bit
Algorithmus	SHA256/Microsoft Software KSP
Speicherort CRL/AIA	Active Directory (LDAP)
Aktualisierungsintervall der Sperrliste	7 Tage für die Basissperrliste 1 Tag für die Deltasperrliste
Online-Responder	Nein
Schlüsselarchivierung	Nein
Name der Zertifizierungsstelle	Ichkanngarnix Enterprise CA
Installation auf Hardware oder als virtuelle Maschine	Virtuell
Server Core oder grafisches UI	Grafisches User-Interface
Verwendungszwecke der Zertifikate	Arbeitsstationsauthentifizierung Webserver
Webdienste	Nein
CPS/CP	Nein
Anpassung der CAPolicy.inf	Nein

Tabelle 2.4 Parameter einer einfachen CA-Infrastruktur

Abbildung 2.50 zeigt die Umgebung.



Abbildung 2.50 Konfiguration der »einfachen« Umgebung

Die Zertifizierungsstelle soll ins Active Directory integriert werden. Dazu ist es notwendig, dass das Computerkonto in die Domäne aufgenommen wird und die Konfiguration der Zertifizierungsstelle mit einem Konto ausgeführt wird, das Organisationsadministratorrechte (*Enterprise Administrators*) besitzt.

Die Active Directory-Zertifikatdienste wurden – wie in Abschnitt 2.3 beschrieben – mit dem Rollendienst *ADCS-Cert-Authority* installiert. Es wurden sonst keine Zusatz-rollen installiert.

2.4.1 Konfiguration der Zertifizierungsstelle

Nach der Installation der Rolle können Sie entweder im Zusammenfassungsfenster oder über die Benachrichtigungsfunktion des Server-Managers den Konfigurationsassistenten für die Einrichtung der Zertifizierungsstelle starten.

Mit einem Klick auf ACTIVE DIRECTORY-ZERTIFIKATDIENSTE AUF DEM ZIELSERVER KONFIGURIEREN (siehe Abbildung 2.51) starten Sie einen Assistenten, der Sie durch die Konfiguration der Zertifizierungsstelle leitet (siehe Abbildung 2.52).



Abbildung 2.51 Hinweis im Server-Manager, dass die Konfiguration noch abgeschlossen werden muss

CAPolicy.inf

>>

Wurde eine *CAPolicy.inf* erstellt und konfiguriert, werden die dort definierten Werte bei der Konfiguration übernommen. Einige Einstellungen werden aber erst angewendet, wenn das CA-Zertifikat erneuert wird.

Das Konto für die Konfiguration muss über lokale Administratorrechte auf dem Server verfügen und – wenn eine Integration in das Active Directory erfolgen soll – über Organisationsadministratorrechte. Diese Rechte können auch an andere Konten delegiert werden, wenn die Verwaltung der Zertifizierungsstelle nicht von den Administratoren des Active Directory durchgeführt werden soll. Bedenken Sie, dass ein Organisationsadministrator auf Systemen, die kein Domänencontroller sind, nur Benutzerrechte besitzt und bei Bedarf in die lokale Gruppe der Administratoren aufgenommen werden muss.

Ē.	AD CS-Konfiguration
Anmeldeinforma	ZIELSERVER PKI-EntCA.corp.ichkanngarnix.de
Anmeldeinformationen	Geben Sie Anmeldeinformationen zur Konfiguration der
Rollendienste	Rollendienste an.
Bestatigung Status	Zum Installieren der folgenden Rollendienste müssen Sie der lokalen Administratorgruppe
Ergebnisse	angehören: • Eigenständige Zertifizierungsstelle • Zertifizierungsstellen-Webregistrierung • Online-Responder
Um die folgenden Rollendienste installieren zu können, müssen Sie der Gruppe der Unternehmensadministratoren angehören: • Unternehmenszertifizierungsstellte verwenden • Zertifikatregistrierungsrichtlinien-Webdienst • Zertifikatregistrierungs-Webdienst • Registrierungsdienst für Netzwerkgeräte	
	Weitere Informationen zu AD CS-Serverrollen
	< Zurück Weiter > Konfigurieren Abbrechen

Abbildung 2.52 Festlegen des Kontos, mit dem die Konfiguration durchgeführt wird

Eine Zertifizierungsstelle gehört meistens zum Tier O (siehe *https://docs.microsoft. com/de-de/windows-server/identity/securing-privileged-access/securing-*

Nach der Konfiguration des zu verwendenden Kontos müssen Sie die Rollendienste auswählen, die im Assistenten konfiguriert werden sollen (siehe Abbildung 2.53).



Abbildung 2.53 Auswahl der zu konfigurierenden Rollendienste

Bei der Auswahl der Dienste stehen nur die über den Server-Manager oder über die PowerShell installierten Rollendienste zur Verfügung. Daher sind in Abbildung 2.53 alle Rollendienste außer ZERTIFIZIERUNGSSTELLE ausgegraut.

Nach der Auswahl der Zertifizierungsstelle legen Sie den INSTALLATIONSTYP fest (siehe Abbildung 2.54). Hier stehen zwei verschiedene Zertifizierungsstellen-Typen zur Auswahl:

- UNTERNEHMENSZERTIFIZIERUNGSSTELLE (Enterprise CA) Eine Unternehmenszertifizierungsstelle ist in das Active Directory integriert und muss auf einem Computer installiert werden, der Mitglied einer Active Directory-Domäne ist. Eine Unternehmenszertifizierungsstelle stellt Zertifikatvorlagen bereit, und Clients (Benutzer oder Computer) können automatisch Zertifikate von dieser CA erhalten, da die Zertifizierungsstelle die Anforderungen der Clients automatisch – basierend auf vergebenen Berechtigungen – prüfen kann. Eine Unternehmenszertifizierungsstelle wird üblicherweise auf der »untersten« Ebene der Infrastruktur verwendet, damit die Vorteile der automatischen Verteilung genutzt werden können.
- EIGENSTÄNDIGE ZERTIFIZIERUNGSSTELLE (Stand-Alone CA) Eine eigenständige Zertifizierungsstelle kann auf einem Arbeitsgruppenrechner installiert werden, der nicht Teil einer Domäne ist. Auf einer eigenständigen (alleinstehenden) Zertifizierungsstelle müssen Zertifikatanforderungen manuell freigegeben werden und es können keine Berechtigungen aus dem Active Directory ausgelesen werden. Auf einer alleinstehenden Zertifizierungsstelle stehen auch keine Zertifikatvorlagen zur Verfügung, die bearbeitet werden können. Alleinstehende Zertifizierungsstellen werden üblicherweise für Stammzertifizierungsstellen und Richtlinien-Zertifizierungsstellen verwendet.

Auf jeder Ebene der Hierarchie kann entschieden werden, um welchen Typ es sich handelt.

Sie können also eine Unternehmenszertifizierungsstelle unterhalb einer eigenständigen Zertifizierungsstelle installieren. Ebenso können Sie theoretisch eine eigenständige Zertifizierungsstelle unterhalb einer Unternehmenszertifizierungsstelle installieren, wenn dies Ihren Anforderungen entspricht.

Abbildung 2.54 Auswahl des Installationstyps der Zertifizierungsstelle

Unabhängig von der Auswahl des Installationstyps wählen Sie im folgenden Schritt den Zertifizierungsstellentyp aus (siehe Abbildung 2.55). Hier legen Sie fest, ob es sich bei der CA um eine STAMMZERTIFIZIERUNGSSTELLE (*RootCA*) oder um eine UNTER-GEORDNETE ZERTIFIZIERUNGSSTELLE (*Subordinate CA, SubCA*) handelt.

Zertifizierungsste	ZIELSERVER llentyp PKI-EntCA.corp.ichkanngarnix.de
Anmeldeinformationen Rollendienste	Geben Sie den Typ der Zertifizierungsstelle an.
Installationstyp	Wenn Sie Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) installieren erstellen oder erweitern Sie eine Hierarchie der Public Key-Infrastruktur (PKI). Eine
ZS-Typ Privater Schlüssel	Stammeren, erstenen oder henden och neuen neuen neuen der robie ney innerstenen och neuen selbst Stammeren zur inzeren selbst signiertes Zertifikat aus. Eine untergeordnete Zertifizierungsstelle empfängt ein Zertifikat von der
Kryptografie	Zertifizierungsstelle, die in der PKI-Hierarchie darüber angesiedelt ist.
ZS-Name	Stammzertifizierungsstelle
Gültigkeitsdauer	Stammzertifizierungsstellen sind die ersten und möglicherweise einzigen Zertifizierungsstellen, die in einer PKI-Hierarchie konfiguriert werden.
Zertifikatdatenbank	
Bestätigung	 Untergeordnete Zertifizierungsstelle
Status	Für untergeordnete Zertifizierungsstellen ist eine eingerichtete PKI-Hierarchie erforderlich. Sie sind zur Ausstellung von Zertifikaten berechtigt, die von der Zertifizierungsstelle stammen, die
Ergebnisse	sich in der Hierarchie über den untergeordneten Zertifizierungsstellen befindet.

Abbildung 2.55 Auswahl, ob es sich um eine RootCA oder eine SubCA handelt

Abhängig von der getroffenen Auswahl wird entweder das CA-Zertifikat selbst erstellt (RootCA) oder es erfolgt eine Abfrage, an welche übergeordnete Zertifizierungsstelle die Zertifikatanforderung gesendet werden soll (SubCA).

Die Konfigurationsschritte auf der linken Seite des Assistenten ändern sich in Abhängigkeit von den ausgewählten Optionen. Die Zertifizierungsstelle wird ein Schlüsselpaar (privater/öffentlicher Schlüssel) erstellen, sofern kein Schlüssel existiert. Der Assistent bietet Optionen zum Erstellen eines neuen Schlüsselpaars und zum Verwenden existierender privater Schlüssel an (siehe Abbildung 2.56).

Privator Schlüsse	ZIELSERVER
Invator Schlusse	PKI-EntCA.corp.ichkanngarnix.de
Anmeldeinformationen Rollendienste	Geben Sie den Typ des privaten Schlüssels an.
Installationstyp ZS-Typ	Die Zertifizierungsstelle benötigt einen privaten Schlüssel, um Zertifikate für Clients zu generieren und auszustellen.
Privater Schlüssel	Neuen privaten Schlüssel erstellen
Kryptografie	Verwenden Sie diese Option, wenn Sie keinen privaten Schlüssel besitzen oder einen neuen privaten Schlüssel erstellen möchten.
ZS-Name	
Gültigkeitsdauer	O Vorhandenen privaten Schlüssel verwenden
Zertifikatdatenbank	Verwenden Sie diese Option, um bei der Neuinstallation einer Zertifizierungsstelle Kontinuität mit zuvor ausgestellten Zertifikaten zu gewährleisten.
Bestätigung	 Zertifikat auswählen und zugehörigen privaten Schlüssel verwenden
Status	Wählen Sie diese Option aus, wenn auf diesem Computer ein Zertifikat vorhanden ist oder
Ergebnisse	wenn Sie ein Zertifikat importieren und den zugehörigen privaten Schlüssel verwenden möchten.
	O Vorhandenen privaten Schlüssel auf diesem Computer auswählen
	Wählen Sie diese Option aus, wenn Sie private Schlüssel von einer vorherigen Installation beibehalten haben oder einen privaten Schlüssel aus einer alternativen Quelle verwenden möchten.
	Weitere Informationen zum privaten Schlüssel

Abbildung 2.56 Optionen zur Schlüsselgenerierung

Wenn Sie sich für die Verwendung eines vorhandenen Schlüssels entscheiden, gibt es die Option, ein bereits auf dem Computer installiertes Zertifikat zu verwenden bzw. ein Zertifikat zu importieren.

V	7		ZIELSERVER
kryptografie fur	Zertinzierungsstelle	PKI-EntCA.corp.id	chkanngarnix.de
Anmeldeinformationen Rollendienste	Geben Sie die Kryptografieoptionen an.		
Installationstyp	Kryptografieanbieter auswählen:	Schlüsselläng	ge:
ZS-Typ	RSA#Microsoft Software Key Storage Provider	▼ 2048	•
Privater Schlüssel Kryptografie	Wählen Sie den Hashalgorithmus aus, mit dem Zertifikate die werden sollen:	ser Zertifizierungsstel	lle signiert
ZS-Name	SHA256	^	
Gültigkeitsdauer	SHA384	=	
Zertifikatdatenbank	SHA512		
Bestätigung	SHAT	V	
Status	Administratorinteraktion bei jedem Zertifizierungsstellenz	ugriff auf den private	n Schlüssel
	zulassen		

Abbildung 2.57 Optionen zur Auswahl des Kryptografieanbieters, der Schlüssellänge und des Signaturalgorithmus

Bei der Auswahl der Kryptografieoptionen (siehe Abbildung 2.57) stehen zahlreiche Kryptografieanbieter zur Verfügung. Tabelle 2.5 listet die Anbieter sowie die Schlüssellängen und Algorithmen auf.

Kryptografieanbieter	Schlüssellänge	Hashalgorithmus
Microsoft Base Smart Card Crypto Provider	1024 2048 4096	SHA1 MD2 MD4 MD5
Microsoft Enhanced Cryptographic Provider v1.0	512 1024 2048 4096	SHA1 MD2 MD4 MD5
ECDSA_P256#Microsoft Smart Card Key Storage Provider	256	SHA1 SHA256 SHA384 SHA512
ECDSA_P521#Microsoft Smart Card Key Storage Provider	521	SHA1 SHA256 SHA384 SHA512
RSA#Microsoft Software Key Storage Provider	512 1024 2048 4096	SHA1 SHA256 SHA384 SHA512 MD2 MD4 MD5
Microsoft Base Cryptographic Provider v1.0	512 1024 2048 4096	SHA1 MD2 MD4 MD5
ECDA_P521#Microsoft Software Key Storage Provider	521	SHA1 SHA256 SHA384 SHA512

Tabelle 2.5 Kryptografieanbieter, Schlüssellängen und Algorithmen

Kryptografieanbieter	Schlüssellänge	Hashalgorithmus
ECDA_P256#Microsoft Software Key Storage Provider	256	SHA1 SHA256 SHA384 SHA512
Microsoft Strong Cryptographic Provider	512 1024 2048 4096	SHA1 MD2 MD4 MD5
ECDSA_P384#Microsoft Software Key Storage Provider	384	SHA1 MD2 MD4 MD5
Microsoft Base DSS Cryptographic Provider	512 1024	SHA1
RSA#Microsoft Smart Card Key Storage Provider	1024 2048 4096	SHA1 SHA256 SHA384 SHA512 MD2 MD4 MD5
DSA#Microsoft Software Key Storage Provider	512 1024 2048	SHA1
ECDSA_P384#Microsoft Smart Card Key Storage Provider	384	SHA1 SHA256 SHA384 SHA512

Tabelle 2.5 Kryptografieanbieter, Schlüssellängen und Algorithmen (Forts.)

Bei der Auswahl der Einstellungen müssen Sie immer zwischen Sicherheit und Kompatibilität abwägen.

Die Option Administratorinteraktion bei jedem Zertifizierungsstellenzu-GRIFF AUF den privaten Schlüssel zulassen (siehe Abbildung 2.57) wird häufig in Verbindung mit *Hardware Security Modules (HSM*) verwendet. Ist diese Option aktiviert, wird bei der Verwendung des privaten Schlüssels der CA eine Authentifizierung abgefragt. Dies ist beim Zugriff auf das HSM notwendig.

Als Name der Zertifizierungsstelle verwendet der Assistent den Hostnamen, gefolgt von »-CA« (siehe Abbildung 2.58). Diesen Namen können Sie gemäß Ihren Vorgaben anpassen. Der Assistent bildet daraus einen *Distinguished Name*, der bei Bedarf manuell geändert werden kann. Die maximale Länge des CA-Namens beträgt 64 Zeichen.

Niewee den Zentifiniemus netelle		ZIELSERVER
Name der Zertifizierungsstelle pki		PKI-EntCA.corp.ichkanngarnix.de
Anmeldeinformationen Rollendienste Installationstyp ZS-Typ Privater Schlüssel Kryptografie ZS-Name	Geben Sie den Namen der Zertifizierungsst Geben Sie einen allgemeinen Namen zur Identifizierung der Zer wird allen von der Zertifizierungsstelle ausgestellten Zertifikaten DN-Suffix werden automatisch generiert, können jedoch geände Allgemeiner Name für diese Zertifizierungsstelle: Ichkanngarnix Enterprise CA	elle an. tifizierungsstelle an. Dieser Name hinzugefügt. Die Werte für das ert werden.
Gültigkeitsdauer	Suffix für Distinguished Name:	
Zertifikatdatenbank	DC=corp,DC=ichkanngarnix,DC=de	
Bestätigung	Vorschau auf Distinguished Name:	
Status	CN=lchkanngarnix Enterprise CA,DC=corp,DC=ichkanngarnix,D	C=de
Ergebnisse		

Abbildung 2.58 Den Namen der Zertifizierungsstelle festlegen

Die Abfrage zur maximalen Laufzeit des CA-Zertifikats (siehe Abbildung 2.59) wird ausschließlich bei der Konfiguration einer Stammzertifizierungsstelle angezeigt.



Abbildung 2.59 Die maximale Laufzeit des CA-Zertifikats definieren

Wird eine untergeordnete Zertifizierungsstelle installiert, bestimmt die Konfiguration der übergeordneten Zertifizierungsstelle die Laufzeit des ausgestellten CA-Zertifikats.

Als Speicherort für die Datenbank (siehe Abbildung 2.60) empfiehlt der Best Practices Analyzer ein Laufwerk (Volume), das nicht das Systemlaufwerk ist. Die Empfehlung basiert darauf, dass die Datenbank eventuell schnell wachsen kann und dadurch das System nicht mehr reagieren wird. Läuft das Systemlaufwerk eines Windows Servers voll, wird das System zuerst sehr träge und stellt dann wohlmöglich den Betrieb verschiedener Dienste ein, bevor es komplett stehen bleibt.

Wenn die Datenbank der Zertifizierungsstelle den gesamten Festplattenplatz des zugewiesenen Laufwerks aufbraucht, können keine Informationen mehr in die Datenbank geschrieben werden und das System wird die Datenbank – und den Dienst – herunterfahren.

Sie sollten also sicherstellen, dass Sie eine Überwachung einrichten, die Sie warnt und alarmiert, wenn eine Warnschwelle des freien Festplattenplatzes erreicht wird. Dazu können Sie entweder Drittanbieterlösungen verwenden oder Sie richten eine Leistungsindikatorenwarnung mithilfe der Leistungsüberwachung (START • PERF-MON) ein.

Besitzt der Server kein weiteres Laufwerk, bleibt nur die Auswahl des Systemlaufwerks.

Zertifizierungsste	llendatenbank	ZIELSERVER PKI-EntCA.corp.ichkanngarnix.de
Anmeldeinformationen Rollendienste	Geben Sie die Orte der Daten	bank an.
Installationstyp	Ort der Zertifikatdatenbank:	
ZS-Typ	C:\Windows\system32\CertLog	
Privater Schlüssel	Ort des Zertifikatdatenbankprotokolls:	
Kryptografie	C:\Windows\system32\CertLog	
ZS-Name		
Gültigkeitsdauer		
Zertifikatdatenbank		
Bestätigung		
Ergebnisse		

Abbildung 2.60 Auswahl des Speicherorts der Datenbank

Nachdem Sie alle Angaben vorgenommen haben, zeigt der Assistent eine Zusammenfassung der Konfiguration wie in Abbildung 2.61 an.

		ZIELSERVER
Bestatigung		PKI-EntCA.corp.ichkanngarnix.de
Anmeldeinformationen	Klicken Sie zum Konfigurieren der folgenden Rollen, Rollendienste oder Features auf	
Rollendienste	Koniiguneren .	
Installationstyp	 Active Directory-Zertifikatdienste 	
ZS-Typ	Zertifizierungsstelle	
Privater Schlüssel	ZS-Typ:	Stammzertifizierungsstelle des Unternehmens
Kryptografie	Kryptografieanbieter:	RSA#Microsoft Software Key Storage Provider
ZS-Name	Hashalgorithmus:	SHA256
Gültigkeitsdauer	Schlüssellänge:	2048
Zortifikatdatophank	Administratorinteraktion	Deaktiviert
Zerlinkaldalenbank	zulassen:	
Bestätigung	Gültigkeitsdauer des Zertifikats:	01.09.2029 20:36:00
	Distinguished Name:	CN=lchkanngarnix Enterprise CA,DC=corp,DC=ichkanngarnix,DC=de
	Ort der Zertifikatdatenbank:	C:\Windows\system32\CertLog
	Ort des Zertifikatdatenbankprotokolls:	C:\Windows\system32\CertLog

Abbildung 2.61 Zusammenfassung und Bestätigung der Konfiguration

Nach der Bestätigung der Konfiguration wird die Zertifizierungsstelle fertiggestellt bzw. werden die Tätigkeiten basierend auf der Konfiguration ausgeführt. In der von mir hier gewählten Konfiguration wird die Zertifizierungsstellenkonfiguration abgeschlossen und der Dienst gestartet (siehe Abbildung 2.62).

Ergebnisse	ZIELSERVER PKI-EntCA.corp.ichkanngarnix.de
Anmeldeinformationen	Die folgenden Rollen, Rollendienste oder Features wurden konfiguriert:
Rollendienste	Active Directory-Zertifikatdienste
Installationstyp	
ZS-Typ	Vertifizierungsstelle Vertifizierungsstelle
Privater Schlüssel	······
Kryptografie	
ZS-Name	
Gültigkeitsdauer	
Zertifikatdatenbank	
Bestätigung	
Status	
Ergebnisse	

Abbildung 2.62 Zusammenfassung der Ergebnisse

Nach Abschluss des Assistenten wird im Server-Manager der Hinweis, dass die CA noch konfiguriert werden muss, entsprechend aktualisiert (siehe Abbildung 2.63).



Abbildung 2.63 Der Hinweis im Server-Manager wurde aktualisiert.

2.4.2 Konfiguration der Zertifizierungsstelle mithilfe der PowerShell

Für die Konfiguration der Zertifikatdienste gibt es seit Windows Server 2012 R2 ein eigenes Modul, das die notwendigen Befehle (Cmdlets) bereitstellt.

Mit dem PowerShell-Cmdlet Get-Command -Module ADCSDeployment können Sie sich die verfügbaren Befehle anzeigen lassen. Ich habe sie in Tabelle 2.6 zusammengefasst.

Cmdlet		Beschreibung
Install-AdcsCe	rtificationAuthority	Dieses Cmdlet installiert eine Zertifizie- rungsstelle (Rollendienst <i>Zertifizierungs- stellen</i>).
Install-AdcsEn Service	rollmentPolicyWeb	Konfiguriert einen Zertifikatregistrie- rungsrichtlinien-Webdienst.
Install-AdcsEn	rollmentWebService	Konfiguriert einen Zertifikatregistrie- rungs-Webdienst.
Install-AdcsNe Service	tworkDeviceEnrollment	Konfiguriert den Registrierungsdienst für Netzwerkgeräte.
Install-AdcsOn	lineResponder	Konfiguriert einen Online-Responder.
Install-AdcsWe	pEnrollment	Konfiguriert die Zertifizierungsstellen- Webregistrierung.
Uninstall-Adcs	CertificationAuthority	Entfernt eine Zertifizierungsstelle. (Der Rollendienst ist nach wie vor installiert.)
Uninstall-Adcs Service	EnrollmentPolicyWeb	Entfernt die Konfiguration des Zertifikat- registrierungsrichtlinien-Webdienstes.

Tabelle 2.6 Die PowerShell-Cmdlets des Moduls »ADCSDeployment«

Cmdlat	Poschroihung
Chluet	Beschleibung
Uninstall-AdcsEnrollmentWebService	Entfernt die Konfiguration eines Zertifi- katregistrierungs-Webdienstes.
Uninstall-AdcsNetworkDevice EnrollmentService	Entfernt die Konfiguration eines Regis- trierungsdienstes für Netzwerkgeräte.
Uninstall-AdcsOnlineResponder	Entfernt die Konfiguration des Online- Responders.
Uninstall-AdcsWebEnrollment	Entfernt die Konfiguration der Zertifizie- rungsstellen-Webregistrierung.

Tabelle 2.6 Die PowerShell-Cmdlets des Moduls »ADCSDeployment« (Forts.)

Falls Sie die Konfiguration der soeben konfigurierten Zertifizierungsstelle lieber mit der PowerShell vornehmen möchten, können Sie folgenden Befehl dazu verwenden:

Install-AdcsCertificationAuthority -CAType EnterpriseRootCA `

-CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
-KeyLength 2048 -HashAlgorithmName "SHA256" `
-CACommonName "Ichkanngarnix Enterprise CA" `
-ValidityPeriod Years -ValidityPeriodUnits 12 `
-DatabaseDirectory "C:\Windows\System32\Certlog" `

Listing 2.4 Installation der Zertifizierungsstelle mit der PowerShell

Die Rückmeldung der PowerShell ist bei einer erfolgreichen Konfiguration eher spartanisch (siehe Abbildung 2.64). Sollte es zu einem Fehler gekommen sein, wird eine Fehlermeldung in rotem Text angezeigt.



Abbildung 2.64 Rückmeldung der PowerShell nach einer erfolgreichen Konfiguration

2.4.3 Schnelle Überprüfung der Konfiguration und Anpassen der Konfiguration

Unsere erste Zertifizierungsstelle ist nun betriebsbereit und wird im Hintergrund auch schon Zertifikate verteilen. Domänencontroller werden – sobald sich eine Unternehmenszertifizierungsstelle im Active Directory registriert hat – diese Zertifizierungsstelle kontaktieren, sofern die Standard-Zertifikatvorlagen veröffentlicht wurden. Ein Domänencontroller hat auf der Zertifikatvorlage das Recht *Lesen, Registrieren und Automatisch Registrieren* und wird damit das Zertifikat automatisch registrieren.

Wenn Sie prüfen möchten, welche Änderungen an Ihrer Umgebung durch die Installation vorgenommen wurden, gibt es verschiedene Prüfpunkte, an denen Sie die Einstellungen und Registrierungen der Zertifizierungsstelle kontrollieren können.

Im Server-Manager auf der Zertifizierungsstelle können Sie sehr einfach den Zustand des CA-Dienstes untersuchen (siehe Abbildung 2.65). Dort erhalten Sie auf dem Dashboard einen Überblick über den Zustand des Dienstes und sehen Einträge aus der Ereignisanzeige.

Server-M	1anager • Dashboard		
 Dashboard Lokaler Server Alle Server AD-Zertifikatdienste Datei-/Speicherdienste ▷ 	Schnellstart Sc	sen lokalen Server konfiguri Rollen und Features hinzufügen Weitere zu verwaltende Server hinzu Servergruppe erstellen Diesen Server mit Cloud-Diensten ve	eren Ifügen erbinden
	AD-Zertifikatdienste 1 Verwaltbarkeit Ereignisse Dienste Leistung BPA-Ergebnisse	Datei-/ 1 Speicherdienste 1 (*) Verwaltbarkeit Ereignisse Leistung BPA-Ergebnisse	Lokaler Server 1 Verwaltbarkeit Ereignisse Dienste Leistung BPA-Ergebnisse

Abbildung 2.65 Übersicht der AD-Zertifikatdienste im Server-Manager

Mit der Installation und Konfiguration der Rolle wurde ein Windows-Dienst registriert (siehe Abbildung 2.66). Dieser wird im Kontext des LOKALEN SYSTEMS ausgeführt und wird in der Dienste-Konsole aufgelistet. Der STARTTYP des Dienstes ist für einen automatischen Start konfiguriert.

Q		Dienste				x
Datei Aktion Ans	icht ?					
🔍 Dienste (Lokal)	Name 🔺	Beschreibung	Status	Starttyp	Anmelden als	^
	Active Directory-Zertifikatdienste	Erstellt, verwaltet und e	Wird ausgeführt	Automatisch	Lokales System	
	🔍 Anmeldedienst	Unterstützt einen sicher	Wird ausgeführt	Automatisch	Lokales System	=
	Anmeldeinformationsverwaltung	Ermöglicht das sichere		Manuell	Lokales System	

Abbildung 2.66 »Active Directory-Zertifikatdienste« als registrierter Dienst

Wenn Sie die Verwaltungskonsole für die Zertifizierungsstelle starten (siehe Abbildung 2.67), erkennen Sie anhand des grünen Icons am Computerkonto neben dem CA-Namen, dass der Dienst gestartet ist.

Sollte es zu Problemen kommen und kann der Dienst nicht gestartet werden, ist hier ein schwarzes Quadrat zu sehen.

<u>ت</u>	ertsrv - [Zertifizierungsstelle	(Lokal)]	- 0	x
Datei Aktion Ansicht ?				
Zertifizierungsstelle (Lokal)	Name	Beschreibung		
🔺 🚽 Ichkanngarnix Enterprise CA	👼 Ichkanngarnix Enterprise CA	Zertifizierungsstelle		
Gesperrte Zertifikate				
Ausgestellte Zertifikate				
Ausstehende Anforderungen				
Fehlgeschlagene Anforderungen				
Zertifikatvorlagen				

Abbildung 2.67 Die Verwaltungskonsole der Zertifizierungsstelle

Die kompletten Optionen der Konsole und die Eigenschaften der Zertifizierungsstelle werden in Abschnitt 2.6 behandelt.

Das Vorhandensein des Knotens ZERTIFIKATVORLAGEN ist ein Indiz dafür, dass es sich bei der Zertifizierungsstelle um eine Unternehmenszertifizierungsstelle handelt. Der Großteil der Konfiguration der Zertifizierungsstelle wird in der Registrierung gespeichert und kann mithilfe des Registrierungs-Editors (*RegEdit*) angezeigt und bearbeitet werden (siehe Abbildung 2.68).

1		Registrierungs-Edito	or	_ D X
Datei Bearbeiten Ansicht Favoriten ?				
▷	^	Name	Тур	Daten ^
⊿ J CertSvc		ab (Standard)	REG_SZ	(Wert nicht festgelegt)
Configuration		ab CACertHash	REG_MULTI_SZ	19 81 f1 e2 65 b4 7f cb d0 55 c4 b4 44 27 a3 46 e1 e0
⊿ lchkanngarnix Enterprise CA		ab CACertPublicationURLs	REG_MULTI_SZ	1:C:\Windows\system32\CertSrv\CertEnroll\%1_%
	Ξ	ab CAServerName	REG_SZ	PKI-EntCA.corp.ichkanngarnix.de
- IncryptionCSP		88 CAType	REG_DWORD	0x00000000 (0) =
▷ - J ExitModules		ab CAXchgCertHash	REG_MULTI_SZ	
▷ - J PolicyModules		ab CAXchgOverlapPeriod	REG_SZ	Days
Performance		B CAXchgOverlapPeriodU	REG_DWORD	0x00000001 (1)
security		ab CAXchgValidityPeriod	REG_SZ	Weeks
		B CAXchgValidityPeriodU	REG_DWORD	0x00000001 (1)
clr antimization v4.0.20210.22		88 CertEnrollCompatible	REG_DWORD	0x00000000 (0)
clr_optimization_v4.0.30319_52		88 ClockSkewMinutes	REG_DWORD	0x0000000a (10)
CmBatt		ab CommonName	REG_SZ	Ichkanngarnix Enterprise CA
CNG		88 CRLDeltaNextPublish	REG_BINARY	a8 79 88 31 e4 24 d3 01
CngHwAssist		ab CRLDeltaOverlapPeriod	REG_SZ	Minutes
▷ - III CompositeBus		88 CRLDeltaOverlapUnits	REG_DWORD	0x00000000 (0)
COMSysApp		ab CRLDeltaPeriod	REG_SZ	Days
		🕮 CRLDeltaPeriodUnits	REG_DWORD	0x00000001 (1)
стурt32		88 CRLEditFlags	REG_DWORD	0x00000100 (256)
▷		18 CRLFlags	REG_DWORD	0x00000002 (2)
▷ - J DCLocator	1	88 CRLNextPublish	REG_BINARY	dc 69 15 05 d2 28 d3 01
< Darmlana de la construcción de		ab CRLOverlapPeriod	REG_SZ	Hours
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet	\Ser	vices\CertSvc\Configuration\lcl	nkanngarnix Enter	prise CA

Abbildung 2.68 Konfigurationseinstellungen des »CertSvc« in der Registrierung

Die Konfiguration liegt unter *HKLM\System\CurrentControlSet\Services\CertSvc\ Configuration\<Name der Zertifizierungsstelle>*. Die Verwaltungstools für die Zertifizierungsstelle lesen und schreiben Konfigurationsänderungen in die Registrierung. Einige Änderungen benötigen einen Neustart des Dienstes, damit die Änderungen wirksam werden.

Der Konfigurationsassistent hat in dem Ordner, der bei der Konfiguration als Datenbankordner angegeben wurde, die Datenbank mit den notwendigen Dateien abgelegt (siehe Abbildung 2.69).

10 1 🕞 11 ≠ 1	CertLo	g		_ 🗆 X
Datei Start Freige	ben Ansicht			~ Ø
🔄 🔄 🔻 🕇 📗 « L	okaler Datenträger (C:) 🔸 Windows 🕨 Sys	stem32 🕨 CertLog	✓ Ċ "CertLog" da	urchsuchen 🔎
🔆 Favoriten	Name	Änderungsdatum	Тур	Größe
E Desktop	🚳 edb.chk	03.09.2017 18:35	Wiederhergestellt	8 KB
🗼 Downloads	📋 edb	03.09.2017 18:35	Textdokument	1.024 KB
🖳 Zuletzt besucht	edbres00001.jrs	01.09.2017 20:41	JRS-Datei	1.024 KB
	edbres00002.jrs	01.09.2017 20:41	JRS-Datei	1.024 KB
🖳 Dieser PC	edbtmp	03.09.2017 16:25	Textdokument	1.024 KB
	📄 Ichkanngarnix Enterprise CA.edb	03.09.2017 18:35	EDB-Datei	1.032 KB
🖤 Netzwerk	tmp.edb	03.09.2017 18:35	EDB-Datei	1.032 KB

Abbildung 2.69 Inhalt des Datenbank-Ordners

Die folgende Liste bietet eine Übersicht über diese Dateien und ihre Verwendung:

- *<Name der CA>.edb* Das Datenbankformat der CA-Dienste ist eine EDB-Datenbankdatei. Die Datenbankdatei hat den Namen *<Name der CA>.edb*.
- ▶ *tmp.edb* eine temporäre Datenbank, die vom CA-Dienst verwendet wird
- *edbtmp.loq* die Transaktions-Logdatei der Temp-Datenbank
- edb.log die Logdatei der CA-Datenbank. Bei dem Datenbanksystem handelt es sich um eine transaktionale Datenbank. Alle Änderungen an der Datenbank werden zuerst in einer Log-Datei gespeichert und im Anschluss in die Datenbankdatei übertragen.
- *edb.chk* Anhand der Checkpoint-Datei stellt das Datenbanksystem fest, welche Inhalte der Logdatei bereits in die Datenbank übertragen wurden.
- edbres00001.jrs und edbres00002.jrs Die beiden Reserve-Dateien sind Platzhalter. Sollte die Festplatte volllaufen und die Datenbank nicht sauber heruntergefahren werden können, können Sie diese beiden Dateien löschen und dann den Dienst beenden, sodass die Datenbank in einen sogenannten Clean Shutdown State überführt werden kann.

Durch die Installation einer Unternehmenszertifizierungsstelle wurden Anpassungen an der Active Directory-Umgebung vorgenommen. Die Informationen wurden im Konfigurationscontainer der AD-Datenbank abgelegt. Diese Informationen werden auf alle Domänencontroller der Gesamtstruktur repliziert. Dies bedeutet, dass die Informationen auf allen Domänencontrollern Ihrer Umgebung lokal gespeichert werden und von dort abgerufen werden können, auch wenn Ihre Umgebung aus mehreren AD-Domänen besteht, die Teil einer Gesamtstruktur (*Forest*) sind.

Den Inhalt der Konfigurationspartition des Active Directory können Sie sich mit jedem LDAP-Browser anzeigen lassen. Windows Server bringen hierfür die Tools *LDP.exe* und *ADSIEdit* mit, die Teil der Remoteserververwaltungstools für Active Directory sind.

Alternativ können Sie auch die Active Directory-Standorte und -Dienste-Konsole verwenden (siehe Abbildung 2.70).

圓層 Active Direct	ory-S	tandorte und -Dienste		
Datei Aktion	Ans	icht ?		
		Spalten hinzufügen/entfernen		
Active Directo		Große Symbole	Тур	Beschreibung
> 📄 Sites		Kleine Symbole	Standortcon	tainer
		Liste		
	٠	Details		
		Dienstknoten anzeigen		
		Anpassen		

Abbildung 2.70 Aktivieren der »Erwachsenenansicht«

Damit die Dienste aus der Konfigurationspartition in der Konsole angezeigt werden, müssen Sie die Ansicht anpassen.

[>>]

Dienstknoten anzeigen

Damit der Menüpunkt DIENSTKNOTEN ANZEIGEN verfügbar ist, muss der oberste Eintrag in der Baumstruktur (Active Directory-Standorte und -Dienste) ausgewählt sein.

Nach der Auswahl der erweiterten Anzeige werden die SERVICES-Informationen angezeigt. Die Einträge für die Zertifikatdienste werden unter dem Container PUBLIC KEY SERVICES aufgelistet (siehe Abbildung 2.71).

Der Container CERTIFICATION AUTHORITIES (RootCA) beinhaltet eine Liste der vertrauenswürdigen Stammzertifizierungsstellen. CAs, die hier eingetragen sind, werden automatisch bei Domänenmitgliedern in den lokalen Speicher der vertrauenswürdigen Stammzertifizierungsstellen übernommen.



Abbildung 2.71 Die »Public Key Services« im Konfigurationscontainer

Unternehmenszertifizierungsstellen (siehe Abbildung 2.72) werden im Active Directory unter ENROLLMENT SERVICES registriert, sodass Clients, die Zertifikate beziehen wollen, eine Liste der Zertifizierungsstellen abrufen und diese kontaktieren können, um Zertifikate zu registrieren.

圓層 Active Directory-Standorte und -Dienste			_		×
Datei Aktion Ansicht ?					
	Ø				
圓層 Active Directory-Standorte und -Dienste	Name	Тур	Beschre	ibung	
> 🛗 Sites	📄 Ichkanngarnix Enterprise CA	pKlEnrollmentService			
V Services					
> AuthN Policy Configuration					
> Claims Configuration					
> Group Key Distribution Service					
> Microsoft SPP					
> MsmqServices					
> 🔛 NetServices					
✓					
> 🖺 AIA					
> 🖺 CDP					
> 📔 Certificate Templates					
Certification Authorities					
Enrollment Services					
> 🖺 KRA					
> 🖺 OID					
> 🗂 RRAS					

Abbildung 2.72 Der Container »Enrollment Services« beinhaltet Unternehmenszertifizierungsstellen. Auf der Zertifizierungsstelle kann das selbstsignierte CA-Zertifikat über die *Verwaltungskonsole* (CertLm.msc) angezeigt werden.

Abbildung 2.73 zeigt, dass es sich um ein selbstsigniertes Zertifikat handelt, denn Antragsteller (AUSGESTELLT FÜR) und Aussteller (AUSGESTELLT VON) sind identisch. Der Schlüssel am Icon zeigt an, dass das System im Besitz des privaten Schlüssels ist.

Ce Ce	ertlm - [Zertifikate - Lokaler	Computer\Eigene Zertifi	kate\Zertifika	ate]	. 🗆 X
Datei Aktion Ansicht ?					
	?				
🗐 Zertifikate - Lokaler Computer	Ausgestellt für 🔺	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwec	Anzeigename
⊿ 📄 Eigene Zertifikate	🕼 Ichkanngarnix Enterprise CA	Ichkanngarnix Enterprise CA	01.09.2029	<alle></alle>	<keine></keine>
📄 Zertifikate					
Vertrauenswürdige Stammzei					
Organisationsvertrauen					

Abbildung 2.73 Prüfung des CA-Zertifikats

Da der Eintrag im Konfigurationscontainer eingetragen ist, wird das CA-Zertifikat im Speicher der vertrauenswürdigen CAs installiert (siehe Abbildung 2.74). Dadurch werden alle Zertifikate, die von der RootCA kommen, als vertrauenswürdig eingestuft. Das Synchronisieren der Clients erfolgt durch ein GPUpdate /force oder durch einen Neustart des Systems (obwohl die Verteilung nicht per Gruppenrichtlinie erfolgt).

🖀 certlm - [Zertifikate - Lokaler Cor	nputer\Vertrauenswürdige Stammzertif	izierungsstellen\Zertifikate] —	
Datei Aktion Ansicht ?			
	? DI		
🗊 Zertifikate - Lokaler Compute 🔺	Ausgestellt für	Ausgestellt von	Ablaufdatum
✓ ☐ Eigene Zertifikate	🔄 Baltimore CyberTrust Root	Baltimore CyberTrust Root	13.05.2025
Zertifikate	🔄 Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	02.08.2028
 Vertrauenswurdige Stamm Zertifikate 	🔄 Copyright (c) 1997 Microsoft C	Copyright (c) 1997 Microsoft Corp.	31.12.1999
	🔄 Ichkanngarnix Enterprise CA	Ichkanngarnix Enterprise CA	01.09.2029
> Zwischenzertifizierungsste	🔄 Microsoft Authenticode(tm) Ro	Microsoft Authenticode(tm) Root	01.01.2000
> 📋 Vertrauenswürdige Heraus	🔄 Microsoft Root Authority	Microsoft Root Authority	31.12.2020
> 🖺 Nicht vertrauenswürdige 2	🔄 Microsoft Root Certificate Auth	Microsoft Root Certificate Authori	10.05.2021

Abbildung 2.74 Die neue RootCA ist im Speicher der vertrauenswürdigen Stammzertifizierungsstellen gelistet.

Wenn Sie die Zertifizierungsstellen-Verwaltungskonsole öffnen und dort die Eigenschaften der CA auswählen, wird als Erstes die Registerkarte ALLGEMEIN angezeigt (siehe Abbildung 2.75). Hier finden Sie die Version des CA-Zertifikats. ZERTIFIKAT NR. 0 bedeutet, dass es sich um das erste Zertifikat der Zertifizierungsstelle handelt. Wenn ein CA-Zertifikat erneuert wird, wird die laufende Nummer hochgezählt.

Ein Klick auf ZERTIFIKAT ANZEIGEN zeigt die kompletten Eigenschaften des CA-Zertifikats an (siehe Abbildung 2.76). Hier können Sie auch die konfigurierten 12 Jahre Laufzeit erkennen.

Überwachung Wiederherstellungs-Agents Sicherheit Ilgemein Richtlinienmodul Beendigungsmodul Enweiterunge Zertifizierungsstelle Ichkanngamix Enterprise CA Zertifizierungsstellenzertifikate: Zertifizierungsstellenzertifikate: Zertifizierungsstellenzertifikate: Zertifikat Nr. 0 Zertifikat anzeigen Kryptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorithmus: SHA256 SHA256	Speicherun	g	Zertifikatver	waltungen	Regis	trierungs-Agents
Ilgemein Richtlinienmodul Beendigungsmodul Erweiterunge Zertifizierungsstelle Name: Ichkanngamix Enterprise CA Zertifizierungsstellenzertifikate: Zertifikat Nr. 0 Zertifikat Nr. 0 Zertifikat anzeigen Kryptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorthmus: SHA256	Überwachu	ung	Wieder	herstellungs-Ag	gents	Sicherheit
Zettfizierungsstelle Name: Ichkanngamix Enterprise CA Zettfizierungsstellenzettfikate: Zettfikat Nr. 0 Zettfikat Nr. 0 Zettfikat anzeigen Kyptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorthmus: SHA256	llgemein	Richtli	nienmodul	Beendigung	smodul	Erweiterungen
Zertifizierungsstelle Name: Ichkanngamix Enterprise CA Zertifizierungsstellenzertifikate: IZertifikat Nr. 0 Zertifikat anzeigen Kyptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorithmus: SHA256	Zertifizien in	neetalla				
Zertifizierungsstellenzertifikate: Zertifizierungsstellenzertifikate: Zertifikat Nr. 0 Zertifikat anzeigen Kyptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorthmus: SHA256	Mama	igaatelle	l-bl			
Zertifizierungsstellenzertifikate: Zertifikat Nr. 0 Zertifikat anzeigen Kryptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorithmus: SHA256	Name:		ichkanng	jamix Enterpris	eLA	
Zertifikat Nr. 0 Zertifikat anzeigen Kryptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorithmus: SHA256	Zertifizierun	ngsstelle	nzertifikate:			
Zertifikat anzeigen Kryptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorithmus: SHA256						
Zertifikat anzeigen Kryptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorithmus: SHA256	Zertifikat N	Nr. 0				
Kyptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorthmus: SHA256	Zertifikat N	Nr. 0				
Kyptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorithmus: SHA256	Zertifikat N	Nr. 0				
Kryptografieeinstellungen Anbieter: Microsoft Software Key Storage Provider Hashalgorithmus: SHA256	Zertifikat N	Nr. O			Zerti	fikat anzeigen
Anbieter: Microsoft Software Key Storage Provider Hashalgorithmus: SHA256	Zertifikat M	Nr. 0			Zerti	fikat anzeigen
Hashalgorithmus: SHA256	Zertifikat M	Nr. 0 eeinstelli	ungen		Zerti	fikat anzeigen
nasnaigoninimus: SHA236	Zertifikat M Kryptografie Anbieter:	Nr. 0 eeinstellu	ungen Microsoft	Software Key	Zerti Storage P	fikat anzeigen Provider
	Zertifikat M Kryptografie Anbieter:	Nr. 0 eeinstellu	ungen Microsoft	Software Key	Zerti Storage P	fikat anzeigen Provider
	Zertifikat N Kryptografie Anbieter: Hashalgorit	Nr. 0 eeinstelli	ungen Microsoft SHA256	Software Key	Zerti Storage P	fikat anzeigen Provider

Abbildung 2.75 Übersicht des CA-Zertifikats



Abbildung 2.76 Eigenschaften des CA-Zertifikats

Die Registerkarte ERWEITERUNGEN listet die Sperrlisten-Verteilungspunkte und den Zugriff auf die Stelleninformationen auf. In den Anforderungen an die Zertifizierungsstelle hatten wir definiert, dass die Sperrlisten und das CA-Zertifikat im Active Directory veröffentlicht werden sollen. Dies ist die Standard-Konfiguration – sofern keine Anpassung in der *CAPolicy.inf* vorgenommen wurde.

Überwachung Wiederherstellungs-Agents Sicherheit Wigemein Richtlinienmodul Beendigungsmodul Erweiterungen Erweiterung auswählen:	Speicherung	Zertifikatver	waltungen	Regist	rierungs-Agents
Allgemein Richtlinienmodul Beendigungsmodul Erweiterungen Erweiterung auswählen: Sperlisten-Verteilungspunkt v Geben Sie Standorte an, von denen Benutzer eine Zertfikatsperliste erhalten können. C:Windows/system32/CertSrv/CertErroll/ <caname><crlnamesuffix><qi< td=""> C:Windows/system32/CertSrv/CertErroll/<caname><crlnamesuffix><qi< td=""> Mage: ServerDNSName>/CertErroll/<caname><crlnamesuffix><qi< td=""> Mit://<serverdnsname>/CertErroll/<caname><crlnamesuffix><qi< td=""> > Veröffentlichen >> III >> Image: ServerDisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichen > In alle Sperlisten einbeziehen. Wird z. Suche von Deltasperlisten verwendet In CDP-Erweiterung des ausgestellten Zertfikats einbeziehen Image: In CDP-Erweiterung des ausgestellten Zertfikats einbeziehen In die IDP-Erweiterung ausgestellter CRLs einbeziehen</qi<></crlnamesuffix></caname></serverdnsname></qi<></crlnamesuffix></caname></qi<></crlnamesuffix></caname></qi<></crlnamesuffix></caname>	Überwachung	Wieder	herstellungs-Ag	jents _	Sicherheit
Erweiterung auswählen: Sperlisten-Verteilungspunkt ✓ Geben Sie Standorte an, von denen Benutzer eine Zertifikatsperliste erhalten können. C:\Windows\system32\CertSrv\CertErroll\ <caname><crlnamesuffix><qi< td=""> C:\Windows\system32\CertSrv\CertErroll\<caname><crlnamesuffix><qi< td=""> ServerDNSName>/CertErroll<<caname><crlnamesuffix><qi=< td=""> Mit:://<serverdnsname>/CertErroll<<caname><crlnamesuffix><qi=< td=""> ServerDNSName>/CertErroll III > III > III > III > III > In alle Sperlisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichen In Sperlisten einbeziehen. Wird z. Suche von Deltasperlisten verwendet In IDP-Erweiterung des ausgestellten Zertifikats einbeziehen In Deltasperlisten an diesem Ort veröffentlichen In die IDP-Erweiterung ausgestellter CRLs einbeziehen In die IDP-Erweiterung ausgestellter CRLs</qi=<></crlnamesuffix></caname></serverdnsname></qi=<></crlnamesuffix></caname></qi<></crlnamesuffix></caname></qi<></crlnamesuffix></caname>	Allgemein Ric	chtlinienmodul	Beendigung	Ismodul	Erweiterunger
Sperfisten-Verteilungspunkt ✓ Geben Sie Standorte an, von denen Benutzer eine Zertfikatsperfiste erhalten können. Zertfikatsperfiste C:\Windows\system32\CertSrv\CertErroll\ <caname><crlnamesuffix><qled http://CServerDNSName>/CertErroll\<caname><crlnamesuffix><delta file://<serverdnsname>/CertErroll</serverdnsname></delta </crlnamesuffix></caname><crlnamesuffix><delta file://<serverdnsname>/CertErroll</serverdnsname></delta </crlnamesuffix></qled </crlnamesuffix></caname> <crlnamesuffix><delta file://<serverdnsname>/CertErroll<crlnamesuffix><delta in ✓ III >> ✓ III >> ✓ Insperfisten an diesem Ort veröffentlichen >> ✓ In alle Sperfisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll >> ✓ In Sperfisten einbeziehen. Wird z. Suche von Deltasperfisten verwendet ✓ In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen ✓ Deltasperfisten an diesem Ort veröffentlichen ✓ In die IDP-Erweiterung ausgestellter CRLs einbeziehen</delta </crlnamesuffix></serverdnsname></delta </crlnamesuffix>	Erweiterung ausw	ählen:			
Geben Sie Standorte an, von denen Benutzer eine Zertifikatsperliste erhalten können. C:\Windows\system32\CertSrv\CertErroll\ <caname><crlnamesuffix><0 Idap://CN=<catruncatedname><crlnamesuffix><0Petta http://cServerDNSName>/CertErroll/<caname><crlnamesuffix><deita file://cServerDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname><crlnamesuffix><deita file://serverDNSName>/CertErroll/<caname></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></deita </crlnamesuffix></caname></crlnamesuffix></catruncatedname></crlnamesuffix></caname>	Sperfisten-Vertei	lungspunkt			Ý
III III In Spertisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll In Spertisten einbeziehen. Wird z. Suche von Deltaspertisten verwendet In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen Deltaspertisten an diesem Ort veröffentlichen In die IDP-Erweiterung ausgestellter CRLs einbeziehen	C:\Windows\sys Idap:///CN= <ca http://<serverd1 file://<serverdn< td=""><td>tem32\CertSrv\0 TruncatedName VSName>/CertE</td><td>CertEnroll\<cal ><crlnames nroll/<caname< td=""><td>Name><cf uffix>,CN= >><crlna< td=""><td>RLNameSuffix>< <servershortna meSuffix><delta< td=""></delta<></servershortna </td></crlna<></cf </td></caname<></crlnames </cal </td></serverdn<></serverd1 </ca 	tem32\CertSrv\0 TruncatedName VSName>/CertE	CertEnroll\ <cal ><crlnames nroll/<caname< td=""><td>Name><cf uffix>,CN= >><crlna< td=""><td>RLNameSuffix>< <servershortna meSuffix><delta< td=""></delta<></servershortna </td></crlna<></cf </td></caname<></crlnames </cal 	Name> <cf uffix>,CN= >><crlna< td=""><td>RLNameSuffix>< <servershortna meSuffix><delta< td=""></delta<></servershortna </td></crlna<></cf 	RLNameSuffix>< <servershortna meSuffix><delta< td=""></delta<></servershortna
Hinzufügen Entfermen Sperilisten an diesem Ort veröffentlichen In alle Sperilisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll In Sperilisten einbeziehen. Wird z. Suche von Deltasperilisten verwendet In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen Deltasperilisten an diesem Ort veröffentlichen In die IDP-Erweiterung ausgestellter CRLs einbeziehen		SName>/CertEn	roll/ <caname:< td=""><td>><crlnam< td=""><td>neSuffix><delta< td=""></delta<></td></crlnam<></td></caname:<>	> <crlnam< td=""><td>neSuffix><delta< td=""></delta<></td></crlnam<>	neSuffix> <delta< td=""></delta<>
 Sperilisten an diesem Ort veröffentlichen In alle Sperilisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll In Sperilisten einbeziehen. Wird z. Suche von Deltasperilisten verwendet In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen Deltasperilisten an diesem Ort veröffentlichen In die IDP-Erweiterung ausgestellter CRLs einbeziehen 	< 111	SName>/CertEn	roll/ <caname:< td=""><td>><crlnam< td=""><td>neSuffix><delta(< td=""></delta(<></td></crlnam<></td></caname:<>	> <crlnam< td=""><td>neSuffix><delta(< td=""></delta(<></td></crlnam<>	neSuffix> <delta(< td=""></delta(<>
 In alle Speritisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll In Speritisten einbeziehen. Wird z. Suche von Deltasperitisten verwendet In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen Deltasperitisten an diesem Ort veröffentlichen In die IDP-Erweiterung ausgestellter CRLs einbeziehen 	<	SName>/CertEn	roll/ <caname Hinz</caname 	<crlnam< td=""><td>ne Suffix><delta(< td=""></delta(<></td></crlnam<>	ne Suffix> <delta(< td=""></delta(<>
 In Sperilisten einbeziehen. Wird z. Suche von Deltasperilisten verwender In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen Deltasperilisten an diesem Ort veröffentlichen In die IDP-Erweiterung ausgestellter CRLs einbeziehen 	< Ⅲ ✓ Spentisten an	diesem Ort veröf	roll/ <caname: Hinz fentlichen</caname: 	> <crlnam< td=""><td>ne Suffix><delta(< td=""></delta(<></td></crlnam<>	ne Suffix> <delta(< td=""></delta(<>
✓ In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen ✓ Deltasperfisten an diesem Ort veröffentlichen In die IDP-Erweiterung ausgestellter CRLs einbeziehen	 Sperfisten an In alle Sperfist Veröffentlichur 	diesem Ort veröf en einbeziehen. ng im Active Dire	roll/ <caname: Hinz fentlichen Legt fest, wo o ctory veröffent</caname: 	v=CRLNam ufügen dies bei ma licht werde	neSuffix> <detta(> Entfermen nueller en soll</detta(
✓ Deltasperfisten an diesem Ort veröffentlichen ☐ In die IDP-Erweiterung ausgestellter CRLs einbeziehen	 ✓ III ✓ Spentisten an ✓ In alle Spentist Veröffentlichur ✓ In Spentisten e 	diesem Ort veröf en einbeziehen. ng im Active Dire einbeziehen. Win	roll/ <caname: Hinz fentlichen Legt fest, wo o ctory veröffent d z. Suche vor</caname: 	<crlnarr ufügen dies bei ma licht werde n Deltasper</crlnarr 	ne Suffix> <detta(< td=""></detta(<>
In die IDP-Erweiterung ausgestellter CRLs einbeziehen	 Sperfisten an In alle Sperfisten er Veröffentlichur In Sperfisten er In CDP-Erweit 	diesem Ort veröf en einbeziehen. ng im Active Dire einbeziehen. Win erung des ausge	roll/ <caname: Hinz fentlichen Legt fest, wo (ctory veröffent d z. Suche vor stellten Zertifik</caname: 	vfügen dies bei ma licht werde n Deltasper ats einbezi	ne Suffix> <detta(< td=""></detta(<>
	 Speriisten an In alle Speriist Veröffentlichur In Speriisten e In CDP-Erweit Deitasperiistei 	diesem Ort veröf en einbeziehen. ng im Active Dire einbeziehen. Win erung des ausge n an diesem Ort 1	roll/ <caname: Hinz fentlichen Legt fest, wo o ctory veröffent d z. Suche vor stellten Zertifik veröffentlichen</caname: 	<crlnan dies bei ma licht werde n Deltasper ats einbezi</crlnan 	International and a second a seco



Eine detaillierte Konfiguration der *Sperrlisten-Verteilungspunkte* (CDP) und der *Zugriff auf Stelleninformationen* (AIA, siehe Abbildung 2.78) wird in Abschnitt 2.6 erläutert.

Eigenschaf	ten vo	on Ichkann	igarnix Ent	erprise	CA ? X		
Speicherun	ig 🛛	Zertifikatverwaltungen Regis			trierungs-Agents		
Überwach	ung	Wiederherstellungs-Agents			Sicherheit		
Algemein	Richt	inienmodul	Beendigung	Erweiterungen			
Erweiterung	auswäh	en:					
Zugriff auf S	Stellenin	omationen			~		
C:\Window Idap:///CN http:// <serv file://<serv< td=""><td colspan="7">C:\Windows\system32\CertSrv\CertEnroll\<serverdnsname>_<caname dap:///CN=<catruncatedname>_CN=AIA.CN=Public Key Services.CN=S http://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><cert file://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><cert< td=""></cert<></caname></serverdnsname></serverdnsname></cert </caname></serverdnsname></serverdnsname></catruncatedname></caname </serverdnsname></td></serv<></serv 	C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<caname dap:///CN=<catruncatedname>_CN=AIA.CN=Public Key Services.CN=S http://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><cert file://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><cert< td=""></cert<></caname></serverdnsname></serverdnsname></cert </caname></serverdnsname></serverdnsname></catruncatedname></caname </serverdnsname>						
<	III >						
✓ In AIA-Er	Hinzufügen Entfernen In AIA-Erweiterung des ausgestellten Zertifikats einbeziehen In Online Certificate Status-Protokoll (OCSP)-Erweiterungen einbeziehen						
[OK	Abb	orechen)bernehme	en Hilfe		

Abbildung 2.78 Quellen zum Abruf des CA-Zertifikats

Eine weitere Konfigurationsanforderung ist das Intervall für die Veröffentlichung von Sperrlisten.

In der CA-Verwaltungskonsole können Sie die Zeiträume durch einen Rechtsklick auf GESPERRTE ZERTIFIKATE und durch Auswahl der Eigenschaften konfigurieren (siehe Abbildung 2.79). Hier gibt es dann die Option, unterschiedliche Intervalle für Basissperrlisten und Deltasperrlisten zu konfigurieren.

Eine Zertifizierungsstelle wird Sperrlisten automatisch erneuern, sobald diese ablaufen. Abhängig von der Konfiguration wird die CA die Sperrlisten an vorgegebenen Speicherorten ablegen.

certsrv - [Zertifizierungsstelle	(Lokal)\Ichkanngarnix Enterprise CA\Gesperrte Zertifikate] 📃 🗖 🗙
Datei Aktion Ansicht ?	
Zertifizierungsstelle (Lokal)	Anforderungs-ID Sperrdatum Effektives Sperrdatum Grund für die Sperrung
 Ichkanngarnix Enterprise CA Gesperrte Zertifikate Ausgestellte Zertifikate 	In dieser Ansicht werden keine Elemente angezeigt.
Ausstehende Anforderungen	Eigenschaften von Gesperrte Zertifikate ? X
🖺 Zertifikatvorlagen	Parameter für Sperflistenveröffentlichung Zertifikatsperfliste anzeigen
	Eine Zertfikatsperiliste beschreibt Zertfikate, die Clients als ungültig betrachten sollen.
	Veröffentlichungsintervall der 📗 Wochen 🗸
	Nächste Aktualisierung: 08.09.2017 20:41
	Deltasperfisten veröffentlichen
	Veröffentlichungsintervall: 1 Tagen V
	Nächste Aktualisierung: 03.09.2017 20:41

Abbildung 2.79 Konfiguration der Sperrlisten

Eine Prüfung der Zertifikatvorlagen zeigt, dass diese Zertifizierungsstelle bereits Zertifikatvorlagen geladen hat und damit diese Zertifikate bereitstellen kann. Eine Konfiguration der *CAPolicy.inf* hätte dies verhindern können.

Die Vorlagen werden im Active Directory gespeichert. Die in Abbildung 2.80 angezeigte Liste ist eine Teilmenge der im AD gespeicherten Vorlagen.

Werden Vorlagen auf einer Zertifizierungsstelle gelöscht, bedeutet dies nicht, dass sie auch in der AD-Datenbank gelöscht werden.

Eine Anforderung an die Infrastruktur war die Gültigkeit der Clientzertifikate. Die maximale Laufzeit soll 5 Jahre betragen. Die maximale Gültigkeitsdauer eines Zertifikats einer eigenständigen Zertifizierungsstelle beträgt 1 Jahr, die maximale Laufzeit einer Unternehmenszertifizierungsstelle 2 Jahre. Diese Werte können Sie mit dem Kommandozeilentool CertUtil anzeigen lassen bzw. anpassen (siehe Abbildung 2.81).

Abbildung 2.80 Anzeige der aktivierten Zertifikatvorlagen

C:\>certutil -getreg ca\val* HKEY_LOCAL_MACHINE\\$Y\$TEM\CurrentControlSet\Services\CertSvc\Com nngarnix Enterprise CA\val*:	ıfiguration∖Ichka
Werte: ValidityPeriod REG_SZ = Years ValidityPeriodUnits REG_DWORD = 2 CertUtil: -getreg-Befehl wurde erfolgreich ausgeführt.	

Abbildung 2.81 So lesen Sie die maximale Laufzeit eines Zertifikats aus, das von der CA ausgestellt wird.

Certutil -getreg liest Registrierungswerte. Mithilfe von RegEdit können Sie die Informationen ebenfalls auslesen.

Viele der Konfigurationen bestehen aus zwei Werten (siehe Abbildung 2.82):

- aus einer Einheit, in der die Zeit angegeben wird (VALIDITYPERIOD)
- ► aus einem Wert, der die Laufzeit angibt (VALIDITYPERIODUNITS)

1) III		Registrierungs-Editor					
Datei Bearbeiten Ansicht Favoriten ?							
⊳ - J CertPropSvc	^	Name	Тур	Daten			
⊿		腿 SetupStatus	REG_DWORD	0x00000001 (1)			
⊿ D Configuration		DignedAttributes	REG_MULTI_SZ	RequesterName			
🔺 🋄 Ichkanngarnix Enterprise CA		ab SubjectTemplate	REG_MULTI_SZ	EMail CommonName Orga			
CSP EncryptionCSP		110 UseDS	REG_DWORD	0x00000001 (1)			
		ab ValidityPeriod	REG_SZ	Years			
⊳ J ExitModules		18 ValidityPeriodUnits	REG_DWORD	0x0000002 (2)			
▷ ····· PolicyModules	÷	8년 ViewAgeMinutes	REG_DWORD	0x00000010 (16)			
Performance		R ViewIdleMinutes	REG_DWORD	0x0000008 (8)			
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\\chkanngarnix Enterprise CA							

Abbildung 2.82 Die »ValidityPeriod« in der Registry

Eine Anpassung der Werte erfolgt über Certutil -setreg mit den entsprechenden Parametern aus Abbildung 2.83.

	Administrator: Eingabeaufforderung
C:\>certutil -setr	g ca\calidityperiodunits 5
HKEY_LOCAL_MACHINE	SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Ichka
nngarnix Enterpris	CA\calidityperiodunits:
Neuer Wert: calidityperiodun CertUtil: -setreg- Der Dienst "CertSv den.	ts REG_DWORD = 5 efehl wurde erfolgreich ausgeführt. " muss neu gestartet werden, damit die Änderungen wirksam wer
C:\>net stop certs	c && net start certsvc
Active Directory-Z	rtifikatdienste wird beendet.
Active Directory-Z	rtifikatdienste wurde erfolgreich beendet.
Active Directory-Z	rtifikatdienste wird gestartet.
Active Directory-Z	rtifikatdienste wurde erfolgreich gestartet.
C:\>_	

Abbildung 2.83 Der Versuch der Anpassung der maximalen Laufzeit eines Zertifikats

Bei der Verwendung von CertUtil in der Kommandozeile sollten Sie genau prüfen, welche Parameter Sie eingeben. Wenn Sie sich den eingegebenen Befehl in Abbildung 2.83 genau anschauen, können Sie feststellen, dass im Befehl ein Tippfehler enthalten ist. Der Befehl hätte CertUtil -setreg ca\validityperiodunits 5 lauten müssen. Bei einem falschen Parameter wird der falsche Wert in die Registrierung eingetragen und bleibt ohne Funktion (siehe Abbildung 2.84).

📲 Registrierungs-Editor				- 0	×	
Datei Bearbeiten Ansicht Favoriter	ъH	ilfe				
Computer\HKEY_LOCAL_MACHINE\SYS	TEM	\CurrentControlSet\Services\Ce	ertSvc\Configuratio	on\EntCASHA1		
> CertPropSvc	^	Name	Тур	Daten		^
CertSvc Configuration EntCASHA1 Performance Security Cht4iscsi	v	(Standard) CACertHash CACertPublicationURLs CACertPublicationURLs CAServerName CAServerName	REG_SZ REG_MULTI_SZ REG_MULTI_SZ REG_DWORD REG_SZ REG_DWORD	(Wert nicht festgelegt) 87 c3 7e a7 81 c0 8e 6b 45 09 77 8a d0 d 1:C:\Windows\system32\CertSrv\CertE 0x0000005 (5) PKI-EntCA.corp.ichkanngarnix.de 0x00000000 (0)	3 c6 nroll	~
<	>	<			>	

Abbildung 2.84 In der Registrierung wurde ein falscher Wert eingetragen.

Sie können in der Ausgabe des Befehls an der Anzeige des »alten« Wertes erkennen, dass ein Wert geändert wurde. Fehlt dieser Teil der Ausgabe bei Ausführung des Befehls, sollten Sie die Syntax und den Wert prüfen, da der Verdacht nahe liegt, dass Ihnen ein Tippfehler unterlaufen ist.

C:\Users\OPeterKloep>certutil -setreg ca\validityperiodunits 5 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ EntCASHA1\ValidityPeriodUnits:

```
Alter Wert:
ValidityPeriodUnits REG DWORD = 2
```

Neuer Wert:

ValidityPeriodUnits REG_DWORD = 5

CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.

Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam werden.

Listing 2.5 Ausgabe der Anpassung mit der Information zum »alten Wert«

Das gleiche Problem besteht, wenn Sie den notwendigen »\« mit einem »/« verwechseln. Die Ausgabe wird hier auch keinen Fehler auswerfen, sondern einen entsprechenden Wert (siehe Abbildung 2.85) in der Registrierung eintragen, der ohne Funktion bleibt und auch nicht den gewünschten Effekt hat.

Registrierungs-Editor				- 0	×		
Datei Bearbeiten Ansicht Favoriter	n Hilf	fe					
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration							
> CertPropSvc	^	Name	Тур	Daten	^		
✓ CertSvc		(Standard)	REG_SZ	(Wert nicht festgelegt)			
Configuration		ab Active	REG_SZ	EntCASHA1			
		🕮 ca/validityperiodunits	REG_DWORD	0x00000005 (5)			
		ab DBDirectory	REG_SZ	C:\Windows\system32\CertLog			
security		🕮 DBFlags	REG_DWORD	0x00000b0 (176)			
cht4iscsi	~	ab DBLogDirectory	REG_SZ	C:\Windows\system32\CertLog	~		
<	>	<			>		

Abbildung 2.85 Bei der Verwendung eines »/« wird der falsche Eintrag eine Ebene höher erstellt.

Nach der Anpassung der Werte muss der Dienst neu gestartet werden, damit die Änderungen aktiv werden. Wurden bereits Zertifikate mit der alten (verkürzten) Laufzeit ausgestellt, werden diese Zertifikate nicht aktualisiert. Die geänderte Konfiguration betrifft nur neu ausgestellte Zertifikate.