PKI und CA in Windows-Netzwerken

Das umfassende Handbuch

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 für die Zertifikatdienste – Es wurden neue PowerShell-Cmdlets für die Verwaltung der Zertifizierungsstelle hinzugefügt, insbesondere für 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 für Netzwerkgeräte* kann mit Windows Server 2016 der Schlüsselnachweis verwendet werden.

- **Neuerungen in Windows Server 2019 und Windows Server 2022:**
  - In Windows Server 2019 und Windows Server 2022 sind keine Neuerungen für die Zertifikatdienste enthalten. Auch die Preview von Windows Server 2025 enthält keine Neuerungen, und es gibt keine Ankündigungen, dass bis zur finalen Version neue Funktionen dazukommen.

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-0 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 ein-

stufigen 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 sicher 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 2.10. Der Einsatz eines HSM kann eventuelle Sicherheitsanforderungen unterstützen, die es ermöglichen, eine Zertifizierungsstelle auf einer Virtualisierungsplattform zu betreiben, ohne dass der Virtualisierungsadministrator Zugriff auf das Schlüsselmaterial der Zertifizierungsstelle erhält.
- **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/files/ppfiles/cert-issu-v15-sec-eng.pdf*) angelehnt sind.

Rolle	Berechtigung	Verwendungszweck
CA-Administrator	Verwaltung der Zertifizierungsstelle	Hauptverwalter der CA mit der Berechtigung, die Rollen zu definieren. Besitzt das Recht, das CA-Zertifikat zu erneuern.
Zertifikatverwaltung	Ausstellen und Verwalten von Zertifikaten	Durchführen von Sperrungen und das Genehmigen von Zertifikatanforderungen, die nicht automatisch genehmigt wurden
Sicherungs-Operator	Sichern und Wiederherstellen von Dateien und Ordnern	Dieses Konto darf das System sichern und wiederherstellen.
Auditor	Verwaltung der Überwachungs- und Sicherheitsprotokolle	Konfiguration, Auswertung der Überwachungsprotokolle (Ereignisanzeige)
Registrierende	Lesen- und Registrieren-Recht auf Zertifikatvorlagen	Benutzer, Computer oder Dienste, die das Recht haben, Zertifikate anzufordern

Tabelle 2.1 Berechtigungsrollen in einer Windows-CA

Lokale Rechte auf der Zertifizierungsstelle

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

- **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 × 7 + 1 = 15 Jahre.

Es wird die maximale Laufzeit definiert

Sollten innerhalb der kommenden 15 Jahre (oder auch eines längeren Zeitraums) die – damals – verwendeten Parameter (wie etwa die Schlüssellänge oder der Algorithmus) als unsicher eingestuft werden, hindert Sie niemand daran, die CA-Zertifikate vor Ablauf der Laufzeit gegen neue Zertifikate auszutauschen.

- **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 Datenmenge 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.

  Erste Browser wie der Firefox von Mozilla verwenden ausschließlich den Online-Responder mit dem OCSP-Protokoll und nutzen keine Sperrlisten mehr.
- **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 nach-

träglich 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 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 Services*, CES)
- Remote-Desktop-Authentifizierung

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.

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 hinter-

legt (siehe Abbildung 2.2), unter dem das CPS oder auch weitere Dokumente der Zertifizierungsstelle abgerufen werden können.

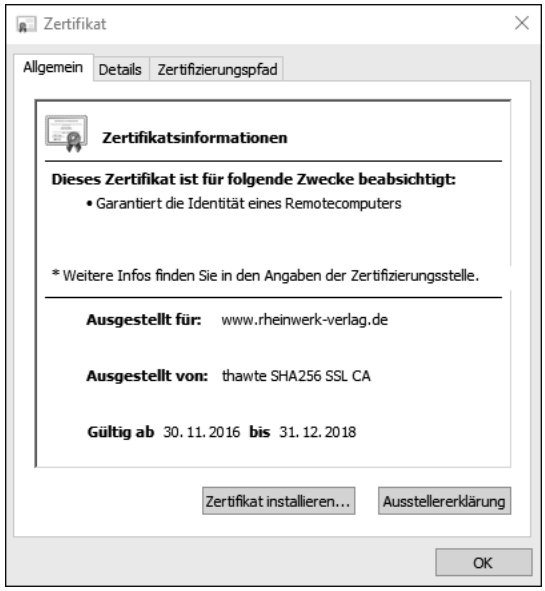

Abbildung 2.1 Option mit Informationen zur Ausstellererklärung (CPS)

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	Einschränkungen bekannt	Bemerkungen
1	Computer	Nein	Nein	Keine	
2	Computer	Nein	Nein	Keine	
3	Benutzer	Nein	Nein	Keine	Veröffentlichung im AD, um doppelte Ausstellung zu verhindern
4	Benutzer	Nein	Ja	Keine	Veröffentlichung im AD

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

Der Export des privaten Schlüssels kann nur mit entsprechender Hardware verhindert werden

Auch wenn durch die Beschreibung in Tabelle 2.3 und auch in der weiteren Konfiguration der Zertifikatvorlagen der Eindruck entstehen kann, dass der Export des privaten Schlüssels kontrolliert – und damit verhindert – werden könnte: Das ist ein Fehlschluss!

Der Client erstellt das Schlüsselpaar und hat damit auch die Kontrolle über den privaten Schlüssel. Soll der Export – und damit das Duplizieren – verhindert werden, muss sichergestellt werden, dass der Schlüssel auf einem sicheren Medium wie einem HSM oder einer SmartCard erstellt wurde.

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).

Der Security Compliance Manager ist bei Microsoft als kostenloser Download unter *https://www.microsoft.com/en-us/download/details.aspx?id=53353* verfügbar.

Microsoft hat das Tool jedoch abgekündigt und wird es 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.

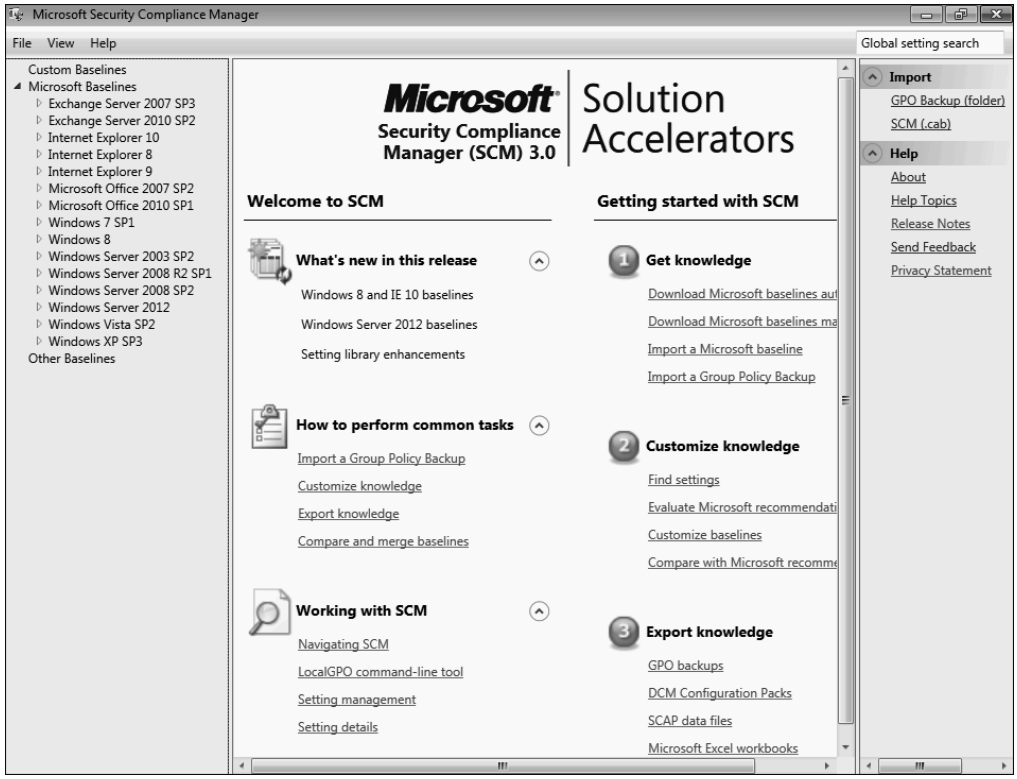

Abbildung 2.3 Der Startbildschirm des Security Compliance Managers

Abbildung 2.4 Suche nach Updates

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!

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.

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).

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 CUSTOMIZED.

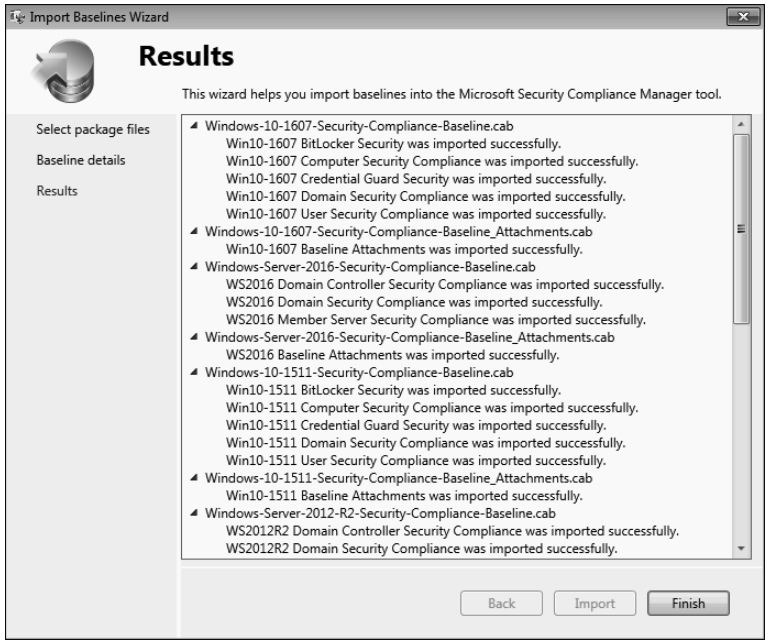

Abbildung 2.6 Ergebnis der Aktualisierung

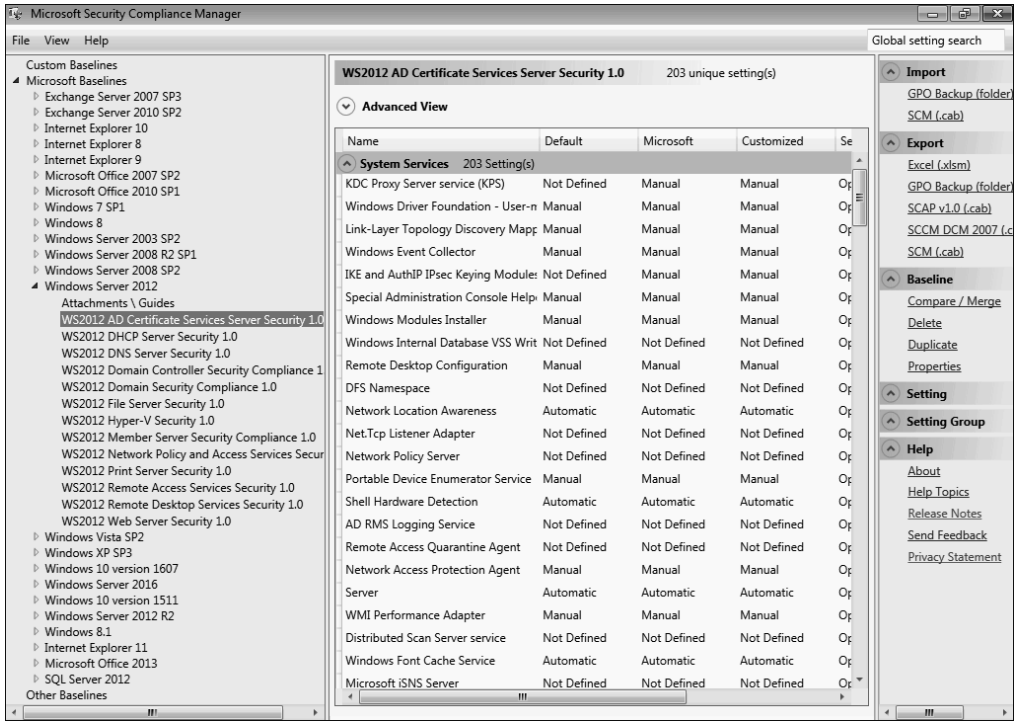

Abbildung 2.7 Anzeige der Vorlagen

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.

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.

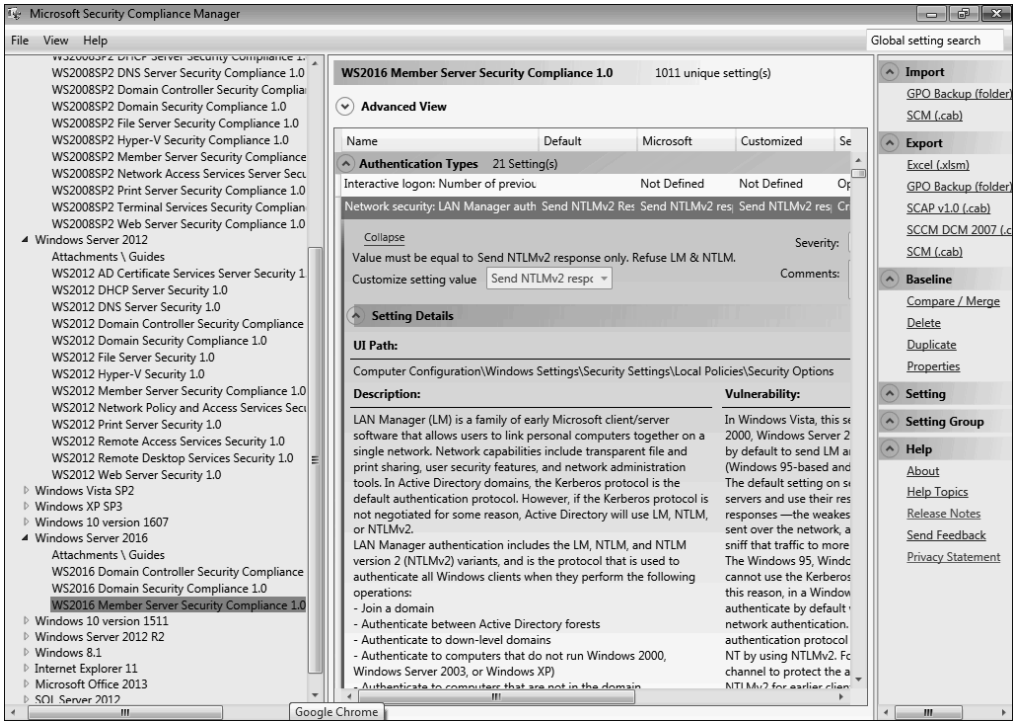

Abbildung 2.8 Sicherheitsoptionen für Windows Server 2016

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.

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.

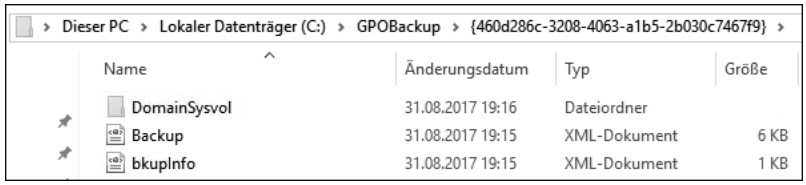

Abbildung 2.9 Inhalt des Backup-Ordners

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\Administrator> New-GPO -Name "WS2012-CA"
Import-GPO -Path 'C:\GPOBackup\' -BackupId '460d286c-3208-4063-a1b5-2b030c7467f9' -TargetName "WS2012-CA"


DisplayName      : WS2012-CA
DomainName       : training.corp.ichkanngarnix.de
Owner            : TRAINING\Domänen-Admins
Id               : 7e0b899e-4c70-4d5d-8019-83c17227aaec
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 31.08.2017 19:44:17
ModificationTime : 31.08.2017 19:44:18
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :

DisplayName      : WS2012-CA
DomainName       : training.corp.ichkanngarnix.de
Owner            : TRAINING\Domänen-Admins
Id               : 7e0b899e-4c70-4d5d-8019-83c17227aaec
GpoStatus        : UserSettingsDisabled
Description      :
CreationTime     : 31.08.2017 19:44:17
ModificationTime : 31.08.2017 19:44:18
UserVersion      : AD Version: 1, SysVol Version: 1
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :
```

Abbildung 2.10 Import der Gruppenrichtlinie

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.

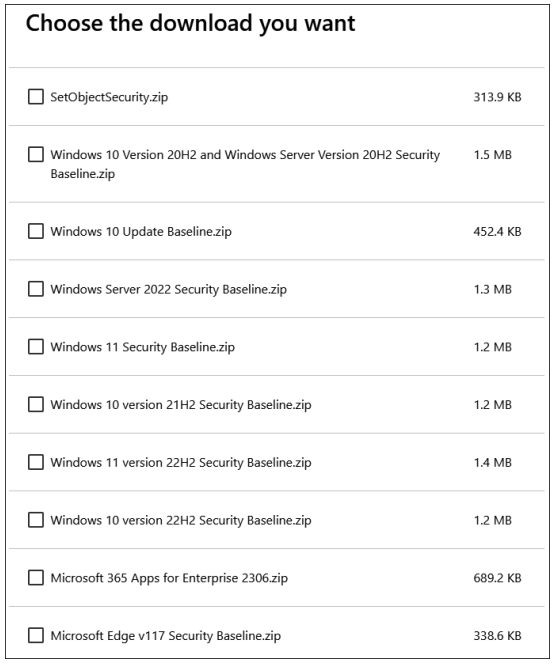

Abbildung 2.12 Auszug aus dem Inhalt des Security Compliance Toolkits

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

- Richtlinien für die aktuellen Betriebssysteme
- Richtlinien für Anwendungen
- Local GPO Tool (LGPO)
- Policy Analyzer sowie weiteren Scripts und Werkzeugen

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.

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

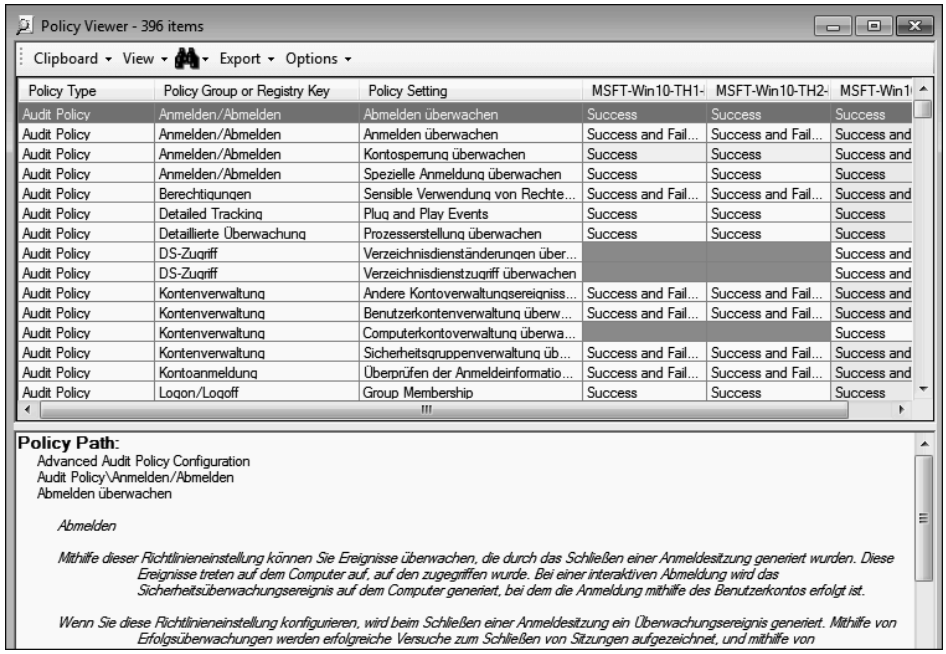

Abbildung 2.13 Informationen zu den empfohlenen Einstellungen

2.3 Notwendige Rechte für die Installation einer Zertifizierungsstelle

Damit Sie die Rollendienste auf einem Server installieren können, müssen Sie über lokale Administratorrechte verfügen. Dieses Recht ist bereits ausreichend, wenn Sie eine eigenständige Zertifizierungsstelle installieren möchten. Wollen Sie stattdessen eine Unternehmenszertifizierungsstelle installieren, die ins Active Directory integriert ist, benötigen Sie zusätzlich Rechte im Active Directory.

Die Elemente, die für das AD relevant sind, werden in der Konfigurationspartition der Datenbank unter dem Container SERVICES\PUBLIC KEY SERVICES abgelegt.

Wenn Sie sich die Objekte anzeigen lassen möchten, können Sie jeden beliebigen LDAP-Browser verwenden. Die einfachste Methode ist die Verwendung der integrierten Konsole *Active Directory Standorte und Dienste* (`dssite.msc`). Hier können Sie – nachdem Sie über ANSICHT • DIENSTKNOTEN ANZEIGEN die Ansicht erweitert haben – die gewünschten Elemente sehen (siehe Abbildung 2.14)

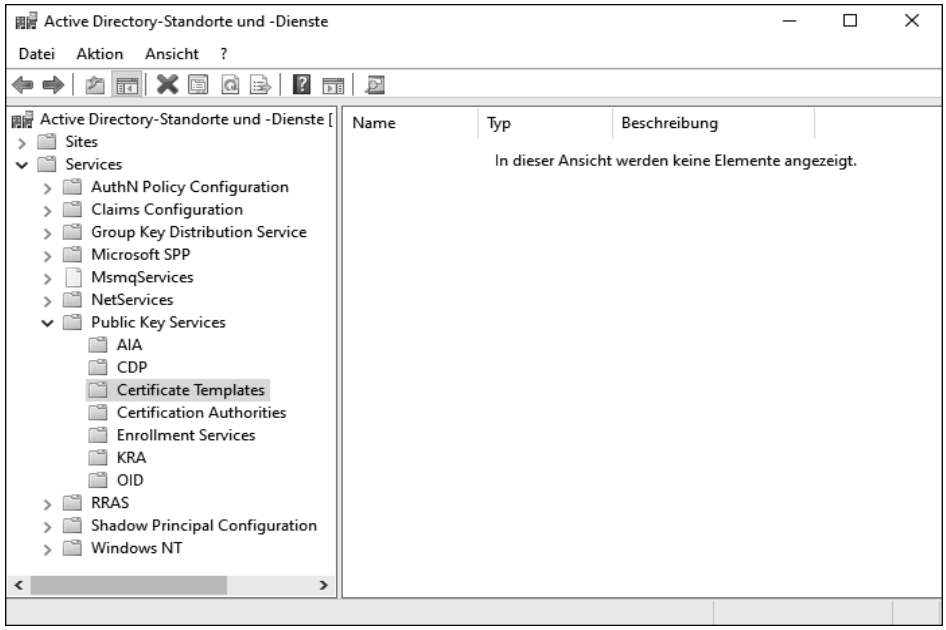

Abbildung 2.14 Anzeige der Container für die Aufnahme der CA-Konfigurationen

Wurde noch keine AD-integrierte Zertifizierungsstelle installiert, sind die Container unterhalb von PUBLIC KEY SERVICES vermutlich leer. Nach der Installation des Active Directory hat standardmäßig nur die Gruppe der Organisations-Admins (Enterprise Admins) das Recht, hier Konfigurationen vorzunehmen (siehe Abbildung 2.15). Dies würde bedeuten, dass ein Konto (ein Administrator), das eine Zertifizierungsstelle installieren und verwalten soll, Mitglied dieser hochprivilegierten Gruppe mit sehr weitreichenden Rechten sein muss.

Um die Sicherheit zu erhöhen und mit möglichst wenigen Rechten zu administrieren, sollten Sie auf dem Container *Public Key Services* die Gruppe berechtigen, die für die Verwaltung der Zertifizierungsstelle(n) zuständig ist.

Beim Aufbau eines Tier-Modells würde ich immer versuchen, die Objekte (Computer, Gruppen, Dienstkonten), die zu einer bestimmten Rolle gehören, in einer eigenen

Organisationseinheitenstruktur zu platzieren, und dem Administrator der Rolle auch die Rechte gewähren, »seine« Objekte selbst zu verwalten. Damit kann ein Administrator einer Zertifizierungsstelle bei Bedarf selbst eine Gruppe anlegen und muss dafür nicht einen Active Directory-Admin kontaktieren oder sich zusätzliche weitreichendere Berechtigungen nehmen.

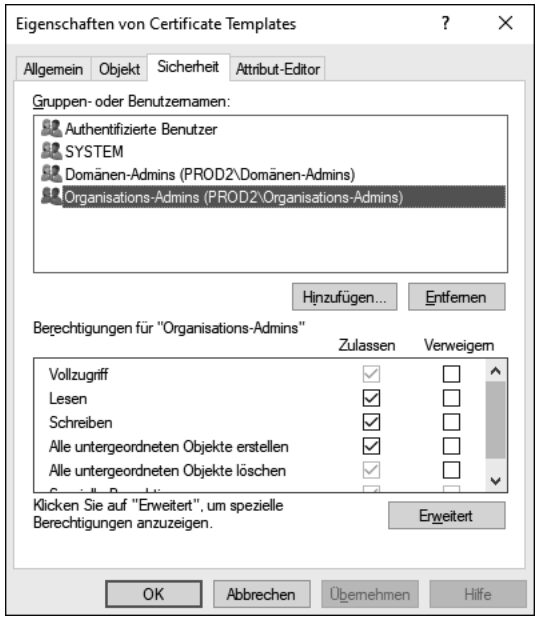

Abbildung 2.15 Gruppe mit Vollzugriff auf Certificate Templates

Weitere Informationen zum Aufbau eines Tier-Modells finden Sie im Buch »Sichere Windows-Infrastrukturen«, das unter der ISBN 978-3-8362-9249-8 beim Rheinwerk Verlag erschienen ist.

ORAZertifikatdienste ist die Gruppe, die für die Verwaltung verwendet wird. Neben lokalen Administratorrechten auf allen Servern, die zu der Rolle *Zertifikatdienste* gehören, sind im Active Directory Rechte delegiert worden, sodass die Gruppe unterhalb der OU *Gruppen* (siehe Abbildung 2.16) Gruppen erstellen darf und unterhalb der anderen OUs (*Server* und *ServiceAccounts*) die jeweiligen Objekttypen anlegen und verwalten darf. Bei der Namenswahl bedeutet die 0, dass es sich um eine Tier-0-Gruppe handelt und damit nur andere Tier-0-Objekte Mitglied sein dürfen. Das »RA« steht für *Rollenadministratoren* und das »Zertifikatdienste« für den Namen der Rolle – so wie im Rollen- und Rechtekonzept definiert.

Das Anlegen der Rolle im Tier-Modell sowie die Delegierung der Rechte müssen mit einem Konto erfolgen, das Mitglied der Gruppe der Administratoren (oder Domänen-Admins oder Organisations-Admins) ist.

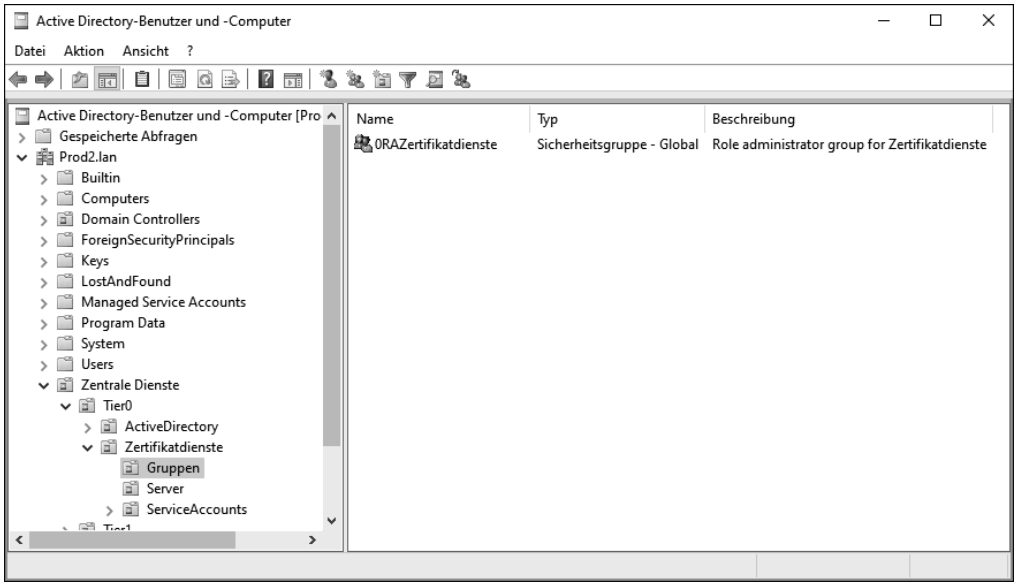

Abbildung 2.16 OU-Aufbau der Rolle »Zertifikatdienste« mit der Administrationsgruppe für die Zertifikatdienste

In der Konsole *Standorte und Dienste* kann nun auf dem Container Public Key Services die Gruppe berechtigt werden. Klicken Sie dazu mit der rechten Maustaste auf PUBLIC KEY SERVICE, und wählen Sie EIGENSCHAFTEN. Wechseln Sie zu der Registerkarte SICHERHEIT, und klicken Sie auf ERWEITERT. Hier können Sie nach einem Klick auf HINZUFÜGEN den Prinzipal (*0RAZertifikatdienste*) auswählen und die Berechtigung auf Vollzugriff setzen. Stellen Sie sicher, dass im Dropdown-Fenster ANWENDEN die Option DIESES UND ALLE UNTERGEORDNETEN OBJEKTE ausgewählt ist (siehe Abbildung 2.17). Bestätigen Sie die Einstellung mit OK, und schließen Sie die Eigenschaften durch zweimal OK.

Abbildung 2.17 Konfiguration der notwendigen Rechte

Bei der Installation und Konfiguration der Rolle werden Windows-interne Gruppen bearbeitet. Dies betrifft die Gruppe *Zertifikatherausgeber* (siehe Abbildung 2.18), die

im Standard-Container mit dem Namen *Users* platziert ist. Hier hat der Administrator der Zertifikatdienste (*ORAZertifikatdienste*) üblicherweise keine Rechte und kann die Mitgliedschaft der Gruppe nicht anpassen. Daher bietet es sich an, dass ein Administrator mit Active Directory-Rechten die Gruppe in die OU der Zertifikatdienste verschiebt (*Tier0\Zertifikatdienste\Gruppen*).

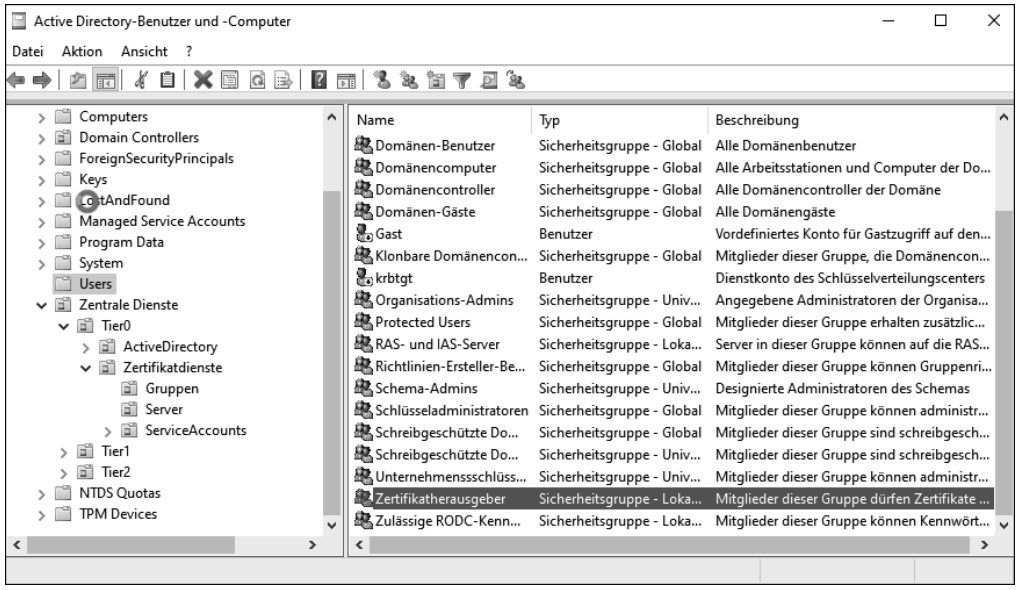

Abbildung 2.18 Der »Wohnort« der Gruppe »Zertifikatherausgeber«

Wird die Installation und Konfiguration der Zertifizierungsstelle nun mit den delegierten Rechten durchgeführt, kann das Mitglied der Gruppe *ORAZertifikatdienste* die Rolle installieren und eine Unternehmenszertifizierungsstelle einrichten. Am Ende des Assistenten werden jedoch Warnungen angezeigt (siehe Abbildung 2.19):

- Die erste Meldung betrifft die Gruppe *Zertifikatherausgeber*, die vor der Konfiguration nicht in die OU der Zertifikatdienste verschoben wurde. Die Konsequenz der fehlenden Mitgliedschaft ist, dass die Zertifizierungsstelle keine Zertifikate im Active Directory veröffentlichen kann. Die Gruppenmitgliedschaft kann nach der Konfiguration angepasst werden. Damit die Berechtigung dann greift, muss der Server neu gestartet werden.
- Die zweite Meldung betrifft die Gruppe *Prä-Windows 2000 kompatibler Zugriff*, die sich im Built-in-Container befindet. Diese Gruppe sollte auch an diesem Ort verbleiben und durch einen Active Directory-Administrator angepasst werden. Die Mitgliedschaft wird gemäß Beschreibung der Fehlermeldung dazu verwendet, die Rollentrennung auf der Zertifizierungsstelle umzusetzen.

- Die letzte Meldung beschreibt den Umstand, dass die Standard-Zertifikatvorlagen nicht unterhalb von Standorten und Diensten erstellt werden konnten, da das Konto bzw. die verwendete Gruppe nicht als Besitzer eingetragen werden konnte. Dadurch sind keine Zertifikatvorlagen vorhanden.

Abbildung 2.19 Drei Warnhinweise nach der Konfiguration der Zertifizierungsstelle

Die notwendige Installation der Zertifikatvorlagen kann mithilfe des `CertUtil`-Kommandozeilentools erfolgen. Führen Sie als ein Administrator, der Mitglied der *ORA-Zertifikatdienste* ist, nach der Delegierung den folgenden Befehl aus, wird die gleiche Fehlermeldung ausgegeben.

```
Microsoft Windows [Version 10.0.26052.1000]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Opeterkloep>CertUtil -installdefaulttemplates
CertUtil: -InstallDefaultTemplates-Befehl ist fehlgeschlagen: 0x8007051b
(WIN32: 1307 ERROR_INVALID_OWNER)
CertUtil: Diese Sicherheitskennung kann nicht als Besitzer des Objekts
zugeordnet werden.
```

Listing 2.1 Fehlermeldung beim Ausführen von CertUtil

CertUtil ist ein Kommandozeilentool, das in jedem Windows-Betriebssystem verfügbar ist und direkt verwendet werden kann. Damit nun die Zertifikatvorlagen angelegt werden, muss ein Administrator der Domäne (z. B. auf einem Domänencontroller) den Befehl ausführen:

```
C:\>CertUtil -installdefaulttemplates
CertUtil: -InstallDefaultTemplates-Befehl wurde erfolgreich ausgeführt.
```

Listing 2.2 Erfolgreiches Installieren der Standardvorlagen

Durch den Befehl werden im Container *Certificate Templates* des Active Directory (siehe Abbildung 2.14) die Standardvorlagen bereitgestellt, aus denen dann im weiteren Verlauf neue Vorlagen erstellt werden können. Abbildung 2.20 zeigt die Berechtigungen auf den Standardvorlagen. Hier ist zu erkennen, dass die Vererbung der Berechtigungen deaktiviert ist und nur Domänen-Admins oder Organisations-Admins die Objekte verwalten dürfen.

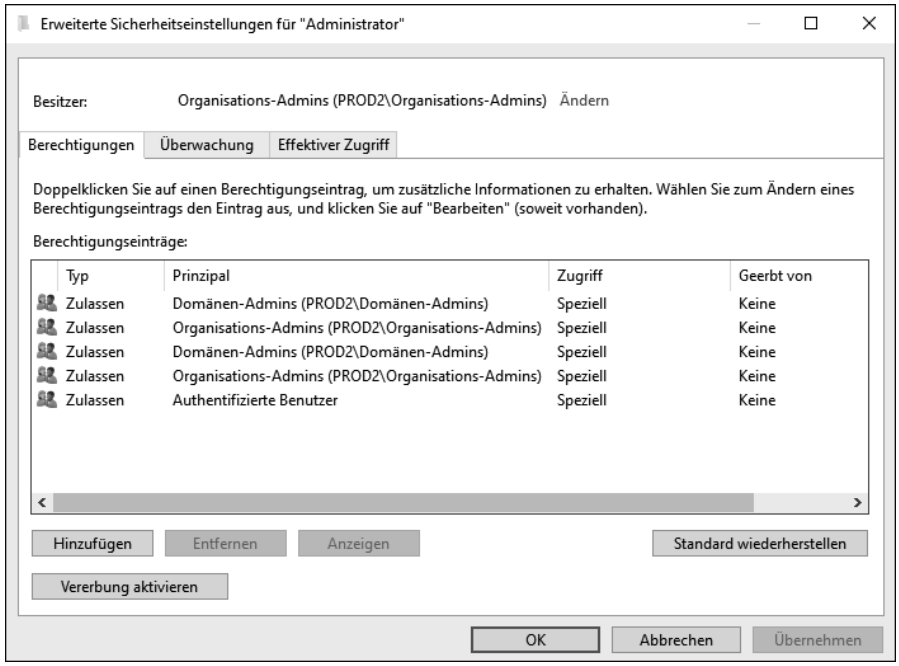

Abbildung 2.20 Ansicht der Berechtigungen auf den Zertifikatvorlagen

Mithilfe eines PowerShell-Scriptes kann ein Active Directory-Administrator nach dem Erstellen der Standardvorlagen direkt (und einmalig) die notwendigen Berechtigungen setzen. Dazu kann entweder das Recht *Lesen und Schreiben* an die Gruppe (*ORAZertifikatdienste*) delegiert werden, oder Sie verwenden einfach dieses Script:

```
###Set CerttemplateACL
$RoleAdminGroup="ORAZertifikatdienste"

$AllCertTemplates=Get-ChildItem "AD:\CN=Certificate Templates,CN=Public Key
Services,CN=Services,$((Get-ADRootDSE).configurationNamingContext)"
$RAGroup=(Get-ADGroup $RoleAdminGroup).sid.value
Foreach ($template in $AllCertTemplates)
{
  Write-Host "Working on Template: $($template.name)" -BackgroundColor Green
  $acl=Get-Acl "AD:\$(($template).distinguishedname)"
  ###Add Read/Write to RoleAdminGroup
  $newsddl=$acl.Sddl+"(A;;LCRPWPRCWDWO;;;$($RAGroup))"
  $acl.SetSecurityDescriptorSddlForm($newsddl)
  Set-Acl -aclObject $acl "AD:\$($template)"
}
```

Listing 2.3 Setzen der Berechtigungen für die Zertifikatvorlagen

Nach der Ausführung des Scriptes sind die *ORAZertifikatdienste* mit den notwendigen Rechten auf den bestehenden Vorlagen ausgestattet (siehe Abbildung 2.21) und können sowohl die alten Vorlagen verwalten als auch neue Vorlagen erstellen. Wird eine bestehende Vorlage dupliziert, werden die vorhandenen Rechte mit übernommen.

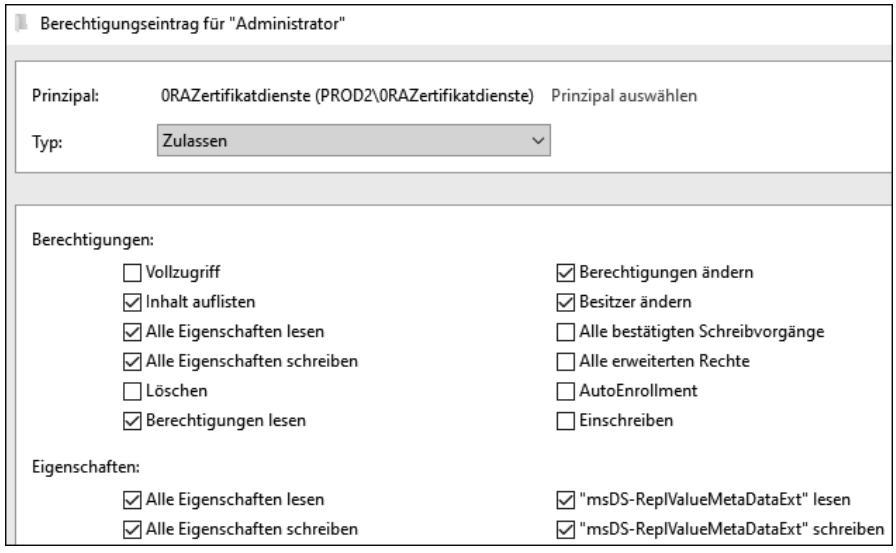

Abbildung 2.21 Delegierte Rechte an die Gruppe »0RAZertifikatdienste«

Damit sind alle notwendigen Rechte delegiert bzw. die notwendigen Konfigurationen durch einen AD-Administrator vorgenommen worden.

Konfiguration der Richtliniendienste (CEP/CES) kann nicht komplett delegiert werden

Wenn Sie den Zertifikatregistrierungsrichtlinien-Webdienst (CEP) oder den Zertifikatregistrierungs-Webdienst (CES) konfigurieren möchten, benötigen Sie zu den Rechten auf dem Server ebenfalls Rechte im Active Directory, die nicht delegiert werden können. Wenn Sie das Tier-Modell wie oben beschrieben einsetzen sollten, muss das Konto für die Konfiguration neben der Rolle 0RAZertifikatdienste auch die Rolle 0RAActiveDirectory besitzen. Nach der Konfiguration der Rolle kann das Recht wieder entfernt werden.

Schauen wir uns nun die Installation etwas genauer an.

2.4 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 2.22). 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.

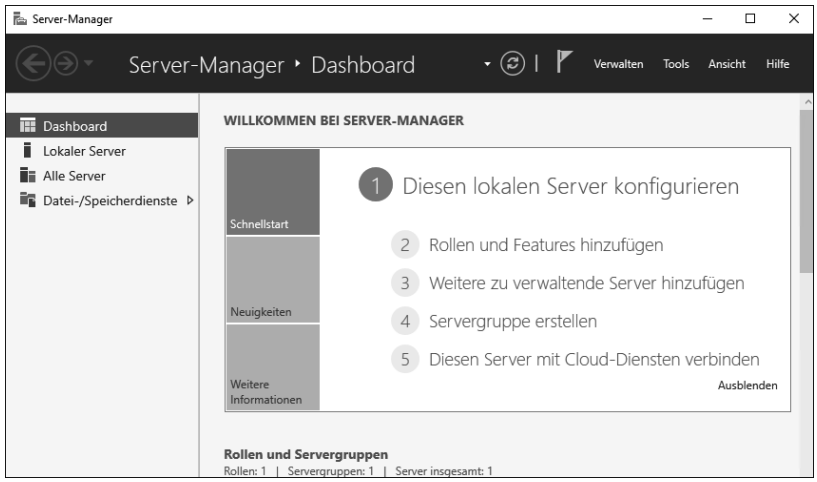

Abbildung 2.22 Der Server-Manager unter Windows Server 2016

Für die Installation der Rolle gibt es keine Unterschiede zwischen Windows Server 2012 R2 und den darauffolgenden Versionen. 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 2.23). 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.

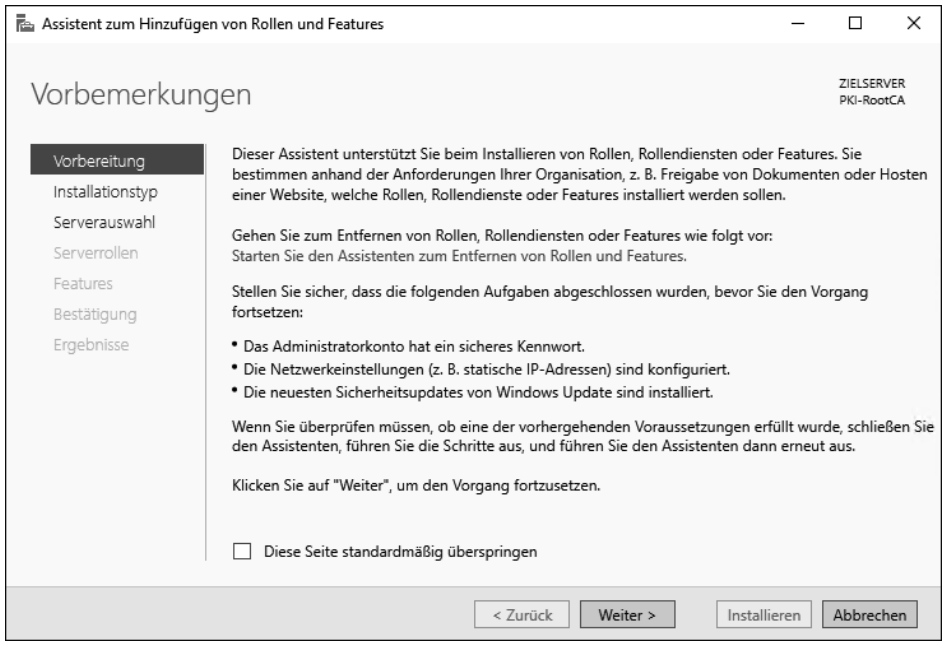

Abbildung 2.23 Der Installationsassistent gibt Empfehlungen.

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 2.24).

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 2.25).

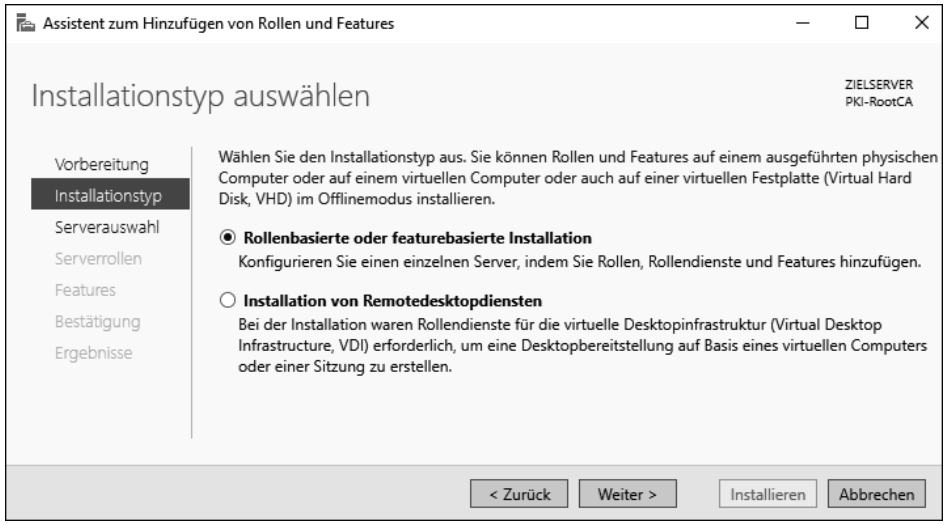

Abbildung 2.24 Auswahl, ob Rollen und Features oder die Remotedesktopdienste installiert werden sollen

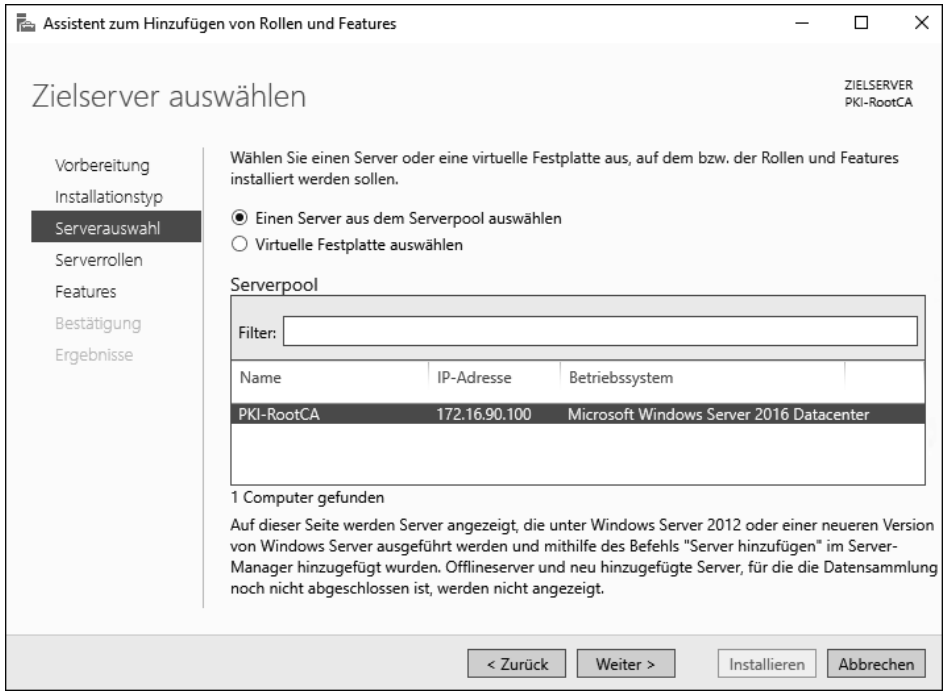

Abbildung 2.25 Auswahl des Servers oder einer virtuellen Festplatte

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.

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 2.26). Im Assistenten zur Installation von Rollen und Features können Sie keine Rollen und Features entfernen.

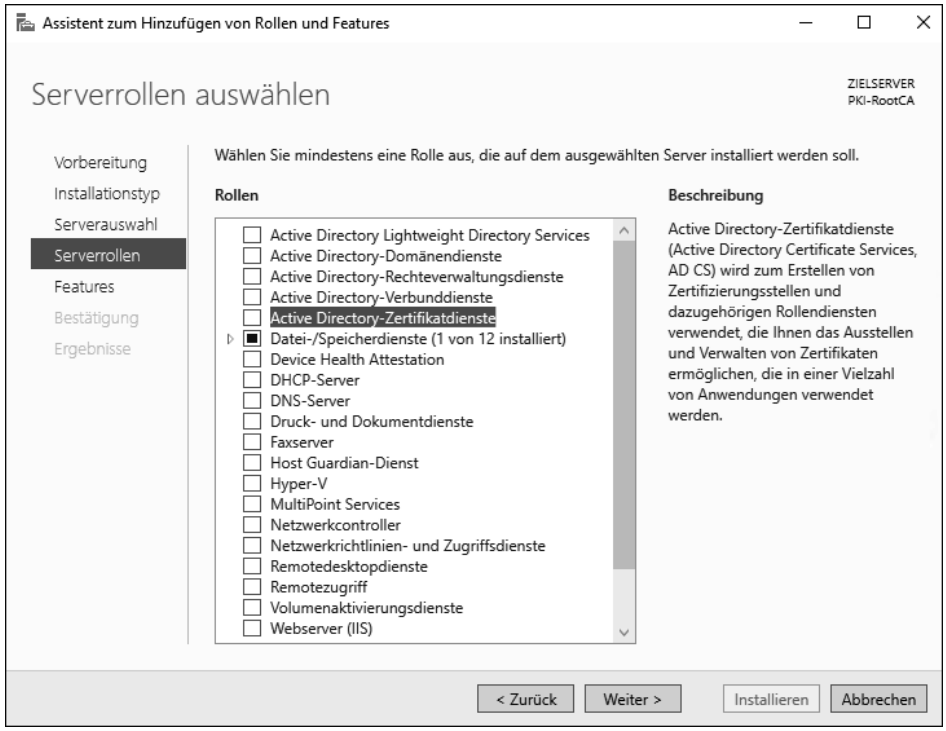

Abbildung 2.26 Auflistung der verfügbaren Rollen auf einem Windows Server

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 2.27, 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.

Abbildung 2.27 Installation der Verwaltungstools

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

Werden die Zertifikatdienste (siehe Abbildung 2.28) 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.

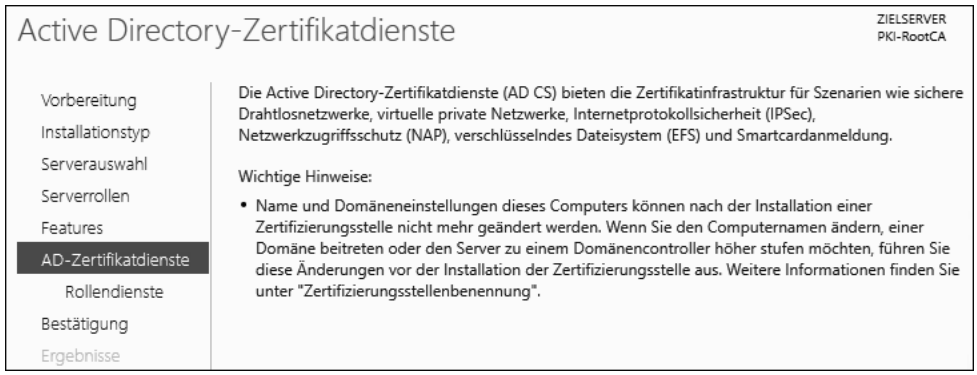

Abbildung 2.28 Informationen zu den Zertifikatdiensten

Vorsicht bei SConfig

Wenn Sie einen Server Core einsetzen (siehe Abschnitt 2.8) 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 2.29):

- 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«).

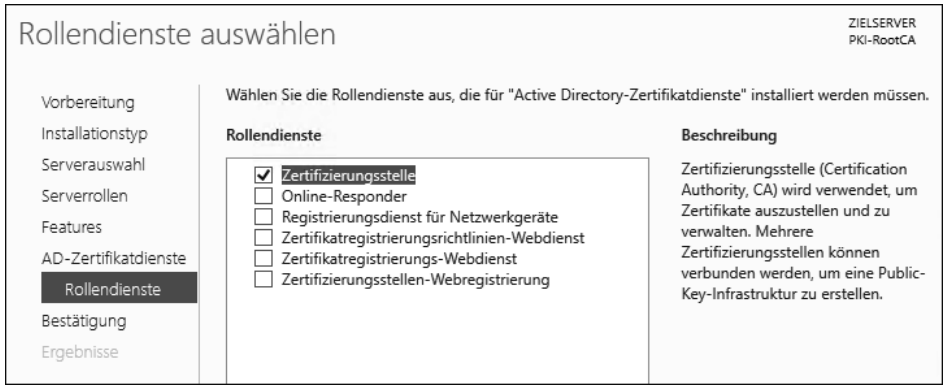

Abbildung 2.29 Rollendienste der Zertifikatdienste

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 2.30).

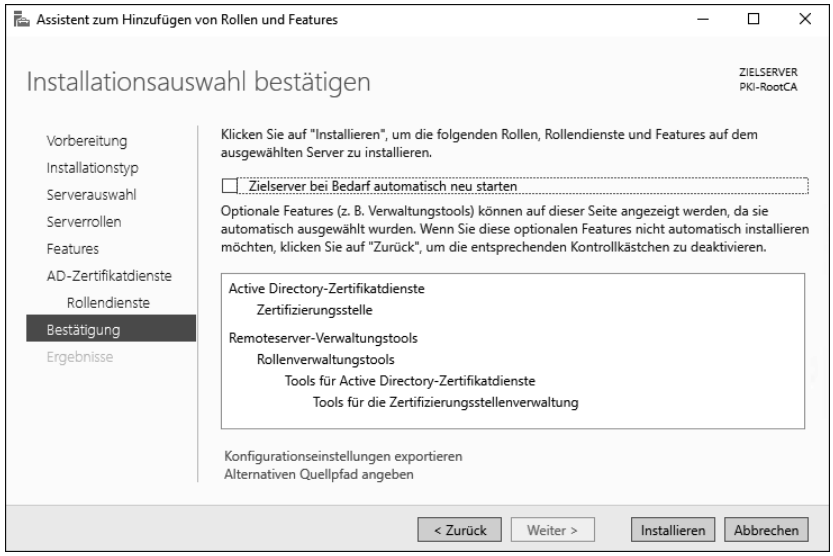

Abbildung 2.30 Bestätigung der Installationsauswahl

Der Fortschritt der Installation wird im Assistenten angezeigt (siehe Abbildung 2.31).

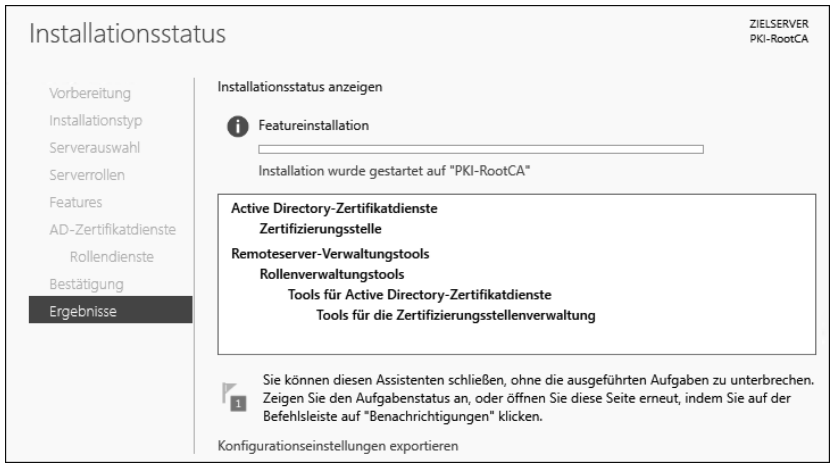

Abbildung 2.31 Anzeige des Fortschritts der Installation

Ist die Installation abgeschlossen, wird eine Zusammenfassung wie in Abbildung 2.32 angezeigt.

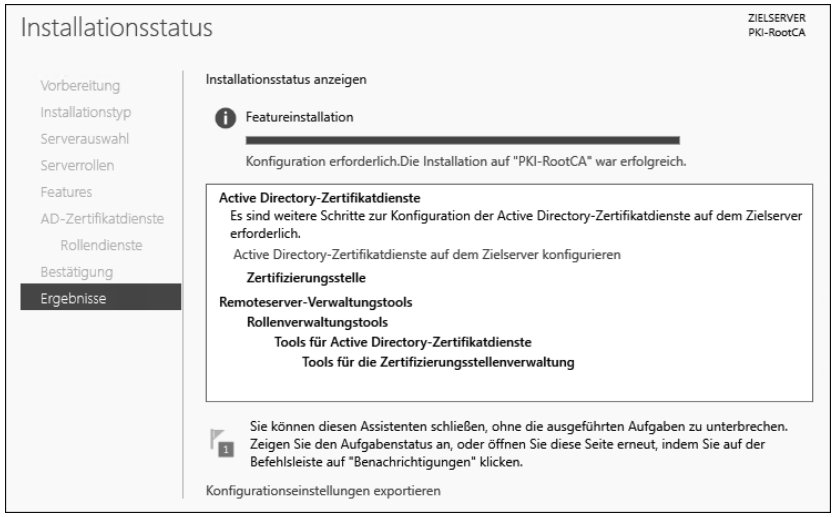

Abbildung 2.32 Zusammenfassung der Installation

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 2.33).

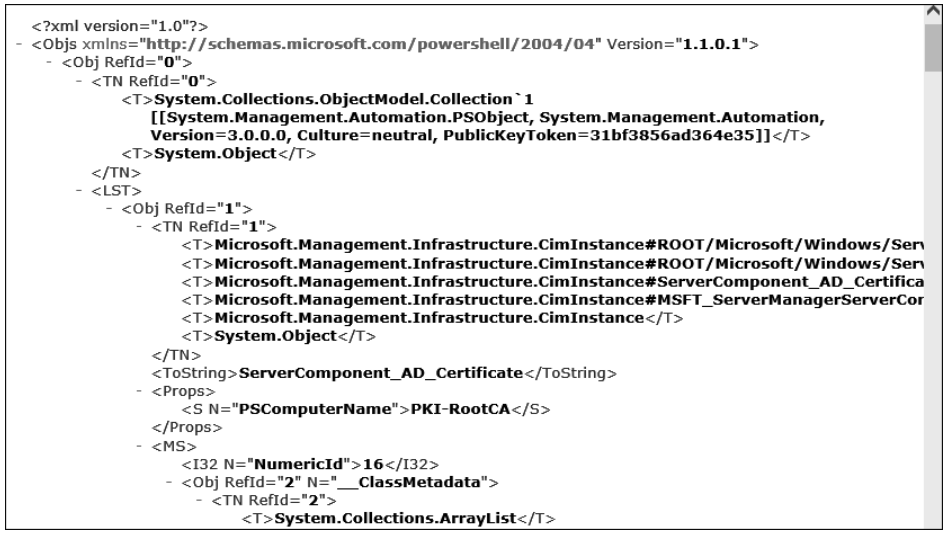

Abbildung 2.33 Die vom Assistenten erstellte XML-Datei

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 2.4 Installation auf einem Server

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

Listing 2.5 Installation auf mehreren Servern

2.4.1 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 2.34 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 2.34 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 2.35).

```
PS C:\> (Get-WindowsFeature AD-Certificate).subfeatures
ADCS-Cert-Authority
ADCS-Online-Cert
ADCS-Device-Enrollment
ADCS-Enroll-Web-Pol
ADCS-Enroll-Web-Svc
ADCS-Web-Enrollment
```

Abbildung 2.35 Anzeigen der Rollendienste mithilfe der PowerShell

Bei der Installation mithilfe der PowerShell tritt häufig der Fehler auf, den Sie in Abbildung 2.36 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-WindowsFeature AD-Certificiate,ADCS-Online-Cert -IncludeAllSubFeature
Install-WindowsFeature : ArgumentNotValid: Die Rolle, der Rollendienst oder der Featurename ist ungültig:
"AD-Certificiate". Der Name wurde nicht gefunden.
In Zeile:1 Zeichen:1
+ Install-WindowsFeature AD-Certificiate,ADCS-Online-Cert -IncludeAllSu ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (AD-Certificiate:String) [Install-WindowsFeature], Exception
    + FullyQualifiedErrorId : NameDoesNotExist,Microsoft.Windows.ServerManager.Commands.AddWindowsFeatureCommand

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
False   No             InvalidArgs    {}
```

Abbildung 2.36 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 PowerShell-Konsolen nicht automatisch mit Administratorrechten ausgeführt. Dies führt dazu, dass Sie – obwohl Sie zur Gruppe der Administratoren gehören – nur mit »normalen« 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 2.37).

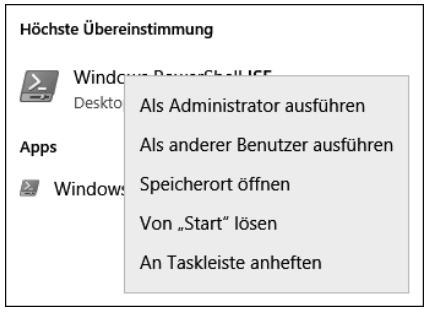

Abbildung 2.37 Ausführen der »PowerShell ISE« als Administrator

Wenn Sie die Konfiguration der Benutzerkontensteuerung (siehe Abbildung 2.38) 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 • Sicherheitseinstellungen • Lokale Richtlinien • Sicherheitsoptionen.

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

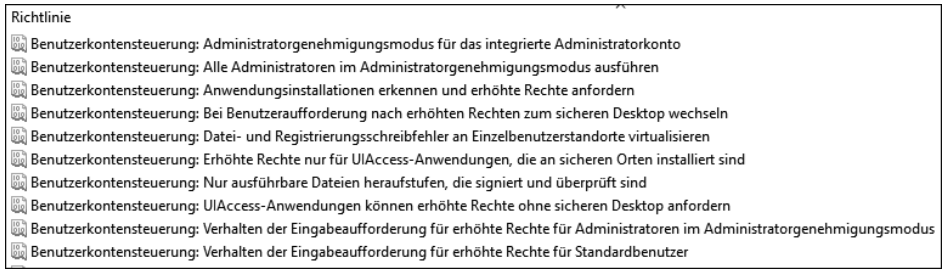

Abbildung 2.38 Konfiguration der Benutzerkontensteuerung mithilfe von Richtlinien

Standardmäßig werden im Bereich Ereignisse (siehe Abbildung 2.39) 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.

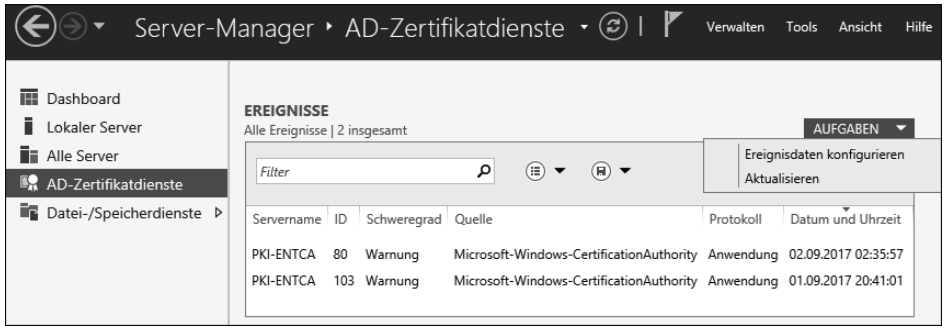

Abbildung 2.39 Der Bereich »Ereignisse« zeigt Meldungen aus der Ereignisanzeige des Dienstes an.

Der Bereich Dienste (siehe Abbildung 2.40) 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.

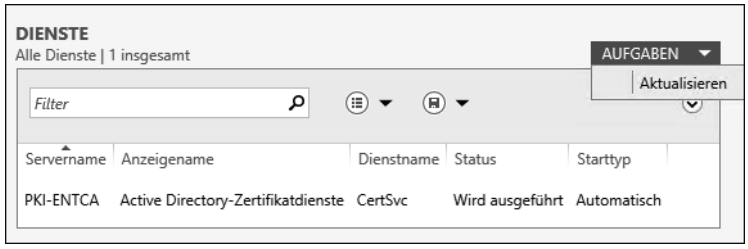

Abbildung 2.40 Anzeige der Dienste, die zu einer Rolle gehören

Der Best Practices Analyzer (BPA) des Server-Managers gleicht die Konfiguration der installierten Rolle mit den Konfigurationsempfehlungen von Microsoft ab (siehe Abbildung 2.41). Von Zeit zu Zeit werden die Regelwerke, die hinter dem BPA stecken, über Windows Update aktualisiert. Mit dem Menüpunkt BPA-Überprüfung starten lassen Sie den ausgewählten Dienst überprüfen. Anschließend werden die Ergebnisse angezeigt.

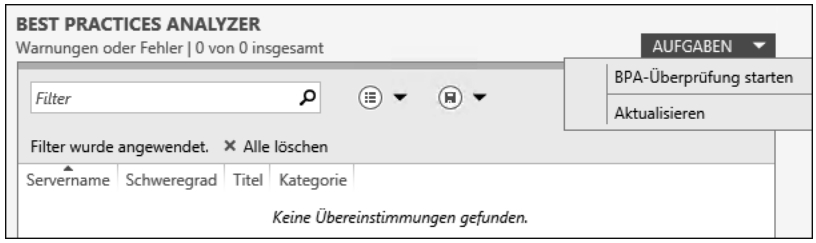

Abbildung 2.41 Der »Best Practices Analyzer« kann eine Rolle überprüfen.

Die *Leistungsanalyse* ist nach der Installation und Konfiguration des Servers nicht aktiv. Sie können sie durch einen Rechtsklick auf den Server • Leistungsindikatoren starten aktivieren. Die Leistungsanalyse sammelt dann Leistungsdaten des Servers (siehe Abbildung 2.42).

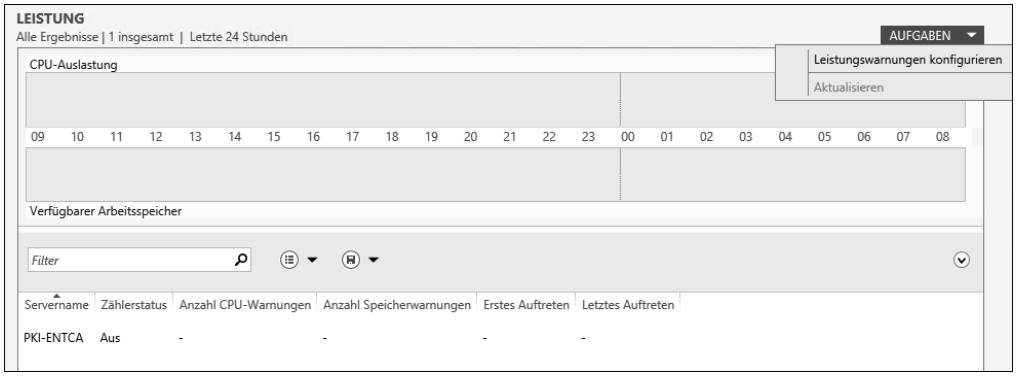

Abbildung 2.42 Abfrage der Leistungsdaten des Servers

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 2.43). Hier startet der normale Assistent zum Hinzufügen oder der Assistent zum Entfernen von Rollen.

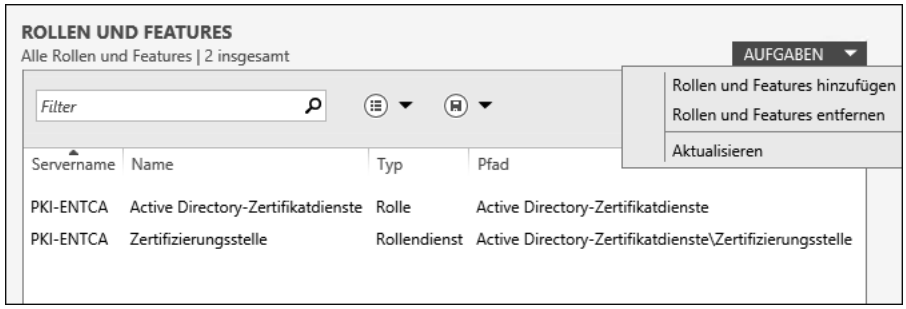

Abbildung 2.43 Hinzufügen und Entfernen von Rollen und Features

2.4.2 Installation der Rolle über das Windows Admin Center

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

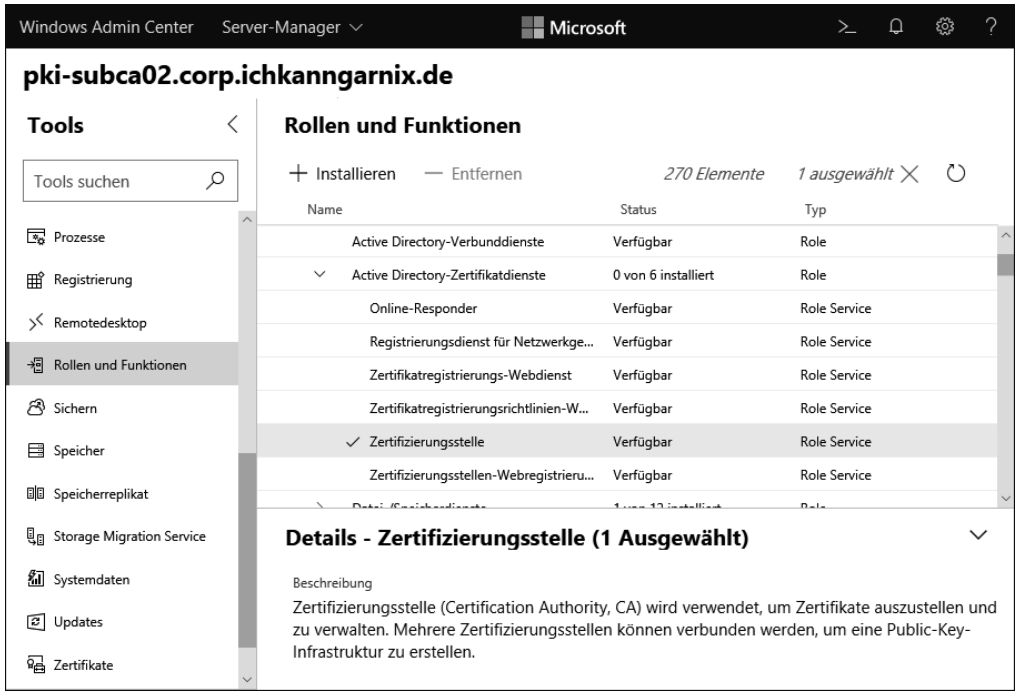

Abbildung 2.44 Installation der Rollendienste mithilfe des Windows Admin Centers

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.

2.4.3 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 2.45).

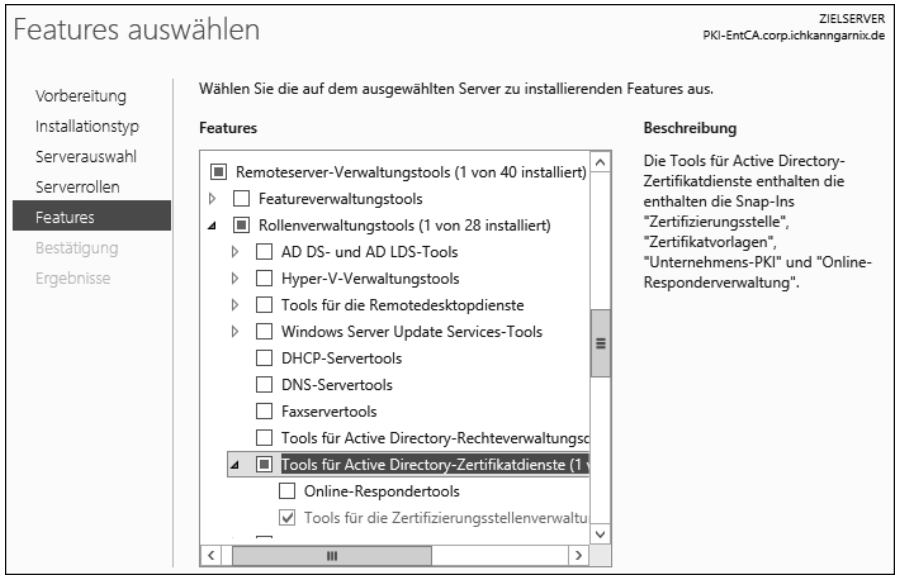

Abbildung 2.45 Remoteserver-Verwaltungstools für die Zertifizierungsstelle

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

```
[ ] Tools für Active Directory-Rechteverwalt... RSAT-ADRMS
[ ] Tools für Active Directory-Zertifikatdie... RSAT-ADCS
    [ ] Online-Respondertools                   RSAT-Online-Responder
    [ ] Tools für die Zertifizierungsstellen... RSAT-ADCS-Mgmt
[ ] Tools für Dateidienste                      RSAT-File-Services
```

Abbildung 2.46 RSAT-Tools in der PowerShell

Die Remoteserver-Verwaltungstools (*Remote Server Administration Tools* (RSAT), siehe Abbildung 2.46) 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. Verwenden Sie Windows Server 2016 oder Windows Server 2019, sollten Sie als Client Windows 10 in der entsprechenden Version nutzen. Das Äquivalent zu Windows Server 2022 ist Windows 11.

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 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)
- **Windows 11 –** Gleiche Verteilmethode wie Windows 10 (nach 1809)

Nach der Installation des Update-Paketes (siehe Abbildung 2.47) sollten Sie prüfen, ob die Verwaltungstools verfügbar sind. In früheren Versionen von Windows-Betriebssystemen mussten die einzelnen Tools separat installiert werden.

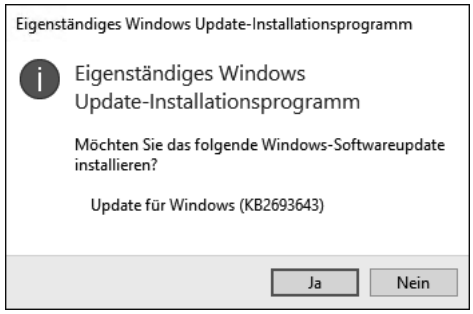

Abbildung 2.47 Installation der RSAT unter Windows 10 (vor 1809)

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 Programme und Features verwaltet. Möchten Sie dieses Tool (Systemsteuerung • Programme • Programme und Features, siehe Abbildung 2.48) über die Kommandozeile öffnen, können Sie mit dem Befehl `appwiz.cpl` den *Application Wizard* direkt starten.

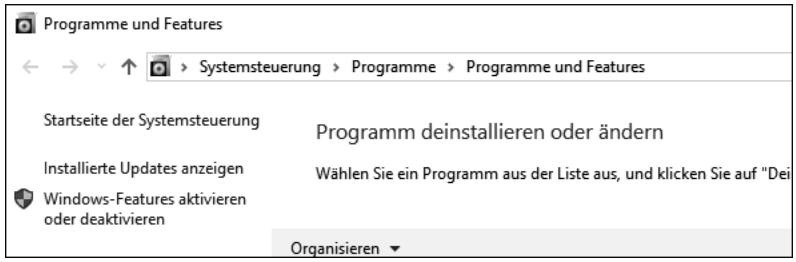

Abbildung 2.48 Sie können die Systemsteuerung verwenden, um die RSAT-Tools auf einem Client zu installieren.

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 2.49).

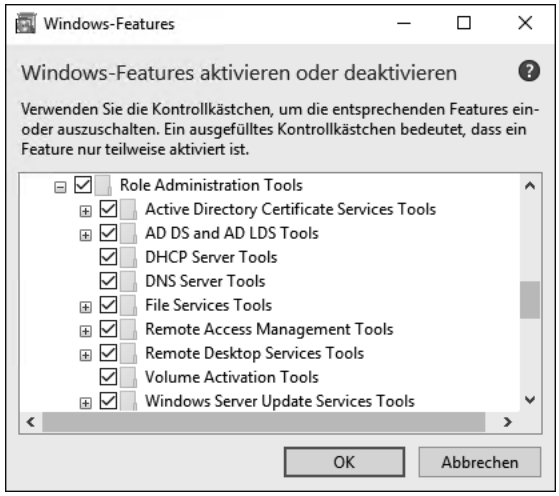

Abbildung 2.49 Übersicht der RSAT-Konsolen, die installiert sind

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 2.50).

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.

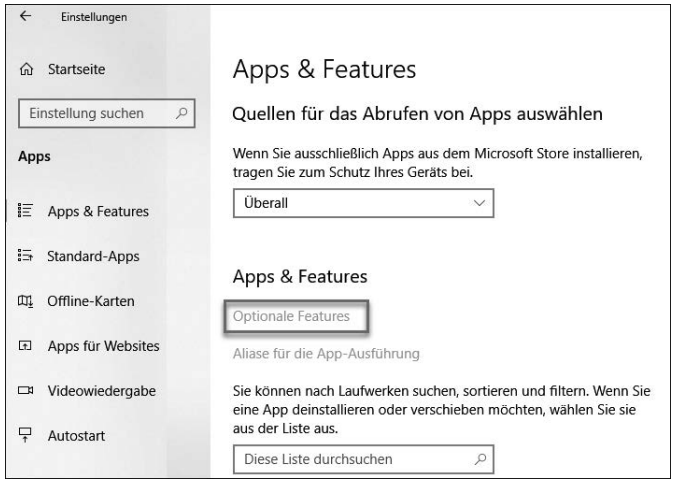

Abbildung 2.50 Option zum Installieren der »Optionalen Features«

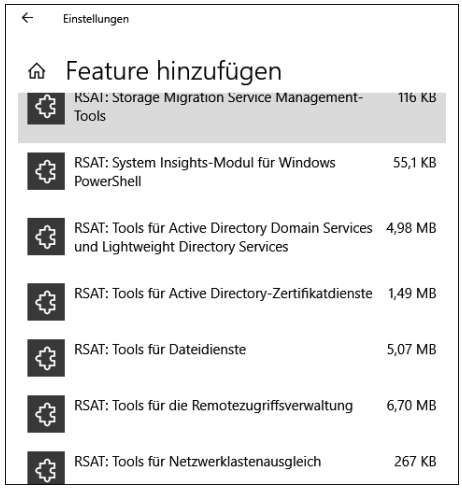

Abbildung 2.51 Auswahl des gewünschten Features

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

2.4.4 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=1.1.1.1.1.1.1
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.

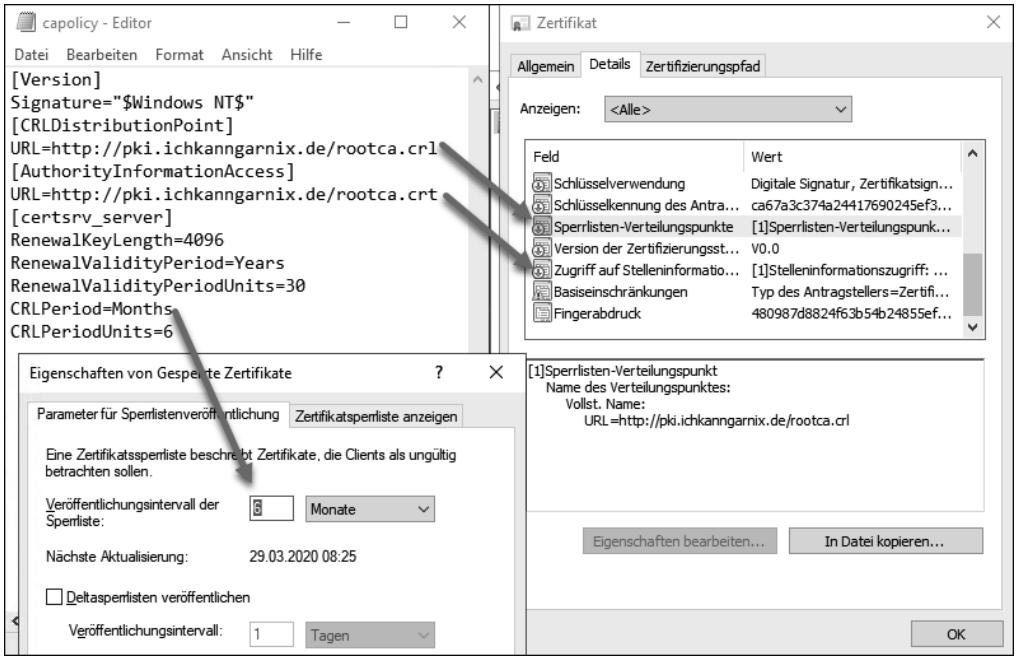

Abbildung 2.52 Der Zusammenhang zwischen der »CAPolicy.inf« und der Konfiguration in der Zertifizierungsstelle

In Abbildung 2.52 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 `CRLPeriodUnits` 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.

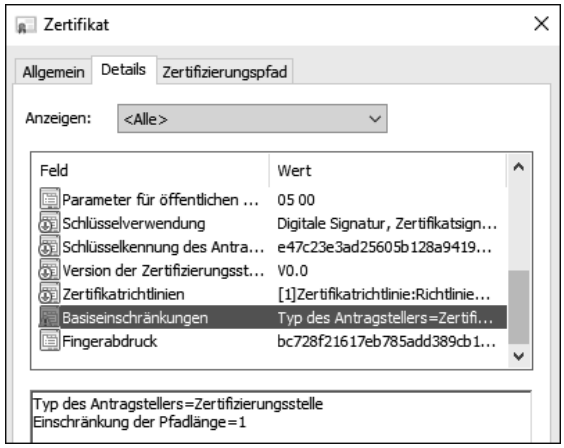

Abbildung 2.53 Auswirkung der konfigurierten Basiseinschränkung

Im Zertifikat der Zertifizierungsstelle wird eine Basiseinschränkung für die Pfadlänge definiert (siehe Abbildung 2.53). 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 2.54 sehen. Wenn die Pfadlänge 0 ist, können mit diesem Zertifikat – das ein CA-Zertifikat sein könnte – keine weiteren (untergeordneten) Zertifikate ausgestellt werden.

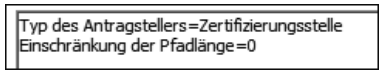

Abbildung 2.54 Auswirkung der Pfadlänge auf ausgestellte Zertifikate

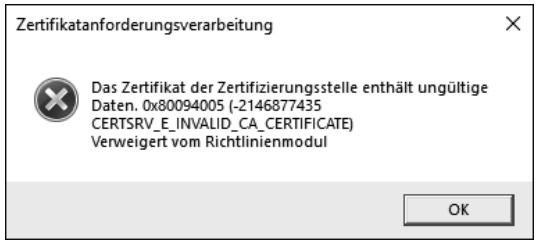

Abbildung 2.55 Anforderung eines Zertifikats auf einer Zertifizierungsstelle mit einer Pfadlänge von 0

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.

Wird nun auf einer Zertifizierungsstelle mit verbleibender Pfadlänge 0 ein Zertifikat angefordert, wird die Anfrage abgelehnt (siehe Abbildung 2.55) 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 2.6 Definition der Namenseinschränkung für eine Zertifizierungsstelle

Diese Einschränkung wird im CA-Zertifikat hinterlegt und kann dort unter den DETAILS abgerufen werden (siehe Abbildung 2.56).

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, 255.255.255.0** – gestattet IP-Adressen aus dem angegebenen Subnetz. Das Format ist: {IP-Netzwerkadresse },{Subnetzmaske}

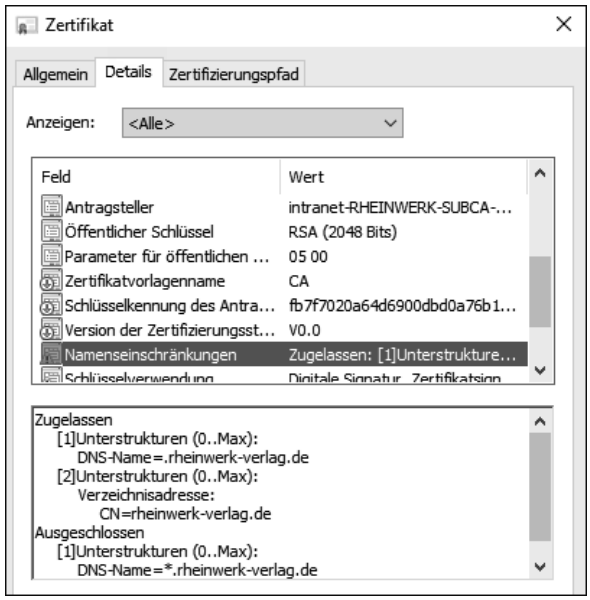

Abbildung 2.56 Im CA-Zertifikat hinterlegte Namenseinschränkungen

Wird nun ein Zertifikat angefordert, das gemäß der Namenseinschränkung nicht gestattet ist, wird die Anforderung mit einem Fehler abgelehnt wie in Abbildung 2.57.

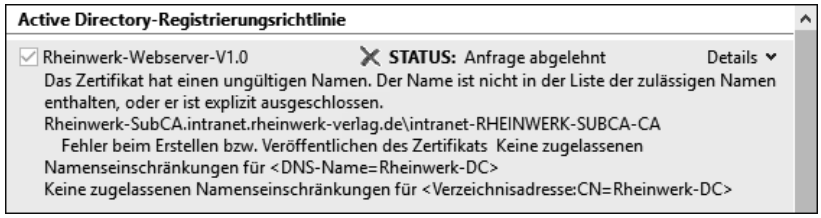

Abbildung 2.57 Verweigern eines Zertifikatrequests aufgrund falscher Namensinformationen

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.

2.5 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 Nutzerzertifikats	5 Jahre
Maximale Laufzeit der Zertifizierungsstelle	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 2.58 zeigt die Umgebung.

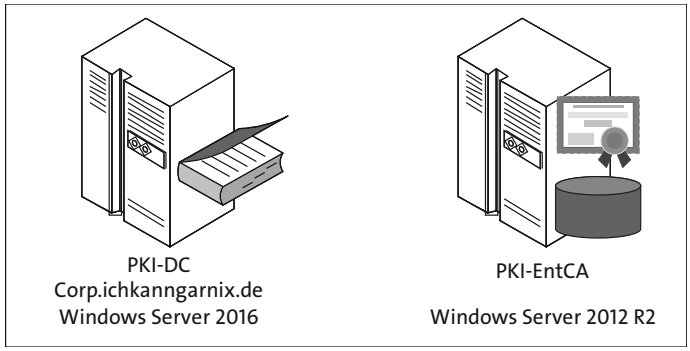

Abbildung 2.58 Konfiguration der »einfachen« Umgebung

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 2.4 beschrieben – mit dem Rollendienst *ADCS-Cert-Authority* installiert. Es wurden sonst keine Zusatzrollen installiert.

2.5.1 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 2.59) starten Sie einen Assistenten, der Sie durch die Konfiguration der Zertifizierungsstelle leitet (siehe Abbildung 2.60).

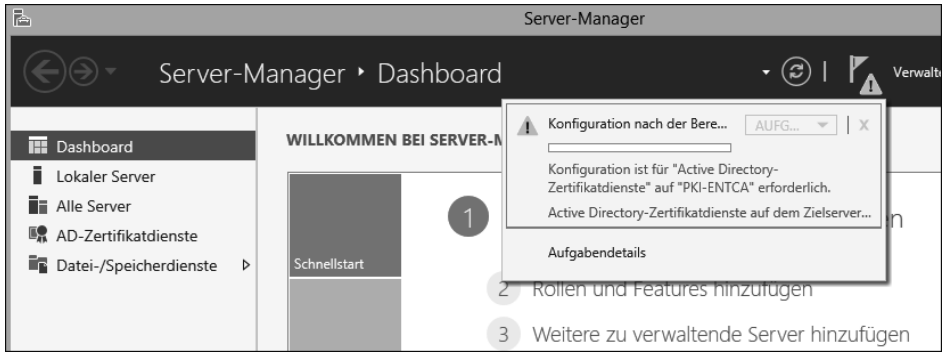

Abbildung 2.59 Hinweis im Server-Manager, dass die Konfiguration noch abgeschlossen werden muss

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.

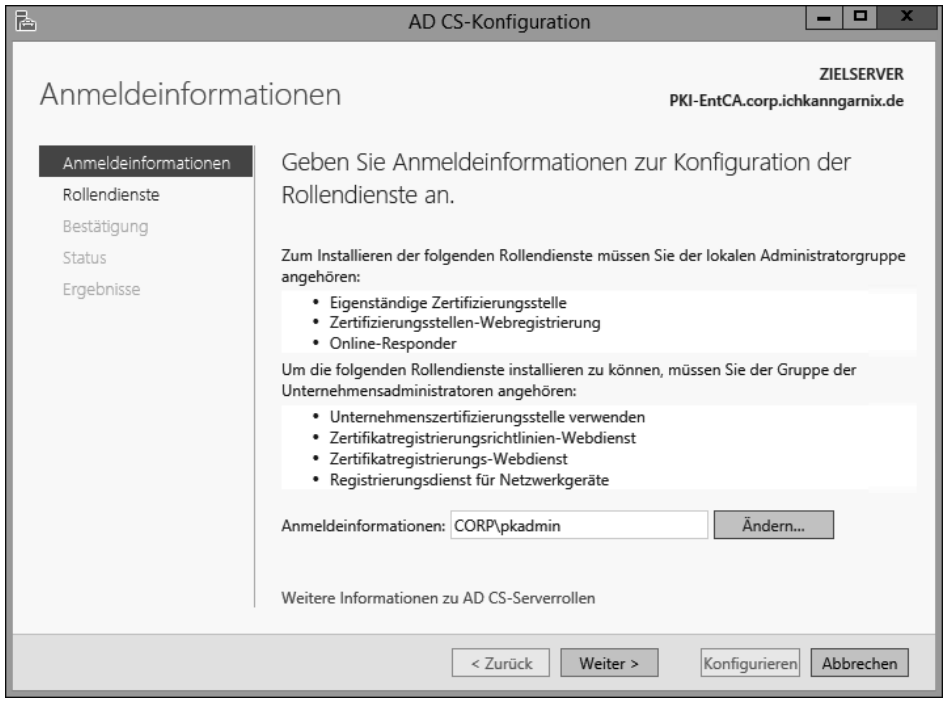

Abbildung 2.60 Festlegen des Kontos, mit dem die Konfiguration durchgeführt wird

Eine Zertifizierungsstelle gehört meistens zum Tier 0 (siehe *https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material*.

Nach der Konfiguration des zu verwendenden Kontos müssen Sie die Rollendienste auswählen, die im Assistenten konfiguriert werden sollen (siehe Abbildung 2.61).

Abbildung 2.61 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 2.61 alle Rollendienste außer ZERTIFIZIERUNGSSTELLE ausgegraut.

Nach der Auswahl der Zertifizierungsstelle legen Sie den INSTALLATIONSTYP fest (siehe Abbildung 2.62). 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.

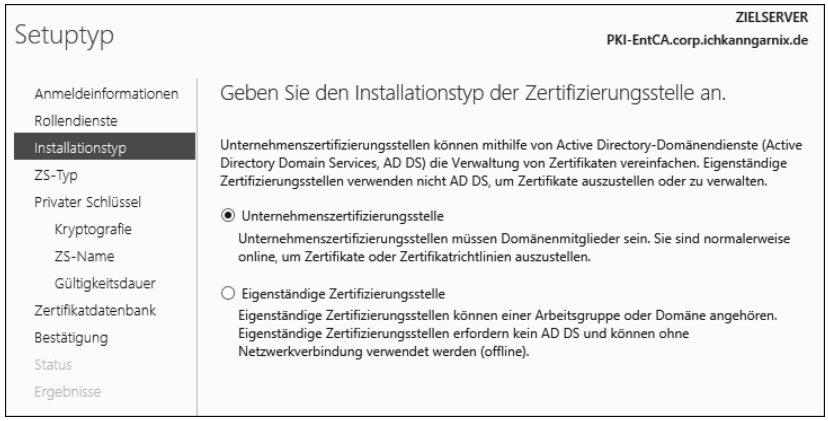

Abbildung 2.62 Auswahl des Installationstyps der Zertifizierungsstelle

Unabhängig von der Auswahl des Installationstyps wählen Sie im folgenden Schritt den Zertifizierungsstellentyp aus (siehe Abbildung 2.63). Hier legen Sie fest, ob es sich bei der CA um eine Stammzertifizierungsstelle (*RootCA*) oder um eine Untergeordnete Zertifizierungsstelle (*Subordinate CA*, *SubCA*) handelt.

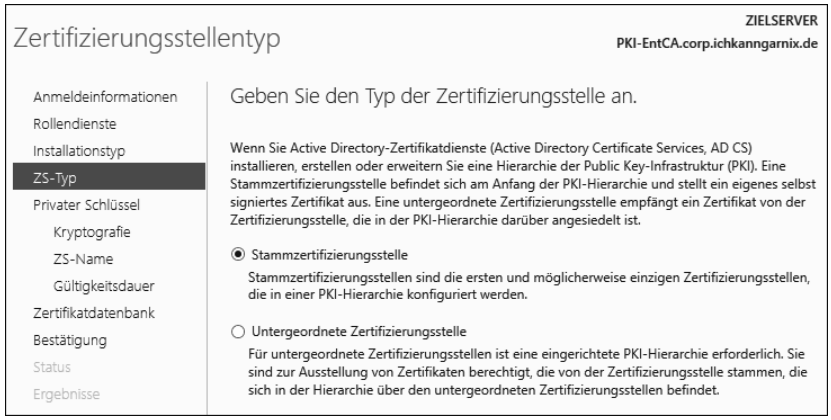

Abbildung 2.63 Auswahl, ob es sich um eine RootCA oder eine SubCA handelt

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 2.64).

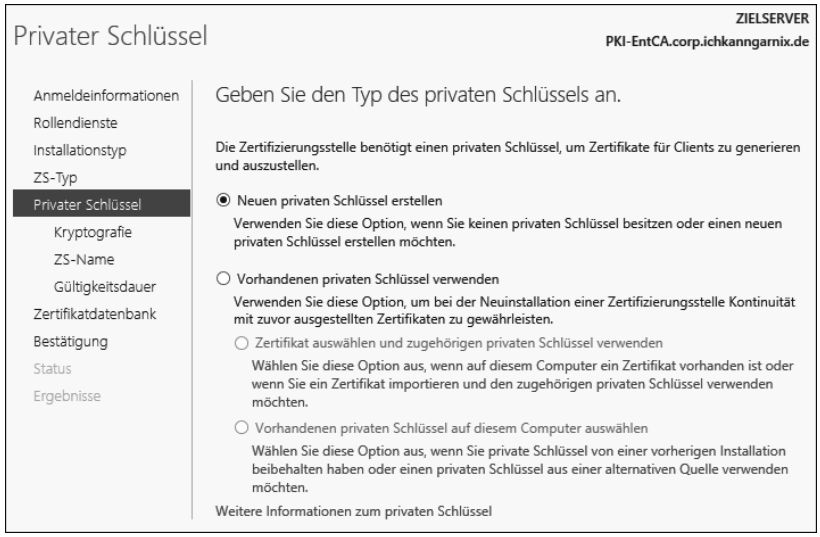

Abbildung 2.64 Optionen zur Schlüsselgenerierung

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.

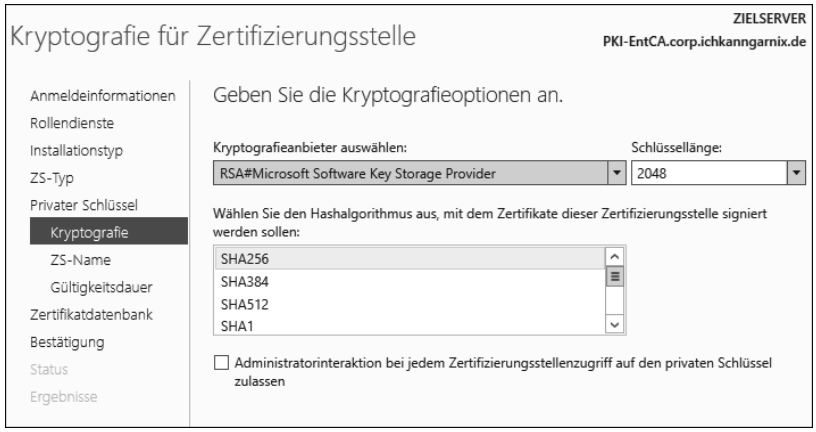

Abbildung 2.65 Optionen zur Auswahl des Kryptografieanbieters, der Schlüssellänge und des Signaturalgorithmus

Bei der Auswahl der Kryptografieoptionen (siehe Abbildung 2.65) 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 Zertifizierungsstellenzugriff auf den privaten Schlüssel zulassen (siehe Abbildung 2.65) 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 2.66). 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.

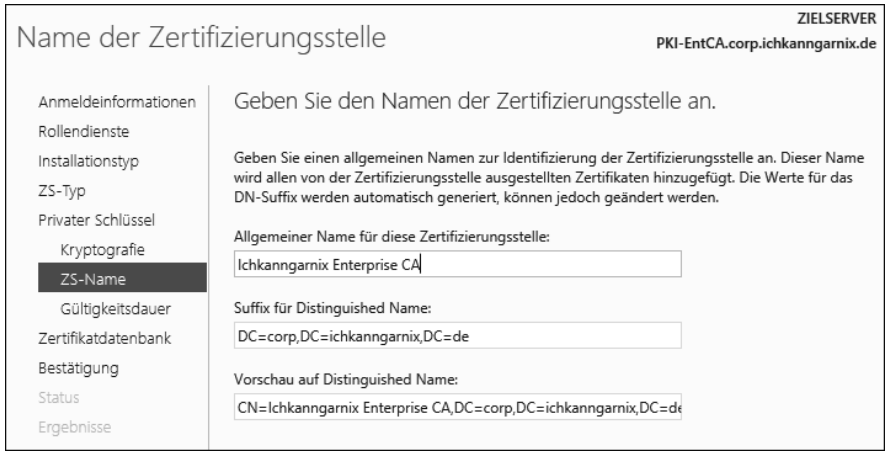

Abbildung 2.66 Den Namen der Zertifizierungsstelle festlegen

Die Abfrage zur maximalen Laufzeit des CA-Zertifikats (siehe Abbildung 2.67) wird ausschließlich bei der Konfiguration einer Stammzertifizierungsstelle angezeigt.

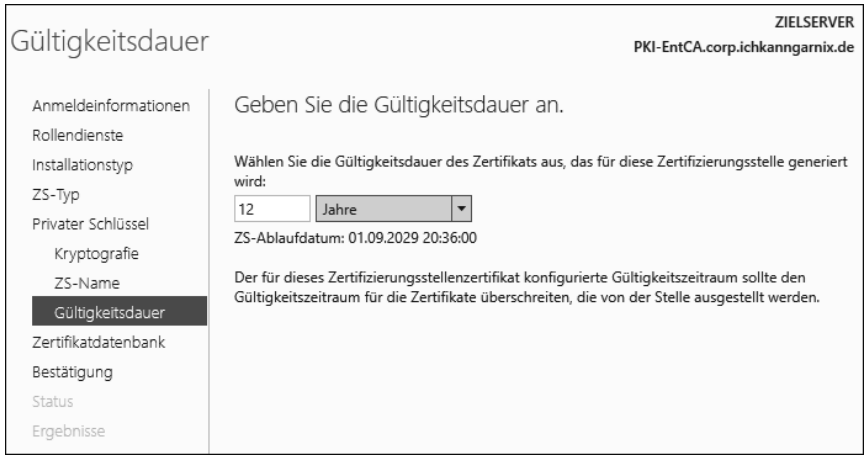

Abbildung 2.67 Die maximale Laufzeit des CA-Zertifikats definieren

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

Als Speicherort für die Datenbank (siehe Abbildung 2.68) 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 • PERFMON) ein.

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

Abbildung 2.68 Auswahl des Speicherorts der Datenbank

Nachdem Sie alle Angaben vorgenommen haben, zeigt der Assistent eine Zusammenfassung der Konfiguration wie in Abbildung 2.69 an.

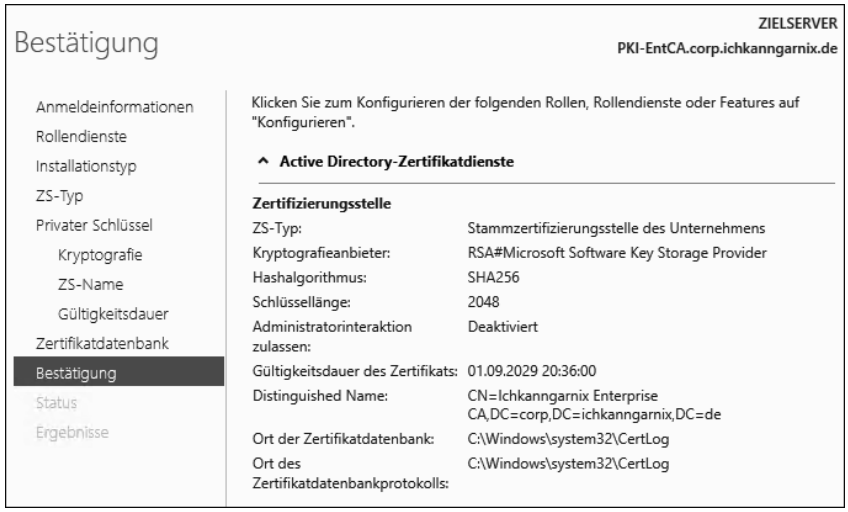

Abbildung 2.69 Zusammenfassung und Bestätigung der Konfiguration

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 2.70).

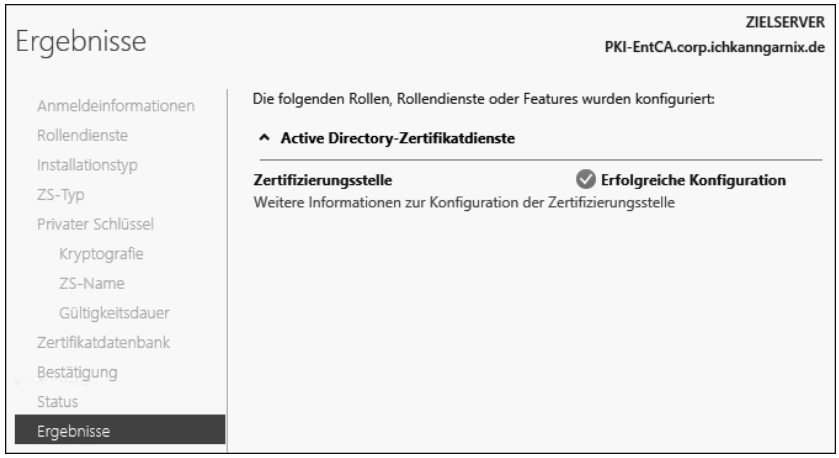

Abbildung 2.70 Zusammenfassung der Ergebnisse

Nach Abschluss des Assistenten wird im Server-Manager der Hinweis, dass die CA noch konfiguriert werden muss, entsprechend aktualisiert (siehe Abbildung 2.71).

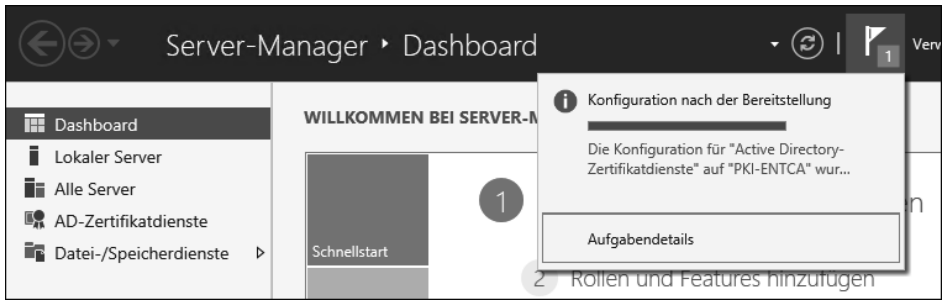

Abbildung 2.71 Der Hinweis im Server-Manager wurde aktualisiert.

2.5.2 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-AdcsCertificationAuthority`	Dieses Cmdlet installiert eine Zertifizierungsstelle (Rollendienst *Zertifizierungsstellen*).
`Install-AdcsEnrollmentPolicyWeb Service`	Konfiguriert einen Zertifikatregistrierungsrichtlinien-Webdienst.
`Install-AdcsEnrollmentWebService`	Konfiguriert einen Zertifikatregistrierungs-Webdienst.
`Install-AdcsNetworkDeviceEnrollment Service`	Konfiguriert den Registrierungsdienst für Netzwerkgeräte.
`Install-AdcsOnlineResponder`	Konfiguriert einen Online-Responder.
`Install-AdcsWebEnrollment`	Konfiguriert die Zertifizierungsstellen-Webregistrierung.
`Uninstall-AdcsCertificationAuthority`	Entfernt eine Zertifizierungsstelle. (Der Rollendienst ist nach wie vor installiert.)

Tabelle 2.6 Die PowerShell-Cmdlets des Moduls »ADCSDeployment«

Cmdlet	Beschreibung
`Uninstall-AdcsEnrollmentPolicyWeb Service`	Entfernt die Konfiguration des Zertifikatregistrierungsrichtlinien-Webdienstes.
`Uninstall-AdcsEnrollmentWebService`	Entfernt die Konfiguration eines Zertifikatregistrierungs-Webdienstes.
`Uninstall-AdcsNetworkDevice EnrollmentService`	Entfernt die Konfiguration eines Registrierungsdienstes für Netzwerkgeräte.
`Uninstall-AdcsOnlineResponder`	Entfernt die Konfiguration des Online-Responders.
`Uninstall-AdcsWebEnrollment`	Entfernt die Konfiguration der Zertifizierungsstellen-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" `
-LogDirectory "C:\Windows\System32\Certlog"
```

Listing 2.7 Installation der Zertifizierungsstelle mit der PowerShell

Die Rückmeldung der PowerShell ist bei einer erfolgreichen Konfiguration eher spartanisch (siehe Abbildung 2.72). Sollte es zu einem Fehler gekommen sein, wird eine Fehlermeldung in rotem Text angezeigt.

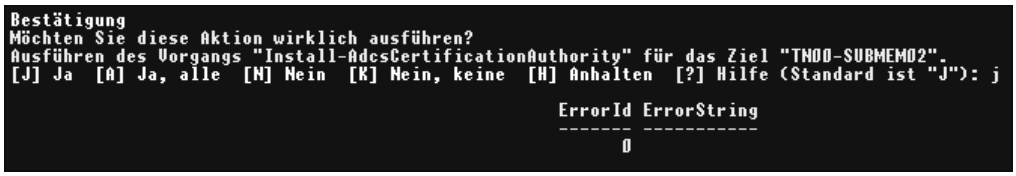

Abbildung 2.72 Rückmeldung der PowerShell nach einer erfolgreichen Konfiguration

2.5.3 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 2.73). Dort erhalten Sie auf dem Dashboard einen Überblick über den Zustand des Dienstes und sehen Einträge aus der Ereignisanzeige.

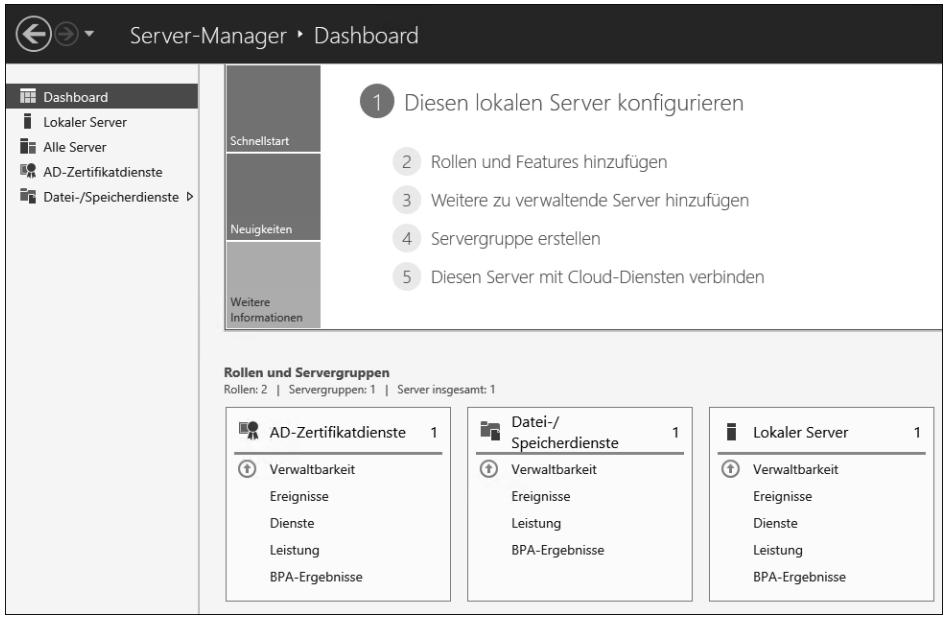

Abbildung 2.73 Übersicht der AD-Zertifikatdienste im Server-Manager

Mit der Installation und Konfiguration der Rolle wurde ein Windows-Dienst registriert (siehe Abbildung 2.74). 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.

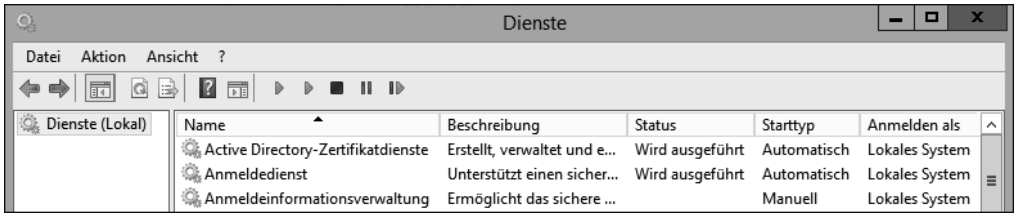

Abbildung 2.74 »Active Directory-Zertifikatdienste« als registrierter Dienst

Wenn Sie die Verwaltungskonsole für die Zertifizierungsstelle starten (siehe Abbildung 2.75), 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.

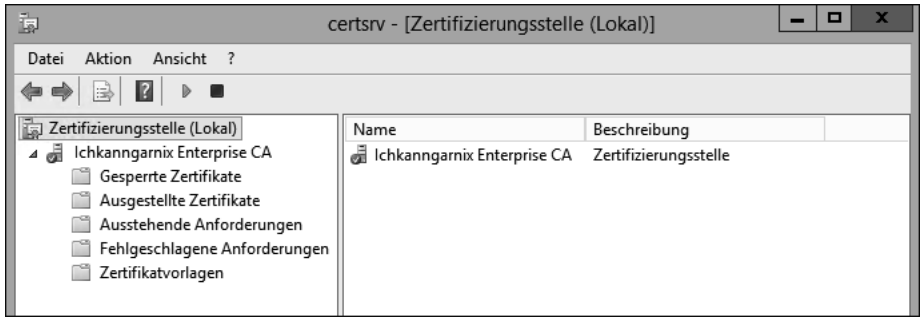

Abbildung 2.75 Die Verwaltungskonsole der Zertifizierungsstelle

Die kompletten Optionen der Konsole und die Eigenschaften der Zertifizierungsstelle werden in Abschnitt 2.7 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 2.76).

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 2.77).

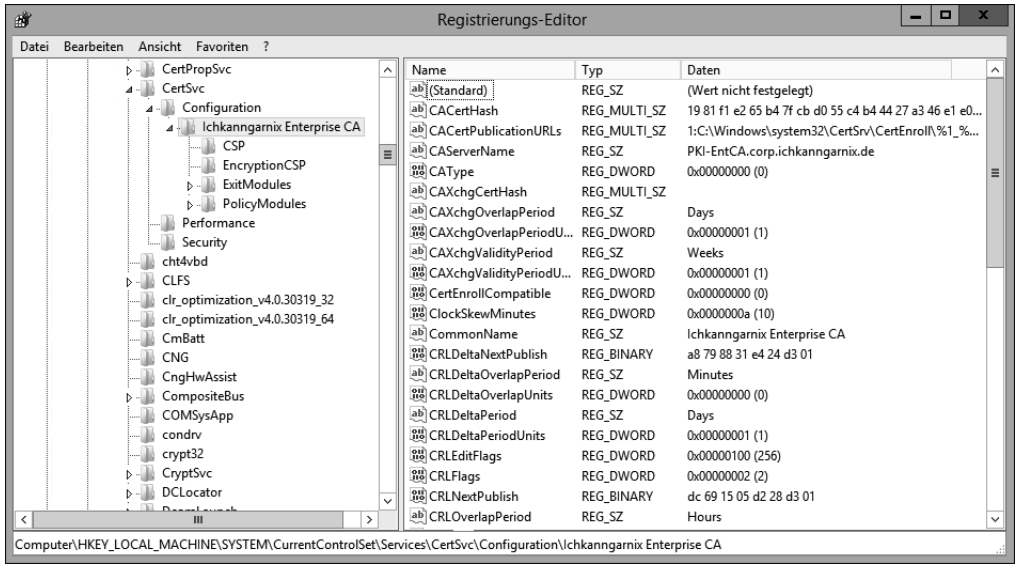

Abbildung 2.76 Konfigurationseinstellungen des »CertSvc« in der Registrierung

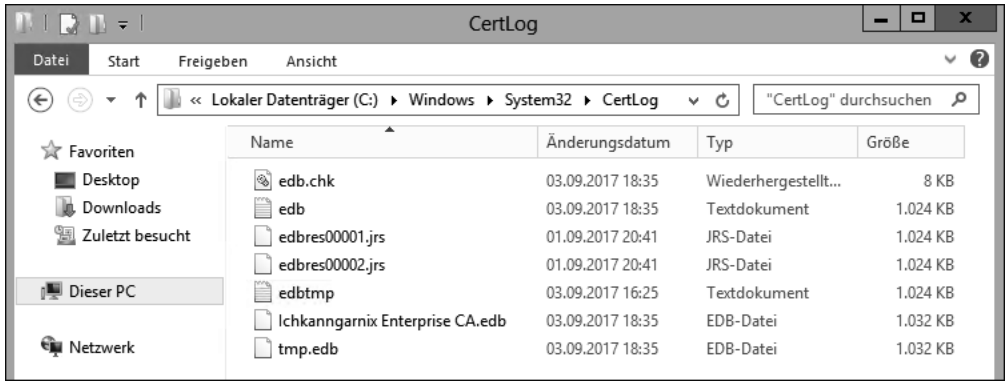

Abbildung 2.77 Inhalt des Datenbank-Ordners

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.log* – 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 2.78).

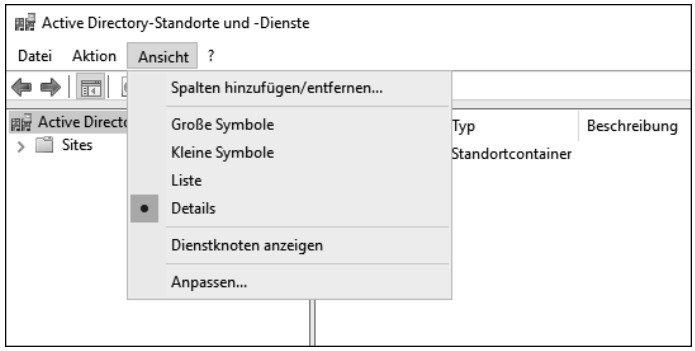

Abbildung 2.78 Aktivieren der »Erwachsenenansicht«

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 2.79).

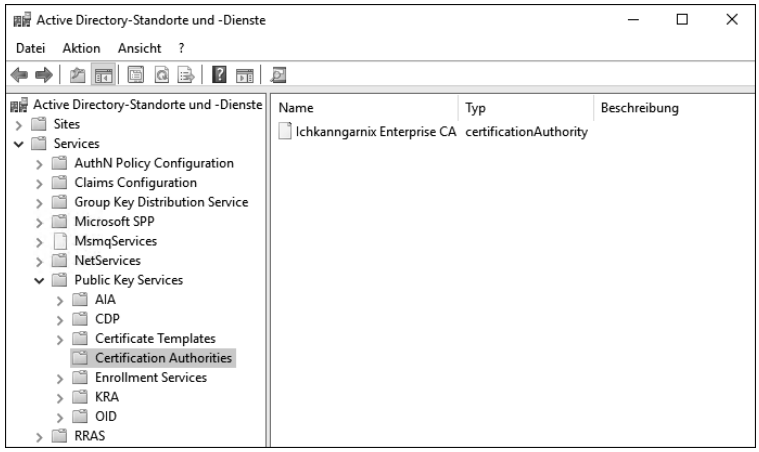

Abbildung 2.79 Die »Public Key Services« im Konfigurationscontainer

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.

Unternehmenszertifizierungsstellen (siehe Abbildung 2.80) 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.

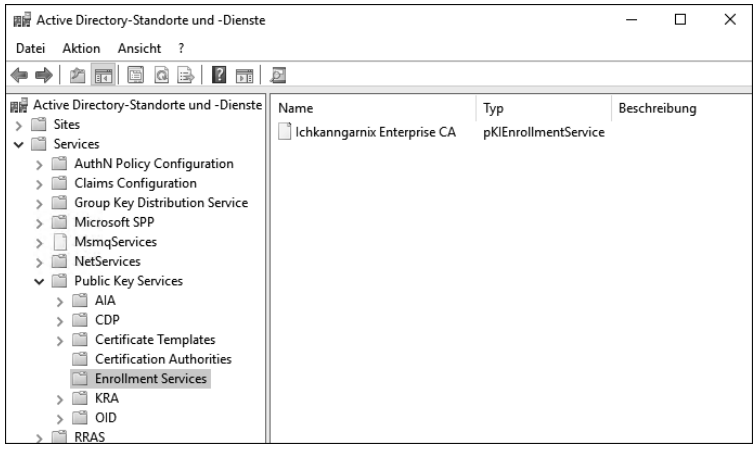

Abbildung 2.80 Der Container »Enrollment Services« beinhaltet Unternehmenszertifizierungsstellen.

Auf der Zertifizierungsstelle kann das selbstsignierte CA-Zertifikat über die *Verwaltungskonsole* (`CertLm.msc`) angezeigt werden.

Abbildung 2.81 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.

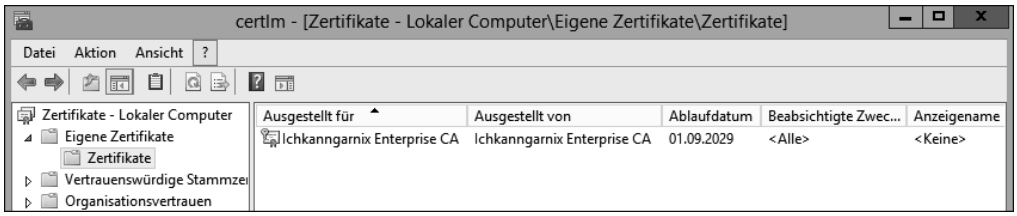

Abbildung 2.81 Prüfung des CA-Zertifikats

Da der Eintrag im Konfigurationscontainer eingetragen ist, wird das CA-Zertifikat im Speicher der vertrauenswürdigen CAs installiert (siehe Abbildung 2.82). 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).

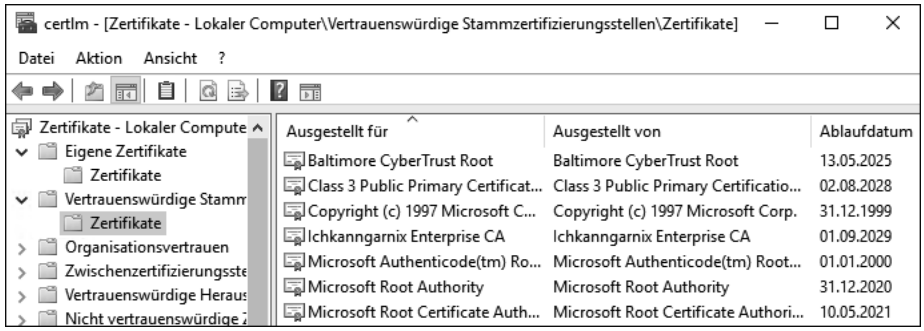

Abbildung 2.82 Die neue RootCA ist im Speicher der vertrauenswürdigen Stammzertifizierungsstellen gelistet.

Wenn Sie die Zertifizierungsstellen-Verwaltungskonsole öffnen und dort die Eigenschaften der CA auswählen, wird als Erstes die Registerkarte ALLGEMEIN angezeigt (siehe Abbildung 2.83). 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 2.84). Hier können Sie auch die konfigurierten 12 Jahre Laufzeit erkennen.

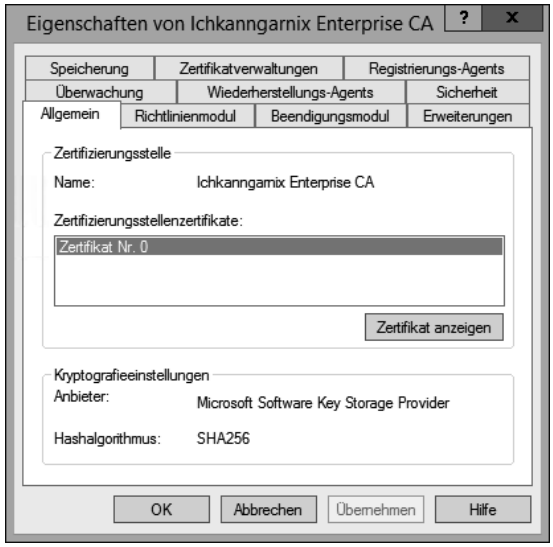

Abbildung 2.83 Übersicht des CA-Zertifikats

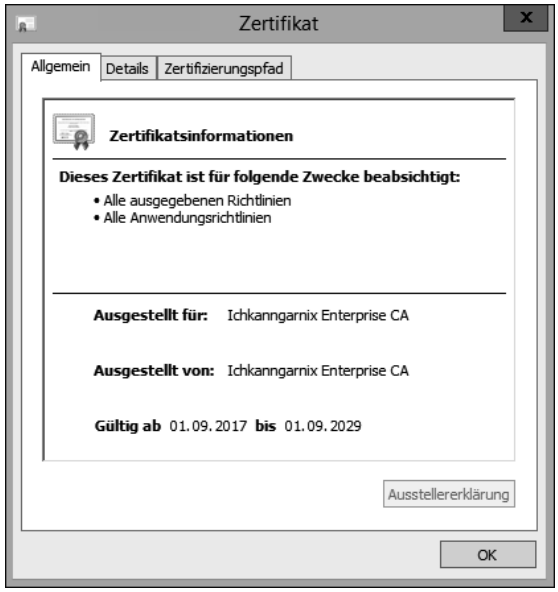

Abbildung 2.84 Eigenschaften des CA-Zertifikats

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.

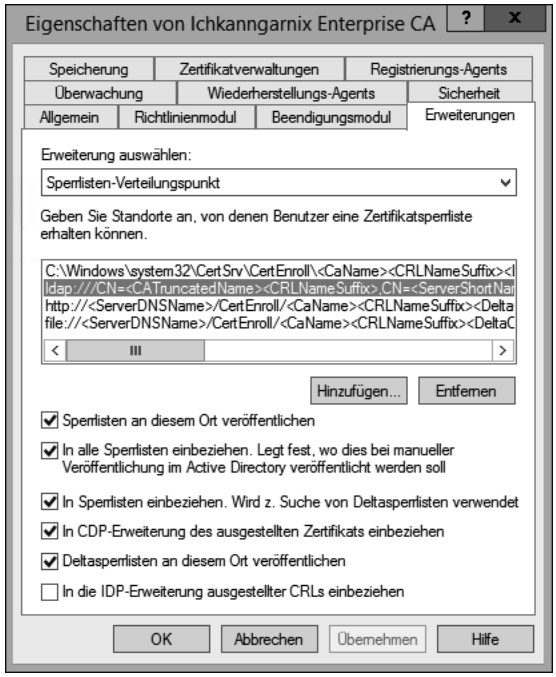

Abbildung 2.85 Die Sperrlisten-Verteilungspunkte, die auf der CA konfiguriert sind

Eine detaillierte Konfiguration der *Sperrlisten-Verteilungspunkte* (CDP) und der *Zugriff auf Stelleninformationen* (AIA, siehe Abbildung 2.86) wird in Abschnitt 3.1.1 erläutert.

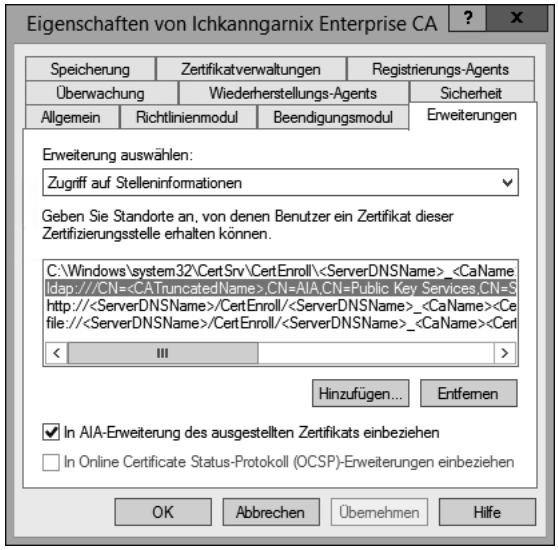

Abbildung 2.86 Quellen zum Abruf des CA-Zertifikats

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 2.87). Hier gibt es dann die Option, unterschiedliche Intervalle für Basissperrlisten und Deltasperrlisten zu konfigurieren.

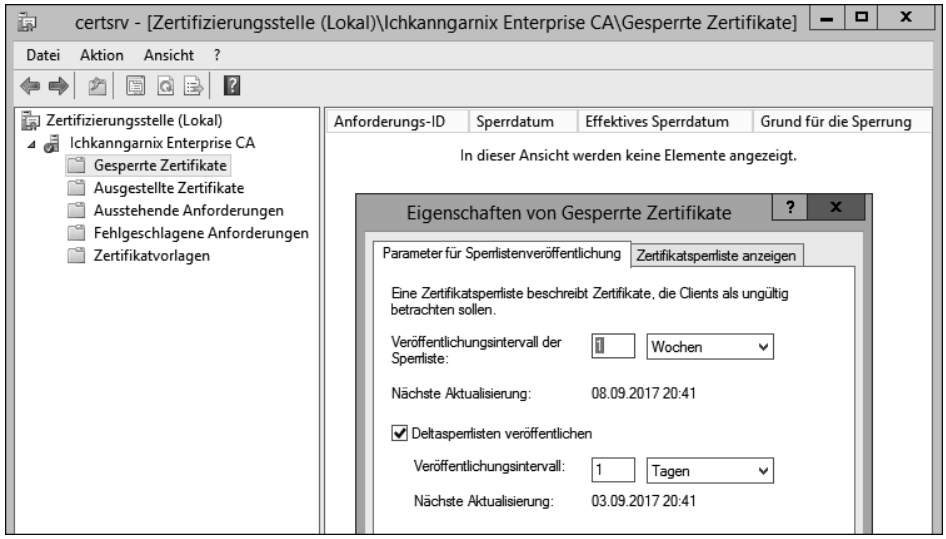

Abbildung 2.87 Konfiguration der Sperrlisten

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

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 2.88 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 2.89).

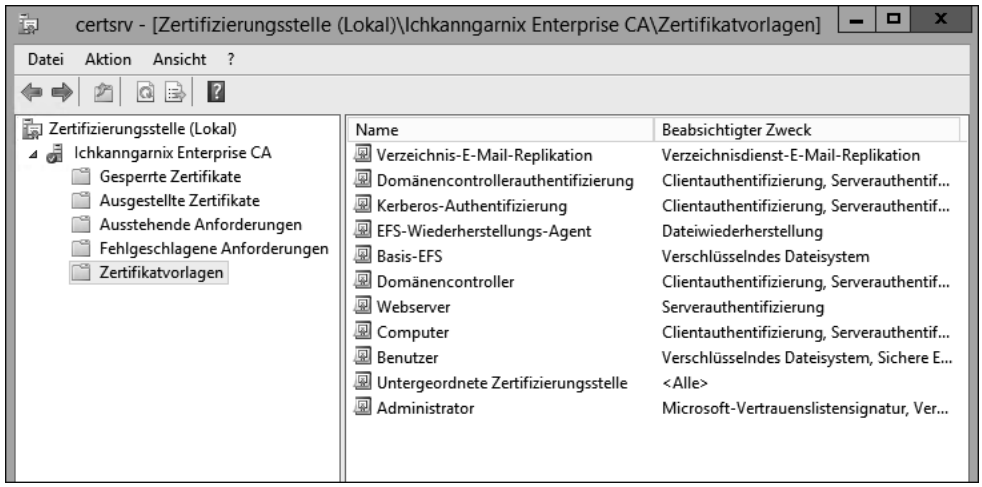

Abbildung 2.88 Anzeige der aktivierten Zertifikatvorlagen

```
C:\>certutil -getreg ca\val*
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Ichka
nngarnix Enterprise CA\val*:

Werte:
  ValidityPeriod            REG_SZ = Years
  ValidityPeriodUnits       REG_DWORD = 2
CertUtil: -getreg-Befehl wurde erfolgreich ausgeführt.
```

Abbildung 2.89 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 2.90):

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

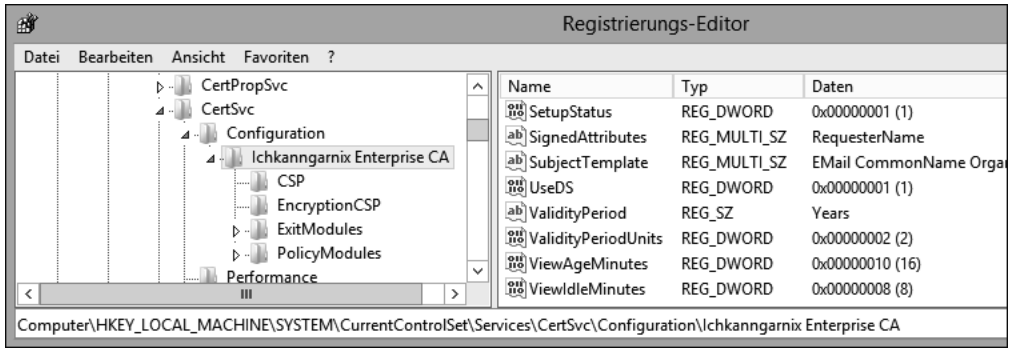

Abbildung 2.90 Die »ValidityPeriod« in der Registry

Eine Anpassung der Werte erfolgt über `CertUtil -setreg` mit den entsprechenden Parametern aus Abbildung 2.91.

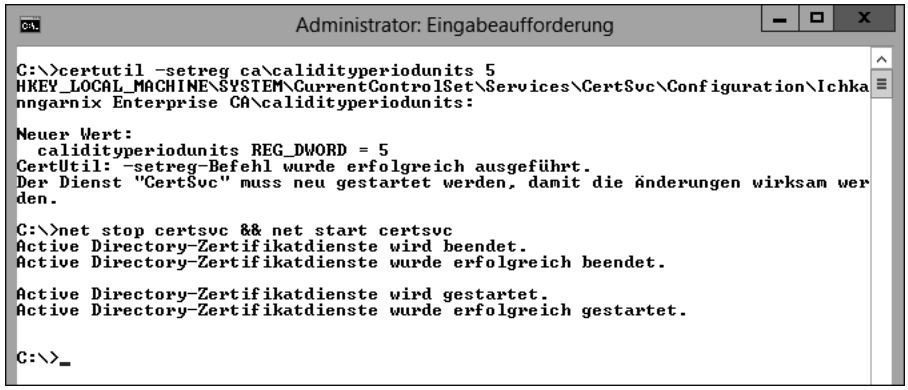

Abbildung 2.91 Der Versuch der Anpassung der maximalen Laufzeit eines Zertifikats

Bei der Verwendung von CertUtil in der Kommandozeile sollten Sie genau prüfen, welche Parameter Sie eingeben. Wenn Sie sich den eingegebenen Befehl in Abbildung 2.91 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 2.92).

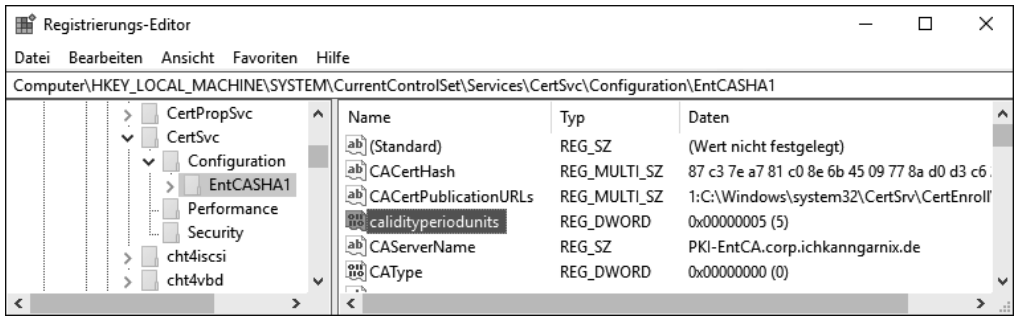

Abbildung 2.92 In der Registrierung wurde ein falscher Wert eingetragen.

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 2.8 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 2.93) in der Registrierung eintragen, der ohne Funktion bleibt und auch nicht den gewünschten Effekt hat.

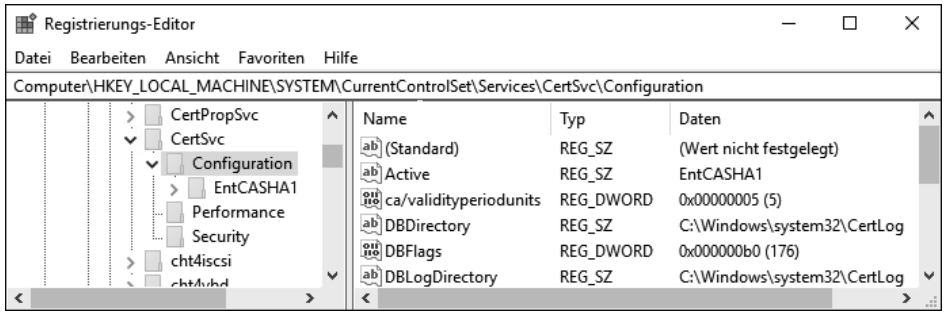

Abbildung 2.93 Bei der Verwendung eines »/« wird der falsche Eintrag eine Ebene höher erstellt.

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.

2.6 Installation einer mehrstufigen CA-Infrastruktur

Nachdem wir im vorigen Abschnitt eine einstufige CA-Infrastruktur installiert haben, werden wir nun die Komplexität und die Sicherheit erhöhen, indem wir eine neue zweistufige CA-Infrastruktur installieren. Für sie wurden die Anforderungen definiert, die Sie in Tabelle 2.7 sehen.

	Konfiguration
Anzahl der Ebenen	2
Sicherheitsanforderungen	Archivierung der privaten Schlüssel für Verschlüsselungszertifikate
Administrative Trennung	Auf der SubCA
Maximale Laufzeit eines Nutzerzertifikats	5 Jahre
Maximale Laufzeit der untergeordneten Zertifizierungsstelle	15 Jahre
Maximale Laufzeit der Stammzertifizierungsstelle	30 Jahre
Schlüssellänge	4096 Bit
Algorithmus	SHA512/Microsoft Software KSP
Speicherort CRL/AIA	*http://crl.ichkanngarnix.de/*
Aktualisierungsintervall der Sperrliste auf der RootCA	6 Monate für die Basissperrliste Keine Deltasperrliste
Aktualisierungsintervall der Sperrliste auf der SubCA	7 Tage für die Basissperrliste 1 Tag für die Deltasperrliste
Online-Responder	Nein
Schlüsselarchivierung	Ja, auf SubCA
Name der Stammzertifizierungsstelle	RootCA
Name der untergeordneten Zertifizierungsstelle	SubCA
Installation auf Hardware oder als virtuelle Maschine	Virtuell
Server Core oder grafisches UI	Grafisches User-Interface
Verwendungszwecke der Zertifikate	verschiedene
Webdienste	Nein
CPS/CP	Nein
Anpassung der CAPolicy.inf	Ja

Tabelle 2.7 Anforderungen an eine zweistufige CA-Infrastruktur