Netz-Weise
Lernen von den Besten.

Installieren einer Zertifikatsserver-Infrastruktur

von Holger Voges

Version 1.0

Freundallee 13 a
30173 Hannover
www.netz-weise.de

Inhalt

Einführung

Verschlüsselung ist spätestens seit der allgemeinen Nutzung des Internet durch jedermann von überall ein extrem wichtiges Thema, weil es sich um ein Netzwerk handelt, das der Kontrolle des Nutzers vollkommen entzogen ist. Man kann den Weg der Daten nicht festlegen und weiß nicht, wer den Datenverkehr mitlesen oder sogar verändern kann.

Um große Datenmengen zu verschlüsseln, bietet sich die sogenannte symmetrische Verschlüsselung an, die alle Daten mit Hilfe einer Zeichenfolge Ver- und wieder Entschlüsseln kann. Der aktuell gängige Standard für symmetrische Verschlüsselung ist AES (Advanced Encryption System). AES verwendet eine Zeichenfolge (den Schlüssel) zum Kodieren der Daten, und nur die Umkehrung der Kodierung mithilfe des Schlüssels kann die Daten entschlüsseln – daher der Begriff symmetrisch. Um AES zu knacken, gibt es derzeit nur eine Methode – das Ausprobieren aller möglichen Schlüssel. Daher steigt die Sicherheit der Verschlüsselung mit der Länge des verwendeten Schlüssels. AES wird aktuell mit 128 und 256 Bit Schlüssellänge verwendet. Ein 256 Bit langer AES-Schlüssel gilt nach derzeitigem Kenntnisstand auch für die NSA mit all Ihrer Rechenpower als so gut wie unknackbar, da die Anzahl der möglichen Schlüssel 2^{256} ist, eine Zahl mit 77 Nullen.

Die Symmetrische Verschlüsselung funktioniert so lange gut, wie Daten nur für Ihren Besitzer verschlüsselt werden – z.B. bei einem Kennwortsafe, bei dem der Nutzer die Daten vor allen fremden Augen schützen will – oder man dem Empfänger einer verschlüsselten Nachricht den Schlüssel direkt übergeben kann. Will man aber Daten im Internet mit einem fremden Gegenüber austauschen, was z.B. bei allen https-Verbindungen der Fall ist, ist AES alleine nicht nutzbar.

Wo ein Wille ist, ist auch ein Weg, und daher haben in den 1970er-Jahren eine Reihe von findigen Köpfen asymmetrische Verfahren entwickelt, die nicht einen, sondern zwei Schlüssel verwenden. Die beiden häufigsten Vertreter sind der Diffie-Hellman Schlüsselaustausch von Whitfield Diffie und Martin Hellman und die RSA-Verschlüsselung, benannt nach Ihren Erfindern Ron Rivest, Adi Shamir und Leonard Adelman. Beide Verfahren haben eine grundsätzlich andere Funktionsweise als AES, da sie Ihre Sicherheit nicht aus der Menge an möglichen Schlüsseln beziehen, sondern auf einem sehr schwierig zu lösendem mathematischem Problem beruhen. Daten, die mit einem der beiden Schlüssel verschlüsselt sind, können nur mit dem zweiten Schlüssel wieder entschlüsselt werden. Dieses Verfahren gilt auch umgedreht – Daten, die mit dem zweiten Schlüssel verschlüsselt werden, können nur mit dem ersten Schlüssel wieder entschlüsselt werden.

Das besondere an den asymmetrischen Verfahren liegt darin, dass der **Empfänger** einer Nachricht damit beginnt, ein Schlüsselpaar mit Hilfe der oben genannten Algorithmen zu generieren. Einen der beiden Schlüssel behält der Empfänger für sich, während er den zweiten Schlüssel an den Versender (Initiator) der Nachricht schickt. Der Schlüssel, den der Empfänger für sich behält, wird als privater Schlüssel bezeichnet, da er immer bei Ersteller verbleibt, während der andere Schlüssel an jedermann weitergegeben werden kann. Er wird als öffentlicher Schlüssel bezeichnet.

Der Versender generiert nun einen (symmetrischen) AES-Schlüssel und verschlüsselt diesen mit Hilfe des öffentlichen Schlüssels des Empfängers. Anschließend kann er den (verschlüsselten) symmetrischen Schlüssel über ein ungesichertes Netzwerk übertragen, denn nur der Empfänger kann den Originalzustand mit Hilfe des privaten Schlüssels wiederherstellen. Dieser Vorgang wird auch als Schlüsselübertragung bezeichnet.

Dieses Verfahren kann auch umgedreht werden, und wird dann als digitale Signatur bezeichnet. Ist eine Datei oder ein Text wie eine E-Mail digital signiert, kann der Empfänger den Urheber prüfen und verifizieren, ob die Nachricht auf dem Transferweg verändert wurde.

Um das zu erreichen, muss der Urheber über den Text oder Code, den er signieren möchte, zuerst einen Hash (eine bessere Checksumme) generieren. Hierfür verwendet man heutzutage normalerweise SHA2 (Secure Hash Algorithm) mit 256, 384 oder 512 Bit Hashlänge. Die Bezeichnung für SHA 2 lautet dann entsprechend SHA 256, SHA 384 oder SHA 512. Die älteren Hashalgorithmen SHA 1 und MD5 sollten nicht mehr für die digitale Signatur verwendet werden, können aber durchaus für weniger sicherheitskritische Funktionen weiterhin verwendet werden.

Der Hash wird vom Urheber nun mit Hilfe seines privaten Schlüssels verschlüsselt. Der verschlüsselte Hash ist die digitale Signatur, die nun direkt an das Dokument oder die Datei angehängt wird.

Um die digitale Signatur zu prüfen, muss der Prüfer im Besitz des öffentlichen Schlüssels sein. Mit diesem kann er die digitale Signatur entschlüsseln – wir erinnern uns, Private Public Key Verschlüsselung funktioniert in beiden Richtungen – und anschließend mit dem Hash vergleichen, den er selbst über das Dokument oder die Datei erzeugt hat. Sind beide Hashes gleich, kann er sicher davon ausgehen, dass die Signatur vom Besitzer des öffentlichen Schlüssels stammte und seit der Erstellung der Signatur keine Veränderungen mehr vorgenommen worden sind.

Damit der öffentliche Schlüssel einem Besitzer eindeutig zugeordnet werden kann, wird ein öffentlicher Schlüssel normalerweise in Form eines X.509-Zertifikats übertragen. Das Zertifikat fungiert als Container für den Schlüssel und beinhaltet außerdem Informationen über den Besitzer, ein Ablaufdatum, eine Reihe von weiteren Informationen und den Verwendungszweck. Der Verwendungszweck schränkt den öffentlichen Schlüssel auf definierte Funktionen wie z.B. E-Mail Verschlüsselung, die Erstellung von Codesignaturen oder verschlüsselten Web-Verkehr ein. Durch diese Einschränkung ist es möglich, unterschiedlichen Sicherheitslevel zu definieren, die die Zertifikatsserver einhalten müssen.

Damit ein Zertifikat nicht verändert werden kann, wird es vom Herausgeber ebenfalls signiert. Hierfür verwendet der Herausgeber seinen eigenen, privaten Schlüssel. Um die Zertifikate eines Zertifikatsservers prüfen zu können, muss der Empfänger eines Zertifikats ebenfalls über den öffentlichen Schlüssel (das Zertifikat) des Zertifikatsservers verfügen. Damit dieses Zertifikat nicht aus dem Internet heruntergeladen werden muss (und damit wieder abgefangen und gefälscht werden könnte), liefern sowohl Windows als auch die gängigen Webbrowser die Zertifikate der größten Zertifizierungsstellen mit. Diese Zertifizierungsstellen werden als Stammzertifizierungsstellen bezeichnet und sind die Quelle (Root) des Vertrauens (Root of Trust).

Die Zertifizierungsstellen lassen sich Zertifikate gut bezahlen. Wenn man Zertifikate nur innerhalb des Unternehmens benötigt, macht es daher Sinn, sich seine eigenen Zertifikatsserver zu installieren, und das ist mit Windows Server problemlos möglich und schnell erledigt. Dabei unterscheidet Windows zwei Typen von Zertifikatsservern (Certificate Authority oder CA):

Alleinstehende CA: Eine alleinstehende CA entspricht vom Typ her den Zertifikatsservern, wie sie auch von den Zertifikatsanbietern verwendet werden. Um ein Zertifikat zu bekommen, muss eine Zertifikatsanforderung auf dem Server eingereicht werden. Diese Anforderung wird dann manuell von einem Mitarbeiter unter anderem auf die Identität des Antragstellers geprüft. Bei https-Zertifikaten ist das recht einfach möglich, bei Benutzerzertifikaten muss aber deutlich mehr Aufwand betrieben werden. Erst wenn sichergestellt ist, dass der Antragsteller wirklich seine korrekten Daten angegeben hat, wird das Zertifikat ausgestellt.

Unternehmens-CA: Eine Unternehmens-CA ist ein Unternehmens-Netzwerk eingebunden und vertraut dem Identitätsdienst des Unternehmens, bei Windows also dem Active Directory. Hat sich ein Computer oder ein Benutzer beim AD mit Benutzernamen und Kennwort authentifiziert, reicht der CA das als Identitätsbeweis aus. Dadurch ist es möglich, das Ausstellen von Zertifikaten

vollständig zu automatisieren. Eine manuelle Prüfung ist hier nicht mehr notwendig. Außerdem erlaubt eine Unternehmens-CA das Anpassen von Zertifikaten an die eigenen Bedürfnisse. Windows CAs stellen hierfür Zertifikats-Vorlagen zur Verfügung.

Normalerweise wird in einem Unternehmen aber nicht nur eine Zertifizierungsstelle bereitgestellt, sondern mehrere, wobei die Zertifizierungsstellen aufeinander aufbauen. Zuerst installiert man eine Stamm-Zertifizierungstelle (Root-CA), die sich Ihr Zertifikat mit Hilfe Ihres privaten Schlüssels selber signiert. Anschließend kann man weitere Zertifizierungsstellen installieren, die sich Ihre öffentlichen Schlüssel von der Root-CA signieren lassen. Man erhält dann eine Vertrauenskette (Chain of Trust), die sich bis zur Root-CA zurückverfolgen lässt. Neben dem Lastausgleich gibt es hierfür einen weit wichtigeren Grund, und der hat mit dem Widerrufen von vorzeitig ungültigen Zertifikaten zu tun.

Wird ein privater Schlüssel nämlich kompromittiert, also z.B. gestohlen, dann muss er vor Ablauf seiner Gültigkeit zurückgezogen gemacht werden. Hierfür werden Zertifikatsrückruflisten oder CRLs (Certificate Revocation Lists) verwendet, die der Zertifikatsserver z.B. auf einem Webserver zentral zum Download zur Verfügung stellt. Hier kann ein Client prüfen, ob das Zertifikat, das er erhalten hat, noch gültig ist. Der Speicherort der CRL wird dabei in jedes Zertifikat "eingeprägt". Kann ein Client eine CRL nicht abrufen, akzeptiert er das Zertifikat nicht, da er nicht sicherstellen kann, dass es nicht zurückgerufen wurde.

Hat man aber nur eine einzige Zertifizierungsstelle, und diese wird kompromittiert, ist es nicht möglich, sie ungültig zu machen, da die Root-CA sich nicht selbst auf Ihre eigene CRL setzen kann. Die CRL ist nämlich von der CA signiert, und würde sie sich selbst auf Ihre CRL setzen, wäre die CRL damit automatisch nicht mehr gültig. Die Katze beißt sich hier in den Schwanz.

Um das Problem zu lösen, kann man eine Root-CA installieren, die dann die Zertifikate für untergeordnete Zertifizierungsstellen ausstellt. Anschließend stellt der Administrator für die Root-CA eine CRL aus, kopiert diese auf einen immer erreichbaren Server, und nimmt die Root-CA anschließen offline. Die Root-CA wird danach nur online genommen, um eine neue CRL auszustellen, oder wenn eine neue CA installiert wird. Alle Nutz-Zertifikate werden von den untergeordneten Zertifizierungsstellen (subordinate CAs) ausgestellt. Wird eine der untergeordneten Zertifizierungsstellen kompromittiert, kann man Sie mit Hilfe der CRL der Root-CA ungültig machen. Da die Root-CA ausgeschaltet ist, ist sie maximal geschützt. Normalerweise wird man die Root-CA als alleinstehende Zertifizierungsstelle installieren, während man die untergeordneten Zertifizierungsstellen als Unternehmens-Zertifizierungsstellen installiert.

Installieren der Zertifikats-Rolle

Für die Installation eines Zertifikats-Servers muss zuerst die Zertifikatserver-Rolle installiert werden. Im Folgenden wird beschrieben, wie Sie die Rolle bereitstellen und welche weiteren Optionen zur Verfügung stehen. In den nächsten beiden Abschnitten wird dann zuerst die Installation einer einstufigen Unternehmens-CA beschrieben, danach die Installation einer zweistufigen Zertifikatserver-Infrastruktur.

Für die Installation der Zertifikatserverrolle benötigen Sie einen Windows Server. Idealerweise sollte der Server nur die Zertifikatsdienste bereitstellen, in kleinen Unternehmen kann aber z.B. auch ein Domänencontroller als CA "missbraucht" werden. Achten Sie darauf, dass der Server nicht umbenannt werden kann, solange er Zertifikatsserver ist!

Starten Sie den Windows Servermanager und wählen Sie aus dem Verwalten-Menü "Rollen und Features hinzufügen" aus. Im Assistenten zum Hinzufügen von Rollen und Features wählen Sie anschließend so lange "Weiter" aus, bis Sie auf dem Register "Serverrollen" angekommen sind. Hier

wählen Sie die Rolle "Active Directory Certificate Services" aus. Im sich nun öffnenden Fenster bestätigen Sie die Installation auch der Verwaltungswerkzeuge mit "Add Features".

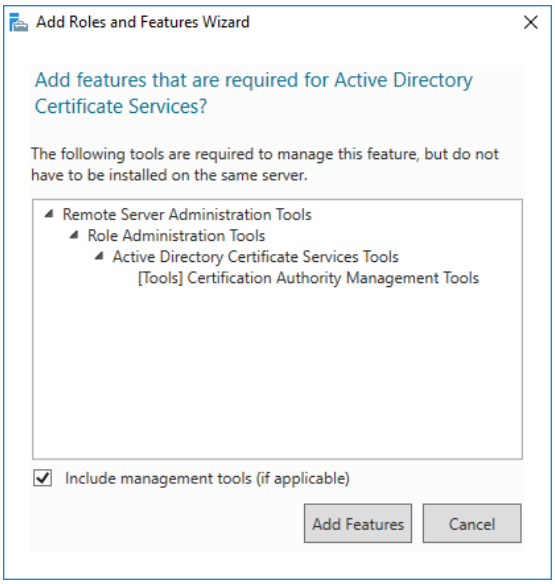


Bild 1 - Installieren Sie auch die Management-Tools

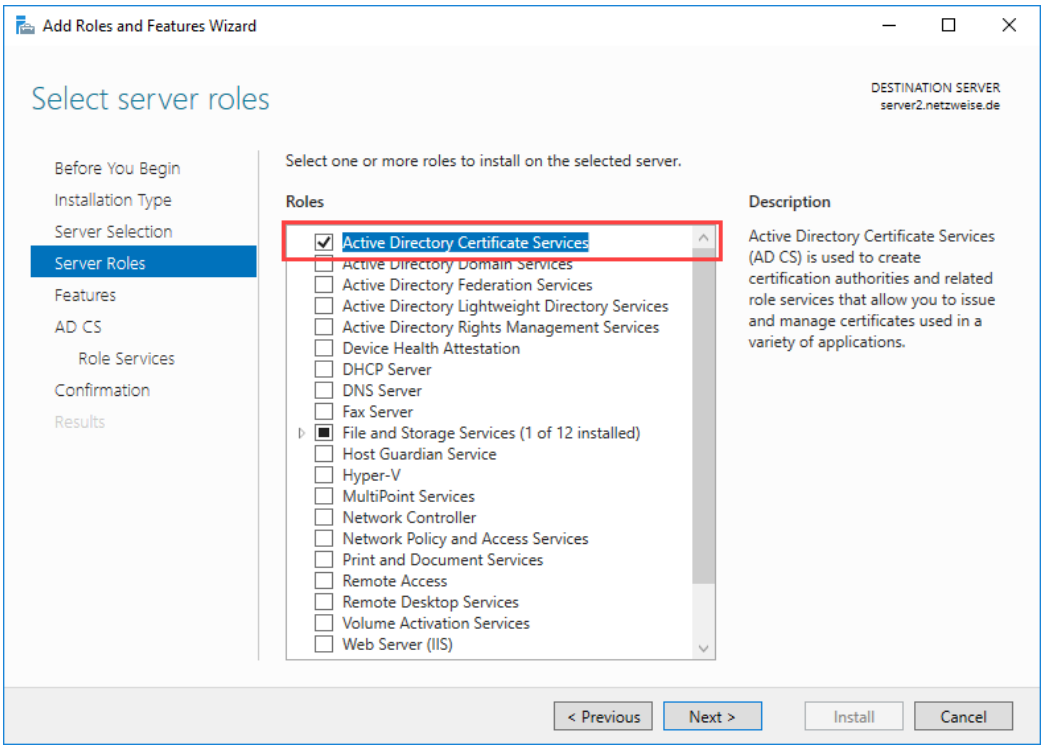


Bild 2 - die Zertifikatsdienste sind anschließend ausgewählt

Führen Sie den Assistenten nun bis zum Register "AD CS – Role Services" fort, und wählen Sie im Auswahlfenster "Certification Authority".

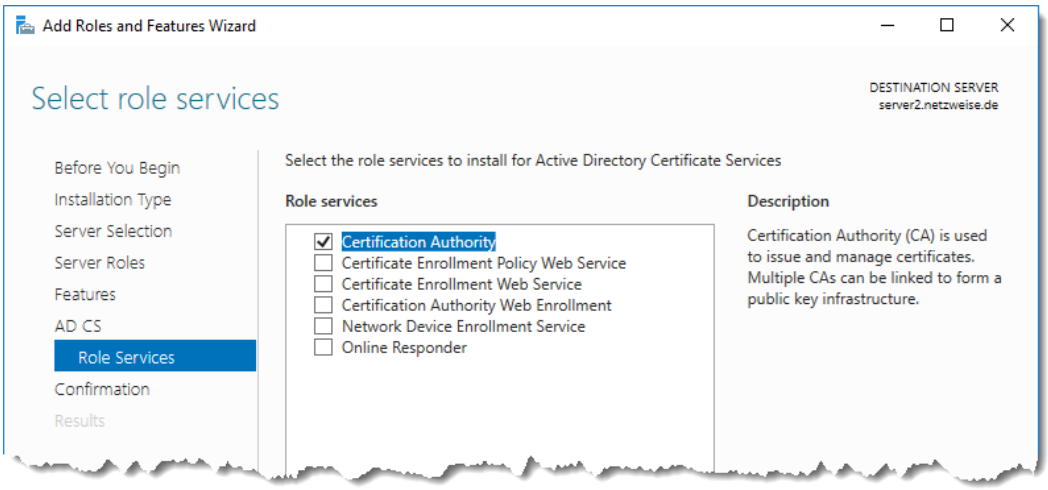


Bild 3 - Wählen Sie nur die Zertifikatsdienst-Rolle aus

Die weiteren Rollen haben folgende Bedeutungen:

Certification Authority Web Enrollment: Mit dieser Rolle installieren Sie eine Webseite, über die es möglich ist, Zertifikatsanforderungen einzureichen. Das ist bei einer Unternehmens-CA normalerweise nicht notwendig, da es jede Menge andere Möglichkeiten gibt, ein neues Zertifikat zu beantragen. Außerdem ist dieses Feature seit Windows Server 2008 nicht mehr weiterentwickelt worden.

Network Device Enrollment Service: Dieser Dienst implementiert das SCEP-Protokoll (Simple Certificate Enrollment Protocol) und erlaubt das automatische verteilen von Zertifikaten für Netzwerkgeräte wie Router oder Switches.

Online Responder: Ein Online Responder erlaubt es einem Client, ein Zertifikat zu überprüfen, ohne die gesamte CRL (Zertifikats-Rückrufliste) herunterladen zu müssen. Ist ein Online Responder installiert, kann ein Client die Seriennummer eines Zertifikats an den Online-Responder schicken, der dann nur das einzelne Zertifikat auf Gültigkeit überprüft. Ein Online-Responder wird normalerweise auf einem separaten Server installiert.

Certificate Enrollment Web Service: Eine Windows Unternehmens-CA wird normalerweise über RPC (Remote Procedure Calls) angesprochen. RPC benötigt neben dem TCP-Port 135 noch eine ganze Reihe weiterer Ports und ist daher außerhalb des Unternehmens-Netzwerkes nicht erreichbar. Um auch Clients außerhalb des Netzwerks das Abrufen von Zertifikaten von der Unternehmens-CA zu erlauben, kann der Certficate Enrollment Web Service (aus dem Internet heraus erreichbar) installiert werden, der die Anfrage per https annimmt und an einen internen Zertifikats-Server weiterleitet.

Certficate Enrollment Police Web Service: Der Policy Web Service erlaubt das Abrufen der Zertifikats-Richtlinien über https. Die Zertifikatsrichtlinie ist ein Dokument, das beschreibt, wie ein Herausgeber seine Zertifikatsserver sichert.

Da die weiteren Rollen nicht benötigt werden, schließen Sie diesen Teil des Setups mit dem Button "Install" ab. Ein abschließender Serverneustart ist nicht notwendig.

Installieren eines alleinstehenden Unternehmens-Zertifikatsservers

Für einfach Testszenarien und kleinere Unternehmen reicht es normalerweise aus, einen einzigen Zertifikatsserver bereitzustellen. Damit die Verteilung der Zertifikate z.B. durch Gruppenrichtlinien automatisiert werden kann, verwendet man eine Unternehmens-CA. Im Folgenden wird der

Installationsvorgang einer alleinstehenden Unternehmens-CA in einer Windows-Domäne auf Windows Server 2016 beschrieben, wobei die Installationsschritte auch für vorige Windows Server Versionen und Windows Server 2019 gültig sind.

Sobald die Installation abgeschlossen ist, können Sie die Zertifikatsdienste konfigurieren, indem Sie "Configure Active Directory Certificate Services on the destination server" auswählen.

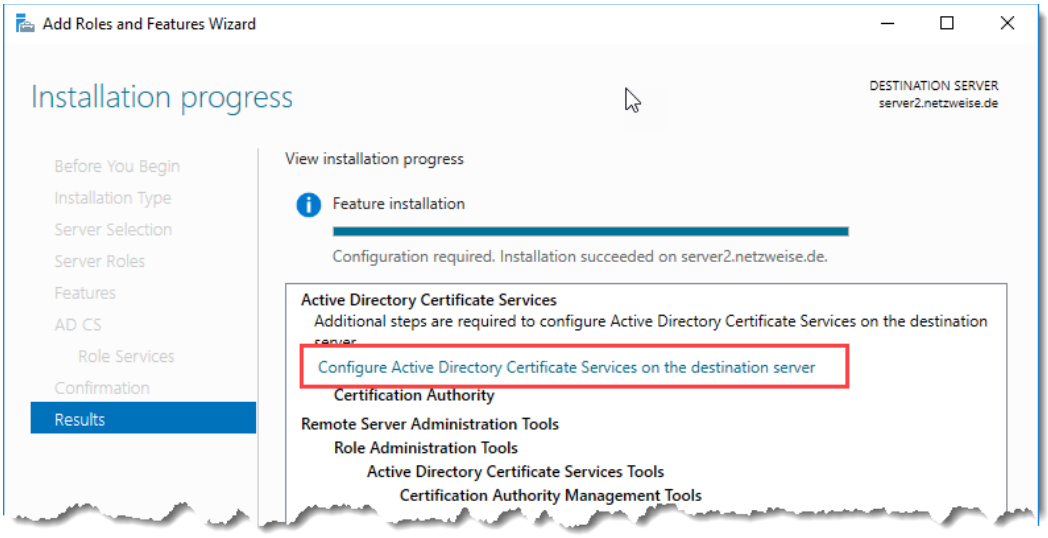


Bild 4 - Starten Sie nun die Konfiguration der Zertifikatsdienste

Sie benötigen für eine Unternehmens-CA einen Benutzer mit Organisations-Administrator-Rechten. Wenn Sie über diese Berechtigungen nicht verfügen, können Sie im AD CS Configuration Assistenten den Installationskontext wechseln.

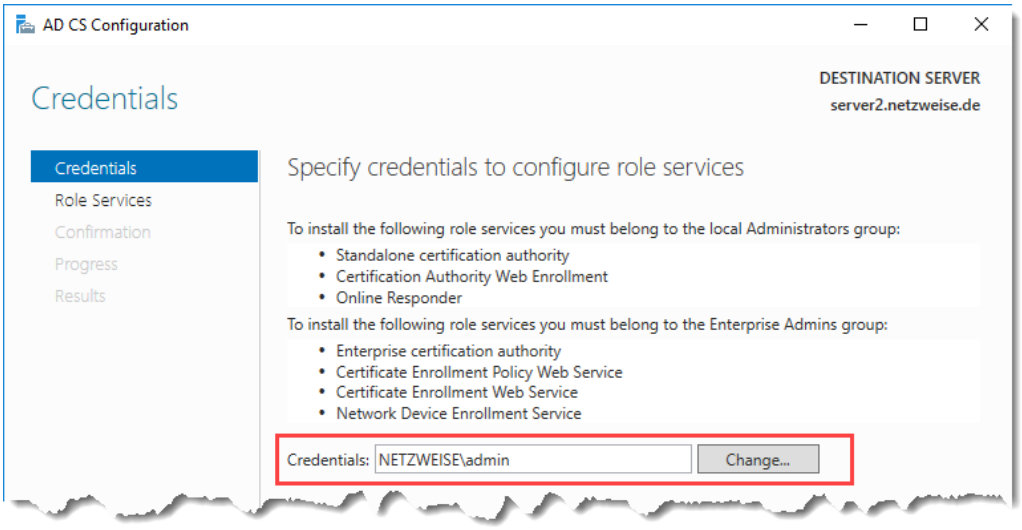


Bild 5 - Prüfen Sie Ihre Berechtigungen und korrigieren Sie sie gegebenenfalls

Im folgenden Fenster wählen Sie die zu installierenden Rollen aus. Da wir im vorigen Installationsschritt nur "Certfication Authority" ausgewählt haben, steht uns nun auch nur diese eine Option zur Verfügung. Wählen Sie sie aus und fahren Sie fort. Im Menü werde nun weitere Konfigurationsschritte hinzugefügt.

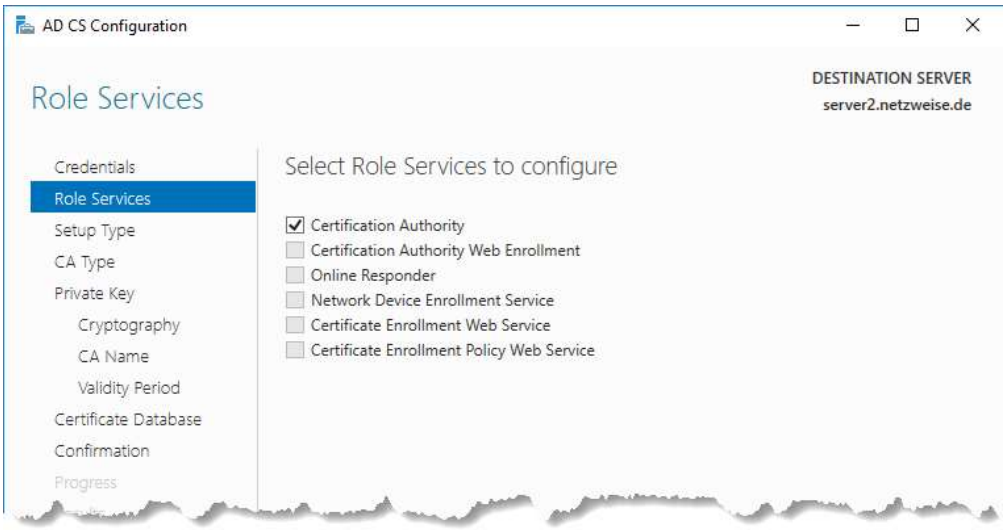


Bild 6 - Mit Auswahl der Role CA werden zusätzliche Optionen angeboten

Wählen Sie unter CA Type "Enterprise CA" aus, um eine Unternehmens-CA zu installieren.

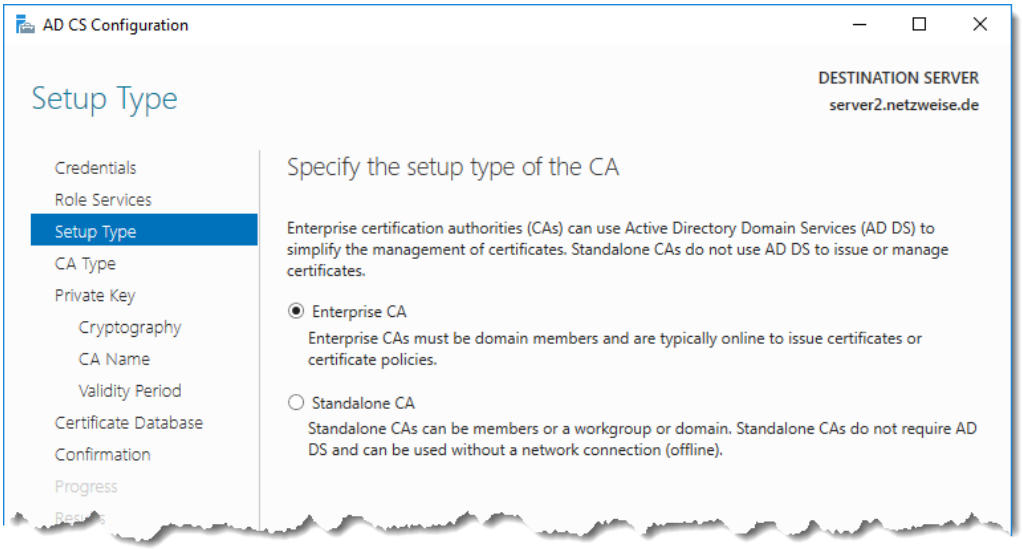


Bild 7 - Wählen Sie Enterprise-CA aus, um Zertifikate automatisch verteilen zu können

Anschließend legen Sie fest, ob es sich um die erste Zertifizierungsstelle handelt, die sich Ihr Zertifikat selber ausstellt, oder ob bereits eine Stammzertifizierungstelle (Root CA) existiert. Wählen Sie hier "Root CA" aus. Eine Root CA wird auch als Vertrauensursprung bezeichnet. Sie ist deshalb besonders, weil Sie Ihren öffentlichen Schlüssel selbst signiert.

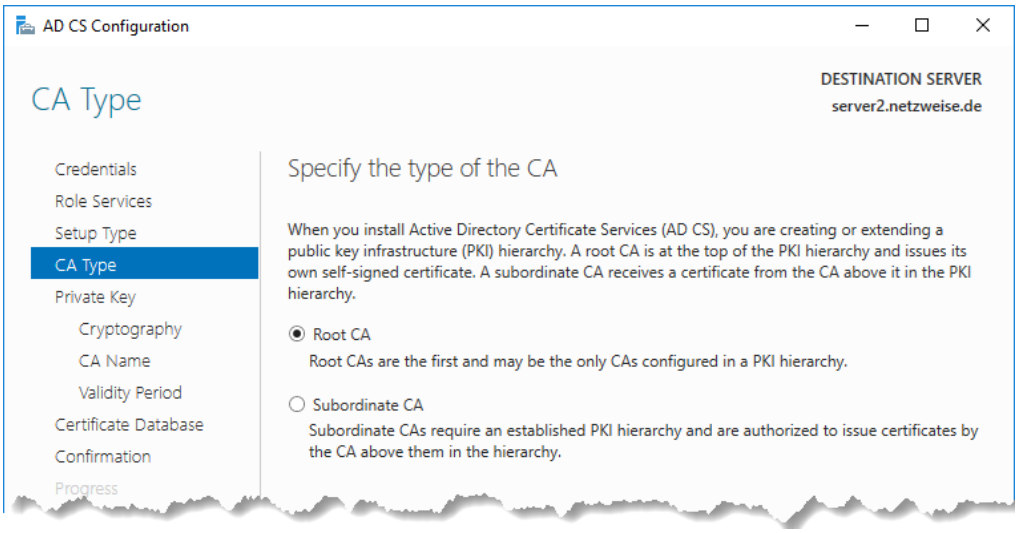


Bild 8 - Eine Root-CA ist die erste Zertifizierungsstelle

Legen Sie als nächstes fest, wie das Schlüsselpaar und das Zertifikat erstellt werden sollen. Erzeugen Sie hierfür ein neues Schlüsselpaar, indem Sie "Create a new private key" auswählen. Einen bestehenden privaten Schlüssel verwenden Sie, um eine CA zu migrieren oder aus einer Sicherung wiederherzustellen.

Bild 9 - Erstellen Sie einen neues Schlüsselpaar, indem Sie "Create a new private key" wählen

Im Register Cryptography legen Sie fest, wie die Schlüssel generiert werden sollen. Der Kryptografische Provider ist die Software, mit der das Schlüsselpaar erzeugt wird. Provider können nachinstalliert werden und legen letztlich fest, welche Verschlüsselungsalgorithmen Ihnen zur Verfügung stehen und wo Sie die Schlüssel speichern können. Natürlich müssen auch Ihre Clients die Verschlüsselungsmethoden unterstützen, die Sie auswählen, daher ist neuer und sicherer nicht unbedingt immer besser. Wir gehen hier davon aus, dass Sie mindestens Windows 7 und Windows Server 2008 als Betriebssystem im Einsatz haben und auch keine Uralten Netzwerkgeräten mehr zum Einsatz kommen. Daher bleiben Sie bei "RSA#Microsoft Software Key Storage Provider", und stellen Sie die Schlüssellänge auf 4096 Bit, da das Zertifikat Ihrer Stammzertifizierungsstelle möglichst sicher sein sollte und die Sicherheit maßgeblich von der Schlüssellänge abhängt. Den Hashalgorithmus stellen Sie auf SHA512 um, was SHA 2 mit 512 Bit Länge entspricht. Den Haken "Allow Administrator interaction when the private key is accessed by the CA" müssen Sie nur setzen, wenn Sie den privaten Schlüssel in einem HSM (Hardware Security Module) speichern wollen. Bei einem HSM handelt es sich um einen externen Hardware-Tresor, der den privaten Schlüssel vor fremdem Zugriff schützt.

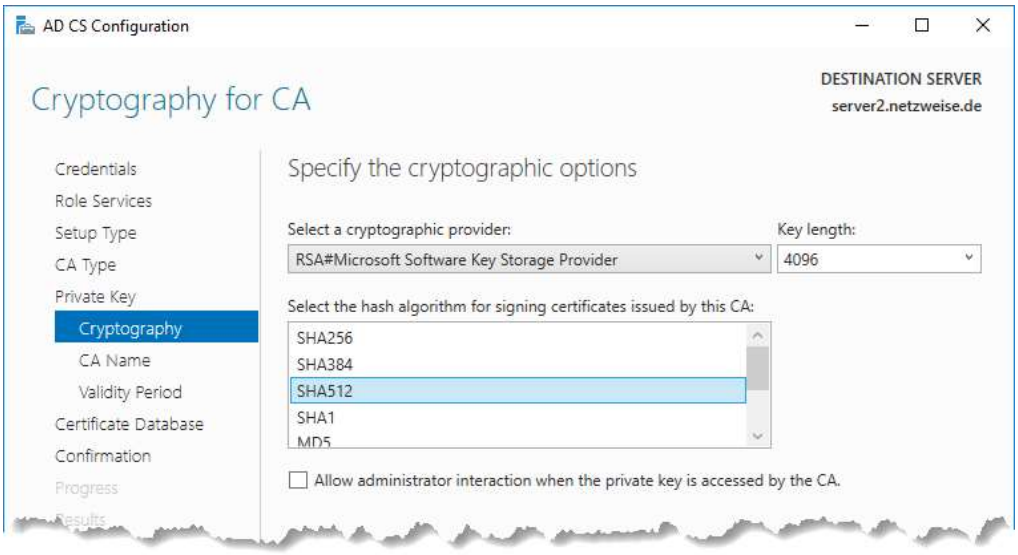


Bild 10 - Legen Sie den Algorithmus fest, der die RSA-Schlüssel generiert

Nachdem Sie die Schlüsselparameter festgelegt haben, geben Sie einen Namen für Ihre Root-CA an. Der Name kann anschließend nicht mehr geändert werden, was aber kein kritisches Problem darstellt, solange Ihr Unternehmen sich nicht umbenennt. Sind Sie häufiger in Unternehmenskäufe verwickelt, ist es eventuell sinnvoll, den Firmennamen nicht in den Namen der CA aufzunehmen.

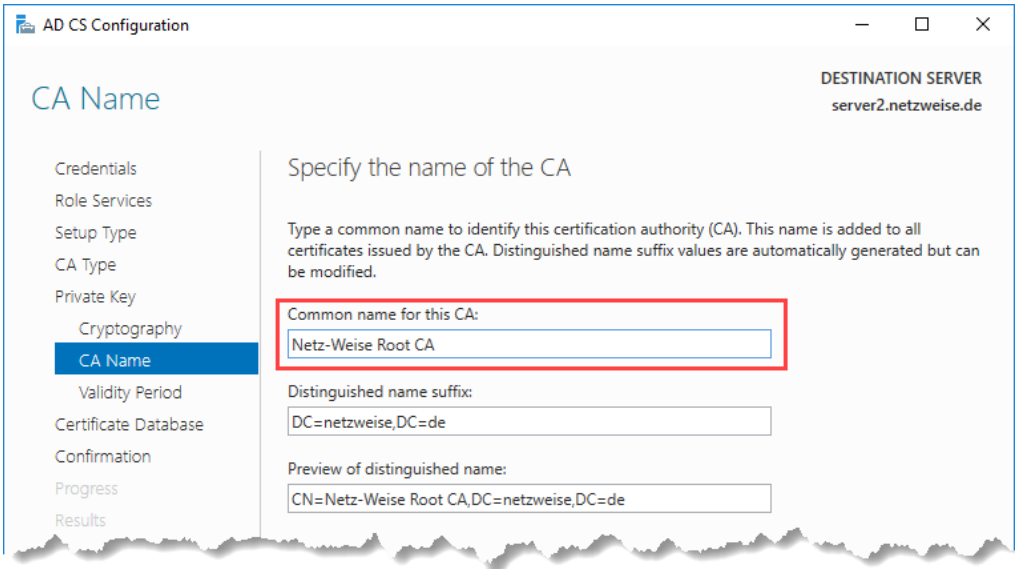


Bild 11 - Der Common name kann nachträglich nicht mehr verändert werden

Jedes Zertifikat hat ein Ablaufdatum. Achten Sie darauf, dass die maximale Laufzeit eines Zertifikats der Restlaufzeit der CA entspricht. Ist das Zertifikat der Stammzertifizierungsstelle nur noch 100 Tage gültig, kann Sie auch nur noch Zertifikate ausstellen, die 100 Tage gültig sind. Wählen Sie die Laufzeit Ihrer Root-CA daher nicht zu kurz.

Wenn die Laufzeit Ihrer CA abgelaufen ist oder die Laufzeit für ausgestellte Zertifikate zu kurz ist, können Sie das Zertifikat verlängern. Der Assistent bietet hierfür aber keinerlei Konfigurationsmöglichkeiten, und die Verlängerung findet später durch ein einfaches Klicken auf "Zertifikat verlängern" in der CA-Verwaltungskonsole statt. Wenn Sie eine produktive CA installieren wollen, sollten Sie die Parameter für die Verlängerung des CA-Zertifikats daher bereits bei der Installation über die Datei CAPolicy.inf angeben, eine Konfigurationsdatei, die während der

Installation aus dem Windows-Ordner ausgelesen wird. Die CAPolicy.inf wird im nächsten Abschnitt "Installieren einer mehrstufigen CA-Infrastruktur" beschrieben.

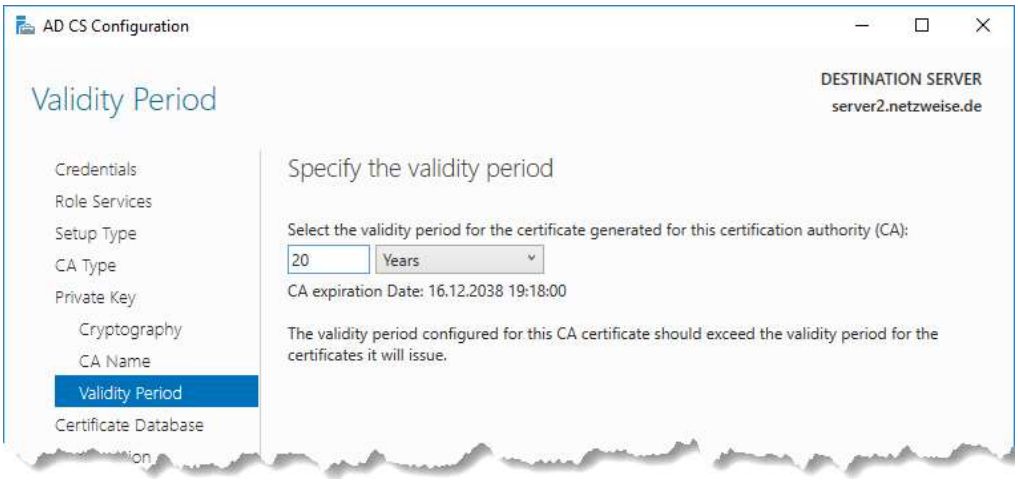


Bild 12 - Je länger die Laufzeit, desto sicherer sollten die Schlüsselparameter gewählt sein

Nun müssen Sie noch den Pfad angeben, an dem das Setup die Datenbank der Zertifizierungsstelle ablegen soll. Achten Sie darauf, dass ausreichend Speicherplatz zur Verfügung steht. Jedes Zertifikat benötigt ca. 10 KB Speicherplatz in der Datenbank. Wenn Sie mehrere 10.000 Zertifikate in der Datenbank verwalten müssen, sollten also ein paar Gigabyte Speicherplatz zur Verfügung haben. Die Datenbank selbst ist eine JET-Datenbank und verwendet das gleiche Format wie Access, Active Directory und Exchange-Server. Für produktive Server sollten Sie außerdem für die Datensicherheit der Festplatten sorgen, da ein Verlust der Datenbank sonst eventuell dazu führt, dass Sie nach der Wiederherstellung gültige Zertifikate im Umlauf haben, die Ihr Zertifikatsserver nicht kennt und auch nicht zurückrufen kann.

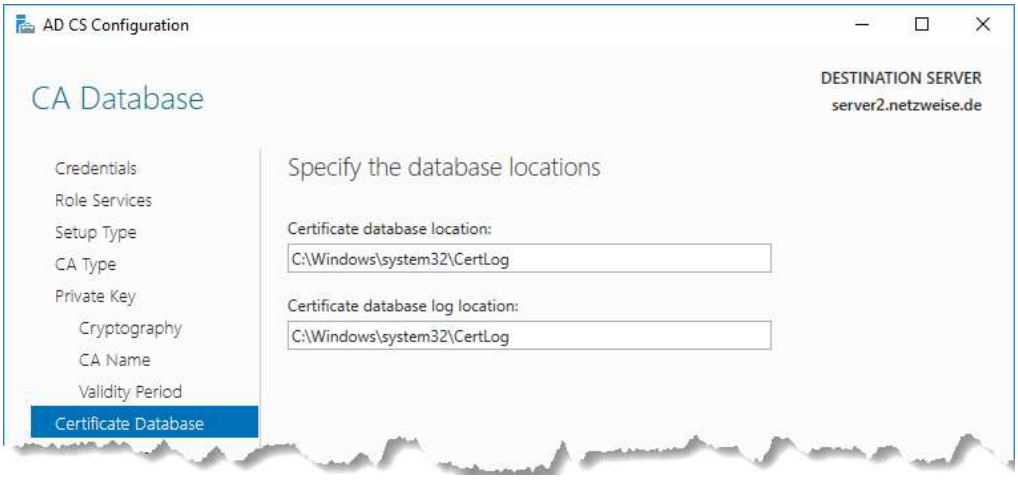


Bild 13 - Legen Sie die Datenbank auf einem RAID-gesicherten Laufwerk ab

Prüfen Sie die eingegebenen Daten noch einmal, da Sie sie nach der Installation nicht mehr ändern können, und wählen Sie anschließend "Configure", um die Konfiguration abzuschließen.

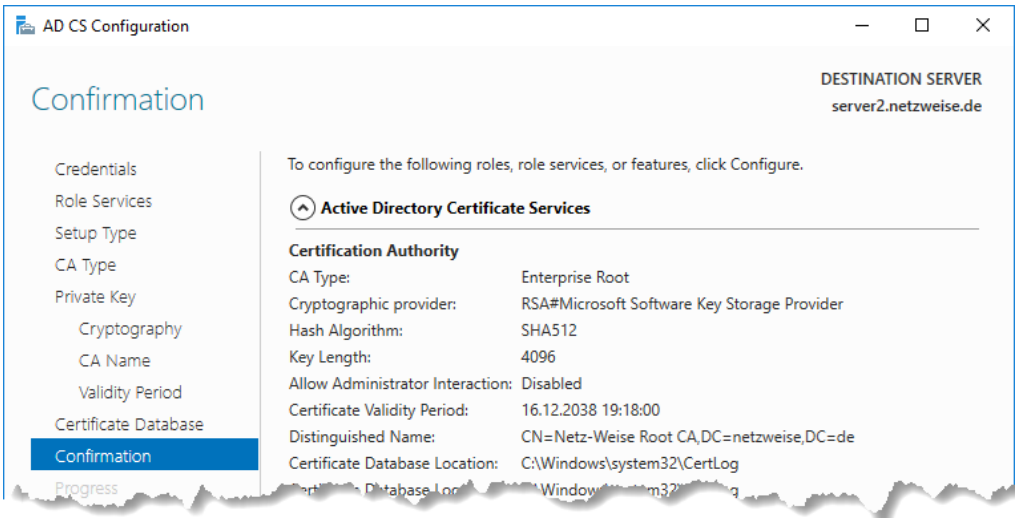


Bild 14 - Prüfen Sie die Konfiguration noch einmal, da eine Änderung hinterher nicht mehr möglich ist

Ist die Konfiguration abgeschlossen, können Sie den Zertifikatsserver über das grafische Tool "Certification Authority" aufrufen, dass Sie im Server-Manager unter Tools finden. Alternativ starten Sie Certsrv.msc über die Kommandozeile, oder administrieren Sie den Server mithilfe des Kommandozeilentools Certutil.exe. Die Unternehmens-CA ist sofort einsatzfähig, da sie Ihre Daten wie die CRL (Zertifikatsrückrufliste) und ihr eigenes Zertifikat über das Active Directory veröffentlicht.

Installieren einer mehrstufigen CA-Infrastruktur

Wie bereits in der Einführung beschrieben, ist eine einstufige Zertifikatsinfrastruktur nicht wirklich sicher, da es nicht möglich ist, eine Root-CA ungültig zu machen. Hat jemand den privaten Schlüssel einer Root-CA erbeutet, kann er damit beliebig eigene Zertifikate signieren. Mit einer zweistufigen Hierarchie wirkt man diesem Problem entgegen, indem alle Nutz-Zertifikate von einer untergeordneten Zertifizierungsstelle ausgestellt werden, deren Zertifikat von der Root-CA signiert wurde. Die Root-CA wird komplett offline genommen, nachdem sie das Zertifikat für die untergeordnete Zertifizierungsstelle ausgestellt hat. Maximale Sicherheit erreicht man, wenn man die Root-CA auf einem echten physikalischen Server installiert und die Festplatte des Servers anschließend entfernt und in einem Tresor aufbewahrt. Bei einer VM besteht nämlich das Risiko, dass die virtuelle Festplattendatei kopiert und der private Schlüssel dann aus der Datei extrahiert wird.

Für eine mehrstufige Hierarchie wird die Root-CA normalerweise nicht als Enterprise-CA installiert, sondern als alleinstehende CA. Diese kann problemloser auch langfristig heruntergefahren und geschützt werden, da sie keine Abhängigkeiten von der Domäne hat. Allerdings muss man in dieser Konfiguration noch ein paar weitere Dinge beachten, die bei einer Enterprise-CA automatisch gelöst sind. Jeder Computer muss nämlich bei der Prüfung eines Zertifikats auch immer testen, ob das Zertifikat eventuell abgelaufen ist. Dafür lädt er die Zertifikatsrückrufliste (CRL) ab und prüft, ob das Zertifikat hier gelistet ist. Wo die Zertifikatsrückrufliste zu finden ist, steht im Zertifikat. Da die Root-CA aber offline ist, muss die Rückrufliste sich auf einem anderen Server befinden, der immer erreichbar ist. Bei einer Enterprise-CA sind das die Domänencontroller, da die CRL von den Zertifikatsservern ins AD hochgeladen wird. Bei einer Alleinstehenden CA muss dies aber eine File- oder Webserver sein.

Der Abrufort der CRL wird als CRL Distribution Point oder CDP bezeichnet. Da er in jedem ausgestellten Zertifikat hinterlegt sein muss, muss er direkt nach der Installation einer

alleinstehenden CA konfiguriert werden. Gleiches gilt für den Authority Information Access (AIA). Der AIA ist der Ort, an dem das Zertifikat einer Zertifizierungsstelle abgerufen werden kann.

Der CDP und der AIA können direkt nach der Installation konfiguriert, oder schon während der Konfiguration über eine Konfigurationsdatei mitgegeben werden. Diese Datei muss manuell erstellt und unter dem Namen CAPolicy.inf im Windows-Ordner abgelegt werden. Die CAPolicy.inf kann auch noch weitere Einstellungen enthalten, wie die Zertifikatrichtlinie (Certificate Policy), eine Ausstellungserklärung (Certificate Practice Statement) und Konfigurationswerte, die bei der Verlängerung des Zertifizierungsstellenzertifikats verwendet werden sollen. Tatsächlich lassen sich diese Daten sogar nur in der CAPolicy.inf konfigurieren.

Eine Zertifikatrichtlinie beschreibt, wie Zertifikate vom Unternehmen gehandhabt werden. Hier könnte z.B. abgelegt sein, wie ein Benutzer sich authentifizieren muss, um ein Zertifikat zu erhalten, und wie man den Verlust eines privaten Schlüssels melden kann. Die Ausstellungserklärung beschreibt, welche Maßnahmen der Betreiber der CA vornimmt, um die CA zu schützen und fasst alle Zertifikatrichtlinien zusammen. Im Zertifikat wird dabei normalerweise auf eine URL verwiesen, unter der diese Daten aufgelistet sind.

Die CAPolicy.inf hat den gleichen Aufbau wie eine .ini-Datei. Sie besteht aus Kategorien, die einzelne Schlüssel-Werte Paare enthalten. Im Folgenden sehen Sie ein simples Beispiel, das für die Konfiguration der Root-CA in diesem Abschnitt verwendet wird.

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

[certsrv_server]
renewalkeylength=4096
RenewalValidityPeriodUnits=30
RenewalValidityPeriod=years
```

Diese CAPolicy.inf beschreibt lediglich die Parameter für die Erneuerung des RootCa-Zertifikats. *Renewalkeylength* gibt die Schlüssellänge an, die bei der Erneuerung eines Zertifikats verwendet werden soll, *RenewalValidityPeriod* die Einheit und *RenewalValidityPeriodUnits* die Menge der Einheiten, die das Zertifikat gültig sein soll. Das RootCA-Zertifikat soll also bei Verlängerung eine Schlüssellänger von 4096 Bit verwenden, und wieder 30 Jahre gültig sein. Der Abschnitt [Version] ist eine Pflichtabschnitt, der immer mit angegeben werden muss.

Eine ausführliche Beschreibung der CAPolicy.inf-Syntax finden Sie unter http://www.windows-infrastructure.de/installation-einer-zweistufigen-pki-two-tier-pki/ und unter https://blogs.technet.microsoft.com/askds/2009/10/15/windows-server-2008-r2-capolicy-inf-syntax/.

Installation der Root-CA

Die Root-CA installieren Sie auf einem alleinstehenden Server, der nicht Mitglied der Domäne ist. Stellen Sie dafür zuerst die Zertifikatserver-Rolle bereit, wie im Abschnitt Installieren der Zertifikats-Rolle beschrieben. Anschließend kopieren Sie die CAPolicy.inf in den %Systemroot%-Ordner und starten die CA-Konfiguration.

Im Register Credentials können Sie das Benutzerkonto wechseln, mit dem die Installation ausgeführt wird. Sie benötigen lokale Administratorrechte, um die Installation abschließen zu können.

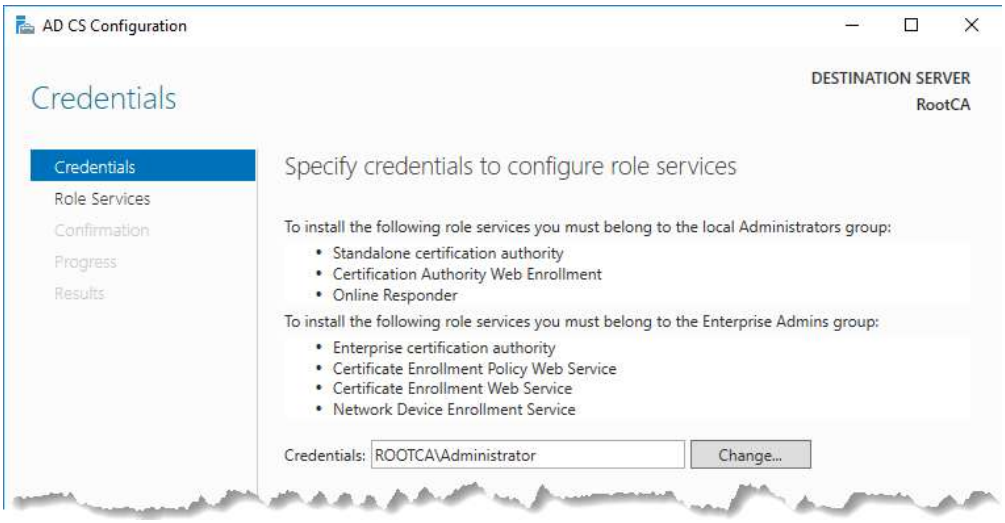


Bild 15 - Sie benötigen lokale Administratorrechte für die Installation

Im nächsten Schritt wählen Sie die zu installierenden Rollendienste aus. Da Sie nur die Zertifikatsautorität installiert haben, können Sie auch nur diese konfigurieren.

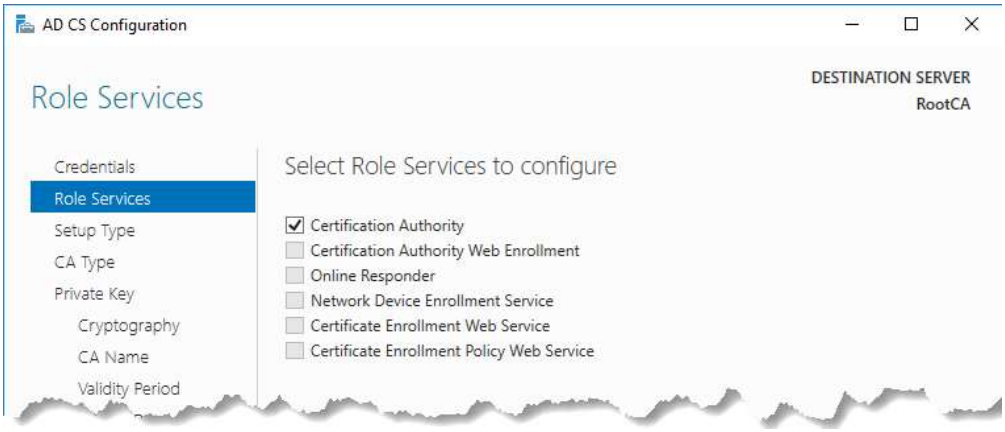


Bild 16 - nur die installierten Dienst lassen sich konfigurieren

Da die Root-CA eine alleinstehende Zertifizierungsstelle ohne Abhängigkeiten vom AD sein soll, wählen Sie im nächsten Schritt "Standalone CA" aus.

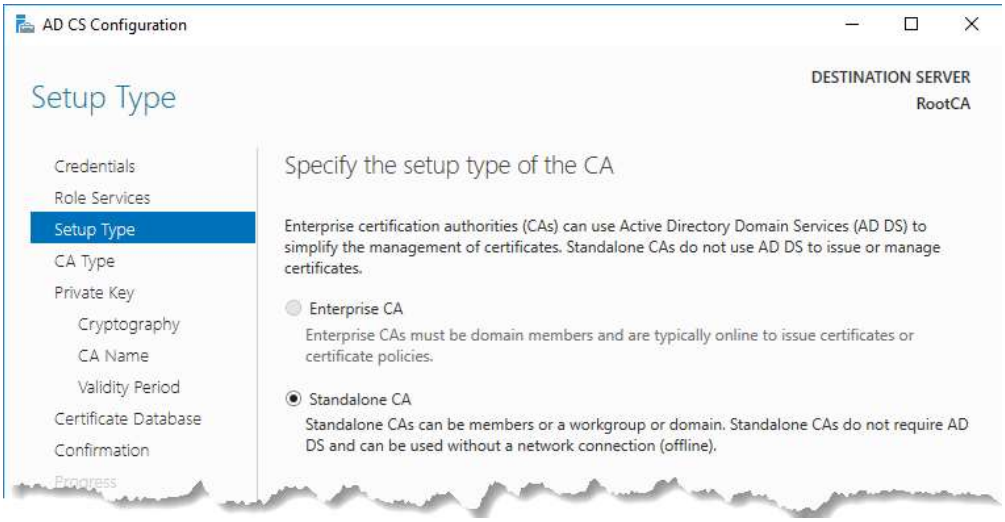


Bild 17 - Die Root-CA wird aus Sicherheitsgründen als Standalone-CA installiert

Wählen Sie als CA-Typ Root-CA aus. Die Root-CA signiert sich als Vertrauensursprung Ihr Zertifikat selbst. Denken Sie daran, dass das Zertifikat der Root-CA nach der Installation auf allen Clients verteilt werden muss, da die Clients der Root-CA (und ihren ausgestellten Zertifikaten) sonst nicht vertrauen. Das kann per Gruppenrichtlinien oder durch Veröffentlichen im AD geschehen.

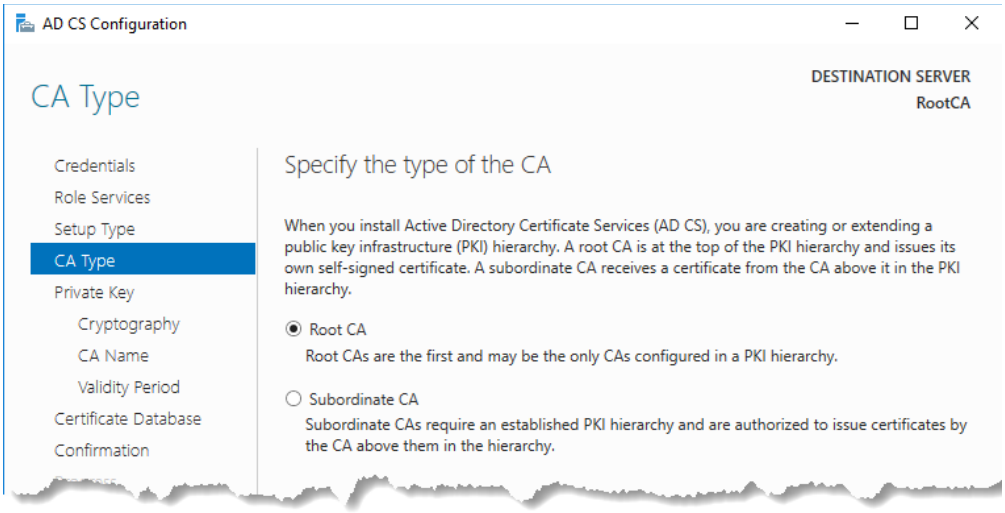


Bild 18 - Die erste Zertifizierungsstelle wird als Root-CA konfiguriert

Die Konfiguration des Schlüsselpaars und des Root-Zertifikats ist identisch mit der Konfiguration, die für die alleinstehende Unternehmens-CA vorgenommen wurde. Die Konfiguration für die Schlüsselverlängerung kann nicht durch den Assistenten vorgenommen werden, ist aber durch die CAPolicy.inf abgedeckt.

Bild 19 - erstellen Sie das Schlüsselpaar

Für die Schlüsselerstellung wird wieder der "RSA#Microsoft Software Key Storage Provider" Provider verwendet. Der Key Storage Provider ist nur für die Erstellung des Schlüsselpaars verantwortlich und hat mit den weiteren Einstellungen der Root-CA nichts zu tun! Für optimale Sicherheit verwenden Sie die höchstmögliche Schlüssellänge von 4096 Bit und SHA2 mit 512 Bit Hashlänge, auch abgekürzt als SHA512.

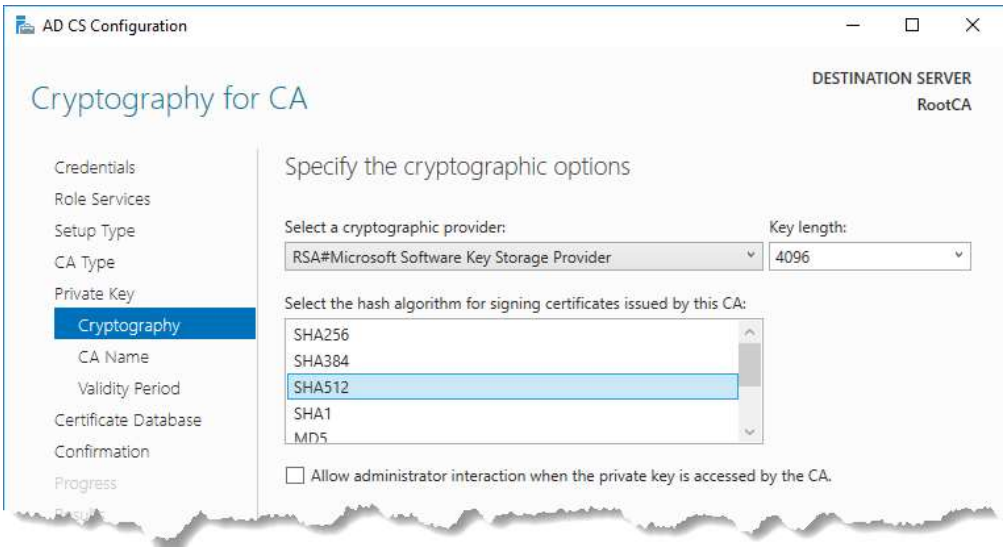


Bild 20 - Legen Sie die RSA-Schlüsselkonfiguration fest

Die CA benötigt einen Namen. Der Name kann nach der Installation nicht mehr verändert werden. Wenn die Wahrscheinlichkeit besteht, dass Ihr Unternehmen in nächster Zeit umbenannt wird, verwenden Sie Ihren Firmennamen besser nicht im Namen der CA.

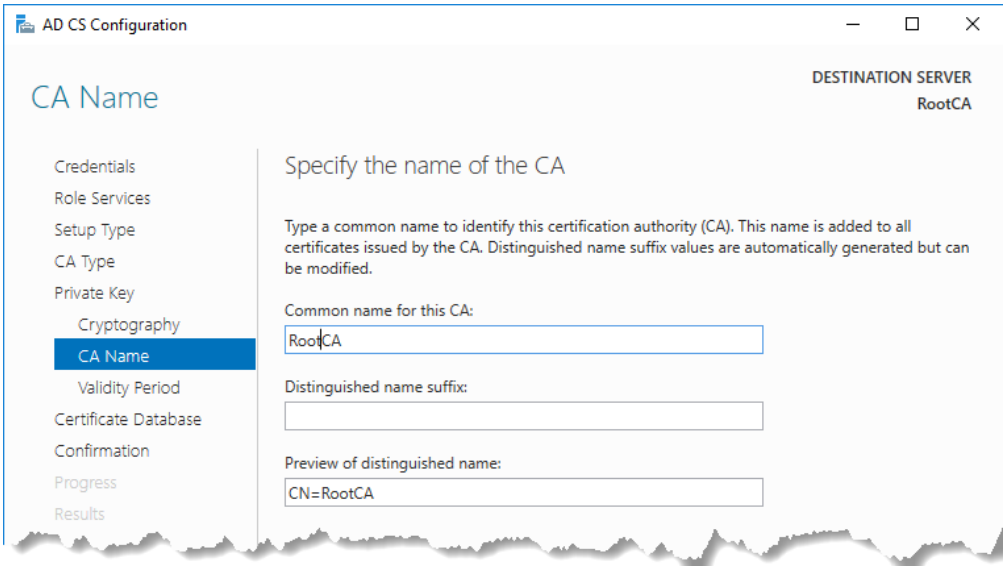


Bild 21 - der Common Name des Zertifizierungsstelle und des Zertifikats der Root-CA

Legen Sie die Gültigkeitsdauer des Root-Zertifikats fest. Bei einer mehrstufigen CA ist die Laufzeit wichtiger als bei einer alleinstehenden CA, denn die Gültigkeitsdauer eines Zertifikats kann niemals länger sein als die Rest-Gültigkeitsdauer des Zertifikats der ausstellenden CA. Hat die Root-CA also eine Gültigkeit von 5 Jahren, kann Sie nach 3 Jahren nur noch Zertifikate mit einer Gültigkeit von maximal 2 Jahren ausstellen. Da die Root-CA aber nur Zertifikate für untergeordnete CAs ausstellt, die wiederum Zertifikate ausstellen müssen, halbiert sich die nutzbare maximale Gültigkeitsdauer mit jeder zusätzlichen Ebene. Hierzu ein kurzes Beispiel:

Sie möchten Zertifikate für Ihre Benutzer ausstellen, die maximal 3 Jahre gültig sind. Damit muss die ausstellende CA über ein Zertifikat verfügen, dass noch mindestens 3 Jahre gültig ist. Da neue Zertifikate, die Sie in einem Jahr ausstellen, immer noch 3 Jahre gültig sein sollen, wählt man sinnigerweise für die ausstellende CA mindestens die doppelte Gültigkeitsdauer der maximalen Gültigkeitsdauer eines Nutzer-Zertifikats, plus einem Puffer, damit das Zertifikat der

Zertifizierungsstelle problemlos verlängert werden kann. Die Verlängerung wird dann normalerweise nach Ablauf von ca. der Hälfte der Laufzeit des Zertifikats der Zertifizierungsstelle vorgenommen, da ab diesem Zeitpunkt ja die Laufzeit der ausgestellten Zertifikate wieder nur so lang sein kann wie das Zertifikat der ausstellenden Zertifizierungsstelle. Da die untergeordnete Zertifizierungsstellen Ihre Zertifikate von der Root-CA beziehen, und für diese die gleiche Regel gilt, muss die Root-CA die doppelte Gültigkeit der Laufzeit der untergeordneten CAs haben, plus einem Puffer. Legen wir also die maximale Laufzeit eines Zertifikats auf 3 Jahre fest, muss die Laufzeit der untergeordneten CAs 6 Jahre plus Puffer (sagen wir 7 Jahre) betragen, und die Laufzeit der Root-CA 14 Jahre plus Puffer, sagen wir also 15 Jahre. Root-CAs in einer mehrstufigen Hierarchie haben daher immer sehr lange Laufzeiten. Die Laufzeit, die für ein Zertifikatsverlängerung verwendet wird, kann übrigens nur in der CAPolicy.inf angegeben werden.

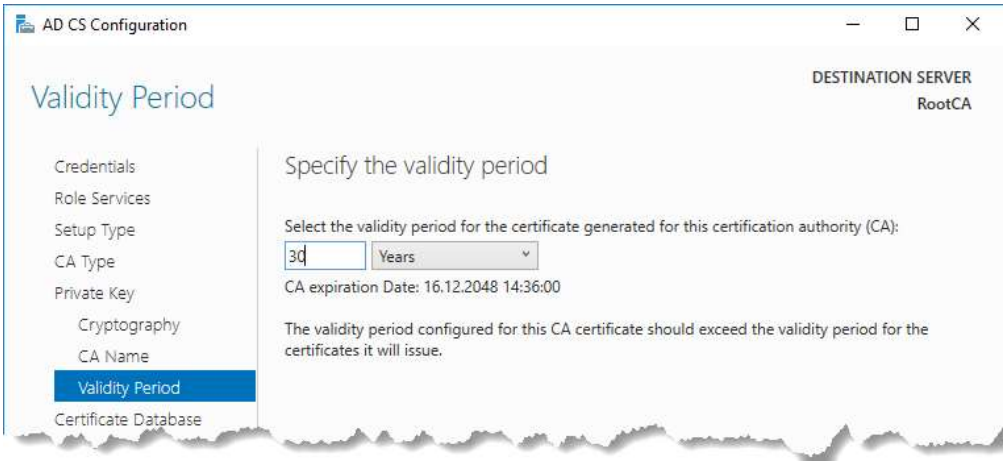


Abbildung 1 - bei 30 Jahren Laufzeit haben Sie eine Menge Puffer oder mind. 2 CA-Hierarchien

Als nächstes legen Sie wieder den Pfad an, der für die Datenbankdateien benutzt werden soll (s. Installieren eines alleinstehenden Unternehmens-Zertifikatsservers) und prüfen noch einmal Ihre Eingabe, bevor Sie die Konfiguration starten.

Nach Beendigung der Konfiguration müssen Sie den CDP und AIA anpassen, sowie die CRL-Konfiguration festlegen. Öffnen Sie hierzu die Zertifizierungsstellen-Konsole, indem Sie sie aus dem Server-Manager aufrufen, oder direkt über CertSrv.msc aus der Kommandozeile. In der Konsole wählen Sie aus dem Kontextmenü der CA "Eigenschaften" aus. Das Anzeigen der Eigenschaften dauert einen Moment. Anschließend wechseln Sie auf die Registerkarte "Erweiterungen" bzw. "Extensions". Hier finden Sie die Veröffentlichungseinstellung der CA für den CDP und AIA.

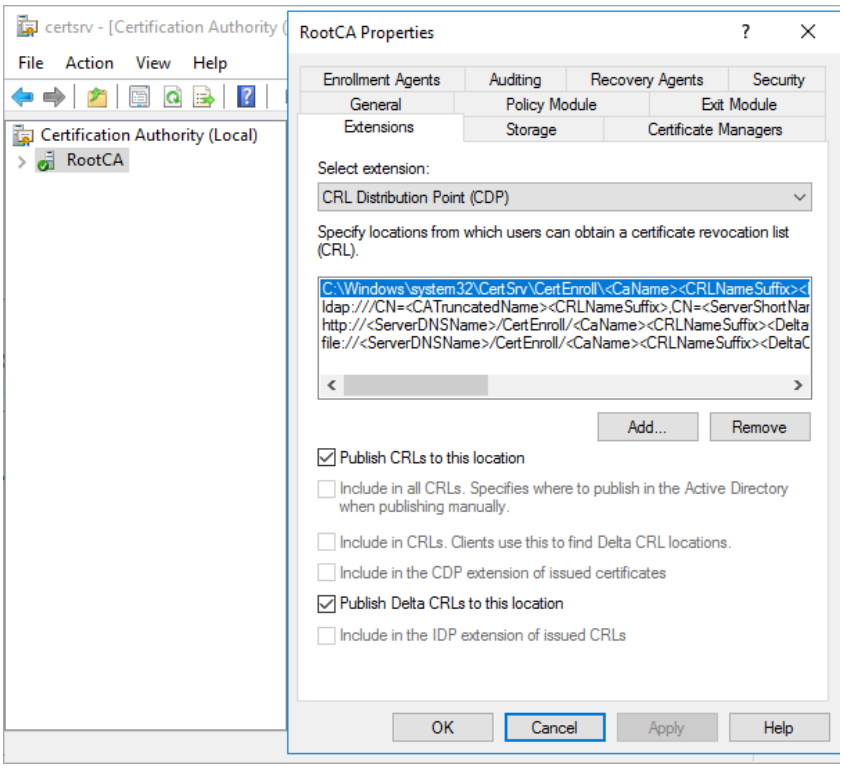


Bild 22 - Mit Erweiterungen sind der CDP und der AIA gemeint

Passen Sie zuerst die Konfiguration des CDP an, indem Sie alle Einträge bis auf den ersten, der auf das lokale Dateisystem verweist, entfernen. Anschließend legen Sie einen neuen Veröffentlichungspfad mit "Add…" an.

Das Fenster "Add Location" erlaubt das Veröffentlichen per HTTP, LDAP und Dateisystempfaden, wobei ein Dateisystempfad auch auf eine Freigabe sein kann. Da alle Client-Betriebssysteme auf einen Webserver zugreifen können, ist dies die am häufigsten gewählte Methode. Sie benötigen hierfür einen Webserver, dessen Installation im Abschnitt "Installation eines Web-Servers zur Veröffentlichung von CRL und AIA" beschrieben ist.

Der Veröffentlichungspfad kann dynamisch mit Hilfe von Variablen erzeugt werden. Die Variablen können Sie über das Listenfeld "Variable" auswählen und mit dem Knopf "Insert" in das "Location:"-Feld einfügen. Da der Pfad zum Webserver fest ist, geben Sie zuerst die URL zum Server sowie das Unterverzeichnis an, in dem die CRL hinterlegt werden soll. Im Beispiel ist das der Pfad "http://Web.netzweise.de/CertEnroll/". Anschließend folgt eine Variable, die den Namen der Datei bestimmt, die generiert wird. Wählen Sie die Variable <CaName>, um den Namen Ihrer CA als Dateinamen anzugeben. Anschließend wählen Sie die Variable <DeltaCRLAllowed>. Diese Variable wird nur ausgewertet, wenn Sie eine DeltaCRL erzeugen, und fügt an den Dateinamen ein "+" an, so dass der Dateiname der DeltaCRL "IhreCA+".crl ist. Sie finden ein Beispiel für die Benennung der Datei im Beschreibungsfeld. Wenn Sie die Daten aus dem Location-Feld gelöscht haben und nicht mehr wissen, was Sie eintragen sollen, können Sie das Beispiel als Orientierungshilfe verwenden.

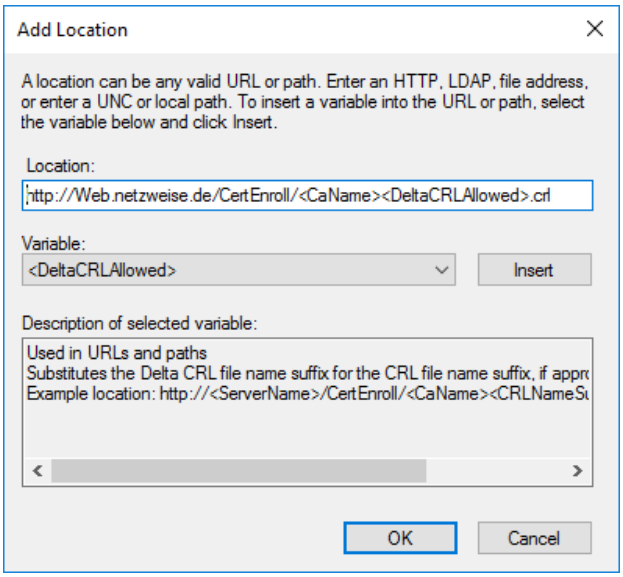


Bild 23 - Die Location besteht aus dem Pfad zur CRL und Variablen für den Dateinamen

Wenn Sie den Pfad bestätigt haben, legen Sie über die Optionen fest, wo der CRL-Pfad veröffentlicht werden soll. Aktivieren Sie "Include in CRLs. Clients use this to find Delta CRL locations", "Include in the CDP extensions of issued certficates" und "Include in the IDP extensions of issued CRLs". Alle anderen Optionen können Sie für per http veröffentlichte CRLs nicht auswählen.

Sie können für jeden hinterlegten Veröffentlichungspfad mehrere Einstellungen vornehmen, die hier mit Ihren deutschen Namen beschrieben sind:

Sperrlisten an diesem Ort veröffentlichen	Gibt an, dass die Sperrliste automatisch an den angegebenen Zielort kopiert wird. Das funktioniert nur mit Dateiservern und LDAP-Pfaden, da das Schreiben in eine URL nicht möglich ist. Wollen Sie eine CRL auf einem Webserver veröffentlichen, müssen Sie sie daher manuell kopieren.
In alle Sperrlisten einbeziehen - Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll	Diese Option kann nur bei LDAP-Pfaden gesetzt werden und gibt an, dass die CRL am angegebenen Pfad im AD veröffentlicht werden soll. Sie ist nur bei alleinstehenden CAs sinnvoll, da Enterprise-CAs Ihre Sperrlisten automatisch im AD veröffentlichen.
In Sperrlisten einbeziehen – wird zur Suche von Deltasperrlisten verwendet	Delta-Sperrlisten sind verkürzte Sperrlisten, die nur die Zertifikate enthalten, die seit dem Veröffentlichen der letzten Sperrliste widerrufen worden sind. Wenn Sie Delta-Sperrlisten veröffentlichen wollen, müssen Sie diese Option setzen. Sie sorgt dafür, dass in allen ausgestellten CRLs der angegeben Pfad als Suchpfad für Delta-CRL-Listen angegeben wird.
In CDP-Erweiterungen des ausgestellten Zertifikats einbeziehen	Legt fest, dass der Sperrlistenpfad in jedes Zertifikat mit aufgenommen wird, dass die CA ausstellt. Dateisystem-Pfade können nicht in einem Zertifikat hinterlegt werden. Ist in einem Zertifikat einer alleinstehenden CA kein CDP hinterlegt, kann der Client Zertifikate der CA nicht validieren und lehnt sie ab.
Deltasperrlisten an diesem Pfad veröffentlichen	Wenn Sie diese Konfiguration aktivieren, werden Delta-Sperrlisten am angegebenen Pfad erstellt. Delta-Sperrlisten

tragen den gleichen Namen wie die Sperrliste, allerdings mit einem "+" am Ende des Namens.

In die IDP-Erweiterungen ausgestellter CRLs einbeziehen

Nicht-Windows-Clients nutzen die IDP-Erweiterung zum Prüfen der Sperrliste. Wenn Sie nicht-Windows-Clients im Einsatz haben, sollten Sie diese Option setzen, damit diese die CRL abrufen und prüfen können.

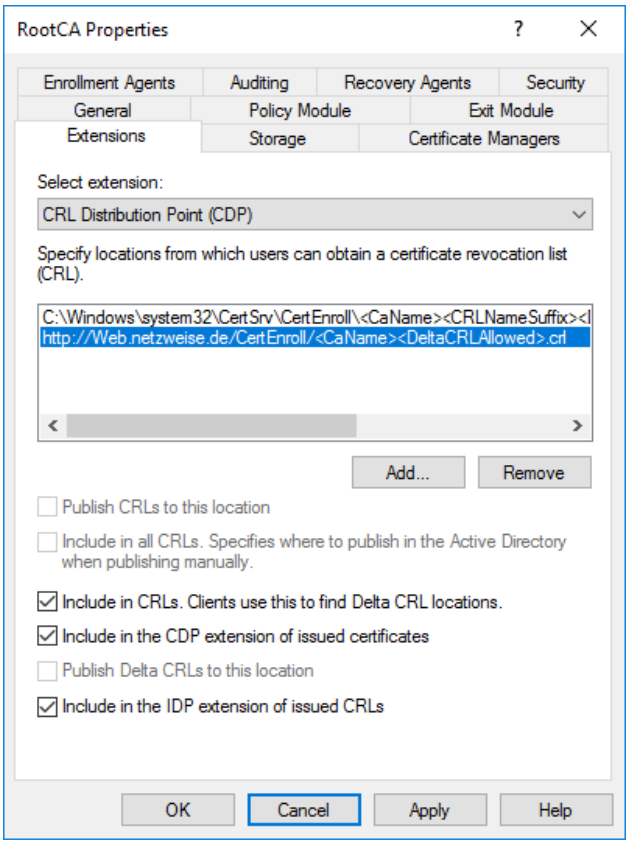


Bild 24 - aktivieren Sie alle aktivierbaren Optionen für die http-basierte CRL

Wenn Sie die Einstellungen übernehmen wollen, fragt Windows Sie, ob die CA neu gestartet werden soll. Wählen Sie nein, da der AIA auch noch konfiguriert werden muss.

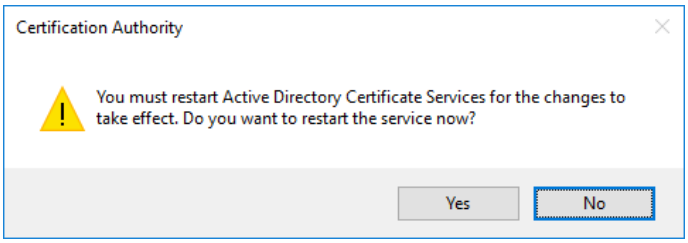


Bild 25 - Starten Sie die CA nicht neu, da noch weitere Konfigurationseinstellungen vorgenommen werden

Wählen Sie unter "Select extensions:" jetzt "Authority Information Access (AIA)" bzw. "Zugriff auf Stelleninformation" aus und entfernen Sie ebenfalls alle Einträge bis auf den Ersten, der das Zertifikate der CA im Dateisystem ablegt. Dann legen Sie wieder einen neuen Veröffentlichungspfad an. Da die CRL und das Zertifikat der CA beide auf dem Webserver hinterlegt werden sollen, geben Sie die gleiche URL an wie für die CRL, im Beispiel also "http://web.netzweise.de/CertEnroll/". Auch hier verwenden Sie zum Erstellen Variablen, und zwar <CaName> für den Namen der CA und

<CertificateName>. <CertficateName> ist tatsächlich nicht der Name des Zertifikats, sondern dessen Versionsnummer. Die Versionsnummer wird gezählt, sobald Sie das Zertifikat der Zertifizierungsstelle erneuern – das erste Zertifikat wird noch ohne Versionsnummer erstellt. Für die AIA wird als Zertifikatsendung .crt verwendet, so dass der vollständige Pfad so aussieht:

```
http://web.netzweise.de/CertEnroll/<CaName><CertificateName>.crt
```

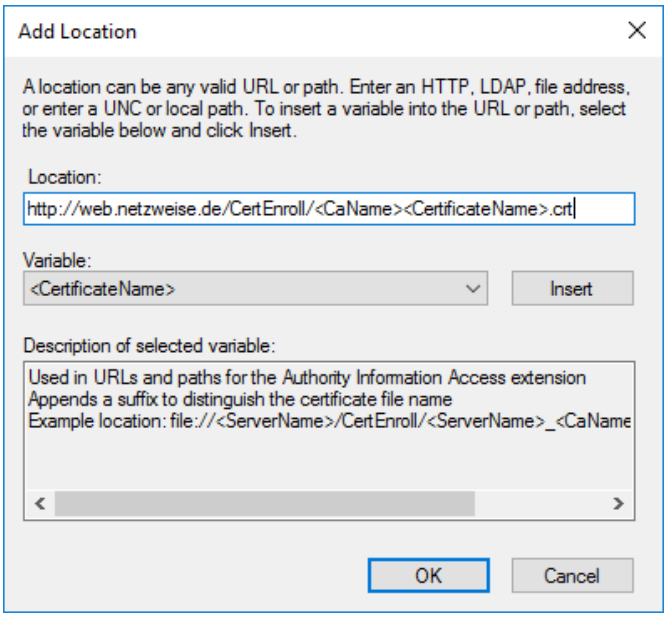


Bild 26 - Geben Sie den Veröffentlichungspfad zum RootCa-Zertifikat an

Nachdem Sie den Pfad angepasst haben, wählen Sie die Option "Include in the AIA extension of issued Certificates" oder "In AIA-Erweiterung des ausgestellten Zertifikats einbeziehen", um die AIA in alle neuen Zertifikate einzutragen.

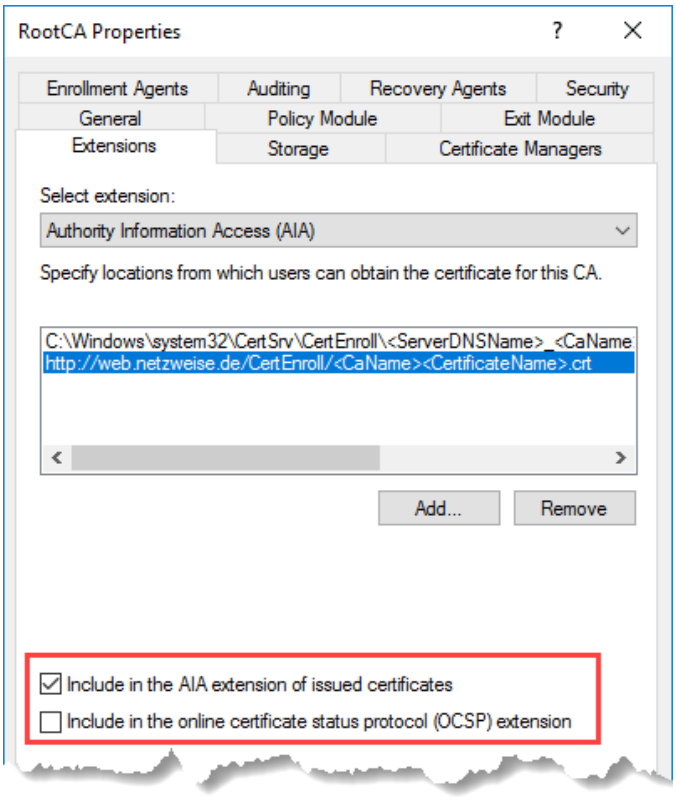


Bild 27 - Der AIA muss in allen neu ausgestellten Zertifikaten enthalten sein

Vergessen Sie nicht, die CA jetzt einmal neu zu starten, um die Änderungen zu übernehmen.

Eigenständige CAs stellen standardmäßig kein Zertifikat aus, das länger als ein Jahr gültig ist. Da die untergeordnete CA aber 15 Jahre gültig sein soll (die Hälfte der Laufzeit der Stamm-Zertifizierungsstelle – wir verzichten bei der Laufzeit in diesem Fall gnädig auf eine Puffer), müssen wir die maximale Laufzeit erhöhen. Das passiert über einen Registry-Key, den wir mit Hilfe des Kommandozeilentools CertUtil.exe einigermaßen bequem anpassen können. Mit dem Parameter -setreg können Sie Konfigurationswerte in der Registrierung direkt setzen:

```
PS> Certutil -setreg ca\validityperiodunits 15
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\RootCA\V
alidityPeriodUnits:

Old Value:
  ValidityPeriodUnits REG_DWORD = 1

New Value:
  ValidityPeriodUnits REG_DWORD = f (15)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS> restart-service certsvc
```

Installation eines Web-Servers zur Veröffentlichung von CRL und AIA

Die Zertifikatsrückrufliste einer CA und das CA-Zertifikat müssen zu jeder Zeit verfügbar sein. Am besten verwenden Sie einen Webserver als CDP und AIA. Installieren Sie hierzu auf einem Server den IIS (Internet Information Service). Die Installation ist ziemlich simpel, da Sie keine großen Anpassungen an der Basisinstallation vornehmen müssen und der Zugriff auf CDP und AIA nicht über https abgesichert werden muss. Tatsächlich ist es sogar empfohlen, den Zugriff nur per http zu konfigurieren. Für die Beispielkonfiguration sind der CDP und der AIA bereits auf der Root-CA unter dem DNS-Namen Web.netzweise.de hinterlegt. Der Computer, auf dem der Webserver installiert ist,

muss also entweder den Namen web tragen, oder es muss ein zusätzlicher A-Record im DNS-Server eingetragen werden.

Auf dem zukünftigen Web-Server aktivieren Sie zuerst die Webserver-Rolle im Server-Manager.

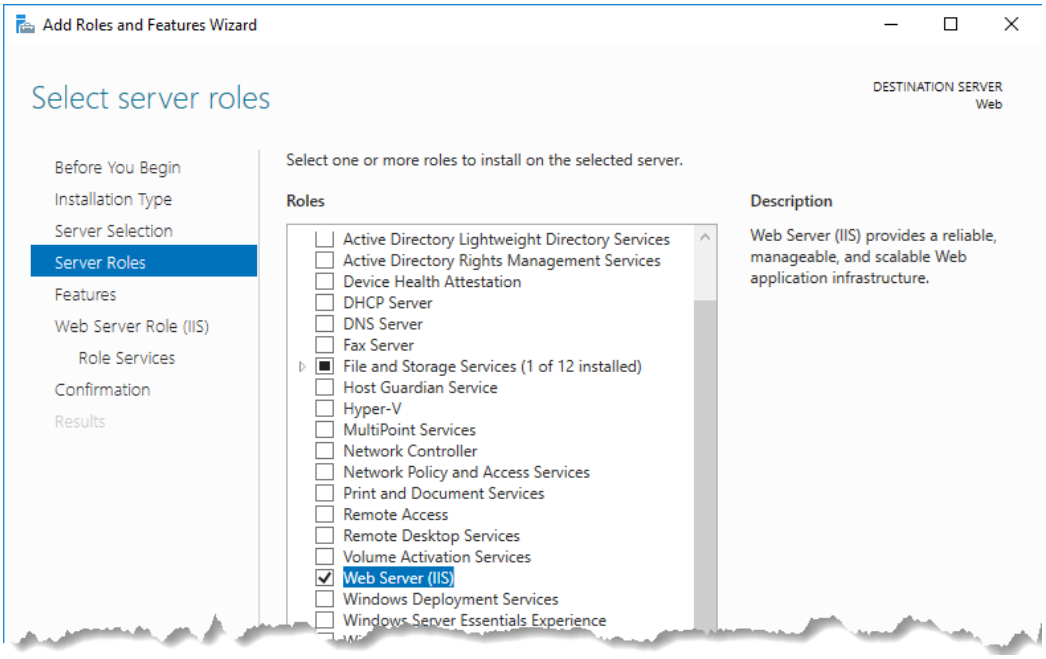


Bild 28 - Die IIS-Server Rolle heißt Web Server(IIS)

Installieren Sie den IIS mit der Standard-Rollenkonfiguration. Sie brauchen keine Anpassungen vornehmen.

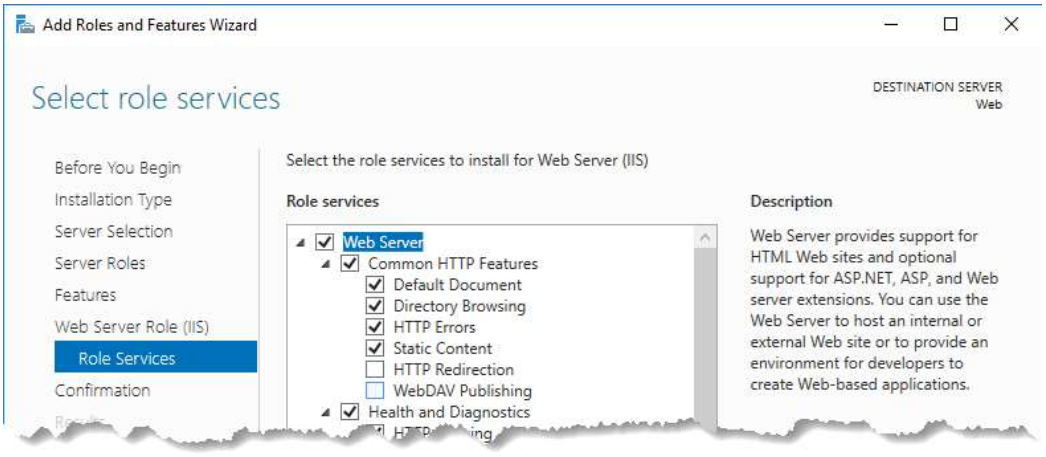


Bild 29 - Installieren Sie die Standard-Funktionen

Sobald die Installation abgeschlossen ist, ist der IIS funktionsfähig. Abschließend müssen sie nur noch die CRL und den das CA-Zertifikat auf den Webserver kopieren. Wenn Sie den Computernamen des Webservers im Browser aufrufen (http://Web.netzweise.de/), wird standardmäßig der Inhalt des Ordners "`%Systemdrive%\Inetpub\wwwroot\`" angezeigt. Da in der CDP- und AIA-Erweiterung der Unterordner `\Certenroll\` angegeben wurde, legen Sie diesen an. Anschließend kopieren Sie die beiden Dateien mit den Endungen *.crl und *.crt aus dem Ordner "%systemroot%\System32\CertSrv\Certenroll" des Root-CA-Servers in den neu erstellen Unterorder auf dem Webserver. Benennen Sie die *.crt-Datei noch in <CaName>.crt um. Die CRT-Datei ist das Zertifikat des Rootservers, und das wird beim ersten Ausstellen und beim Verlängern des Zertifikats

in den Certenroll-Ordner kopiert, allerdings unter dem Namen <ServerShortName>_<CaName><Version>.crt, was nicht der Vorgabe entspricht, die wir in der Erweiterung auf der Root-CA konfiguriert haben. Benennen Sie die Datei daher in den korrekten Namen um, im Beispiel "RootCA.crt".

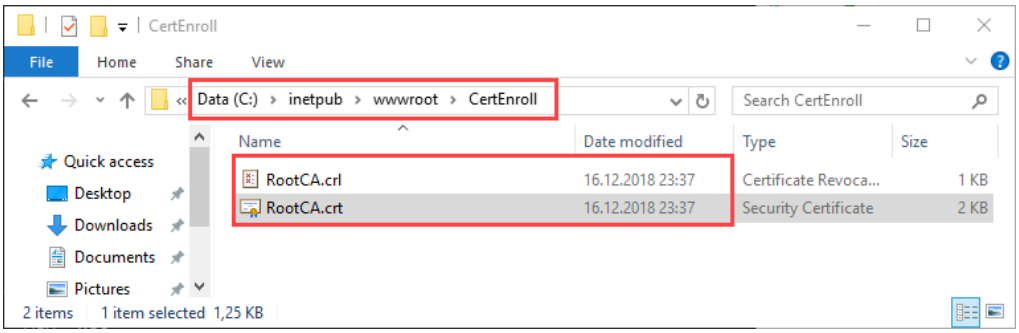


Bild 30 - unter inetput\wwwroot befindet sich der Stammordner des IIS

Anschließend können Sie von einem beliebigen Server aus testen, ob die beiden Dateien verfügbar sind, indem Sie in einem Webbrowser den die URL des Servers mit Unterverzeichnis und Dateinamen angeben:

`http://web.netzweise.de/CertEnroll/RootCA.crl`

Haben Sie alles richtig gemacht, sollte Ihnen die Datei zum Download angeboten werden.

Verteilen des Root-CA Zertifikats auf die Domänen-Clients

Die neu installierte Root-CA ist nutzlos, solange Ihre Clients der Root-CA nicht vertrauen. Um die Root-CA vertrauenswürdig zu machen, müssen Sie das Root-CA Zertifikat auf den Clients den vertrauenswürdigen Stammzertifizierungsstellen hinzufügen. Das geht über Gruppenrichtlinien oder noch einfacher, indem Sie das Zertifikat im AD hinterlegen. Da Sie für den AD-Zugriff einen Computer brauchen, der Mitglied der Domäne ist, bietet sich hierfür der Web-Server an, denn hier haben Sie das Zertifikat der Root-CA ja gerade abgelegt.

Zum Veröffentlichen verwenden sie Certutil.exe mit dem Parameter -dspublish. Außerdem müssen Sie den Pfad zum Zertifikat mit dem Parameter -f angeben, und Sie müssen festlegen, wohin im AD das Zertifikat veröffentlich werden soll:

Certutil.exe -dspublisch -f <ZertifikatsDatei> RootCA

In unserem Beispiel wechseln Sie auf dem Webserver in den Inetpub\wwwroot\CertEnroll-Order:

```
PS> certutil -dspublish -f RootCA.crt RootCA
ldap:///CN=RootCA,CN=Certification Authorities,CN=Public Key
Services,CN=Services,CN=Configuration,DC=netzweise,DC=de?cACertificate

Certificate added to DS store.

ldap:///CN=RootCA,CN=AIA,CN=Public Key
Services,CN=Services,CN=Configuration,DC=netzweise,DC=de?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.
```

Installieren der untergeordneten CA

Nachdem die Root-CA installiert und die CRL verfügbar ist, können Sie nun die untergeordnete CA installieren. Grundsätzlich gestaltet sich der Installationsprozess ähnlich zur Installation der Root-CA, daher gehe ich hier nur auf die Besonderheiten ein.

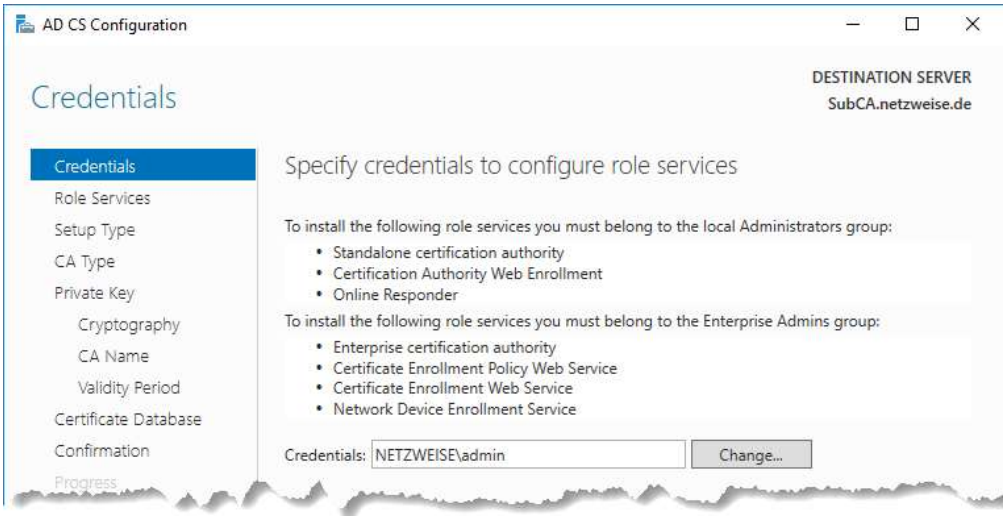


Bild 31 - Verwenden Sie ein Benutzerkonto, das Organisationsadministrator-Rechte hat

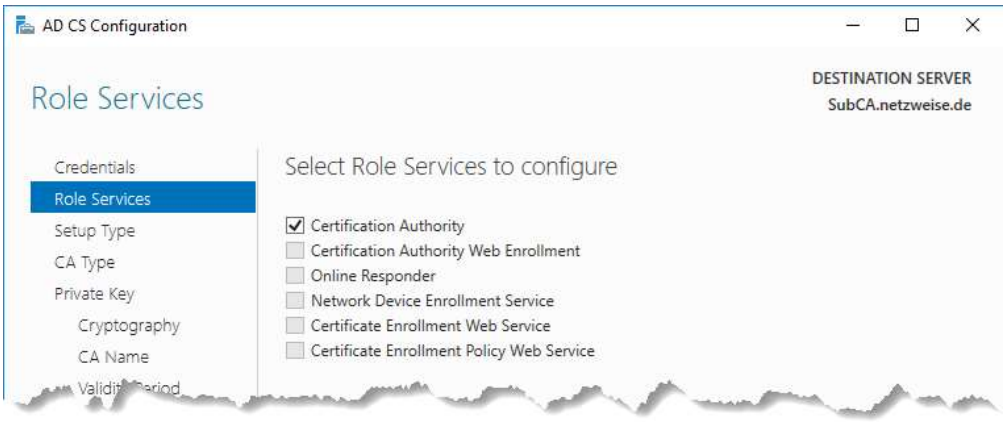


Bild 32 - Installatieren Sie die Zertifikatsserver-Rolle

Die untergeordnete CA soll Zertifikate in der Domäne automatisch ausrollen können und muss daher als Unternehmenszertifizierungsstelle (Enterprise CA) installiert werden.

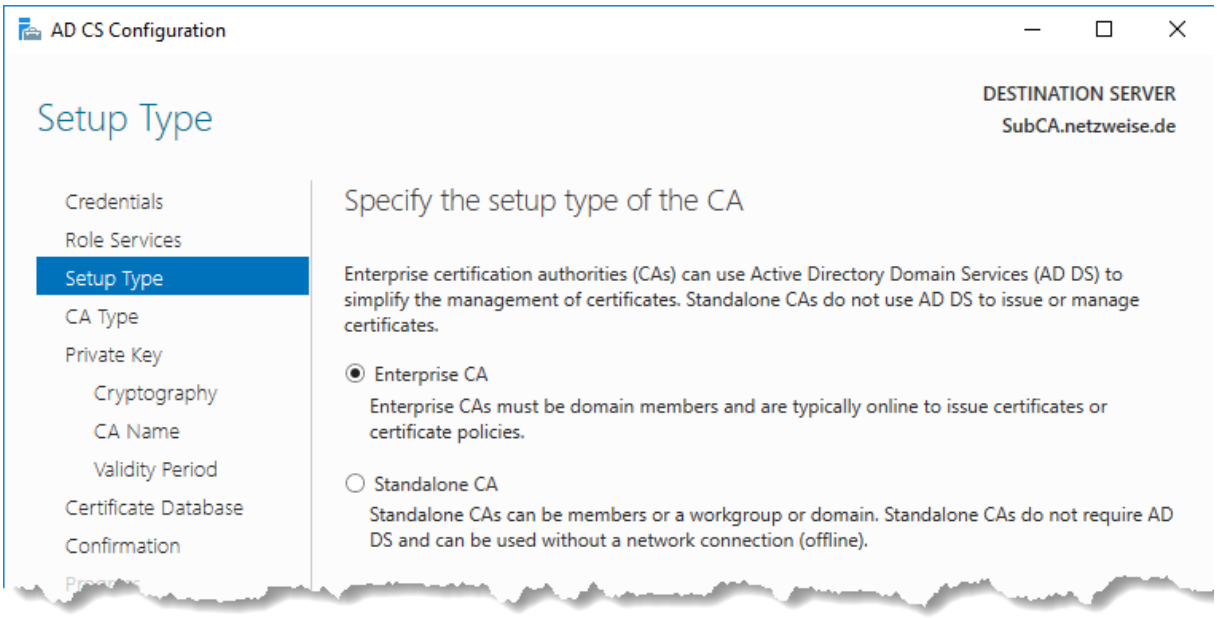


Bild 33 - Die Sub-CA ist eine Unternehmens-CA

Wählen Sie als Typ der Zertifizierungsstelle "Untergeordnete Zertifizierungsstelle" oder englisch "Subordinate CA" aus.

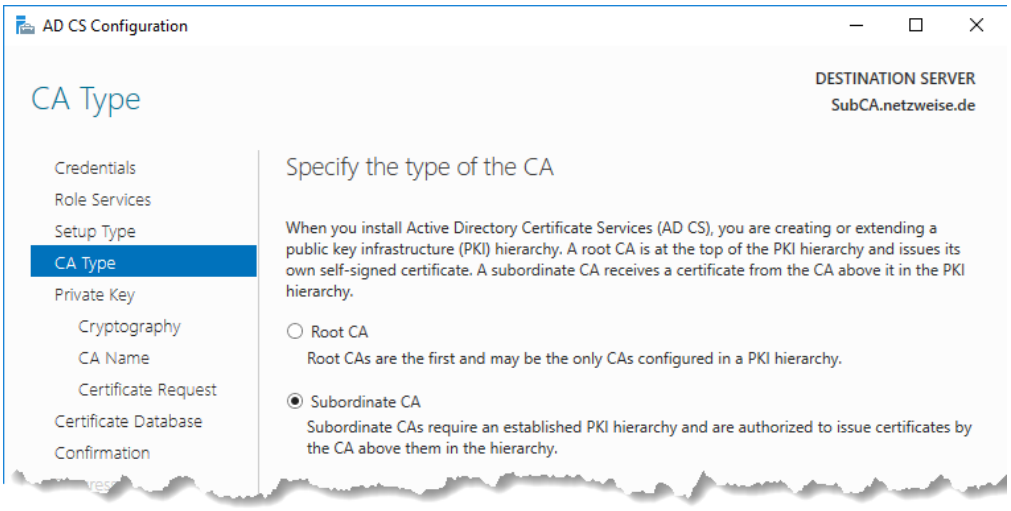


Bild 34 - Die neue Zertifizierungsstelle ist der Root-CA untergeordnet

Da es sich um eine Neuinstallation handelt, wird wieder ein neues Schlüsselpaar generiert, das anschließend von der Root-CA signiert werden muss.

Bild 35 - vorhandene Schlüsselpaare werden nur bei einer Wiederherstellung verwendet

Auch die untergeordnete Zertifizierungsstelle sollte nur mit möglichst sicheren Algorithmen arbeiten.

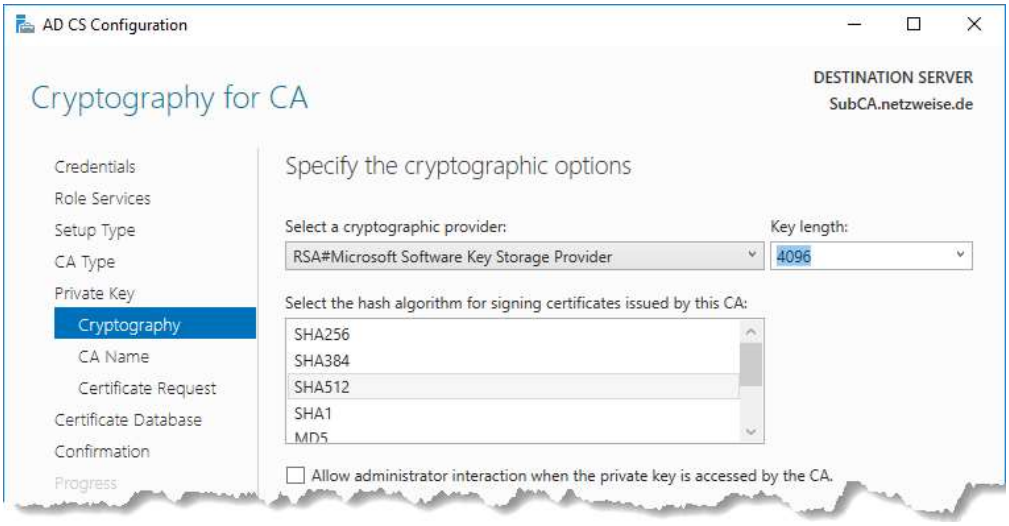


Bild 36 - Wählen Sie den RSA#Microsoft Software Key Storage Provider mit 4096 Bit Schlüssellänge und SHA512

Legen Sie den Namen für die SubCA fest. Im Beispiel heißt Sie SubCA1.

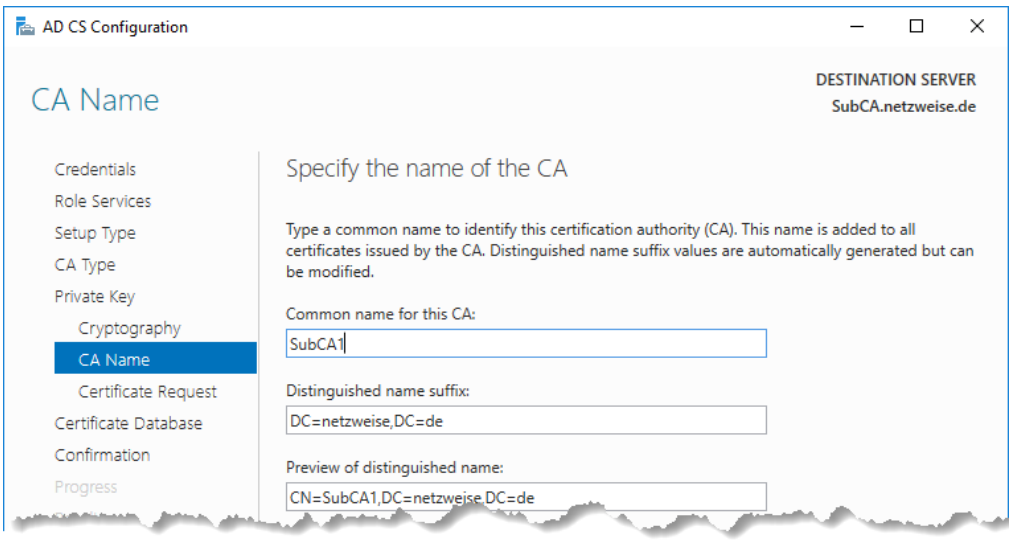


Bild 37 - Geben Sie einen Namen für die CA an

Die untergeornete CA kann sich Ihren Schlüssel nicht selber ausstellen. Daher muß Sie ein Zertifikatsrequest für Ihren öffentlischen Schlüssel generieren, der dann bei der Root-CA eingereicht wird. Da die Root-CA nicht im AD arbeitet, können Sie keinen automatischen Request schicken. Speichern Sie die Anforderung stattdessen in einer Textdatei.

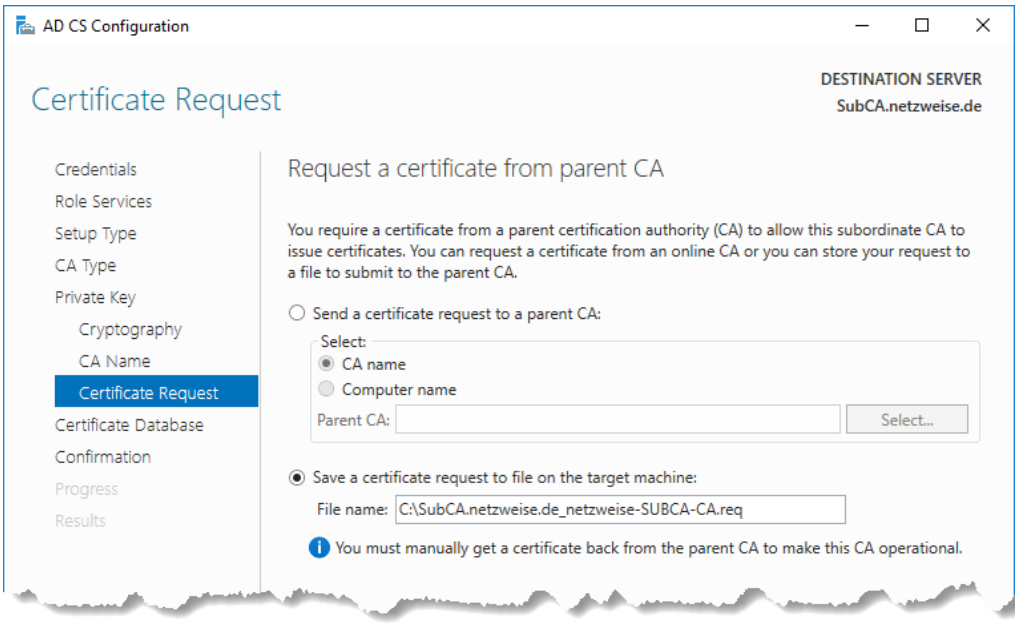


Bild 38 - speichern sie die Zertifikatsanforerung im Dateisytem

Sie müssen die Datei, in der sich die Anforderung befindet, nun auf die Root-CA kopieren und dort einreichen. Nachdem Sie die Datei kopiert haben, öffnen Sie die Zertifikatsverwaltungskonsole und dann das Kontextmenü der Root-CA. Dort finden Sie einen Eintrag "Submit new request". Wenn Sie ihn auswählen, öffnet sich ein Explorer-Fenster. Wählen Sie die Anforderungsdatei aus, um sie zu importieren.

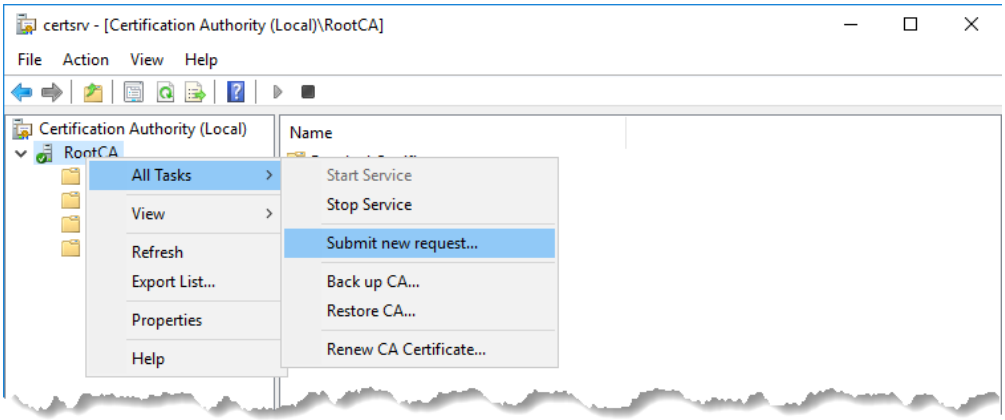


Bild 39 - aus dem Kotextmenü der CA können Sie eine Anforderung öffnen

Der Request wird jetzt im Container "Pending requests" (Ausstehende Anforderungen) angezeigt. Öffnen Sie das Kontextmenü der offenen Anfrage und wählen Sie "Issue", um das Zertifikat für die untergeordnete CA auszustellen.

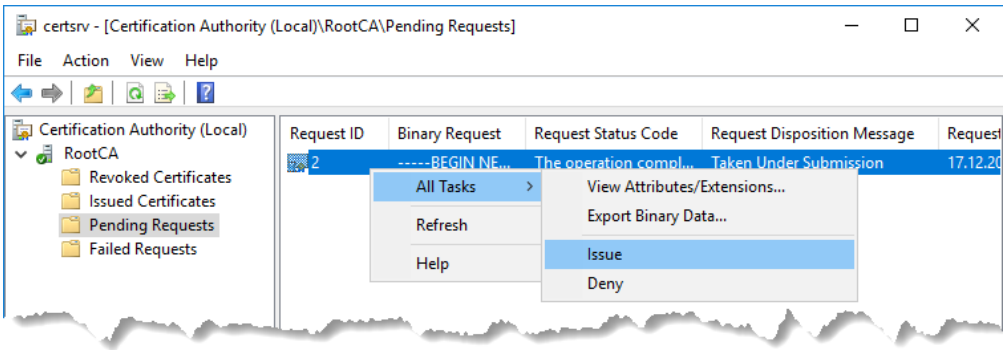


Bild 40 - Stellen Sie das Zertifikat mit Issue aus

Um das Zertifikat zu exportieren, öffnen Sie es mit einem Doppelklick aus dem Container "Issued Certificates" und wählen auf der Registerkarte "Details" "Copy to File…". Anschließend speichern Sie das Zertifikat im Dateisystem des Servers.

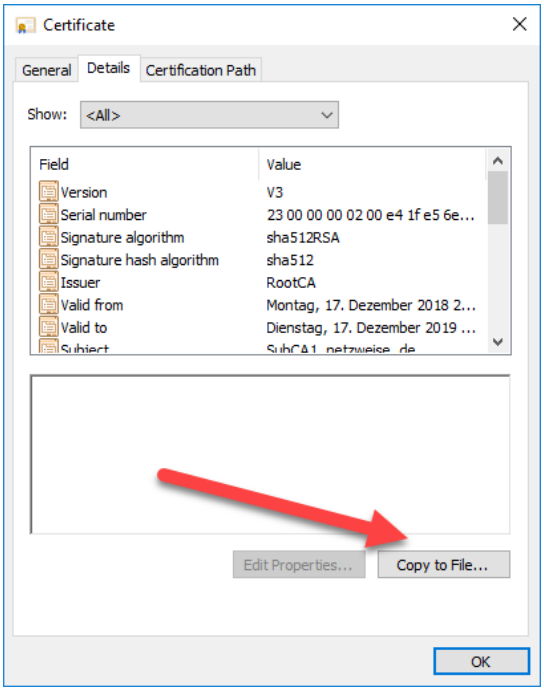


Bild 41 - Sie müssen das Zertifikat öffnen, um es exportieren zu können

Der Assistent leitet Sie durch den Export. Für den Import muss das Zertifikat als .P7B-Datei vorliegen. Aktivieren Sie auch die Checkbox "Include all certificates in the certification path if possible". Diese Option speichert nicht nur das Zertifikat der untergeordneten Zertifizierungsstelle in der Datei, sondern auch das Zertifikat der Root-CA.

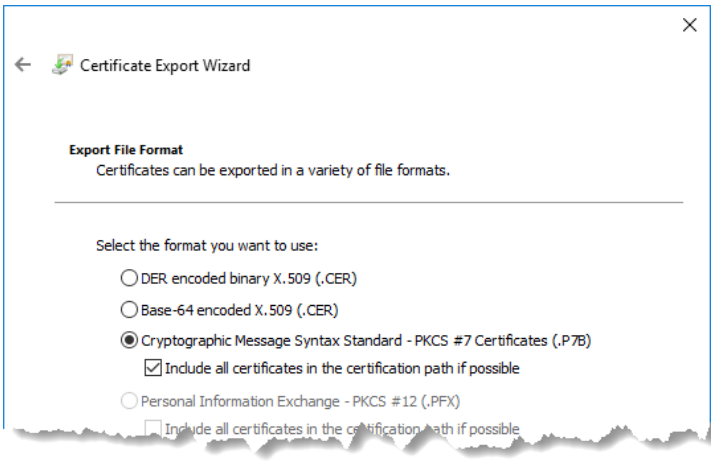


Bild 42 - Exportieren Sie das Zertifikat als .P7B-Datei, um die komplette Zertifikatskette exportieren zu können

Anschließend legen Sie die Datei im Dateisystem ab und kopieren Sie sie zurück auf die untergeordnete Zertifizierungsstelle.

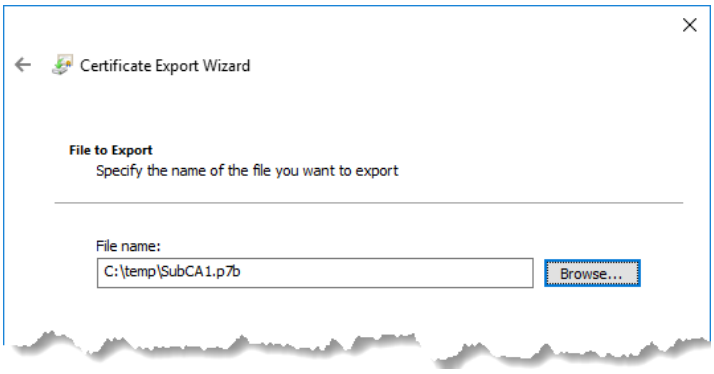


Bild 43 - Speichern Sie die Datei und kopieren Sie sie auf die untergeordnete CA

Nun können Sie den Zertifikatsdienst auf der untergeordneten Zertifizierungsstelle über das Kontextmenü der CA starten.

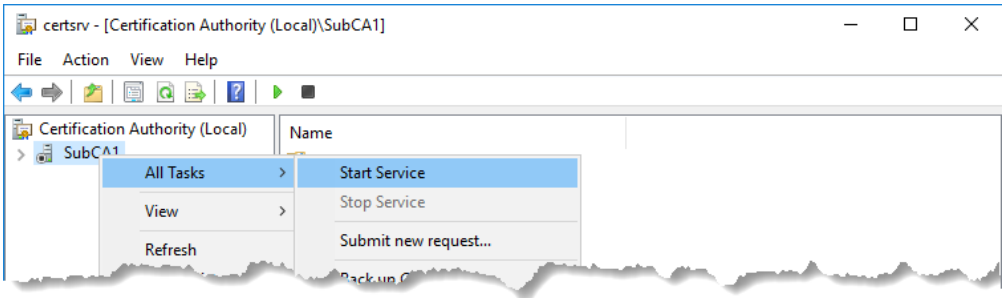


Bild 44 - Starten Sie den Zertifikatsdienst

Das Zertifikat der untergeordneten Zertifizierungsstelle muss jetzt installiert werden.

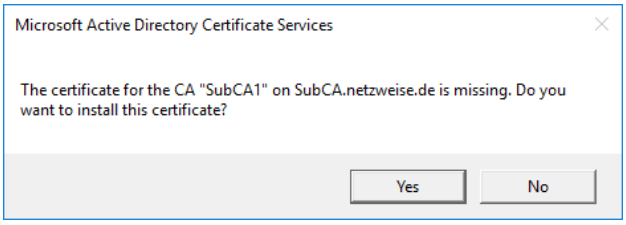
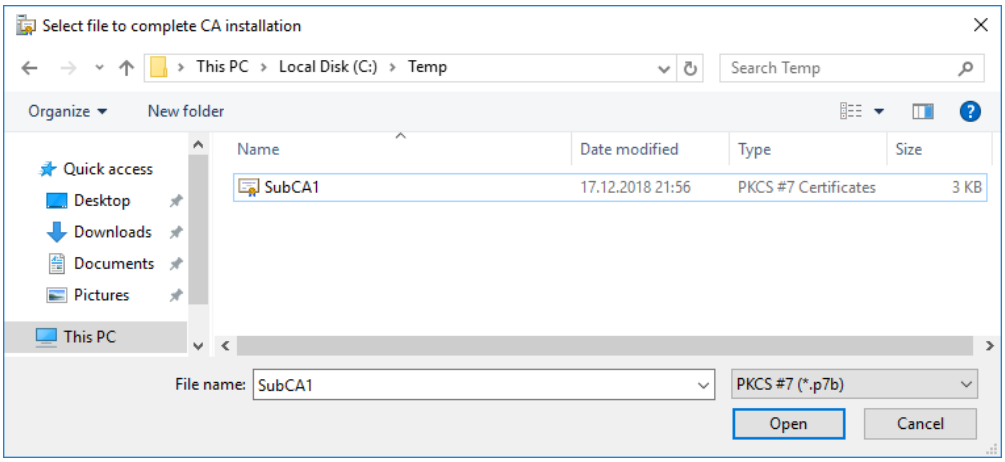


Bild 45 - Bestätigen Sie die Installation des Zertifikats

Geben Sie im Explorer den Speicherort an, an dem Sie die .P7B-Datei gespeichert haben.



Wenn das Zertifikat korrekt ausgestellt wurde und die untergeordnete Zertifizierungsstelle die CRL finden kann, startet die untergeordnete Zertifizierungsstelle und ist einsatzbereit.

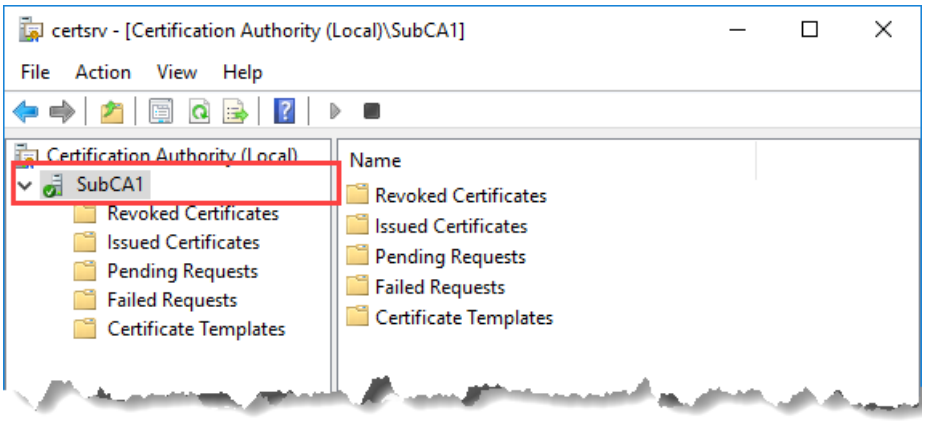


Bild 46 - Der grüne Button mit weißem Haken zeigt an, dass die CA einsatzbereit ist.

Nun können Sie die Root-CA offline nehmen. Die untergeordnete Zertifizierungsstelle läuft jetzt, ohne dass sie die Root-CA erreichen muss.

Fehlerbehebung beim Starten der untergeordneten Zertifizierungsstelle

Wenn die untergeordnete Zertifizierungsstelle nicht startet und stattdessen einen Fehler wirft, kann sie vermutlich die CRL nicht abrufen. Prüfen Sie daher zuerst, ob die CRL über den Webserver verfügbar ist, indem Sie vom Webbrowser der untergeordneten CA aus versucht, die CRL herunterzuladen. Geben Sie dafür die URL zur CRL im Webbrowser ein. Im Beispiel ist die korrekte URL "`http://web.netzweise.de/CertEnroll/RootCA.crl`". Klappt das einwandfrei, haben Sie eventuell auf der Root-CA einen Tippfehler beim angeben des Pfads zur CRL gemacht. Prüfen Sie den Pfad in der Zertifikatskonsole der Root-CA. Haben Sie hier einen Fehler gemacht, müssen Sie zuerst den Fehler in der CRL-Erweiterung korrigieren und dann für die untergeordnete CA ein neues Zertifikat erstellen.

Öffnen Sie hierfür das Kontextmenü der untergeordneten CA und wählen Sie "Renew CA Certificate…".

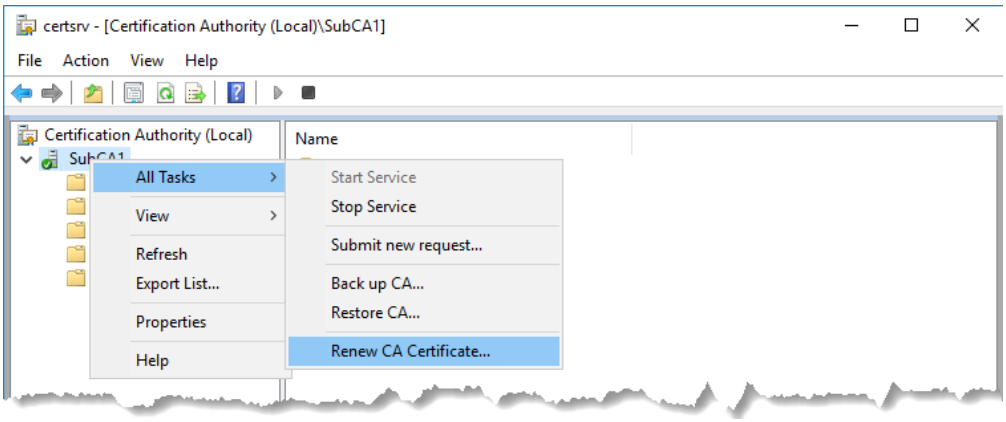


Bild 47 - Fordern Sie eine Zertifikatserneuerung an

Sie werden gewarnt, dass während der Zertifikats-Erneuerung die Zertifikatsdienste gestoppt werden müssen. Bestätigen Sie das.

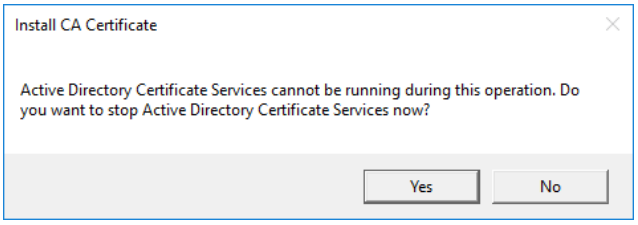


Bild 48 - Die Dienste müssen beendet werden, aber sie funktionieren ja eh nicht

Sie können ein neues Schlüsselpaar erzeugen, aber das ist in diesem Fall nicht notwendig. Letztlich ist es aber egal, welche Option Sie hier wählen, denn Sie haben ja eh noch keine Zertifikate ausstellen können.

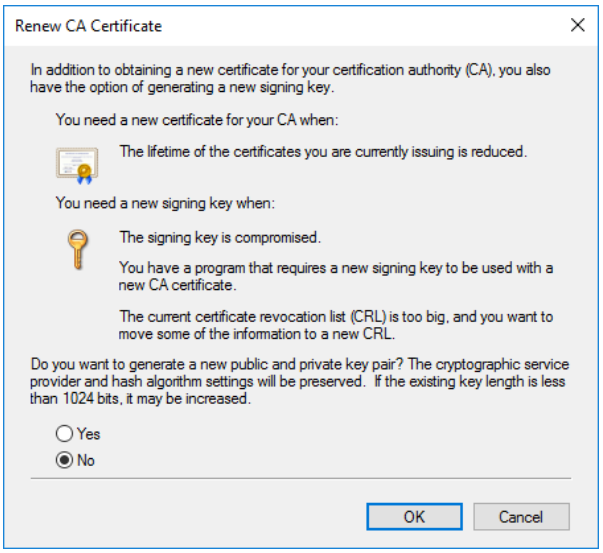


Bild 49 - Erstellen Sie ein neues Schlüsselpaar - oder auch nicht

Im nächsten Fenster werden Sie gefragt, an welchen Computer Sie die Anforderung senden wollen. Beenden Sie den Assistenten hier durch Auswahl von "Cancel".

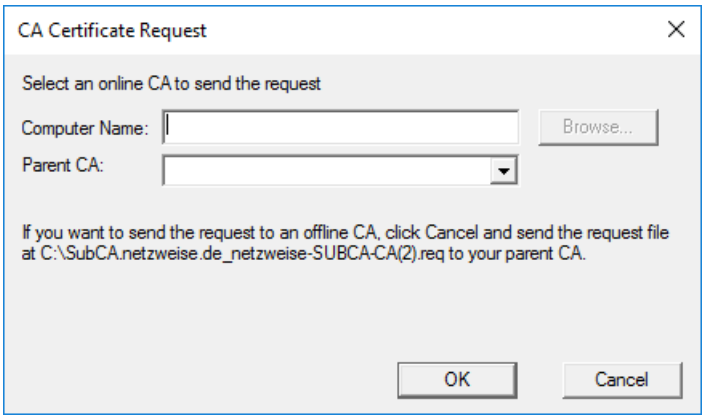


Bild 50 - Beenden Sie den Request-Assistenten

Der Assistent hat den Request jetzt als Request-Datei im Root des Systemlaufwerks abgelegt. Sie können den neuen Request jetzt nehmen und wie oben beschrieben zur erneuten Zertifizierung auf der Root-CA einreichen und das Zertifikat dann wieder auf der Sub-CA installieren.

Über den Autor

Holger Voges ist IT-Trainer und Consultant. Seine IT-Karriere begann mit einem Atari 520 ST+ Mitte der 80er Jahre. Seine ersten Erfahrungen mit großen Netzwerken hat er im Systembetrieb der Volkswagen Financial Services 1999 gewonnen. Ab dem Jahr 2000 war er dann als freiberuflicher IT-Trainer für verschiedene Schulungsunternehmen im Bereich Braunschweig und Hannover tätig, bis er 2002 mit zwei Mitstreitern sein erstes Schulungsunternehmen LayerDrei in Braunschweig gründete. Nach seinem Ausstieg bei LayerDrei war er dann mehrere Jahre als freiberuflicher Consultant vor allem im SQL-Server Umfeld u.a. für T-Home Entertain, e.on und Hewlett-Packard unterwegs. 2012 hat er das Schulungsunternehmen Netz-Weise IT-Training gegründet.

Im Dezember 2016 erschien sein Buch "Gruppenrichtlinien in Windows Server 2016, 2012 und 2008 R2", dass er in der 3. Auflage übernommen hat, und das im Dezember 2018 in 4. Auflage komplett überarbeitet erschienen ist. Außerdem ist er regelmäßiger Sprecher z.B. auf der europäischen Powershell-Konferenz und auf verschiedenen anderen Veranstaltungen.

Netz-Weise IT-Training hat sich auf Firmenschulungen im professionellen IT-Umfeld spezialisiert und bietet Schulungen u.a. im Bereich Microsoft, VMware, Linux und Oracle an.