secorvo
security consulting

PKI von der Stange

Secorvo White Paper

Aufbau einer unternehmensinternen PKI für die Authentifizierung von Benutzern und Computern

Version 1.0
Stand 01. März 2011

Hans-Joachim Knobloch

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100

info@secorvo.de
www.secorvo.de

Inhaltsübersicht

Abkürzungen

ACL	Access Control List
AD	Active Directory
AIA	Authority Information Access (Zertifikatserweiterung)
C	Country (optionaler Bestandteil eines Distinguished Name)
CA	Certification Authority
CDP	CRL Distribution Points (Zertifikatserweiterung)
CD-R	Compact Disk - Recordable
CN	Common Name (optionaler Bestandteil eines Distinguished Name)
CNAME	Canonical Name (DNS Alias)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DC	Domain Component (optionaler Bestandteil eines Distinguished Name)
DER	Distinguished Encoding Rules
DNS	Domain Name System
EAP	Extensible Authentication Protocol
HSM	Hardware Security Modul
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol (via TLS)
IE	Internet Explorer
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Server
IP	Internet Protocol
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
L	Locality (optionaler Bestandteil eines Distinguished Name)
L2TP	Layer 2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
LDAPS	Secure Lightweight Directory Access Protocol (via TLS)
MD5	Message Digest 5 Hashverfahren
NAC	Network Access Control
O	Organization (optionaler Bestandteil eines Distinguished Name)
OCSP	Online Certificate Status Protocol

OU	Organizational Unit (optionaler Bestandteil eines Distinguished Name)
PEM	Privacy Enhanced Mail
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastruktur
PUK	PIN Unblocking Key
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Service
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman Kryptoverfahren
S/MIME	Secure Multipurpose Internet Mail Extensions
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SMTPS	Secure Simple Mail Transfer Protocol (via TLS)
SP	State or Province (optionaler Bestandteil eines Distinguished Name)
SSL	Secure Socket Layer
TLS	Transport Layer Security
UPN	Universal Principal Name
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

Historie

Version	Datum	Änderung	Autor
1.0	01.03.2011	Erste veröffentlichte Fassung des White Papers	Hans-Joachim Knobloch

1 Zusammenfassung

Dieses White Paper richtet sich hauptsächlich an Unternehmen, die in ihrer internen Infrastruktur Computer oder Benutzer mit Verfahren auf Grundlage von Public-Key-Zertifikaten – beispielsweise SSL/TLS – authentifizieren wollen, aber noch nicht über die dafür benötigte Public Key Infrastruktur verfügen.

Es wird eine einfache PKI beschrieben, die ein für viele Anwendungsfälle ausreichendes Basis-Sicherheitsniveau bietet. Der hier vorgestellte Aufbau einer PKI ist standardkonform, orientiert sich an den Konventionen der „Best Practice“ und kann in das Active-Directory eines Unternehmens oder einer Organisation integriert werden.

Der Aufbau dieser PKI mit den Windows Server 2003, 2008 oder 2008 R2 integrierten Microsoft Certificate Services und ihre Nutzung zur Ausstellung von Authentifikationszertifikaten werden Schritt für Schritt so detailliert beschrieben, dass ein erfahrener AD-Administrator auch ohne PKI-Expertenwissen eine solche „PKI von der Stange“ umsetzen kann.

Abschließend wird ein Ausblick auf Alternativen zum Erzielen eines höheren Sicherheitsniveaus und auf Ausbaumöglichkeiten zur erweiterten Nutzung der hier dargestellten PKI gegeben.

Die Lektüre dieses White Papers setzt PKI-Grundkenntnisse voraus; für eine Einführung in diese grundlegenden Konzepte und Begriffe aus der Welt der PKI sei auf das Secorvo White Paper „Public Key Infrastrukturen – Vertrauensmodelle und PKI Komponenten“ [Bar_11] verwiesen. Darüber hinaus werden für die Schritt-für-Schritt-Anleitung hinreichende Kenntnisse der Windows-Administration vorausgesetzt.

2 Motivation

Bis vor einigen Jahren war der Austausch von verschlüsselten und signierten E-Mails einer der hauptsächlichen Treiber für den Aufbau von unternehmensweiten Public Key Infrastrukturen. Daneben haben sich jedoch vermehrt Verfahren etabliert, die Public-Key-Zertifikate für die Authentifikation von Computern und Benutzern einsetzen, namentlich die folgenden:

- **SSL** oder **TLS**, so mittlerweile der offizielle Name des Protokolls nach [RFC_5246], ist nicht nur auf die Sicherung von Web-Zugriffen per HTTP(S) beschränkt, sondern erlaubt beispielsweise auch den Schutz von Directory-Abfragen via LDAP(S) oder die verschlüsselte Übertragung von E-Mails zwischen Mail-Servern via SMTP(S), die man in vielen Fällen recht einfach aktivieren kann, sobald nur die benötigten SSL/TLS-Serverzertifikate vorhanden sind.
  SSL/TLS-Clientzertifikate wiederum ermöglichen u. a. praktisch allen gängigen Web-Browsern eine einfache und sehr sichere Anmeldung des jeweiligen Anwenders an Web-basierten Applikationen.
- **IEEE 802.1x** nutzt in der sehr sicheren und in der Regel eben so benutzerfreundlichen Variante mit **EAP-TLS** Public-Key-Zertifikate zur Anmeldung von Computern oder Benutzern an Netzwerken wie Ethernet (IEEE 802.3) oder WLAN (IEEE 802.11) und ermöglicht so eine wirkungsvolle Netzwerkzugangskontrolle (Network Access Control). Ähnlich wie bei SSL/TLS in den gängigen Browsern ist die benötigte PKI-Anwendungssoftware in Windows XP und neueren Windows-Clients bereits enthalten und kann recht einfach genutzt werden, sobald die benötigten Zertifikate erstellt sind.

- Auch im RAS- und VPN-Bereich können Public-Key-Zertifikate mit der seit Windows XP integrierten Client-Software oder mit den VPN-Clients verschiedener anderer Hersteller für die Anmeldung von Computern oder Benutzern per **IPsec** oder **L2TP** mit **EAP-TLS** genutzt werden.

Alle diese Anwendungen von Authentifikationsverfahren haben einige Faktoren gemeinsam, welche die Konzeption einer dafür passenden PKI vereinfachen:

- Es handelt sich dabei sehr häufig um unternehmensinterne Anwendungen; die Zertifikate brauchen außerhalb der eigenen Infrastruktur nicht als gültig validiert werden.[1]
- Die relevanten Benutzer und Computer sind (evtl. mit Ausnahme einzelner Appliances, Server- oder Gateway-Systeme) im Active Directory des Unternehmens registriert.
- Die Anwendungen benötigen kein besonderes Verzeichnis, über das sie die Zertifikate von Kommunikationspartnern ermitteln und beziehen können. Die betreffenden Zertifikate werden entweder beim Verbindungsaufbau bilateral ausgetauscht oder über das AD bezogen.
- Das Sicherheitsniveau braucht in aller Regel nicht höher zu sein als es bereits herkömmlich für die Verwaltung von AD-Konten oder RAS/VPN-Einwahlkonten gehandhabt wird. Bei vielen Unternehmen bedeutet dies, dass beispielsweise auf eine strenge Rollentrennung und ein Vier-Augen-Prinzip verzichtet werden kann.

Zusammen mit der Tatsache, dass mit den Microsoft Certificate Services seit Windows Server 2003 [2] eine vielseitig nutzbare PKI-Software als Teil der Windows Serversoftware zur Verfügung steht, ermöglichen es diese Faktoren, eine einfache PKI für derartige Anwendungen zu entwerfen. Tatsächlich installieren in vielen Unternehmen Server- oder AD-Administratoren kurzerhand die Certificate Services, um Zertifikate für einen Test- oder beschränkten Produktivbetrieb von Authentifikationsverfahren zu erstellen.

Diesen Administratoren will dieses White Paper zur Hand gehen. Während im allgemeinen eine Public Key Infrastruktur „maßgeschneidert“ konzipiert und umgesetzt werden sollte, um eine optimale Balance von Sicherheit, Anwenderfreundlichkeit, Umsetzungs- und Betriebsaufwand zu erzielen, lässt sich in den geschilderten, eingeschränkten Anwendungsfällen häufig auch eine PKI „von der Stange“ vorteilhaft einsetzen.

---

1 Für öffentlich erreichbare Internetauftritte bietet es sich dagegen meist an, SSL/TLS-Serverzertifikate bei öffentlichen Trustcentern zu beziehen, deren Root-CA-Zertifkate in den Browsern weltweit bereits als Vertrauensanker vorinstalliert ist.

2 Die Certificate Services waren bereits in der Server-Version von Windows 2000 enthalten. Flexibel an verschiedenste PKI-Anwendungen anpassbare Certificate Templates wurden jedoch erst mit Windows 2003 eingeführt.

3 PKI-Architektur und Rahmenbedingungen

Im vorigen Kapitel wurde die Idee einer „PKI von der Stange“ motiviert. Nun wollen wir das Konzept einer solchen PKI vorstellen, die in vielen Fällen für die Nutzung geschilderten PKI-Anwendungen mit zertifikatsbasierten Authentifikationsverfahren ausreicht.

3.1 Einsatzbereich

Die hier beschriebene PKI ist für Unternehmen gedacht, deren Computer und Benutzer (nahezu) vollständig in einem einzigen Active Directory erfasst sind und für Anwendungen, die dieses AD und die darin registrierten Computer als wesentlichen Teil ihrer Infrastruktur nutzen. Daneben können auch vereinzelte Appliances, Server- oder Gateway-Systeme, die nicht im AD enthalten sind, mit SSL/TLS-Serverzertifikaten ausgestattet werden.

3.2 PKI-Hierarchie

3.2.1 Root-CA und Issuing-CA

Grundsätzlich gehen wir von einer zweistufigen PKI-Hierarchie aus, bestehend aus einer Root-CA als Vertrauensanker (in Windows-Sprechweise: „vertrauenswürdige Stammzertifizierungsstelle“) und einer untergeordneten Sub-CA, nachfolgend auch Issuing-CA genannt, da sie die Anwenderzertifikate für Benutzer und Computer ausstellt.

Für eine mindestens zweistufige Hierarchie sprechen die folgenden Gründe:

- Die Root-CA wird neben ihrer Sperrliste zunächst nur ein weiteres CA-Zertifikat ausstellen, selbst im Fall einer späteren Erweiterung der PKI nur einige wenige. Daher kann sie im Gegensatz zur Issuing-CA, die beständig für die Ausstellung neuer Anwenderzertifikate zur Verfügung stehen muss, offline auf einem System ohne jeglichen Netzwerkanschluss betrieben werden. Alleine schon dadurch erreicht sie ein höheres Sicherheitsniveau und kann im Notfall bei einer Kompromittierung der online betriebenen Issuing-CA deren Zertifikat sperren.
- Bei einem späteren Ausbau der PKI können weitere Issuing-CAs der Root-CA untergeordnet werden, ohne dass deswegen aufwändig ein neuer Vertrauensanker verteilt werden muss. Gleiches gilt für die Sperrung und Neuausstellung des CA-Zertifikats der ersten Issuing-CA im Notfall.

Von einer drei- oder mehrstufigen PKI-Hierarchie wird dagegen in der Regel Abstand genommen, weil es meist keine vergleichbar stichhaltigen sicherheitstechnischen oder organisatorischen Gründe gibt, die den Betriebsaufwand für eine oder mehrere zwischengelagerte CAs zwischen Root- und Issuing-CA rechtfertigen. Sofern doch solche organisatorischen Gründe vorliegen, beispielsweise regional unterschiedlich geregelte IT- und Personal-Verantwortung in einem globalen Unternehmensgeflecht, ist stets eine detaillierte Planung vonnöten.

3.2.2 Namenskonzept

Für den Distinguished Name von CAs hat sich als eine Best Practice (u. a. in [CoPKI_09]) die Konvention eingebürgert, als Organization (O) Namensbestandteil die korrekte Bezeichnung des Unternehmens (bzw. sinngemäß der Behörde oder anderen Rechtsperson) zu verwenden, in dessen Verantwortung die PKI betrieben wird und als Country (C) den zweistelligen ISO-3166-Ländercode des Landes, in dem das Unternehmen unter diesem

Namen registriert ist. Anhand dieser Angaben kann ein Dritter, der ein Zertifikat prüft, in der Regel am einfachsten nachvollziehen und überprüfen, wer die PKI betreibt, und einschätzen, wie viel Vertrauen er diesem PKI-Betreiber und damit dem Zertifikat entgegen bringt.

Zusätzlich sollte ein Common Name (CN) verwendet werden, der eine eindeutige Zuordnung ermöglicht, falls eine Organisation mehrere CAs betreibt, und nützliche Zusatzinformationen zu der jeweiligen CA erkennen lässt. Solche Zusatzinformationen können beispielsweise die Angabe sein, ob es sich um eine Root- oder Issuing-CA handelt, wann Gültigkeit des jeweiligen CA-Zertifikats endet oder für welche Anwendungsbereiche die CA zuständig ist.

Optional kann ein Organizational Unit (OU) Namensbestandteil eingeschoben werden, um bspw. in einem größeren Unternehmen anzugeben, welcher Organisationsbereich die CA verantwortlich betreibt oder für welchen Teilbereich sie Zertifikate erstellt.

Beispiele für einen solchen vollständigen Distinguished Name einer CA wären:

- CN= Secorvo Root CA 2022, O=Secorvo Security Consulting GmbH, C=DE
- CN=CA for computer certificates, OU=EMEA, O=ACME Inc., C=US

Dem gegenüber gibt es für die Subject Distinguished Names und sonstige Namensinformationen (z. B. E-Mail-Adresse, Windows-UPN, IP-Adresse oder DNS-Name) für Anwenderzertifikate keine einheitliche Konvention. Die Namen in Anwenderzertifikaten müssen sich einerseits nach den jeweiligen Anwendungen richten, die diese Namen auswerten, andererseits danach, welche Informationen überhaupt im AD-Konto des betreffenden Computers oder Benutzers registriert sind.

Eine Besonderheit bilden die Locality (L) und State or Province (SP) Namensbestandteile, die vielerlei SSL/TLS-Serversoftware traditionell bei der Erzeugung eines Zertifizierungsantrags (CSR) als obligatorisch anzugeben einfordert. Diese beiden Informationen werden aber von Browsern in aller Regel nicht ausgewertet, tragen praktisch nichts zum besseren Verständnis des Anwenders bei, der das Zertifikat betrachtet.[3] Daher werden diese beiden Namensbestandteile in den Zertifikaten der hier vorgestellten PKI unterdrückt, selbst wenn sie in einem Zertifizierungsantrag enthalten sind.

Eine besondere Rolle im Namenskonzept spielen schließlich zwei Arten von URLs, die eine CA in den von ihr ausgestellten Zertifikaten vermerken kann:

- In einer oder mehreren **CDP**-URLs wird angegeben, wo eine PKI-Anwendung die Sperrliste abrufen kann, die sich auf das betreffende Zertifikat bezieht, und über die es ggf. gesperrt würde.
- Eine oder mehrere **AIA**-URLs geben an, wo eine PKI-Anwendung das Zertifikat der ausstellenden CA abrufen kann, falls es nicht lokal vorliegt. Eine derartige AIA-URL kann insbesondere dazu helfen, das Zertifikat der Issuing-CA abzurufen, um die Zertifikatskette vom Anwenderzertifikat bis zur Root-CA zu vervollständigen.
  Zusätzlich könnte als AIA-URL angegeben werden, wo ein OCSP-Responder zu erreichen ist, der eine Online-Sperrauskunft über das betreffende Zertifikat abgeben kann. Ein OCSP Responder ist jedoch kein Bestandteil der hier beschriebenen PKI (vgl. die Abschnitte 0 und 6.2.4).

Die Vorgabe bei der Installation der Microsoft Certificate Services ist es, in der CDP- und AIA-Erweiterung jeweils eine LDAP-URL aufzuführen, die auf das lokale Active Directory

[3] So ist bspw. nicht intuitiv klar, ob sich diese Angaben auf den Sitz des Unternehmens beziehen, das den Server betreibt, oder auf den Standort des Servers selbst; letzteres ist bei Servern, die durch Nutzung von Cloud-Computing-Dienstleistungen realisiert werden, praktisch nicht mehr zu ermitteln.

verweist, und eine HTTP-URL, die auf den Webserver verweist, der für die Zertifikatsbeantragung per Web-Interface an die Certificate Services angegliedert ist. Dieser Vorgabe folgt auch die hier vorgestellte PKI. Allerdings empfiehlt es sich, als Hostnamen für die HTTP-URL nicht den eigentlichen Rechnernamen des Webservers zu verwenden, sondern dafür einen speziellen DNS-Alias (CNAME) wie etwa „pki.acme.us“ einzurichten, der bei Bedarf auch auf einen anderen, bspw. extern im Internet sichtbaren Webserver verweisen kann (vgl. Abschnitt 6.2.1).

3.3 Unterstützte PKI-Funktionen

3.3.1 Registrierung der Zertifikatsinhaber und Beantragung von Zertifikaten

Eine explizite Registrierung der Zertifikatsinhaber braucht nicht statt zu finden, da auf die bereits in dem jeweiligen Benutzer- oder Computer-Konto im AD registrierten Informationen zurück gegriffen werden kann. Das Recht zur Beantragung von Zertifikaten eines bestimmten Typs wird über die übliche Windows Rechte- und Gruppenverwaltung erteilt.

Eine gewisse Ausnahme bilden die SSL/TLS-Serverzertifikate, besonders solche für Systeme, die nicht im AD registriert sind. Hier wird das Recht zur Beantragung eines solchen Serverzertifikats den in Frage kommenden Systemadministratoren erteilt. Der jeweilige Systemadministrator muss dann in der Regel bei der Erstellung eines Zertifizierungsantrags (CSR) mit der betreffenden Serversoftware die Namensinformation eingeben und den CSR über eine Weboberfläche bei der Issuing-CA einreichen. Bei Bedarf kann ein PKI-Administrator manuell die Korrektheit des CSR prüfen, bevor das betreffende Zertifikat erstellt wird. Im Fall einer Ablehnung durch die Issuing-CA muss der Serveradministrator einen korrigierten CSR erstellen und einreichen.

3.3.2 Sperrung und Publikation

Sowohl Root- als auch Issuing-CA publizieren ihre Zertifikate und Sperrlisten im AD und über den an die Issuing-CA angegliederten Webserver. Während die Issuing-CA regelmäßig automatisiert eine neue CRL erstellt und publiziert, ist dies der offline betriebenen Root-CA nicht möglich. Für letztere müssen daher neue CRLs manuell erstellt, exportiert und in das AD und den Webserver zur Publikation importiert werden.

Anwenderzertifikate von Benutzern oder Computern werden in der hier dargestellten PKI nicht im AD publiziert, da ihre Veröffentlichung für die betrachteten Authentifikationsverfahren (vgl. Abschnitt 2) nicht benötigt wird.

3.3.3 Nicht unterstützte PKI-Funktionen

Um das PKI-Konzept nicht unnötig zu überfrachten werden einige mögliche PKI-Funktionen nicht berücksichtigt (vgl. jedoch die Ausblicke in Abschnitt 6.2).

Dies betrifft besonders die folgenden PKI-Funktionen, weil deren zielgerichtete Nutzung ein individuelles organisatorisches Konzept erfordert und/oder die Funktion von der in vielen Unternehmen noch nicht komplett abgelösten Windows XP und Windows Server 2003 Software nicht unterstützt wird:

- Inkrementelle Sperrlisten (Delta-CRL)
- Online-Sperrabfragen (OCSP)
- Schlüsselarchivierung (Key Backup) und Schlüsselwiederherstellung (Key Recovery) von Schlüsseln zu Verschlüsselungszertifikaten

- Stellvertretende Zertifikatsbeantragung über einen Enrollment-Agent

Das Roaming von Zertifikaten und damit verbundenen Schlüsseln, d. h. die automatisierte Übertragung auf weitere Windows-Arbeitsplätze, an denen ein Anwender sich nach der Erstellung seines Benutzerzertifikats anmeldet, wird nicht explizit berücksichtigt. Sofern nicht im AD ein Roaming von Benutzerprofilen umgesetzt wird, wird ggf. an jedem neuen Windows-Arbeitsplatz, an dem ein Benutzer sich anmeldet, ein weiteres Zertifikat für ihn erstellt.

3.4 Sicherheitsniveau

Die hier vorgestellte PKI zielt auf ein Basis-Sicherheitsniveau, das dem der AD-Rechte- und Kontenverwaltung vergleichbar ist. Bei der AD-Rechteverwaltung ist davon auszugehen, dass Enterprise- und Domänenadministratoren sich prinzipiell in großem Umfang Rechte aneignen und bspw. über zurückgesetzte Passwörter auf beliebige Benutzerkonten zugreifen können. Genau so werden bei der PKI von der Stange keine besonderen Anstrengungen unternommen, um zu verhindern, dass Enterprise- und Domänenadministratoren sich unter Missbrauch ihrer besonderen Rechte Anwenderzertifikate erschleichen können.

3.4.1 Organisatorische Sicherheitsaspekte

Bei der Root-CA ist es durch Aufteilen von Passwörtern unter zwei oder mehrere Administratoren möglich, ein rudimentäres Vier-Augen-Prinzip zu nutzen (vgl. die Abschnitte 4.1.1 und 4.1.4).

Für die Issuing-CA wird kein Vier-Augen-Prinzip umgesetzt und auch die optionale Rollentrennung der Microsoft CA nicht genutzt (vgl. den Ausblick in Abschnitt 6.1.1).

3.4.2 Kryptoalgorithmen und Schlüssellängen

Als Public Key Algorithmus wird RSA mit 2048 Bit Schlüssellänge genutzt; für die Signatur von Zertifikaten und CRLs in Verbindung mit SHA-1 als Hashfunktion.

Zwar muss die Sicherheit des SHA-1 seit Jahren zunehmend als zweifelhaft eingeschätzt werden. Jedoch wird die neuere SHA-2 Hashfunktion von Windows-Versionen vor Windows Vista nicht oder nur mit Zusatzsoftware unterstützt. Sobald Windows XP und Server 2003 nicht mehr unterstützt werden müssen, können neue Zertifikate mit RSA/SHA-2 erstellt werden (vgl. den Ausblick in Abschnitt 6.2.4). Dabei ist es wichtig zu wissen, dass die Sicherheit von bereits erstellten Signaturen durch in den nächsten Jahren zu erwartende „Kollisionsangriffe“ gegen SHA-1 nicht nachträglich beeinflusst wird; alleine die nach dem ersten erfolgreichen Kollisionsangriff neu erstellten Zertifikate wären potentiell betroffen.[4]

RSA mit 2048 Bit Schlüssellänge wird derzeit bis zum Jahr 2030 als ausreichend sicher eingeschätzt [NIST_07]. Längere Schlüssel können Ursache von Kompatibilitätsproblemen mit Netzwerkkomponenten älteren Datums oder mit manchen Java Laufzeitumgebungen sein, kürzere sollten aus Sicherheitsgründen vermieden werden. Auch in diesem Punkt

[4] Kollisionsangriffe ermitteln ein Paar von Datensätzen, die unter der angegriffenen Hashfunktion denselben Hashwert besitzen. Wenn dann der erste, harmlose Datensatz als Zertifikat signiert wird, so ist diese Signatur gleichzeitig und von der CA unbeabsichtigt für das Zertifikat gültig, das sich als „böser Zwilling“ aus dem anderen Datensatz ergibt.
Speziell die Kollisionsangriffe, die in den vergangenen Jahren gegen MD5 und abgeschwächte Varianten des SHA-1 entwickelt und mehrfach verbessert wurden, erzeugen die kollidierenden Datensätze stets paarweise, gegenseitig aufeinander abgestimmt. Es ist damit nicht möglich, zu einem vorab festgelegten Datensatz einen zweiten, kollidierenden zu ermitteln.

bilden SSL/TLS-Serverzertifikate eine gewisse Ausnahme: Verschiedene SSL/TLS-Serversoftware, besonders in Appliances, erlaubt es nicht, Schlüssel mit einer Länge von mehr als 1024 Bit zu erzeugen. In diesem Fall ist entweder ein Update der betreffenden Software oder Appliance durchzuführen oder aber SSL/TLS-Serverzertifikate auch für diese kürzere Schlüssellänge auszustellen (einzustellen im entsprechenden Certificate Template, vgl. Abschnitt 5.4.1). Eine Schlüssellänge von 1024 Bit sollte bei RSA aber auf keinen Fall unterschritten werden. Umgekehrt kann, falls die oben angesprochenen Bedenken hinsichtlich von Kompatibilitätsproblemen bei Schlüssellängen jenseits von 2048 Bit im Vorfeld ausgeräumt werden können, für die Root-CA (ggf. auch für die Issuing-CA) ein 4096 Bit Schlüssel eingesetzt werden, um an dieser Stelle die Sicherheitsreserve weiter zu erhöhen.

3.4.3 Gültigkeitszeiträume

Für die Lebensspanne einer PKI ist zunächst die Gültigkeitsdauer des Root-CA-Zertifikats maßgeblich, das als Vertrauensanker verteilt wird.

Ein verbreiteter Ansatz bei der Konzeption einer maßgeschneiderten PKI ist es, abhängig vom dahinter stehenden Anwendungs- und Geschäftsmodell, die Gültigkeitsdauer eines Root-CA-Zertifikats relativ groß, d. h. 20 Jahre und länger[5], zu wählen. Dadurch wird die Notwendigkeit, ein neues Root-CA-Zertifikat an viele externe Parteien, ggf. sogar weltweit, auszurollen, entsprechend lange hinausgeschoben. Innerhalb dieses Zeitraums werden dann meist mehrere überlappende Gültigkeitsintervalle von nacheinander genutzten CA-Zertifikaten einer Issuing-CA vorgesehen. Dadurch ergibt sich u. a. eine bessere zeitliche Schadensbegrenzung in dem Fall, dass der Schlüssel der Issuing-CA unentdeckt kompromittiert würde.

Für die PKI von der Stange wollen wir aufgrund der folgenden Überlegungen von dieser Praxis abweichen:

- Sofern keine triftigen Sicherheitsgründe entgegen stehen, wollen wir bei der „PKI von der Stange“ in allen Punkten klaren und einfachen Lösungen den Vorzug geben, die bei ihrer Umsetzung kein tiefgreifendes PKI-Know-How, keine detaillierte Analyse der individuellen Gegebenheiten und eher geringen Betriebsaufwand erfordern.
- Angesichts des oben in Abschnitt 3.1 skizzierten Einsatzbereichs kann sich die Gültigkeitsdauer der Root- und Issuing-CA-Zertifikate an der zu erwartenden Lebensdauer der IT-Infrastruktur orientieren, innerhalb der die Zertifikate der PKI genutzt werden.
- Nach zwei solchen Generationswechseln darf plausibel erwartet werden, dass auch eine neue PKI oder eine vergleichbare Sicherheitsinfrastruktur ausgerollt wird.
- Solange nur interne Anwendungen die PKI nutzen gibt es keinen Grund, das Root-CA-Zertifiktat extern an vielerlei Zertifikatsnutzer, ggf. mehr oder minder unkontrolliert (bspw. per Download-Angebot) zu verteilen. Damit entfällt auch die Motivation, die zeitliche Gültigkeit des Root-CA-Zertifikats als Vertrauensanker möglichst lange auszudehnen.
- Wählt man die Gültigkeitsdauer des Issuing-CA-Zertifikats kleiner als die des Root-CA-Zertifikats, so wird nach einigen Jahren eine Erneuerung des Issuing-CA-Zertifikats (mit oder ohne Wechsel des Schlüsselpaars) und ein rechtzeitiger Umstieg auf dieses Zertifikat für die Erstellung neuer Anwenderzertifikate erforderlich. Je nach Ausgestaltung

[5] Auf gängigen Windows-Arbeitsplatzsystemen sind mehrere Root-CA-Zertifikate mit einer Gültigkeitsdauer von mehr als 35 Jahren vorinstalliert.

des Wechsels müssen dabei für eine Übergangszeit parallel zwei Sperrlisten gepflegt werden. Dies alles erhöht den Betriebsaufwand und die Fehleranfälligkeit.

- Eine (entdeckte oder unentdeckte) Kompromittierung einer Issuing-CA auf einem Mitgliedsserver des Active Directory würde in aller Regel auf generelle Sicherheitsprobleme beim Serverbetrieb hindeuten, deren Konsequenzen weit über die PKI-Anwendungen hinaus reichen könnten. Für das angepeilte Basis-Sicherheitsniveau sollte die gängige Absicherung von Windows-Servern und deren Betrieb hinreichenden Schutz gegen Kompromittierung der darauf betriebenen CA gewährleisten. Daneben bleibt selbstverständlich die Möglichkeit der Sperrung des Issuing-CA-Zertifikats durch die Root-CA, sofern eine Kompromittierung entdeckt oder hinreichend sicher vermutet.wird

Folgt man diesen Überlegungen, sollte in der Regel als Lebensdauer der PKI 10 bis 15 Jahre angesetzt werden, um mit ausreichender zeitlicher Reserve ein oder zwei Generationen einer Unternehmens-IT-Infrastruktur abzudecken.[6] Ansonsten können auch abweichende Gültigkeitsintervalle für die Zertifikate der Root- und Issuing-CA festgelegt werden (vgl. die Hinweise zur Konfiguration in Anhang A).

Die CRL der Root-CA muss wie oben geschildert in einem manuellen Prozess erstellt, exportiert und ins AD importiert werden. Um dies nicht zu aufwändig zu gestalten, ist eine Gültigkeitsdauer von drei, sechs oder zwölf Monaten ratsam. Da eine nicht rechtzeitig erneuerte CRL zu Verfügbarkeitsproblemen bei den die PKI nutzenden Anwendungen führt, sollte der Gültigkeitsdauer noch eine Karenzfrist von ein bis zwei Monaten zugeschlagen werden, um die Unwägbarkeiten bei der Durchführung des manuellen Prozesses (z. B. Krankheit der betreffenden Mitarbeiter) abzufangen.

Die oben genannten Gründe für eine zweistufige PKI-Hierarchie legen nicht nahe, dass die Issuing-CA für einen kürzeren Gültigkeitszeitraum ausgelegt wird. Daher kann ihr CA-Zertifikat ebenfalls bis zum Gültigkeitsende der Root-CA ausgestellt und bei Bedarf später immer noch vor dem geplanten Ablauf gesperrt und durch ein neues ersetzt werden.

Die CRL der Issuing-CA wird automatisiert erneuert und veröffentlicht. Hier ist eine Gültigkeitsdauer von einem bis sieben Tagen mit Zuschlag einer Karenzfrist von einem bis vier Tagen ratsam, um einerseits eine Sperrung von Anwenderzertifikaten zügig wirksam werden zu lassen, andererseits aber auch eine ausreichende Reaktionszeit beim Auftreten von Problemen im automatischen Ablauf (z. B. Absturz des CA-Rechners) zu belassen.

Die Gültigkeit von Anwenderzertifikaten sollte als Faustregel mindestens ein Jahr betragen und fünf Jahre nicht überschreiten. Oft ist ein Gültigkeitszeitraum von drei Jahren ein guter Kompromiss, der bei hoher Fluktuation unter den Zertifikatsinhabern verkürzt und bei unangemessen hohem Aufwand für eine Zertifikatserneuerung (bspw. bei Rechnern, die für vier Jahre geleast werden) verlängert werden kann.

3.4.4 Weitere technische Sicherheitsaspekte

Für das angepeilte Basis-Sicherheitsniveau reicht es aus, die CA-Schlüssel beider CAs in Software im Zertifikatsspeicher des jeweiligen Servers abzulegen. Auf den Einsatz eines Hardware Security Moduls, das das PKI-Konzept organisatorisch und technisch aufwändiger gestalten würde, wird verzichtet (vgl. den Ausblick in Abschnitt 6.1.2).

---

6 Zum Vergleich: 15 Jahre vor der Erstellung dieses White Papers war Windows 95 das neueste Arbeitsplatzbetriebssystem und Windows NT 4.0 erschien erst einige Monate später.

4 PKI-Aufbau: Schritt für Schritt

In den nachfolgenden Anleitungen geben die in `fester Schriftweite` gesetzten Textpassagen Bezeichnungen aus dem Windows-System wieder, besonders die vom Anwender zu aktivierenden Dialogelemente (Icons, Buttons, Kartenreiter, Eingabefelder, Checkboxen etc.), einzugebende Kommandos und Dateinamen. Für <Platzhalter in spitzen Klammern> sind jeweils individuelle Bezeichnungen aus der aufzubauenden PKI einzusetzen.

4.1 Root-CA

4.1.1 Systemvoraussetzungen und vorbereitende Schritte

Als Root-CA kommt ein Stand-Alone-Rechner zum Einsatz, der nicht ins AD integriert ist. Als zusätzliche Sicherheitsmaßnahme können nach der Systeminstallation alle Netzwerkschnittstellen im Gerätemanager deaktiviert werden. Auch eine Festplattenvollverschlüsselung (z. B. per Windows BitLocker oder TrueCrypt) kommt als zusätzliche Sicherheitsmaßnahme in Frage. In diesem Fall ist die PIN oder das Pre-Boot-Passwort zum Starten des Systems wie unten für das lokale Administrator-Passwort beschrieben aufzuteilen und versiegelt zu hinterlegen.

Der Rechner sollte, solange er nicht gebraucht wird, sicher verschlossen verwahrt werden, bspw. in einem Tresor oder Stahlschrank. Das genaue Behältnis und die Schließregelungen müssen sich nach den vorhandenen, individuellen Gegebenheiten beim PKI-Betreiber richten.

Als Serversoftware kann Windows Server 2003, 2008 oder 2008 R2 eingesetzt werden; dabei ist jeweils die Standard Edition des Betriebssystems ausreichend. Nachfolgend wird von Windows Server 2008 (mit Bezeichnungen in der englischen Benutzeroberfläche) ausgegangen. Die einzelnen Schritte und Konfigurationsdateien sind jedoch auch auf die anderen Server-Betriebssysteme übertragbar.

Die Installation sollte als „Root-Key-Zeremonie“ von mehreren Personen durchgeführt und überwacht werden.[7] Dabei sollten Karten, Umschläge und Siegel für die versiegelte Hinterlegung von Passwörtern und Datenträgern (bspw. CD-R-Rohlinge und/oder USB-Sticks; wenige MByte sind ausreichend) für die Hinterlegung des Root-CA-Schlüssels in ausreichender Anzahl bereit stehen. Für die Hinterlegung sollten jeweils mindestens zwei Exemplare erstellt und an unterschiedlichen Orten (bspw. ein Satz in einem Tresor vor Ort und ein zweiter in einem Bankschließfach) hinterlegt werden. Wiederum müssen sich die genauen Orte und Schließregelungen nach den vorhandenen Gegebenheiten beim PKI-Betreiber richten. Dabei kann in der Regel die anzutreffende Art der Hinterlegung eines Enterprise-Administrator-Passworts als Richtschur dienen.

Falls ein rudimentäres Vier-Augen-Prinzip umgesetzt werden soll, ist nach der Grundinstallation des Betriebssystems, noch vor der Installation der Certificate Services, das Passwort des lokalen Administratorkontos so zu ändern, dass die erste Hälfte des Passworts nur einem oder zwei PKI-Administratoren bekannt ist und die zweite Hälfte einem oder zwei

[7] Zumindest dann, wenn die betreffende PKI in einer Produktivumgebung eingesetzt werden soll. Für Testumgebungen kann in diesem Punkt ggf. der organisatorische Aufwand verringert werden, solange nur die Test-PKI hinsichtlich ihrer technischen Schnittstellen hinreichend mit der produktiven PKI identisch bleibt.

anderen PKI-Administratoren. Die beiden Passworthälften sind in getrennten, versiegelten Umschlägen zu hinterlegen, ohne Vier-Augen-Prinzip ist das ganze Passwort in einem einzelnen versiegelten Umschlag sicher zu verwahren. In beiden Fällen sollte das Passwort insgesamt mindestens 12 Zeichen lang sein.

Damit die nachfolgend konfigurierten Audit-Einstellungen der Certificate Services wirksam werden, muss in der lokalen Audit-Policy des Servers die Protokollierung des „Object Access“ sowohl für den „Success“- als auch den „Failure“-Fall aktiviert sein.

4.1.2 Installation

Die Installation der Certificate Services für die Root-CA wird vom lokalen Administrator durchgeführt.

Vorbereitend muss die Datei `capolicy.inf` (siehe Anhang A.1.1) im `%SystemRoot%` Verzeichnis des Servers abgelegt werden. Die Einstellungen darin sorgen dafür, dass der Best Practice entsprechend in dem während des Installationsvorgangs erstellten Root-CA-Zertifikat die KeyUsage-Erweiterung als kritisch markiert wird.

Danach sind die folgenden Schritte durchzuführen:

1. `Start\Server Manager\Roles\Add Roles`
   - `Active Directory Certificate Services` auswählen
2. Weiter bis zum Schritt `Role Services`
   - `Certification Authority` auswählen
   - `Certification Authority Web Enrollment` nicht auswählen
3. Weiter zum Schritt `Setup Type`
   - `Standalone` auswählen
4. Weiter zum Schritt `CA Type`
   - `Root CA` auswählen
5. Weiter zum Schritt `Private Key`
   - `Create a new private key` auswählen, weiter zum Teilschritt `Cryptography`
   - RSA#`Microsoft Software Key Storage Provider` auswählen (unter Windows 2003: `Microsoft Enhanced Cryptographic Provider 1.0`)
   - `Key character length` 2048 auswählen
   - `Hash algorithm` `sha1` auswählen, weiter
6. Weiter zum Schritt `CA Name`
   - Als `Common name for this CA` den CN des vorab festgelegten Distinguished Name der Root-CA (vgl. Abschnitt 3.2.2) in der Schreibweise ohne „CN=“ eintragen.
   - Als `Distinguished Name Suffix` die O- und C-Komponenten des vorab festgelegten Distinguished Name der Root-CA (vgl. Abschnitt 3.2.2) in der Schreibweise „O=Acme Inc.,C=US” eintragen.
   - Den angezeigten `Preview of distinguished name` sorgfältig auf Korrektheit prüfen.

7. Weiter zum Schritt `Validity Period`
   - Die gewählte PKI-Lebenszeit in Jahren (vgl. Abschnitt 3.4.3) eintragen.
8. Weiter zum Schritt `Certificate Database`
   - Hier können die Vorgaben belassen werden. Falls es im Hinblick auf Backup-Prozeduren für die Root-CA vorteilhafter ist, können aber `Certificate database` und `log` auch in ein separates Verzeichnis oder eine eigene Partition gelegt werden.
9. Bestätigen und weiter bis zum Abschluss des Installationsassistenten.

4.1.3 Konfiguration

Als Ergebnis der im vorigen Abschnitt beschriebenen Installation ist unter Administrative Tools eine neue Managementkonsole mit dem Titel `Certification Authority` zu finden. Über das Eigenschaftsfenster der CA in dieser Managementkonsole können einige wesentliche Konfigurationseinstellungen vorgenommen werden.

Da jedoch andere benötigte Konfigurationseinstellungen nur über die Kommandozeile oder direkt über einen Registry Editor zugänglich sind, wird die gesamte Konfiguration über den Aufruf des Kommandozeilen-Skripts `caconfig.cmd` (siehe Anhang A.1.2) vorgenommen. Der Einsatz eines Kommandozeilenskripts bietet den zusätzlichen Vorteil, dass die einzelnen Einstellungen vor der Ausführung einfacher geprüft werden können und dadurch bereits dokumentiert sind.

4.1.4 Sicherung des Root-CA-Schlüssels

Über die Benutzeroberfläche der Certificate Services oder andere Betriebssystemschnittstellen kann ein Backup des Root-CA-Zertifikats zusammen mit dem zugehörigen geheimen Schlüssel (der dann per Passphrase verschlüsselt wird) im PKCS#12 Standardformat erstellt werden. Eine derartige Sicherung wird nur ein Mal benötigt, um den Root-CA-Schlüssel in dieser Form für eine eventuell benötigte Rekonstruktion einer zerstörten Root-CA zu hinterlegen, danach nicht mehr.

Der folgende Ablauf erstellt dieses Backup zur Hinterlegung, prüft, ob eine Wiederherstellung damit möglich ist, und verhindert gleichzeitig einen künftigen unautorisierten Export über Betriebssystemschnittstellen[8]:

1. `Start\Administrative Tools\Certification Authority`
   - Knoten der Root-CA auswählen
   - `Action\All Tasks\Backup CA...`
2. Weiter bis zum Schritt `Items to Back Up` des Backup-Assistenten
   - `Private Key and Certificate` auswählen
   - `Certificate database` nicht auswählen
   - Als `Location` ein Verzeichnis auf einem Datenträger zur Hinterlegung auswählen
3. Weiter zum Schritt `Select a Password`

[8] Ein unautorisierter Export mittels zusätzlicher „Hacker“-Software bleibt theoretisch möglich.

- Selbst wenn im Regelbetrieb das rudimentäre Vier-Augen-Prinzip nicht umgesetzt werden soll, ist bei der Sicherung des Root-CA-Schlüssels das Vier-Augen-Prinzip anzuwenden: Daher ist an dieser Stelle von zwei verschiedenen PKI-Adminstratoren jeweils eine Hälfte des Passworts zweimal so einzugeben, dass sie dem anderen PKI-Administrator nicht bekannt wird. Die beiden Passworthälften sind in getrennten, versiegelten Umschlägen zu hinterlegen. Das Passwort sollte insgesamt mindestens 12 Zeichen lang sein.

4. Weiter bis zum Abschluss des Backup-Assistenten.

Durch diese Prozedur wird auf dem Datenträger für die Hinterlegung des Root-CA-Schlüssels eine PKCS#12 Datei mit dem Namen <Common Name (CN) der Root-CA>`.p12` angelegt, die das Root-CA-Zertifikat und den mit dem zweigeteilten Passwort verschlüsselten zugehörigen geheimen Schlüssel enthält.

Nun kann das CA-Zertifikat aus dem Zertifikatsspeicher des Root-CA-Servers gelöscht und mitsamt dem zugehörigen Schlüssel aus dem Backup wiederhergestellt werden:

5. `Start\mmc.exe`
   - `File\Add or Remove Snap-ins...`
   - `Certificates\Computer account` hinzufügen
   - Das Hinzufügen abschließen
6. Knoten `Certificates\Personal\Certificates` auswählen
   - Das Root-CA-Zertifikat auswählen
   - Löschen und dabei die Warnung bestätigen
7. Knoten `Certificates\Personal\Certificates` auswählen
   - `Action\All Tasks\Import...`
8. Weiter bis zum Schritt `File to Import` des Import-Assistenten
   - Die zuvor gesicherte Datei <Common Name (CN) der Root-CA>`.p12` auswählen. (Dazu muss der gesuchte Dateityp im Auswahldialog auf `Personal Information Exchange (*.p12,*.pfx)` umgestellt werden.)
9. Weiter zum Schritt `Password`
   - An dieser Stelle ist müssen die beiden PKI-Administratoren ihre jeweilige, zuvor beim Export gewählte und hinterlegte Passworthälfte wieder eingeben.
   - `Mark this key as exportable` darf nicht ausgewählt werden.
     Hierdurch wird ein nachträglicher erneuter Export über Betriebssystemschnittstellen verhindert.
10. Weiter bis zum Abschluss des Import-Assistenten.
11. Öffnen eines Kommandozeilenfensters zum Neustart der Certificate Services mit dem wiederhergestellten Schlüssel
    - Kommandozeile `net stop certsvc`
    - Kommandozeile `net start certsvc`

Nach der erfolgreichen Wiederherstellung der Root-CA muss die erstellte Sicherungskopie (PKCS#12-Datei) auf weitere Datenträger kopiert bzw. gebrannt werden, um sie später zusammen mit den versiegelten Passwörtern in entsprechender Anzahl zu hinterlegen.

4.1.5 Export und Publikation von Root-CA-Zertifikat und -CRL

Das CA-Zertifikat der Root-CA muss als Vertrauensanker im AD publiziert werden. Zusätzlich wird eine aktuelle, gültige CRL der Root-CA im AD benötigt. Dazu müssen diese beiden Datenelemente als Dateien über einen Transfer-Datenträger (bspw. ein USB-Stick) von der offline betriebenen Root-CA ins AD übertragen werden.

Hierzu muss zunächst der lokale Administrator der Root-CA den Transfer-Datenträger anschließen und das Kommandozeilen-Skript `export_ca_crl.cmd` (siehe Anhang A.1.3) aufrufen.

Danach ist der Transfer-Datenträger auf vertrauenswürdigem Wege[9] einem Enterprise-Administrator des AD zu übergeben, der ihn anschließt und das Kommandozeilen-Skript `import_ca_crl.cmd` (siehe Anhang A.2.3) aufruft.

Nach dem erfolgreichen erstmaligen Import wird das Root-CA-Zertifikat im AD publiziert; ggf. ist dabei eine Karenzzeit für die Replikation auf alle Domain Controller einzuplanen. Danach übernehmen alle an das AD angeschlossenen Computer beim nächsten (Online-)Neustart oder Group Policy Refresh dieses Zertifikat als Vertrauensanker in ihren lokalen Zertifikatsspeicher.

Dieser Ablauf ist regelmäßig rechtzeitig vor Ablauf der CRL der Root-CA zu wiederholen, um die im AD und per HTTP publizierte Root-CA-CRL zu erneuern.

4.2 Issuing-CA

4.2.1 Systemvoraussetzungen und vorbereitende Schritte

Als Issuing-CA kommt ein ins AD integrierter, online betriebener Server zum Einsatz. Es sollten die im jeweiligen Unternehmen üblichen Vorkehrungen zur Härtung und physischen Sicherung von kritischen Windows-Servern zum Einsatz kommen; d. h. in der Regel ein Betrieb im Rechenzentrum vergleichbar einem Domain Controller.

Der Server kann prinzipiell in einer beliebigen Domäne des AD betrieben werden. Um die Anzahl der zugriffsberechtigten Domain-Administratoren einzugrenzen, hat es sich als Best Practice etabliert, Certificate Services in der Root-Domäne des AD oder einer anderen Domäne zu betreiben, in der kritische Serversysteme aber keine Workstations oder Endbenutzer angesiedelt sind (sofern eine solche Domäne im betreffenden AD existiert).

Dabei muss kein dedizierter Server zum Einsatz kommen. Im hier beschriebenen Anwendungsfall können die Certificate Services ohne nennenswerte Leistungseinbußen in einer Virtualisierungsinstanz oder auf einem vorhandenen Server mit betrieben werden. Auch der Betrieb auf einem Domain Controller ist grundsätzlich nicht ausgeschlossen, sollte aber vermieden werden, wenn andere geeignete Server zur Verfügung stehen.

Als Serversoftware kann Windows Server 2003, 2008 oder 2008 R2 eingesetzt werden; dabei wird jeweils mindestens die Enterprise Edition des Betriebssystems benötigt. Nachfolgend wird, wie schon bei der Root-CA, von Windows Server 2008 (mit Bezeichnungen in der englischen Benutzeroberfläche) ausgegangen. Die einzelnen Schritte und Konfigurationsdateien sind jedoch auch auf die anderen Server-Betriebssysteme übertragbar. Um eine CA auf einem Windows Server 2008 oder 2008 R2 in einem Windows-

9 Hier ist eine unternehmensspezifisch geeignete organisatorische Regelung zu etablieren, um sicherzustellen, dass die Daten unverfälscht übertragen werden, bspw. durch persönliche Übergabe zwischen einander bekannten Administratoren.

2003-basierten AD zu installieren, muss zunächst ein Schema-Update des AD auf das Directory Schema von Windows 2008 erfolgen.

Damit die nachfolgend konfigurierten Audit-Einstellungen der Certificate Services wirksam werden, muss in der für den CA-Server maßgeblichen Group Policy die Protokollierung des „Object Access“ sowohl für den „Success“- als auch den „Failure“-Fall aktiviert sein.

Da die Issuing-CA die Web-Enrollment Schnittstelle der Certificate Servces nutzen soll, kann bereits vorab der Web Server Dienst (IIS) auf dem System installiert werden.

4.2.2 Installation

Die Installation der Certificate Services für die Issuing-CA wird von einem Administrator durchgeführt, der zugleich Enterprise-Administrator, Domänen-Administrator der Domäne des CA-Servers und lokaler Administrator dieses Servers sein muss.

Vorbereitend muss die Datei `capolicy.inf` (siehe Anhang A.2.1) im `%SystemRoot%` Verzeichnis des Servers abgelegt werden. Deren Einstellungen sorgen dafür, dass der Best Practice entsprechend die KeyUsage-Erweiterung im während der Installation erstellten Zertifizierungsantrag (CSR) als kritisch markiert wird.

Danach sind die folgenden Schritte durchzuführen:

1. `Start\Server Manager\Roles\Add Roles`
   - `Active Directory Certificate Services` auswählen
2. Weiter bis zum Schritt `Role Services`
   - `Certification Authority` auswählen
   - `Certification Authority Web Enrollment` auswählen
     Ggf. die Nachfrage wegen noch nicht installierter Web Server Komponenten mit `Add Required Role Services` bestätigen
   - `Online Responder` nicht auswählen
   - `Network Device Enrollment Service` nicht auswählen
3. Weiter zum Schritt `Setup Type`
   - `Enterprise` auswählen
4. Weiter zum Schritt `CA Type`
   - `Subordinate CA` auswählen
5. Weiter zum Schritt `Private Key`
   - `Create a new private key` auswählen, weiter zum Teilschritt `Cryptography`
   - `RSA#Microsoft Software Key Storage Provider` auswählen
     (unter Windows 2003: `Microsoft Enhanced Cryptographic Provider 1.0`)
   - `Key character length` 2048 auswählen
   - `Hash algorithm` `sha1` auswählen, weiter
6. Weiter zum Schritt `CA Name`
   - Als `Common name for this CA` den CN des Distinguished Name der Issuing-CA (vgl. Abschnitt 3.2.2) in der Schreibweise ohne „CN=“ eintragen.

- Als `Distinguished Name Suffix` die O- und C-Komponenten des Distinguished Name der Issuing-CA (vgl. Abschnitt 3.2.2) in der Schreibweise „O=Acme Inc.,C=US" eintragen; dabei den in Form von DC (Domain Compontents) vorgegebenen AD-Domänennamen überschreiben.
- Den angezeigten `Preview of distinguished name` sorgfältig auf Korrektheit prüfen.

7. Weiter zum Schritt `Certificate Request`
   - `Save a certificate request to file` auswählen
   - Pfad und Dateiname auf einem Transfer-Datenträger auswählen
     Als Dateiname sollte <Common Name (CN) der Issuing-CA>`.req` verwendet werden
8. Weiter zum Schritt `Certificate Database`
   - Hier können die Vorgaben belassen werden. Falls es im Hinblick auf Backup-Prozeduren für die Issuing-CA vorteilhafter ist, können `Certificate database` und `log` auch in ein separates Verzeichnis oder eine eigene Partition gelegt werden.
9. Bestätigen und weiter bis zum Abschluss des Installationsassistenten.

4.2.3 Zertifizierung durch die Root-CA

Der in dem zuvor beschriebenen Ablauf erstellte Transfer-Datenträger mit der Datei <Common Name (CN) der Issuing-CA>`.req` muss nun zur Erstellung des Sub-CA-Zertifikats für die Issuing-CA auf vertrauenswürdigem Wege an den oder die PKI-Administratoren der Root-CA übergeben werden. In der Regel geschieht dies im Rahmen eines Projekts zum PKI-Aufbau als persönliche Übergabe zwischen den bekannten Projektbeteiligten. Nicht selten sind auch die PKI-Administratoren der Root-CA und der Issuing-CA identisch.

Der PKI-Administrator der Root-CA schließt den Transfer-Datenträger an den Rechner der Root-CA an und führt die folgenden Schritte durch:

1. `Start\Administrative Tools\Certification Authority`
   - Knoten der Root-CA auswählen
   - `Action\All Tasks\Submit new request ...`
   - Datei <Common Name (CN) der Issuing-CA>`.req` auf dem Transfer-Datenträger auswählen
2. Knoten `Pending Requests` in der Managementkonsole `Certification Authority` auswählen
   - Den neu importierten Request auswählen
     (Falls die Liste der `Pending Requests` leer ist, ggf. `Action\Refresh` aufrufen)
   - `Action\All Tasks\Export Binary Data...`
   - Als `Column` das Datenbankattribut `Binary Request` auswählen
   - `View formatted test version of data` auswählen

- In einem Editor-Fenster wird eine dekodierte Version des Zertifikatsantrags angezeigt. Hier sollte der Root-CA PKI-Administrator besonders die folgenden Punkte noch einmal prüfen:
  - Der Distinguished Name der Issuing-CA im Feld `Subject` muss korrekt sein.
  - Die `Public Key Length` muss `2048 bits` sein.
  - Das Attribut `Certificate Extensions` muss die folgenden Angaben zu Erweiterungen enthalten:
    - `Basic Constraints`: `Critical`, `Subject Type = CA`
    - `Key Usage`: `Critical`, `Certificate Signing, Off-line CRL Signing, CRL Signing (06)`
- Editor-Fenster schließen

3. Nach erfolgreicher Prüfung: `Action\All Tasks\Issue`
   - Ansonsten wäre ggf. die Installation der Issuing-CA bis zu diesem Punkt zu wiederholen.
4. Knoten `Issued Certificates` auswählen
   - Das neu erstellte Zertifikat auswählen
     (Falls die Liste der `Issued Certificates` mehrere Zertifikate enthält das mit der höchsten `Request ID`)
   - `Action\Open`
   - Kartenreiter `Details\Copy to File...`
5. Im Zertifikats-Export-Assistenten zum Schritt `Export File Format` gehen
   - `DER encoded binary` auswählen
6. Weiter zum Schritt `File to Export`
   - Datei <Common Name (CN) der Issuing-CA>`.cer` auf dem Transfer-Datenträger auswählen
7. Den Zertifikats-Export-Assistenten abschließen
8. Abmelden, den Rechner der Root-CA herunterfahren und wieder entsprechend der Schließregelung verwahren.

Abschließend ist der Transfer-Datenträger mit dem erstellten Zertifikat wieder einem PKI-Administrator der Issuing-CA auszuhändigen.

4.2.4 Konfiguration

Ähnlich wie bei der Root-CA (vgl. Abschnitt 4.1.3) wird der Großteil der Konfiguration über den Aufruf eines Kommandozeilen-Skripts `caconfig.cmd` (siehe Anhang A.2.2) vorgenommen. Der Einsatz eines Kommandozeilenskripts bietet den Vorteil, dass die einzelnen Einstellungen vor der Ausführung einfacher geprüft werden können und dadurch bereits dokumentiert sind.

Nach dem Lauf dieses Skripts muss der PKI-Administrator den Transfer-Datenträger mit dem von der Root-CA für die Issuing-CA erstellten CA-Zertifikat an den Server anschließen und dann folgende Schritte durchführen:

1. Die Datei <Common Name (CN) der Issuing-CA>.cer vom Transfer-Datenträger nach %SystemRoot%\System32\CertSrv\CertEnroll kopieren, um das CA-Zertifikat der Issuing-CA auf dem Webserver zum Download verfügbar zu machen.
2. Start\Administrative Tools\Certification Authority
   - Knoten der Issuing-CA auswählen
   - Action\All Tasks\Install CA Certificate...
   - Datei <Common Name (CN) der Issuing-CA>.cer auf dem Transfer-Datenträger auswählen
     (Dazu muss der gesuchte Dateityp im Auswahldialog auf X.509 Certificate (*.cer,*.crt) umgestellt werden.)
   - Action\All Tasks\Start Service
3. Knoten Certificate Templates auswählen
   - Alle Templates auswählen und löschen, um die Erstellung von Zertifikaten der vordefinierten Typen zu deaktivieren.
4. Knoten Revoked Certificates auswählen
   - Action\All Tasks\Publish
   - New CRL auswählen und bestätigen
5. Knoten Certificate Templates auswählen
   - Alle angezeigten Templates auswählen
   - Action\Delete und den Warnhinweis bestätigen

Mit Schritt 4 wird eine neue Sperrliste entsprechend der konfigurierten Einstellungen erstellt und publiziert.

Schritt 5 deaktiviert sämtliche vordefinierten Certificate Templates, nach denen die Issuing-CA in der Standardkonfiguration Zertifikate erstellt, damit nicht unbeabsichtigt derartige Zertifikate erstellt werden. Danach können wie in Kapitel 5 beschrieben passende Certificate Templates für alle benötigten Zertifikatstypen bzw. PKI-Anwendungen erstellt und aktiviert werden.

4.2.5 Sicherung des Issuing-CA-Schlüssels

Prinzipiell kann auch der Schlüssel der Issuing-CA in einem Verfahren wie dem in Kapitel 4.1.4 für die Root-CA beschriebenen gesichert und für eine Wiederherstellung hinterlegt werden. Dies ist jedoch nicht notwendig, solange der gesamte Server, auf dem die CA betrieben wird, in ein entsprechendes Backup-Verfahren einbezogen ist. Im Katastrophenfall besteht zudem die Möglichkeit, dass die Root-CA eine neue Issuing-CA zertifiziert und die bestehende sperrt.

Daher bleibt der folgende Ablauf, um einen Export des CA-Schlüssels über Betriebssystemschnittstellen zu verhindern:

1. Start\Administrative Tools\Certification Authority
   - Knoten der Issuing-CA auswählen
   - Action\All Tasks\Backup CA...
2. Weiter bis zum Schritt Items to Back Up des Backup-Assistenten

- `Private Key and Certificate` auswählen
- `Certificate database` nicht auswählen
- Als `Location` ein temporäres Verzeichnis auswählen.

3. Weiter zum Schritt `Select a Password`
   - An dieser Stelle sollte ein mindestens 12-stelliges Passwort eingegeben werden, das nur während dieses Ablaufs gebraucht wird.
4. Weiter bis zum Abschluss des Backup-Assistenten.
5. `Start\mmc.exe`
   - `File\Add or Remove Snap-ins...`
   - `Certificates\Computer account` hinzufügen
   - Das Hinzufügen abschließen
6. Knoten `Certificates\Personal\Certificates` auswählen
   - Das Issuing-CA-Zertifikat auswählen
   - Löschen und dabei die Warnung bestätigen
7. Knoten `Certificates\Personal\Certificates` auswählen
   - `Action\All Tasks\Import...`
8. Weiter bis zum Schritt `File to Import` des Import-Assistenten
   - Die zuvor gesicherte Datei <Common Name (CN) der Issuing-CA>`.p12` in dem temporären Verzeichnis auswählen.
     (Dazu muss der gesuchte Dateityp im Auswahldialog auf `Personal Information Exchange (*.p12,*.pfx)` umgestellt werden.)
9. Weiter zum Schritt `Password`
   - Das in Schritt 3 vergebene Passwort erneut eingeben.
   - `Mark this key as exportable` darf nicht ausgewählt werden.
     Hierdurch wird ein erneuter Export über Betriebssystemschnittstellen verhindert.
10. Weiter bis zum Abschluss des Import-Assistenten.
11. Öffnen eines Kommandozeilenfensters zum Neustart der Certificate Services mit dem wiederhergestellten Schlüssel
    - Kommandozeile `net stop certsvc`
    - Kommandozeile `net start certsvc`

Nach der erfolgreichen Wiederherstellung muss die erstellte PKCS#12-Datei in dem temporären Verzeichnis sicher gelöscht werden.

5 PKI-Nutzung: Zertifikate für Computer und Benutzer

5.1 Generelles Vorgehen

5.1.1 Certificate Templates

Für jeden der nachfolgend beschriebenen Typen von Anwenderzertifikaten ist ein entsprechendes Certificate Template anzulegen oder zu modifizieren und in der Issuing-CA zu aktivieren.

Dies muss ein Administrator vornehmen, der sowohl Enterprise-Administrator (zur Bearbeitung der Certificate Templates im AD) als auch lokaler Administrator des Servers der Issuing-CA (zur Konfiguration der CA) ist. Der allgemeine Ablauf hierzu ist der folgende:

1. `Start\Administrative Tools\Certification Authority`
   - Knoten `Certificate Templates` auswählen
   - `Action\Manage`
2. Es öffnet sich die Management Konsole `Certificate Templates`
   - Das jeweils nachfolgend genannte Ausgangs-Template als Vorlage auswählen.
   - Entweder `Action\Duplicate Template...` (zur Neuanlage als Kopie einer Vorlage) oder `Action\Properties` (zur Modifikation eines bestehenden Templates) auswählen.
     Im Falle einer Kopie die Template-Version `Windows 2003 Server` auswählen.
   - Die Einstellungen für den benötigten Zertifikatstyp wie jeweils unten beschrieben vornehmen und das Eigenschaftsfenster schließen.
     Die unten beschriebenen Konfigurationshinweise beziehen sich auf eine Issuing-CA unter Windows Server 2008. Bei einer Windows Server 2003 basierten Issuing-CA sind jeweils zusätzlich die folgenden Einstellungen vorzunehmen:
     - Kartenreiter `Request Handling`
       - `Minimum key length`: `2048`
     - Kartenreiter `Extensions`
       - Erweiterung `Key Usage` auswählen, `Edit...`
       - `Make this extension critical` auswählen und bestätigen
   - Die Managementkonsole `Certificate Templates` schließen und zur Managementkonsole der `Certification Authority` zurückkehren
3. Es öffnet sich die Management Konsole `Certificate Templates`
   - Knoten `Certificate Templates` auswählen
   - `Action\New\Certificate Template to Issue...`
   - Das neu konfigurierte Certificate Template auswählen und bestätigen.

Danach können unmittelbar Zertifikate des betreffenden Typs ausgestellt werden.

5.1.2 Rechteverwaltung

Ob ein Benutzer oder Computer ein Zertifikat eines bestimmten Typs beziehen kann, hängt davon ab, ob er über die Rechte `Read`, `Enroll` und ggf. `Autoenroll` verfügt, die mittels der ACL des jeweiligen Certificate Template vergeben werden.

Je nach dem beabsichtigten Einsatzbereich der jeweiligen PKI-Anwendung können u. U. vordefinierte Sicherheitsgruppen und -prinzipale wie z. B. `Authenticated Users`, `Enterprise Domain Controllers`, `Domain Computers` oder `Domain Users` verwendet werden, denen diese Rechte zugewiesen werden.

Ansonsten hat sich folgende Vorgehensweise als Best Practice eingebürgert:

- In AD-Forests mit nur einer Domäne oder falls nur Benutzer oder Computer aus einer bestimmten Domäne mit Zertifikaten ausgestattet werden sollen, wird eine globale Sicherheitsgruppe angelegt, die die betreffenden Benutzer oder Computer direkt und/oder als Zusammenfassung weiterer globaler Gruppen enthält. Dieser globalen Gruppe werden die `Read`, `Enroll` und ggf. `Autoenroll Rechte` für das betreffende Certificate Template zugewiesen.
- In AD-Forests mit mehreren Domänen wird in jeder Domäne eine globale Sicherheitsgruppe angelegt, die die betreffenden Benutzer oder Computer direkt und/oder als Zusammenfassung weiterer globaler Gruppen enthält. Zusätzlich wird eine universelle Sicherheitsgruppe angelegt, die als Mitglieder die globalen Gruppen der einzelnen Domänen enthält und der dann die `Read`, `Enroll` und ggf. `Autoenroll Rechte` für das betreffende Certificate Template zugewiesen werden.

Lokalen Sicherheitsgruppen sollten in ACLs von Certificate Templates keine Rechte zugewiesen werden.

5.2 Domain Controller Zertifikate

5.2.1 Certificate Template

Sobald ein Domain Controller über ein Domain Controller Zertifikat verfügt, bietet er Zugriff auf das AD auch per LDAPS an. Daneben werden Domain Controller Zertifikate u. a. für eine Windows-Anmeldung per Smartcard benötigt.

Für Domain Controller Zertifikate kann ein bestehendes Certificate Template verwendet werden. Sofern alle Domain Controller im AD unter Windows Server 2003 oder neuer betrieben werden, sollte hierzu das vordefinierte Template `Domain Controller Authentication` verwendet werden.

Optional kann die folgende Änderung an diesem Template vorgenommen werden:

- Kartenreiter `General`
    - `Validity Period`:
      Voreinstellung sind 2 Jahre, je nach geplanter Laufzeit der Domain Controller kann hier ein abweichender Wert eingestellt werden (vgl. die Überlegungen zum Gültigkeitszeitraum von Anwenderzertifikaten in Abschnitt 3.4.3). Da Domain Controller Zertifikate grundsätzlich per Auto-Enrollment bezogen und verlängert werden sollten, ergibt sich jedoch letztlich kein großer Unterschied, so dass im Zweifel die Standardeinstellung beibehalten werden kann.

Weitere Modifikationen an dem vordefinierten Certificate Template brauchen nicht vorgenommen werden, bevor es wie oben beschrieben aktiviert wird.[10]

5.2.2 Enrollment

Zum Auto-Enrollment von Domain Controller Zertifikaten müssen in der für die Domain Controller im AD maßgeblichen Group Policy (bspw. in der `Default Domain Controllers Policy`) unter `Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Certificate Serivces Client – Auto Enrollment` die folgenden Einstellungen konfiguriert sein:

- `Configuration Model`: auf `Enabled` eingestellt
- `Renew expired certificates` ausgewählt
- `Update certificates` ausgewählt

Wenn diese Einstellungen getätigt und das Certificate Template wie oben beschrieben aktiviert wurde, beziehen alle Domain Controller beim nächsten Neustart oder Group Policy Refresh automatisch ein Domain Controller Zertifikat.

Falls die Issuing-CA nicht unter Windows Server 2008 und nach Möglichkeit auf einem regulären Mitgliedsserver im AD, sondern unter Windows 2003 auf einem Domain Controller installiert wurde, kann es sein, dass für andere Domain Controller keine Zertifikate erstellt werden können. In diesem Fall muss manuell die vordefinierte Gruppe `Enterprise Domain Controllers` in die Gruppe `CERTSVC_DCOM_ACCESS` der Domäne der Issuing-CA aufgenommen werden. Näheres hierzu findet sich im Microsoft Knowledge Base Artikel Nr. 903220.

5.3 Maschinenzertifikate für IEEE 802.1x

5.3.1 Certificate Template

Für Maschinenzertifikate zur Verwendung für Network Access Control per IEEE 802.1x mit EAP-TLS sollte ein neues Certificate Template ausgehend vom vordefinierten Template `Computer` angelegt und aktiviert werden.

Folgende Änderungen sind an der Kopie vorzunehmen[10]:

- Kartenreiter `General`
  - `Template Display Name`:
    Hier sollte ein eindeutiger, möglichst selbsterklärender Name gewählt werden. Ggf. kann auch eine Versionsnummer des Templates in den Namen aufgenommen werden.[11]
  - `Validity Period`:
    Je nach geplanter Laufzeit der betreffenden Computer sollte hier ein Wert zwischen einem und fünf Jahren eingestellt werden (vgl. die Überlegungen zum

10 Unter Windows Server 2003 muss zusätzlich noch die minimale Schlüssellänge und die Kritikalität der Erweiterung zur Schlüsselverwendung eingestellt werden, vgl. Abschnitt 5.1.1.

11 Daneben wird innerhalb der Certificate Template Verwaltung stets automatisch eine Versionsnummer geführt.

Gültigkeitszeitraum von Anwenderzertifikaten in Abschnitt 3.4.3). Da Maschinenzertifikate genau wie Domain Controller Zertifikate grundsätzlich per Auto-Enrollment bezogen und verlängert werden sollten, ergibt sich jedoch letztlich kein großer Unterschied, so dass im Zweifel die Voreinstellung beibehalten werden kann.

- Kartenreiter `Subject Name`
  - `Subject name format`:
    Voreinstellung ist `None`, d. h. nur der DNS-Name des Servers in der Erweiterung Subject Alternative Name (Microsoft-Bezeichnung: `alternate subject name`).[12] Je nachdem, ob und über welche Namensbestandteile ein für IEEE 802.1x eingesetzter RADIUS-Server die Zuordnung von Maschinenzertifikat zu einem RADIUS-Konto oder einer Zugangsgruppe vornimmt, kann es ratsam sein, zusätzlich hier einen der Werte `DNS Name`, `Common Name` (CN des Computerkontos im AD) oder `Fully Distinguished Name` (voller Name des Computerkontos im AD) einzustellen. Generell sollte die Zuordnung von Zertifikat zu Konto bzw. Zugangsgruppe zunächst getestet werden.
- Kartenreiter `Security`
  - Alle vordefinierten `Enroll` und `Autoenroll` Rechte entfernen.
  - Eine geeignete Sicherheitsgruppe (vgl. die Überlegungen in Abschnitt 5.1.2) hinzufügen und mit den Rechten `Read`, `Enroll` und `Autoenroll` versehen.

5.3.2 Enrollment

Zum Auto-Enrollment von Maschinenzertifikaten müssen in der für die betreffenden Computer im AD maßgeblichen Group Policy (bspw. in der `Default Domain Policy`) unter `Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Certificate Serivces Client – Auto Enrollment` die folgenden Einstellungen konfiguriert sein:

- `Configuration Model`: auf `Enabled` eingestellt
- `Renew expired certificates` ausgewählt
- `Update certificates` ausgewählt

Wenn diese Einstellungen getätigt und das Certificate Template wie oben beschrieben konfiguriert und aktiviert wurde, beziehen Computer, die die Rechte `Read`, `Enroll` und `Autoenroll` in Bezug auf das Certificate Template besitzen, beim nächsten (Online-)Neustart oder Group Policy Refresh automatisch ein Maschinenzertifikat.

12 Den Vorgaben von [RFC_5280] und [CoPKI_09] zufolge darf der Subject Name nicht leer bleiben, auch wenn dies nicht grundsätzlich zu einem Fehler führt. Vgl. die Übersicht zu PKI-Standards in [Bar_11].

5.4 SSL/TLS-Clientzertifikate

5.4.1 Certificate Template

Für die SSL/TLS-Clientauthentifikation mit dem RSA-Verfahren wird nur eine Signaturfunktion benötigt, jedoch keine Verschlüsselung. Um zu vermeiden, dass die betreffenden Zertifikate ungewollt zur Verschlüsselung von Daten verwendet werden, ohne dass für diesen Fall zusätzliche Maßnahmen wie Key-Backup (vgl. Abschnitt 6.2.6) eingerichtet sind, sollten sie dementsprechend als nur für Signatur zu Authentifkationszwecken[13] geeignet markiert sein.

Es sollte ein neues Certificate Template ausgehend vom vordefinierten Template `User Signature Only` angelegt und aktiviert werden.

Folgende Änderungen sind an der Kopie vorzunehmen[10]:

- Kartenreiter `General`
  - `Template Display Name`:
    Hier sollte ein eindeutiger, möglichst selbsterklärender Name gewählt werden. Ggf. kann auch eine Versionsnummer des Templates in den Namen aufgenommen werden.[11]
  - `Validity Period`:
    Je nach geplanter Laufzeit der betreffenden Computer sollte hier ein Wert zwischen einem und fünf Jahren eingestellt werden (vgl. die Überlegungen zum Gültigkeitszeitraum von Anwenderzertifikaten in Abschnitt 3.4.3).
- Kartenreiter `Subject Name`
  - `Subject name format`:
    Voreinstellung ist `Fully Distinguished Name` (voller Name des Benutzers im AD einschließlich Pfadkomponenten), zusätzlich die E-Mail-Adresse im Subject Distinguished Name sowie E-Mail-Adresse und der Windows-Kontoname (UPN) in der Erweiterung Subject Alternative Name (Microsoft-Bezeichnung: `alternate subject name`).
    Je nachdem, ob und über welche Namensbestandteile ein Webserver oder eine Web-Applikation die Zuordnung von Clientzertifikat zu einem Benutzerkonto oder einer Zugriffsgruppe vornimmt, kann es ratsam sein, hier den Wert `Common Name` (CN des Computerkontos im AD) einzustellen, um nicht unnötig die (ggf. während der Laufzeit des Zertifikats schon wieder überholte) Zuordnung des Benutzers zu einer bestimmten Domäne und bestimmten Organisationseinheiten (OUs) im AD sichtbar werden zu lassen. Generell sollte die Zuordnung von Zertifikat zu Web-Applikations-Konto zunächst getestet werden.
    Die Aufnahme der E-Mail-Adresse in den Subject Distinguished Name (und nicht nur in die Subject Alternative Name Erweiterung) sollte den Empfehlungen von [RFC_5280] zufolge unterbleiben. Sie ist jedoch zulässig und besonders in Verbindung mit der Einstellung, nur den `Common Name` aus dem AD in den Subject Distinguished Name zu übernehmen, ein probates Mittel, diesen auch bei zufälliger Namensgleichheit zwischen zwei Benutzern eindeutig zu gestalten.
    Unabhängig davon, an welcher Stelle die E-Mail-Adresse aufgenommen werden

13 D. h. auch nicht für Non-Repudiation bzw. Content Commitment, vgl. [RFC_5280] Kapitel 4.2.1.3.

soll, ob in den Subject Distinguished Name oder in die Erweiterung Subject Alternative Name, bleibt zu bedenken, dass dann SSL/TLS-Clientzertifikate nur für diejenigen Benutzer erstellt werden können, für die eine E-Mail-Adresse im AD hinterlegt ist. Ist dies nicht der Fall, sollte daher auf die Aufnahme der E-Mail-Adresse in das Zertifikat komplett verzichtet werden.

- Kartenreiter `Extensions`
  - Erweiterung `Application Policies` auswählen, `Edit...`
  - `Secure Email` löschen und bestätigen
- Kartenreiter `Security`
  - Alle vordefinierten `Enroll` und `Autoenroll` Rechte entfernen.
  - Eine geeignete Sicherheitsgruppe (vgl. die Überlegungen in Abschnitt 5.1.2) hinzufügen und mit den Rechten `Read`, `Enroll` und `Autoenroll` versehen.

5.4.2 Enrollment

Zum Auto-Enrollment von SSL/TLS-Clientzertifikaten müssen in der für die betreffenden Benutzer im AD maßgeblichen Group Policy (bspw. in der `Default Domain Policy`) unter `User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Certificate Serivces Client – Auto Enrollment` die folgenden Einstellungen konfiguriert sein:

- `Configuration Model`: auf `Enabled` eingestellt
- `Renew expired certificates` ausgewählt
- `Update certificates` ausgewählt

Wenn diese Einstellungen getätigt und das Certificate Template wie oben beschrieben konfiguriert und aktiviert wurde, beziehen Benutzer, die die Rechte `Read`, `Enroll` und `Autoenroll` in Bezug auf das Certificate Template besitzen, beim nächsten (Online-)Anmeldevorgang oder Group Policy Refresh automatisch ein SSL/TLS-Clientzertifikat.

5.5 SSL/TLS-Serverzertifikate

5.5.1 Certificate Template

Es sollte ein neues Certificate Template ausgehend vom vordefinierten Template `Web Server` angelegt und aktiviert werden.

Folgende Änderungen sind an der Kopie vorzunehmen[10]:

- Kartenreiter `General`
  - `Template Display Name`:
    Hier sollte ein eindeutiger, möglichst selbsterklärender Name gewählt werden. Ggf. kann auch eine Versionsnummer des Templates in den Namen aufgenommen werden.[11]
  - `Validity Period`:
    Je nach geplanter Laufzeit der betreffenden Server sollte hier ein Wert zwischen

einem und fünf Jahren eingestellt werden (vgl. die Überlegungen zum Gültigkeitszeitraum von Anwenderzertifikaten in Abschnitt 3.4.3).

- Kartenreiter `Request Handling`
  - `Minimum key length`:
    Hier sollten `2048` eingestellt werden.
    Bei Interoperabilitätsproblemen mit bestehender Serversoftware, für die SSL/TLS-Serverzertifikate erstellt werden sollen können ggf. auch `1024` eingestellt werden (vgl. Abschnitt 3.4.2). In diesem Fall sollte die `Validity Period` bei einem Jahr belassen werden und ggf. nach einem Update der betreffenden Serversoftware auf neue Zertifikate mit 2048 Bit Schlüssellänge gewechselt werden.
- Kartenreiter `Issuance Requirements`:
  - Abhängig von der Anzahl der zu erwartenden Anträge für SSL/TLS-Serverzertifikate und den zur Verfügung stehenden Ressourcen für die PKI-Administration kann hier `CA certificate manager appoval` ausgewählt werden. In diesem Fall muss ein PKI-Administrator die Erstellung eines beantragten Serverzertifikats manuell freigeben; andernfalls wird das Zertifikat unmittelbar nach Beantragung durch einen berechtigten Serveradministrator automatisch erstellt.
    Die manuelle Freigabe ermöglicht dem PKI-Administrator, zu prüfen, ob der Antrag korrekt ist, besonders die darin enthaltenen, ins Zertifikat aufzunehmenden Namensbestandteile. Ggf. kann dann die Ausstellung des Zertifikats verweigert und der betreffende Serveradministrator aufgefordert werden, einen korrigierten Zertifizierungsantrag einzureichen.
- `Minimum key length`:
  Kartenreiter `Security`
  - Alle vordefinierten `Enroll` und `Autoenroll` Rechte entfernen.
  - Eine geeignete Sicherheitsgruppe (vgl. die Überlegungen in Abschnitt 5.1.2) hinzufügen und mit den Rechten `Read`, `Enroll` und `Autoenroll` versehen.
    Im Fall von SSL/TLS-Serverzertifikaten sind die Mitglieder dieser Sicherheitsgruppe nicht die Server selbst, die ja oft nicht einmal als Computer im AD registriert sind, bspw. Unix-/Linux-basierte Webserver oder Appliances. Stattdessen sind die Serveradministratoren in diese Sicherheitsgruppe aufzunehmen, die SSL/TLS-Serverzertifikate für die von ihnen betreuten Serversysteme beantragen sollen.

Bei Bedarf können auch zwei verschiedene Templates für SSL/TLS-Serverzertifikate angelegt werden: eines mit 1024 Bit minimaler Schlüssellänge und einer Gültigkeitsdauer von einem Jahr und ein weiteres mit 2048 Bit minimaler Schlüssellänge bei längerer Gültigkeitsdauer.

5.5.2 Enrollment

Zur Beantragung von SSL/TLS-Serverzertifikaten wird die Web-Enrollment-Schnittstelle der Certificate Services verwendet.

Die Mehrzahl der gängigen SSL/TLS-Serversoftware ist in der Lage, einen Zertifizierungsantrag (CSR) im PKCS#10 Format in der beispielhaft in Anhang B dargestellten Form zu erstellen. In aller Regel muss der Serveradministrator, der den CSR erstellt, dabei

- die Schlüssellänge des zu erstellenden Schlüsselpaars (wenn möglich 2048 Bit) sowie

- die gewünschten Namensbestandteile des Serverzertifikats (als CN sollte in aller Regel der für SSL/TLS-Verbindungen verwendete DNS-Name des betreffenden Servers angegeben werden)

angeben. Details zum Vorgehen sollten in der jeweiligen Dokumentation der Serversoftware zu finden sein.

Um den erstellten CSR per Internet Explorer bei der Issuing-CA einzureichen, muss der Serveradministrator an einem Computer, der Mitglied des AD ist, mit seinem AD-Benutzerkonto angemeldet sein, das per Gruppenmitgliedschaft über die `Enroll` Rechte für das Certificate Template für SSL/TLS-Serverzertifikate verfügt. Dazu sind folgende Schritte notwendig.

1. Aufruf des IE mit der URL[14]
   `http://`<DNS Alias (CNAME) des Servers der Issuing-CA>`/CertSrv`
   - Sofern im IE die Option für den automatischen, integrierten Windows-Logon aktiviert und der Web-Enrollment-Server im Browser der lokalen Intranet Zone zugeordnet ist, wird keine gesonderte Anmeldung benötigt.
     Ansonsten muss der Benutzer sich im Browser nochmals mit seinem AD-Benutzernamen und Passwort anmelden.
2. Aufruf von `Request a certificate`
3. Aufruf von `Submit a Certificate Request by using a base64-encoded CMC or PKCS#10 file`
   - In das Feld `Saved Request` ist per Cut&Paste der Text des CSR (einschließlich der `BEGIN` und `END NEW CERTIFICATE REQUEST` Zeilen) zu übertragen.
   - Als `Certificate Template` ist – falls mehrere zur Auswahl angezeigt werden – dasjenige für SSL/TLS-Serverzertifikate auszuwählen.
   - Das Feld `Saved Request` kann leer bleiben
4. Aufruf von `Submit>`

Abhängig davon, ob im Certificate Template die oben beschriebene Option `CA certificate manager appoval` aktiviert ist oder nicht, erscheint danach entweder der Hinweis, dass das das Zertifikat erst noch freigegeben und später abgerufen werden muss oder aber das neu erstellte Zertifikat wird direkt zum Download angeboten.

In letzterem Fall stehen die Zertifikatskodierungen `DER encoded` oder `Base64 encoded` sowie der Download des Serverzertifikats alleine oder der ganzen Zertifikatskette im PKCS#7-Format zur Auswahl. Welche dieser Formate benötigt wird, richtet sich wiederum nach der eingesetzten SSL/TLS-Serversoftware. In den meisten Fällen sollte der Download des einzelnen Serverzertifikats im Base64-Format eine geeignete Wahl sein. Dieses Format wird im OpenSSL-Umfeld, bspw. bei einem Apache Webserver mit modSSL, ebenfalls verwendet und dort als „PEM-Format“ bezeichnet.

Im Falle, dass die Option `CA certificate manager appoval` aktiviert ist, muss ein PKI-Administrator den Zertifikatsantrag in den folgenden Schritten prüfen und freigeben:

1. `Start\Administrative Tools\Certification Authority`
2. Knoten der Issuing-CA öffnen und Knoten `Pending Requests` auswählen

[14] Sobald der IIS für die Web-Enrollment-Schnittstelle selbst mit einem SSL/TLS-Serverzertifikat versehen ist, sollte HTTPS anstelle von HTTP verwendet werden.

- Den neu eingegangenen Request auswählen
- `Action\All Tasks\Export Binary Data...`
- Als `Column` das Datenbankattribut `Binary Request` auswählen
- `View formatted test version of data` auswählen
- In einem Editor-Fenster wird eine dekodierte Version des Zertifikatsantrags angezeigt. Hier sollte der PKI-Administrator der Issuing-CA besonders die folgenden Punkte noch einmal prüfen:
  - Die Namensbestandteile des Distinguished Name im Feld `Subject` müssen korrekt sein (vgl. Abschnitt 3.2.2).
  - Falls das Attribut `Certificate Extensions` Angaben zur Erweiterung Subject Alternative Name (SubjectAltName) enthält, müssen auch deren Namensbestandteile alle korrekt sein.
  - In der Ansicht des Requests in der Managementkonsole Certification Authority ist in der Spalte `Requester Name` das AD-Benutzerkonto ersichtlich, über das der Zertifizierungsantrag bei der Issuing-CA eingereicht wurde. Soweit für den PKI-Administrator nachprüfbar, muss der Serveradministrator, der der Inhaber dieses AD-Benutzerkontos ist, auch verantwortlich für den oder die Server sein, deren DNS-Name im CN des Subject Distinguished Name und/oder in der Erweiterung SubjectAltName aufgeführt ist.
- Editor-Fenster schließen

3. Nach erfolgreicher Prüfung: `Action\All Tasks\Issue`
   - Ansonsten wäre ggf. der betreffende Serveradministrator aufzufordern, einen korrigierten Zertifizierungsantrag zu erstellen und einzureichen.

Das auf diese Weise erstellte Zertifikat braucht nicht manuell publiziert zu werden.

Nach Aufforderung durch den PKI-Administrator der Issuing-CA oder nach hinreichender Wartezeit muss der Serveradministrator wiederum die Web-Enrollment Seiten aufrufen. Da die Information über die Request ID des ausstehenden Zertifikats in einem lokalen Cookie gespeichert wird, muss er dazu denselben Browser verwenden, über den er das SSL/TLS-Serverzertifikat beantragt hatte, und die folgenden Schritte ausführen:

1. Aufruf des IE mit der URL[14]
   `http://`<DNS Alias (CNAME) des Servers der Issuing-CA>`/CertSrv`
   - Sofern im IE die Option für den automatischen, integrierten Windows-Logon aktiviert und der Web-Enrollment-Server im Browser der lokalen Intranet-Zone zugeordnet ist, wird keine gesonderte Anmeldung benötigt.
     Ansonsten muss der Benutzer sich im Browser nochmals mit seinem AD-Benutzernamen und Passwort anmelden.
2. Aufruf von `View the status of a pending certificate request`
3. Auswahl des betreffenden Requests

Anschließend wird genau wie oben für den Fall der automatischen Zertifikatsausstellung ohne manuelle Freigabe beschrieben das SSL/TLS-Serverzertifikat zum Download angeboten.

5.6 Weitere Betriebsprozesse

Neben dem Enrollment der Anwenderzertifikate und der regelmäßigen Publikation aktueller CRLs müssen mindestens noch die folgenden Betriebsprozesse für die PKI etabliert werden:

- Verlängerung oder Neuausstellung von Anwenderzertifikaten
- Sperrung von Anwenderzertifikaten
- Betriebsüberwachung der PKI

5.6.1 Verlängerung oder Neuausstellung

Streng genommen können Zertifikate nicht verlängert werden, da das Gültigkeitsende fest im Zertifikat verankert ist. Wenn nach Ablauf eines Zertifikats weiterhin Bedarf durch PKI-Anwendungen besteht, kann entweder ein neues Zertifikat für das bestehende Schlüsselpaar erstellt oder aber ein neues Schlüsselpaar generiert und entsprechend der vorhandenen Zertifikatsinformationen ein neues Zertifikat dazu erstellt werden.

Zertifikate, die per Auto-Enrollment bezogen wurden, werden automatisch über den gleichen Prozess durch neue Schlüsselpaare und Zertifikate ersetzt. Dies trifft für alle der oben beschriebenen Zertifikatstypen mit Ausnahme der SSL/TLS-Serverzertifikate zu. Für letztere ist zur Verlängerung der gleiche Ablauf wie beim erstmaligen Enrollment durchzuführen; dabei kann ein neuer Zertifizierungsantrag erstellt oder der vorige wiederverwendet werden.

5.6.2 Sperrung

Durch wen, auf welchem Wege und in welcher Form die Sperrung eines Anwenderzertifikats bei der PKI-Administration beantragt wird, muss sich nach den individuellen Gegebenheiten beim PKI-Betreiber und nach dem betroffenen Zertifikatstyp richten. Die folgenden Beispiele mögen die Bandbreite denkbarer Lösungen illustrieren:

- Ein Vorgesetzter informiert die PKI-Adminstration über das Ausscheiden eines Mitarbeiters. Die PKI-Administration überprüft diese Information durch telefonischen Rückruf bei der Personalabteilung. Anschließend sperrt sie das SSL/TLS-Clientzertifikat des betreffenden Mitarbeiters.
- Ein Mitarbeiter der AD-Benutzerverwaltung informiert einen persönlich bekannten PKI-Administrator über die Suspendierung oder Löschung eines AD-Benutzerkontos. Letzterer sperrt das zugehörige SSL/TLS-Clientzertifikat.
- Das Helpdesk sendet der PKI-Administration wöchentlich eine freigezeichnete Aufstellung der neu installierten oder außer Betrieb genommenen Arbeitsplatzrechner per Hauspost zu. Daraufhin werden die vor einer Neuinstallation erstellten[15] Maschinenzertifikate der betreffenden Computer sowie alle Maschinenzertifikate von außer Betrieb genommenen Rechnern gesperrt.
- Ein Serveradministrator meldet der PKI-Administration per E-Mail an eine eigens für Sperranträge eingerichtete E-Mail-Adresse, dass ein von ihm betreuter SSL/TLS-Server außer Betrieb genommen wurde. Ein PKI-Administrator überprüft darauf hin, dass das

[15] Nach einer Neuinstallation wird ein Rechner in der Regel per Auto-Enrollment ein neues Maschinenzertifikat beziehen. Das vorherige, noch gültige Zertifikat wird dadurch überflüssig und sollte – genau wie nach einer Außerbetriebnahme – gesperrt werden, um einen möglichen Missbrauch auszuschließen.

SSL/TLS-Serverzertifikat für den betreffenden Server von eben diesem Server-administrator beantragt wurde, und sperrt es.

In allen diesen Fällen kann ein PKI-Administrator der Issuing-CA nach der jeweiligen Überprüfung, ob der Sperrantrag berechtigt ist, das betroffene Zertifikat durch folgende Schritte sperren und eine aktualisierte CRL publizieren:

1. `Start\Administrative Tools\Certification Authority`
   - Knoten der Issuing-CA auswählen und aufklappen
2. Knoten `Issued Certificates` auswählen
3. Das zu sperrende Zertifikat in der angezeigten Liste identifizieren und auswählen.
   - Für die Identifikation des zu sperrenden Zertifikats kann abhängig von der im Sperrantrag übermittelten Information beispielsweise eines oder mehrere der folgenden angezeigten Felder herangezogen werden:
     - `Requester Name`
     - `Certificate Template`
     - `Serial Number`
     - `Certificate Expiration Date`
     - `Issued Common Name`
     - `Issued Email Address`
4. `Action\All Tasks\Revoke Certificate`
   - `Reason Code` kann bei `Unspecified` belassen werden.
     Alternativ kann unter den Vorgaben der für den jeweiligen Vorgang am besten passende Sperrgrund gewählt werden; alleine `Certificate Hold` sollte nicht verwendet werden.
   - `Date and Time` können bei der momentanen Uhrzeit belassen werden.
   - Sperrung mit `Yes` bestätigen.
5. Knoten `Revoked Certificates` auswählen
   - `Action\All Tasks\Publish`
   - `New CRL` auswählen und bestätigen

5.6.3 Betriebsüberwachung

In welcher Form eine laufende Betriebsüberwachung und ggf. Auditierung erfolgt, muss sich nach den individuellen Gegebenheiten beim PKI-Betreiber richten. Die entsprechenden Prozesse sollten sich daran orientieren, wie im Hause die Betriebsüberwachung und Auditierung der AD-Benutzerverwaltung ausgeprägt und etabliert ist.

In der in Kapitel 4 beschriebenen Konfiguration der PKI von der Stange werden sicherheits-relevante Operationen der Root- oder Issuing-CA (z. B. Erstellen von Zertifikaten und CRLs, Durchführen einer Sperrung oder Konfigurationsänderungen) jeweils im „Security Log“ des Windows Ereignisprotokolls auf demjenigen Server aufgezeichnet, auf dem die betreffende CA betrieben wird.

6 Ausblick: Alternativen und Ausbaumöglichkeiten

Alternativ zur der in den vorigen Kapiteln vorgestellten PKI von der Stange können die Microsoft Certificate Services auch für den Aufbau einer PKI mit einem erhöhten Sicherheitsniveau eingesetzt und die PKI auf verschiedenste Weise erweitert werden. In all diesen Fällen sollte eine genaue, individuelle Planung vorausgehen. Daher werden im Rahmen dieses White Papers nur die jeweils wichtigsten Aspekte als Ausblick dargestellt.

6.1 Alternativen bei Aufbau und Betrieb

6.1.1 Rollentrennung

Beim Einsatz der Windows Serversoftware in der Enterprise Edition oder höher kann eine Rollentrennung aktiviert werden, die es erzwingt, dass ein einzelner Benutzer nur eine einzige der folgenden Aufgaben wahrnehmen kann:

- Verwalten der CA
- Freigeben von Zertifizierungsanträgen und Sperren von Zertifikaten
- Backup und Restore der CA
- Verwalten und Löschen der zugehörigen Audit-Logs

Einschränkend ist jedoch anzumerken, dass ein einzelner Administrator mit hinreichenden Rechten die Rollentrennung auch wieder deaktivieren kann.

6.1.2 Hardware-Sicherheit der CA-Schlüssel

Anstelle wie bei der PKI von der Stange den geheimen Schlüssel der CA in Software auf dem Serversystem zu speichern, kann dieser Schlüssel auch in einem Hardware Security Modul oder einer Smartcard abgelegt werden. Hierdurch wird einerseits wirkungsvoll verhindert, dass der Schlüssel ausgelesen und kopiert werden kann. Andererseits können zusätzliche, über die Windows-Rechteverwaltung hinaus gehende Maßnahmen zur Aktivierung des Schlüssels vorgesehen werden, bspw. eine PIN-Eingabe durch einen oder mehrere PKI-Administratoren.

6.2 Ausbaumöglichkeiten

6.2.1 Nutzung der Zertifikate über das interne AD hinaus

Grundsätzlich können die von der hier beschriebenen PKI erstellten Zertifikate auch über die Grenzen des AD hinaus eingesetzt werden, z. B. für den Zugriff von Mitarbeitern und Geschäftspartnern auf SS/TLS-geschützte Server von anderen Endgeräten aus. Hierfür müssen zwei Voraussetzungen gegeben sein:

- Das Zertifikat der Root-CA muss auf den betreffenden, die PKI nutzenden Systemen durch einen dortigen Administrator oder Benutzer als Vertrauensanker installiert werden.
- Die Sperrlisten von Root- und Issuing-CA müssen von den betreffenden, die PKI nutzenden Systemen aus abrufbar sein. Dafür kann bspw. der in den CDP- und AIA-URLs verwendete DNS-Alias des Servers der Issuing-CA auf einen Webserver umgelegt werden, der vom Internet aus erreichbar ist, und die CRLs und CA-Zertifikate dort abgelegt werden.

Sollen darüber hinaus auch Zertifikate für Anwender jenseits des eigenen AD erstellt werden, so muss für diese ein eigenes Benutzerkonto angelegt werden oder ein vorhandener AD-Benutzer stellvertretend für die externen Nutzer die Zertifikate beantragen.

Für die Dokumentation der PKI – besonders gegenüber externen Teilnehmern und Nutzern – haben sich Certificate Policy, Certification Practice Statement und/oder PKI Disclosure Statement, jeweils mit standardisierter Gliederung, eingebürgert. Für Informationen zu diesen Dokumenten und ihre Erstellung sei auf das Secorvo White Paper „Das Policy-Rahmenwerk einer PKI“ [BaK_08] verwiesen.

6.2.2 Roaming von Benutzerzertifikaten

Um zu vermeiden, dass für einen AD-Benutzer bei der Anmeldung an einem neuen, bisher noch nicht von ihm genutzten Computer ein weiteres Zertifikat erstellt wird, gibt es drei Möglichkeiten:

- den Einsatz von Roaming Profiles, über die auch Benutzerverzeichnisse, Desktop und andere benutzerspezifische Einstellungen propagiert werden,
- die Publikation neu erstellter Benutzerzertifikate ins AD verbunden mit der Certificate Template Einstellung, kein neues Zertifikat zu erstellen, wenn bereits eines im AD vorgefunden wird (was jedoch den Nachteil hat, dass Zertifikate nur am jeweils ersten Arbeitsplatz eines jeden Benutzers zur Verfügung stehen) oder
- den Einsatz des Credential Roaming über zusätzliche AD-Attribute.

6.2.3 Benachrichtigung und Erinnerungen

Mittels des SMTP-Exit-Moduls der Certificate Services können bei jeder Beantragung, Erstellung, Sperrung etc. eines Zertifikats automatisch E-Mails verschickt werden.

Zertifikate, die per Auto-Enrollment bezogen wurden, werden i. d. R. rechtzeitig vor Ablauf automatisch erneuert. Um auch für andere Zertifikate rechtzeitig vor deren Ablauf den jeweiligen Zertifikatsinhaber über die ggf. fällige Erneuerung zu informieren, muss Fremdsoftware ergänzt werden, die regelmäßig die Zertifikatsdatenbank durchforstet und bei Bedarf die betreffenden Erinnerungs-Mails verschickt.

6.2.4 Nutzung neuer PKI-Funktionen von Windows 7 und Windows Server 2008 R2

Mit dem Erscheinen von Windows Vista wurde die Microsoft Crypto API um neue Module erweitert, die auch neuere Kryptoalgorithmen unterstützen. Im Hinblick auf die PKI besonders interessant sind dabei SHA-2 als Hashfunktion zum Ersatz des SHA-1 und Public-Key-Verfahren auf der Basis elliptischer Kurven als Alternative zu RSA. Um Zertifikate zu erstellen, die diese neueren Algorithmen nutzen, müssen Certificate Templates der Version `Windows 2008 Server` konfiguriert werden, die, wie der Name nahe legt, mit Certificate Services von Windows Server 2008 oder höher zur Verfügung stehen.

Seit Windows Server 2008 steht auch ein OCSP-Responder als Teil der Certificate Services zur Verfügung, der Online-Statusauskünfte über den Sperrstatus eines Zertifikats geben kann. Eine HTTP-URL, unter der ein solcher OCSP-Responder erreichbar ist, könnte in die AIA-Erweiterung der erstellten Anwenderzertifikate aufgenommen werden. Es gelten jedoch dabei zwei Einschränkungen:

- Windows-Clients unterstützen OSCP erst ab Windows Vista, d. h. solange noch mehrheitlich Windows XP Clients genutzt werden, ist es nicht sinnvoll, einen OCSP-Responder einzusetzen.
- Der OCSP-Responder arbeitet auf der Basis von CRLs und markiert seine Antworten als eben so lange gültig, wie die der Auskunft zu Grunde liegende CRL. D. h. weder ist es damit möglich, die Erstellung von CRLs komplett zu ersetzen, noch können damit „frischere“ Sperrinformationen verbreitet werden als es dem Erstellungsrhythmus der CRLs entspricht.

Um diese Einschränkungen zu vermeiden muss ggf. eine Fremdsoftware als OCSP-Responder eingesetzt werden.

Mit Windows 2008 R2 und Windows 7 Clients wird darüber hinaus über die sog. HTTP-Enrollment Schnittstelle die Erstellung von Zertifikaten für Benutzer und Computer eines anderen AD-Forests unterstützt, sofern zwischen dem AD-Forest der PKI und demjenigen der Zertifikatsinhaber eine Vertrauensbeziehung besteht. Selbst ein Auto-Enrollment über AD-Forest-Grenzen hinweg wird damit möglich.

Das HTTP-Enrollment bietet zugleich einen Ansatz für einen weitgehenden Schutz der PKI gegen den Missbrauch von Windows-Administratorrechten. Dazu kann die PKI in einem eigenen AD-Forest eingerichtet werden, in dem nur die PKI-Administratoren selbst über Administrationsrechte verfügen, während zu dem AD-Forest, in dem die Zertifikatsinhaber verwaltet werden, lediglich eine Vertrauensbeziehung eingerichtet wird.

6.2.5 Weitere PKI-Anwendungen

Für weitere PKI-Anwendungen ist in der Regel jeweils ein neues Certificate Template zu erstellen. U. U. können auch Zertifikate für verschiedene Anwendungen kombiniert werden. So könnte bspw. das Maschinenzertifikat so modifiziert werden, dass es auch für den IPsec-Verbindungsaufbau genutzt werden kann.

6.2.6 Key Backup und Recovery

Bei Zertifikaten, deren zugehöriges Schlüsselpaar für die Ver- und Entschlüsselung von persistent gespeicherten Daten genutzt werden soll, ist stets im Vorfeld zu klären, wie der Fall gehandhabt werden soll, dass der geheime Schlüssel nicht oder nicht mehr greifbar ist, bspw. nach einem Festplattenabsturz.

Eine Lösungsmöglichkeit für dieses Dilemma besteht im Einsatz von Key-Backup und -Recovery. Zum Key-Backup mit einer Microsoft-basierten PKI werden ein oder mehrere Key-Recovery-Agents benannt und mit speziell gekennzeichneten Zertifikaten ausgestattet. In Certificate Templates für Verschlüsselungszertifikate kann dann bestimmt werden, dass das Zertifikat nur erstellt wird, wenn gleichzeitig eine verschlüsselte Kopie des zugehörigen geheimen Schlüssels hinterlegt wird. Im Recovery-Fall kann dann der PKI-Administrator diese Kopie aus der CA-Datenbank exportieren und anschließend einer der benannten Key-Recovery-Agents ihn entschlüsseln, um ihn dem Anwender wieder zur Verfügung zu stellen. Durch diesen zweigeteilten Ablauf wird eine gewisse Form des Vier-Augen-Schutzes beim Key-Recovery erreicht.

6.2.7 Smartcards und Zertifikate

Schon seit Windows 2000 ist es Anwendern möglich, sich per Smartcard an Windows anzumelden, wenn sie über ein entsprechend gekennzeichnetes Zertifikat und Schlüsselpaar

auf der Smartcard verfügen. Natürlich sind die Microsoft Certificate Services in der Lage, entsprechende Zertifikate zu erstellen.

Zur Initialisierung der entsprechenden Smartcards kann einem Anwender die Rolle eines sog. Certificate Enrollment Agents übertragen werden. Damit wird es möglich, an einem Arbeitsplatz unter der Benutzerkennung dieses Certificate Enrollment Agents Smartcards für viele andere Benutzer zu initialisieren und mit den passenden Zertifikaten zu versehen.

Dennoch sollten bei größeren Anwenderzahlen, spätestens ab ca. 50 Benutzern, die Certificate Services nicht alleine für die Personalisierung und Verwaltung von Smartcards und Smartcard-Zertifikaten verwendet, sondern mit einem Smartcard Management-System kombiniert werden, das u. a. eine automatisierte Verwaltung von PINs und PUKs bereit stellt.

6.2.8 Erweiterte Nutzung des Web-Interfaces

Die Web-Enrollment Schnittstelle der Microsoft PKI kann ggf. auch mit anderen Browsern als dem Internet Explorer verwendet werden, bspw. um SSL/TLS-Clientzertifikate für Firefox-Browser (die einen eigenen Zertifikats- und Schlüsselspeicher mitbringen) zu erstellen. Teilweise sind dafür Anpassungen der Standard-Webseiten erforderlich.

Über Anpassungen der Web-Enrollment-Seiten können auch unnötige Optionen vor dem Benutzer verborgen und die Schnittstelle an das Look&Feel des jeweiligen Intranets angepasst werden.

Schließlich ist es möglich, über neu erstellte Web-Enrollment-Seiten weitergehende Funktionen zu realisieren, bspw. den Zugriff auf Benutzerinformationen in weiteren LDAP-Verzeichnissen neben dem eigenen AD oder die automatische Korrektur von Namensbestandteilen in Serverzertifikaten.

Anhang A Konfigurationsdateien

Einzelne Passagen in den nachfolgenden Konfigurationsdateien, die vor deren Einsatz noch entsprechend der in Kapitel 3 beschriebenen Namenskomponenten oder Konfigurationsparameter individuell angepasst werden müssen, sind grau hinterlegt.

An den Stellen, an denen als Teil von LDAP-URLS, die sich auf das Active Directory beziehen, „DC=<Domämenname der Root-Domäne des AD in einzelnen Komponenten>“ aufgeführt ist, ist für jede Einzelkomponente des Root-Domänennamens jeweils ein eigenes, per Komma getrenntes DC-Element einzusetzen, also z. B.:

- `DC=secorvo,DC=de` für die AD-Domäne secorvo.de
- `DC=ad-root,DC=acme,DC=us` für die AD-Domäne ad-root.acme.us

Als „<Lebensdauer der PKI in Jahren>“ sollte in dem Fall, dass die Gültigkeitsdauer von Root-CA-Zertifikat und Issuing-CA-Zertifikat gleich gewählt werden (vgl. Abschnitti 3.4.3) eben diese Anzahl von Jahren eingesetzt werden, ansonsten die geplante Gültigkeitsdauer des Issuing-CA-Zertifikats. Die Werte im Konfigurationsskript für die Root-CA (Anhang A.1.2) legen direkt die Gültigkeitsdauer der von der Root-CA ausgestellten Zertifikate für Issuing-CAs fest. Im Konfigurationsskript für die Issuing-CA (Anhang A.2.2) wird damit eine Obergrenze für die Gültigkeitsdauer der von dieser CA ausgestellten Anwenderzertifikate vorgegeben. Maßgeblich für die tatsächlich verwendete Gültigkeitsdauer von Anwenderzertifikaten ist jedoch die Vorgabe im jeweiligen Certificate Template, die allenfalls entsprechend dieser Obergrenze gekappt wird. An dieser Stelle in Anhang A.2.2 kann also ggf. auch ein kleinerer Wert als die Gültigkeitsdauer des Issuing-CA-Zertifikats eingetragen werden, um die Auswirkungen einer Fehlkonfiguration der Gültigkeitsdauer in einem Certificate Template für Anwenderzertifikate zu begrenzen.

A.1 Konfigurationsdateien für die Root-CA

A.1.1 Vor der Installation: capolicy.inf

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

[Extensions]
2.5.29.15=AwIBBg==
critical=2.5.29.15
```

A.1.2 Nach der Installation: caconfig.cmd

```
@echo off
rem ########################################################################
rem
rem Skript zur Konfiguration einer Microsoft CA
rem
rem Copyright (c) 2009 Secorvo Security Consulting GmbH
rem
rem ########################################################################

rem ### Certtificate Services beenden
net stop certsvc

rem ### Audit-Events
certutil -setreg CA\AuditFilter 127

rem ### Maximale Gueltigkeisdauer für Zertifikate
certutil -setreg CA\ValidityPeriod Years
certutil -setreg CA\ValidityPeriodUnits <Lebensdauer der PKI in Jahren>

rem ### Parameter für Verlängerung von Zertifikaten
certutil -setreg CA\RenewalKeyLength 2048
certutil -setreg CA\RenewalValidityPeriod Years
certutil -setreg CA\RenewalValidityPeriodUnits <Lebensdauer der PKI in Jahren>

rem ### Sperrlistenintervall und (davon) Karenzzeit
certutil -setreg CA\CRLPeriod Months
certutil -setreg CA\CRLPeriodUnits <Gültigkeitszeitraum der Root-CRL in Monaten (inkl. Karenzzeit)>
certutil -setreg CA\CRLOverlapPeriod Months
certutil -setreg CA\CRLOverlapUnits <Karenzzeit der Root-CRL-Gültigkeit in Monaten>

rem ### Keine Deltasperrlisten verwenden
certutil -setreg CA\CRLDeltaPeriodUnits 0

rem ### CRL Distribution Points
certutil -setreg CA\CRLPublicationURLs
"1:C:\Windows\System32\CertSrv\CertEnroll\<Common Name (CN) der Root-
CA>.crl\n10:ldap:///CN=<Common Name (CN) der Root-CA>,CN=<(Fiktiver) Servername der Root-
CA>,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=<Domämenname der
Root-Domäne des AD in einzelnen
Komponenten>?CertificateRevocationList?base?ObjectClass=cRLDistributionPoint\n2:http
://<DNS Alias (CNAME) des Servers der Issuing-CA>/CertEnroll/<Common Name (CN) der Root-
CA>.crl"

rem ### Authority Information Access
certutil -setreg CA\CACertPublicationURLs
"1:C:\Windows\System32\CertSrv\CertEnroll\<Common Name (CN) der Root-
CA>.cer\n2:ldap:///CN=<Common Name (CN) der Root-CA>,CN=AIA,CN=Public Key
Services,CN=Services,CN=Configuration,DC=<Domämenname der Root-Domäne des AD in einzelnen
Komponenten>?cACertificate?base?ObjectClass=certificationAuthority\n2:http://<DNS
Alias (CNAME) des Servers der Issuing-CA>/CertEnroll/<Common Name (CN) der Root-CA>.cer"

rem ### KeyUsage Zertifikatserweiterung nach RFC Vorgabe
certutil -setreg policy\EditFlags -EDITF_ADDOLDKEYUSAGE

rem ### Ggf. Netscape Zertifikatstyp Erweiterung aus dem Request uebernehmen
certutil -setreg policy\EnableRequestExtensionList +2.16.840.1.113730.1.1

rem ### Neustart der Certificate Services
net start certsvc

:end
```

A.1.3 Export von CA-Zertifikat und CRL: export_ca_crl.cmd

Das folgende Skript erstellt eine neue CRL und exportiert CA-Zertifikat und CRL auf einen angeschlossenen Transfer-Datenträger (bspw. USB-Stick).

```
@echo off

<Laufwerksbuchstabe des Transfer-Datenträgers>
cd < Transfer-Verzeichnis>

rem Export des CA-Zertifikats
certutil -ca.cert <Common Name (CN) der Root-CA>.cer

rem Neuerstellung einer CRL
certutil -CRL

rem Export der neu erstellten CRL
certutil -GetCRL <Common Name (CN) der Root-CA>.crl

:end
```

A.2 Konfigurationsdateien für die Issuing-CA

A.2.1 Vor der Installation: capolicy.inf

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

[Extensions]
2.5.29.15=AwIBBg==
critical=2.5.29.15
```

A.2.2 Nach der Installation: caconfig.cmd

```
@echo off
rem ########################################################################
rem
rem Skript zur Konfiguration einer Microsoft CA
rem
rem Copyright (c) 2009 Secorvo Security Consulting GmbH
rem
rem ########################################################################

rem ### Certtificate Services beenden
net stop certsvc

rem ### Audit-Events
certutil -setreg CA\AuditFilter 127

rem ### Maximale Gueltigkeisdauer für Zertifikate
rem ### (kann ggf. durch Template herabgesetzt werden)
certutil -setreg CA\ValidityPeriod Years
certutil -setreg CA\ValidityPeriodUnits <Lebensdauer der PKI in Jahren>

rem ### Parameter für Verlängerung von Zertifikaten
certutil -setreg CA\RenewalKeyLength 2048
certutil -setreg CA\RenewalValidityPeriod Years
certutil -setreg CA\ValidityPeriodUnits <Lebensdauer der PKI in Jahren>

rem ### Sperrlistenintervall und (davon) Karenzzeit
certutil -setreg CA\CRLPeriod Hours
certutil -setreg CA\CRLPeriodUnits <Gültigkeitszeitraum der CRL in Stunden (inkl. Karenzzeit)>
certutil -setreg CA\CRLOverlapPeriod Hours
certutil -setreg CA\CRLOverlapUnits <Karenzzeit der CRL-Gültigkeit in Stunden >

rem ### Keine Deltasperrlisten verwenden
certutil -setreg CA\CRLDeltaPeriodUnits 0

rem ### CRL Distribution Points
certutil -setreg CA\CRLPublicationURLs
"1:C:\Windows\System32\CertSrv\CertEnroll\<Common Name (CN) der Issuing-
CA>.crl\n11:ldap:///CN=<Common Name (CN) der Root-CA>,CN=<Servername der Issuing-
CA>,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=<Domämenname der
Root-Domäne des AD in einzelnen
Komponenten>?CertificateRevocationList?base?ObjectClass=cRLDistributionPoint\n2:http
://<DNS Alias (CNAME) des Servers der Issuing-CA>/CertEnroll/<Common Name (CN) der Issuing-
CA>.crl"

rem ### Authority Information Access
certutil -setreg CA\CACertPublicationURLs
"1:C:\Windows\System32\CertSrv\CertEnroll\<Common Name (CN) der Issuing-
CA>.cer\n2:ldap:///CN=<Common Name (CN) der Issuing-CA>,CN=AIA,CN=Public Key
Services,CN=Services,CN=Configuration,DC=<Domämenname der Root-Domäne des AD in einzelnen
Komponenten>?cACertificate?base?ObjectClass=certificationAuthority\n2:http://<DNS
Alias (CNAME) des Servers der Issuing-CA>/CertEnroll/<Common Name (CN) der Issuing-CA>.cer"

rem ### KeyUsage Zertifikatserweiterung nach RFC Vorgabe
certutil -setreg policy\EditFlags -EDITF_ADDOLDKEYUSAGE

rem ### Unterdruecken von State und Locality DN-Attributen
rem ### aus Zertifikatsantraegen
certutil -setreg CA\SubjectTemplate
"EMail\nCommonName\nOrganizationalUnit\nOrganization\nDomainComponent\nCountry"
```

```
rem ### Uebernahme von unerwuenschten Zertifikatserweiterungen
rem ### aus dem Request unterdruechen
certutil -setreg policy\EnableEnrolleeRequestExtensionList ""
certutil -setreg policy\EnableRequestExtensionList ""

rem ### Ggf. Netscape Zertifikatstyp Erweiterung aus dem Request uebernehmen
certutil -setreg policy\EnableRequestExtensionList +2.16.840.1.113730.1.1

:end
```

A.2.3 Import von Root-CA-Zertifikat und -CRL: import_ca_crl.cmd

Das folgende Skript ist von einem Enterprise Administrator auf einem am AD angeschlossenen Server oder einer Workstation mit installiertem AdminPak aufzurufen. Es importiert das CA-Zertifikat und die CRL von einem angeschlossenen Transfer-Datenträger (bspw. USB-Stick) in das AD.

Im Regelbetrieb der Installation der Issuing-CA können die beiden auskommentierten `Copy` Anweisungen aktiviert und das Skript von einem Enterprise Administrator auf dem Server der Issuing-CA aufgerufen werden. Damit werden dann CA-Zertifikat und CRL zugleich in das Verzeichnis kopiert, über das sie per HTTP publiziert werden.

```
@echo off

<Laufwerksbuchstabe des Transfer-Datenträgers>
cd < Transfer-Verzeichnis>

rem Import des CA-Zertifikats
certutil -f -dspublish <Common Name (CN) der Root-CA>.cer
rem copy /Y <Common Name (CN) der Root-CA>.cer %SystemRoot%\System32\CertSrv\CertEnroll

rem Import der neu erstellten CRL
certutil -f -dspublish <Common Name (CN) der Root-CA>.crl
rem copy /Y <Common Name (CN) der Root-CA>.crl %SystemRoot%\System32\CertSrv\CertEnroll

:end
```

Anhang B Beispiel eines Zertifizierungsantrags

Die folgende Datei ist ein Beispiel eines PKCS#10 CSR in Base64-Kodierung in der Form, die von der Mehrzahl der gängigen SSL/TLS-Serversoftware erstellt wird.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEoTCCA4kCAQAwgZIxCzAJBgNVBAYTAkRFMQ4wDAYDVQQIDAVCYWRlbjESMBAG
A1UEBwwJS2FybHNydWhlMSkwJwYDVQQKDCBTZWNvcnZvIFNlY3VyaXR5IENvbnN1
bHRpbmcgR21iSDEUMBIGA1UECwwLV2hpdGUgUGFwZXIxHjAcBgNVBAMMFXdoaXRl
cGFwZXIuc2Vjb3J2by5kZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMeyXF1C4VNzBFAd+/69v8TDwdM04lq6bJ8siAeP1oITT2qBwqyTCjN2kC+O9Rxk
TsY0Em65WwknBN2+f0fMKpdBzZTwf1iFz3pjxedn4ms9B3pdI0MnDdBFxXPX+nJX
PYgkKlPunc6gUA9vNZ5s95gKjhEUwFc/mRODlwjkXt8AoAQKKdQCAsycraHL37Wt
yjJV6diumGzfoSX1fhdLs/ec8dsBLcn26WxtLobeqOYxe52oE9ozeJnsuaWh/7sK
krXYiJt0rLFd+NhoMkC5PNwXqAxlWEpCZe+s63tq9OK7K6HGCqNkMr7mjfalWPSW
XklPcEfAWwrwtGiFAfZQ9xMCAwEAAaCCAccwGgYKKwYBBAGCNw0CAzEMFgo2LjAu
NjAwMi4yMGMGCSsGAQQBgjcVFDFWMFQCAQUMJ2tpdHRhMDAzLmNvbGxlZ2UtcGtp
LnRlc3RsYWIuc2Vjb3J2by5kZQwZQ09MTEVHRS1QS0lcYWRtaW5pc3RyYXRvcgwL
SW5ldE1nci5leGUwcgYKKwYBBAGCNw0CAjFkMGICAQEeWgBNAGkAYwByAG8AcwBv
AGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwBy
AGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgMBADCBzwYJKoZIhvcNAQkOMYHB
MIG+MA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggrBgEFBQcDATB4BgkqhkiG
9w0BCQ8EazBpMA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwCwYJYIZI
AWUDBAEqMAsGCWCGSAFlAwQBLTALBglghkgBZQMEAQIwCwYJYIZIAWUDBAEFMAcG
BSsOAwIHMAoGCCqGSIb3DQMHMB0GA1UdDgQWBBQgMvXNPE/yAy+0sbsaelwnHdUd
KTANBgkqhkiG9w0BAQUFAAOCAQEAdwIbUdwqs9aSkDpsOywGhzHAAoMse2NIKPxH
yJ5bkBEflq6hh8i7FA29ApceLfaJz0LE8Ko6z5QGyDcIS9u5MCPE2HEQQt8HLy52
avfv1i4rLwtUsiKChOcdtmfdVXDlku4ZS/6XDqE+a50IaKdip7BDkF+GF57AO7Pp
IzI3HeGwGV+ugNSdldqhkM5ew2XJlQkVJwott7gdlCDuLPDcOHUombTrpcsyXKqj
/o5c6cVENAXNwM/3u5ixflg2hMaQ0z3sPKwdOP23kk7RkCPntpRVdZuY9QadL0AF
Z5wcjtjnTlDE+CCkjCJrU3+MvHr9uXhPBZoYFbTcV8Bq7TxS4A==
-----END NEW CERTIFICATE REQUEST-----
```

Anhang C Literatur

[BaK_08] P Barzin, S. Kelm: *Das Policy-Rahmenwerk einer PKI: Certificate Policy, Certification Practice Statement, PKI Disclosure Statement*, Secorvo White Paper, WP15, Version 1.1, 27.03.2008, http://www.secorvo.de/publikationen/secorvo-wp15.pdf

[Bar_11] P Barzin: Public *Key Infrastrukturen – Vertrauensmodelle und PKI Komponenten*, Secorvo White Paper, WP16, Version 1.0, 01.03.2011, http://www.secorvo.de/publikationen/secorvo-wp16.pdf

[CoPKI_09] T7 e.V. und TeleTrusT e.V.: Common PKI Specifications for Interiotable Applications, Version 2.0, 20.02.2009, http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf

[Kom_04] B. Komar: *Microsoft Windows Server 2003 PKI and Certificate Security*, Microsoft Press, 2004

[Kom_08] B. Komar: *Windows Server 2008 PKI and Certificate Security*, Microsoft Press, 2008

[Mack_03] H. Mack: PKI-*Unterstützung in Windows 2000 und Windows 2003 Server*, Secorvo White Paper, WP08, Version 2.01, 08.05.2003, http://www.secorvo.de/publikationen/secorvo-wp08.pdf

[NIST_07] National Institute of Standards and Technology (NIST): Recommendation for Key Management – Part 1: General. Special Publication SP 800-57, März 2007 http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

[RFC_5246] T. Dierks, E. Rescorla: *RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2*, August 2008, http://www.rfc-editor.org/rfc/rfc5264.txt

[RFC_5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk: *RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Mai 2008, http://www.rfc-editor.org/rfc/rfc5280.txt