Root CA Zertifikatswechsel

Secorvo White Paper

Version 1.0
Stand 30.September 2002

Ingmar Camphausen, Dr. Holger Petersen, Claus Stark

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

E-Mail info@secorvo.de
Internet http://www.secorvo.de

Inhaltsübersicht

Abkürzungen

CA	Certification Authority
CD	Compact Disc
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
DNSSEC	Domain Name Service Security
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Internet X.509 Public Key Infrastructure
PSE	Personal Security Environment
WoT	Web of Trust
WPKI	Wireless PKI
X.509	ITU-T Recommendation X.509 [ITUT00]

1 Zusammenfassung

Die flächendeckende Einführung von Public-Key-Infrastrukturen (PKI) im Unternehmensbereich, in den öffentlichen Behörden sowie über den Betrieb von Trustcentern für den breiten Massenmarkt schreitet voran. Dabei entstehen in der Regel hierarchisch strukturierte PKIs, bei denen die Gültigkeitsprüfung der Zertifikate von der Gültigkeit des Root CA-Zertifikats abhängt. Sofern dieses Zertifikat ausläuft, sich sein Inhalt ändert oder es gesperrt werden muss, besteht das Problem, ein neues Root-Zertifikat auszustellen und authentisch an die Teilnehmer der PKI zu verteilen, ohne dass dabei der Wirkbetrieb beeinträchtigt wird. Viele derzeit eingesetzte Lösungen sparen die Probleme, die sich aus dem Wechsel des Root CA-Zertifikats ergeben, aus, meist verbunden mit der Hoffnung, dass das Problem technisch gelöst sein werde, bevor es „in einigen Jahren“ auftritt. Damit gibt es oft auch keinen wirksamen Notfallplan für den Fall, dass ein vorzeitiger Zertifikatswechsel, z.B. aufgrund einer Schlüsselkompromittierung, notwendig wird.

Dieses Whitepaper, das auf einem Beitrag für die Konferenz „Enterprise Security“ im März 2002 in Paderborn basiert [CaPeSt02] und dieses in einigen Punkten erweitert, diskutiert die zahlreichen Gründe, die zum Zertifikatswechsel der Root CA führen können, benennt einige der damit verbundenen organisatorischen und technischen Probleme und diskutiert und bewertet mögliche Lösungsansätze.

2 Motivation

Der Zertifikatswechsel einer Root CA ist erforderlich, wenn sich Daten oder Attribute, die Bestandteil des Root-Zertifikats sind, ändern oder ungültig werden (semantisch oder syntaktisch) oder der zum Zertifikat gehörende private Schlüssel nicht mehr verfügbar ist oder kompromittiert wurde. Im letzten Fall ist der Zertifikatswechsel der Root CA immer von einem Schlüsselwechsel begleitet. Ferner kann der Zertifikatswechsel aus organisatorischen Gründen planmäßig erforderlich werden. Zusammenfassend lassen sich folgende Gründe für einen Zertifikatswechsel der Root CA benennen:

- *Kompromittierung des privaten Schlüssels* der Root CA, z.B. durch Diebstahl oder unbefugten Zugang zum privaten Schlüssel (beispielsweise durch Entwenden einer Hardware-PSE[1] oder „Hacken“ der Software-PSE), sei es dauerhaft oder temporär oder aufgrund von Schwächen des mathematischen Problems, auf dem die Sicherheit des privaten Schlüssels beruht,
- *Kompromittierung des Signaturverfahrens*, mit dem das Root CA-Zertifikat signiert wurde; z.B. durch Schwächen der kryptographischen Algorithmen (Hash- oder Signaturverfahren) oder mittlerweile ungeeignete Schlüssellängen,
- *Verlust* des privaten Schlüssels der Root CA oder der zugehörigen PIN,
- *semantische Änderungen oder Erneuerung des Zertifikatsinhaltes*, z.B. aufgrund Ablaufs der Gültigkeitsdauer, Änderung von Zertifikats-Erweiterungen (Extensions) wie etwa Änderung des zulässigen Verwendungszwecks (**keyUsage**), der Rolle der CA oder der Poli-

[1] PSE = Personal Security Environment

cy, unter der das Zertifikat ausgestellt wurde[2], oder Änderung des Root CA-Namens (z.B. bei Umstrukturierungen oder Firmenübernahmen),

- *syntaktische Änderungen* am Zertifikatsformat, z.B. durch Umstellung auf eine andere Zeichencodierung im Distinguished Name (z.B. Wechsel zu Unicode im Rahmen der Internationalisierung),
- *Organisatorische Gründe,* wie z.B. Wechsel des Zertifizierungsdiensteanbieters oder vorfristigen CA-Schlüsselwechsel als „Sperrlistenersatz“, falls keine Sperrung von nachgeordneten Zertifikaten möglich ist, z.B. [WPKI00, RFC2541].

Zertifikate nach X.509 [ITUT00] werden in der Regel nur mit einer zeitlich beschränkten Gültigkeit ausgestellt, um den oben genannten Wechselgründen durch einen durch Zeitablauf bedingten Zertifikatswechsel begegnen zu können und nicht bei jedem Zertifikatswechsel einen permanenten Eintrag in eine Sperrliste (CRL) zu erzwingen. Damit lässt sich im Falle einer Sperrung ein Zeitpunkt ermitteln, ab dem das Zertifikat aus der Sperrliste gelöscht werden kann, sofern es nicht z.B. aus rechtlichen Gründen für einen bestimmten, längeren Zeitraum aufbewahrt werden muss.

Abbildung 1 verdeutlicht wesentliche Bestandteile eines Public-Key-Zertifikats nach X.509 [ITUT00] und zeigt Gründe auf, die zum Zertifikatswechsel führen können (*kursiv*). Die gestrichelten Linien zeigen Elemente, die nur indirekt mit dem Zertifikat in Zusammenhang stehen. Hierzu gehören die Policy, unter der ein Zertifikat ausgestellt wird (und die etwa als Attribut im Zertifikat auftauchen kann), sowie der private Schlüssel, der in einer mathematischen Relation zum öffentlichen Schlüssel steht, aber nicht selbst Bestandteil des Zertifikates ist.

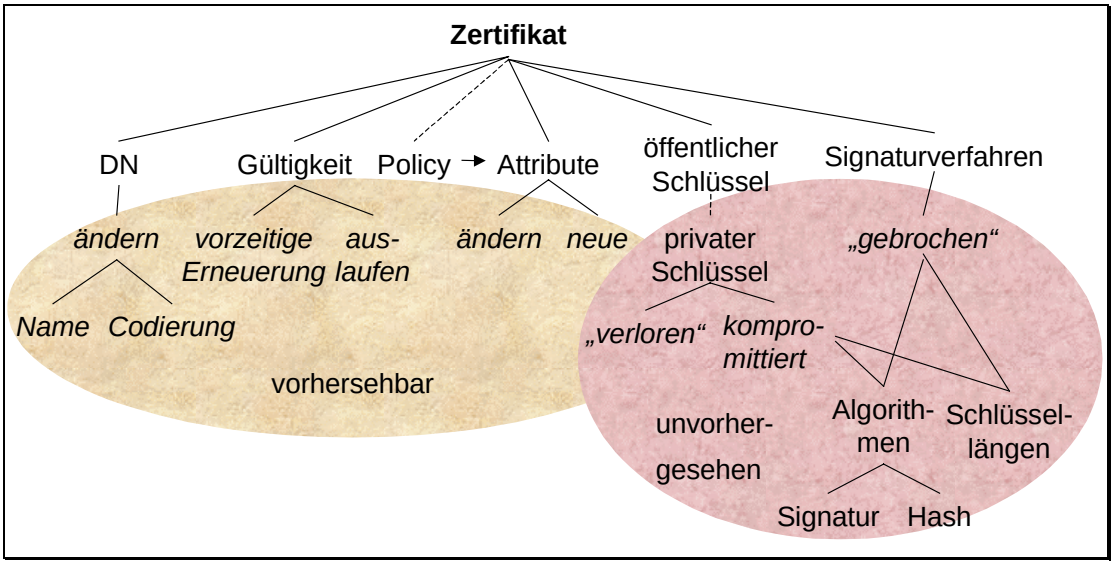

Abb. 1: Zertifikatsbestandteile und Gründe für ihre Änderung

[2] Um die Probleme beim Wechsel der Policy zu vermeiden, werden Root CA-Zertifikate in der Praxis meist ohne Policy-Erweiterung ausgestellt. Die Policy wird erst bei der Ausstellung der Level 1 CA-Zertifikate oder den Endbenutzer-Zertifikaten durch eine entsprechende Zertifikatserweiterung in das Zertifikat eingebracht.

Das wesentliche Problem beim Zertifikatswechsel der Root-CA ist die authentische Verteilung des neuen Sicherungsankers an die Teilnehmer. Dieses Problem tritt bereits bei der initialen Verteilung des Root CA-Schlüssels auf und wird im folgenden näher beleuchtet.

Wie wird die authentische Verteilung des Root CA-Zertifikats initial gelöst?

Der Nutzer einer PKI erhält das Zertifikat der Root CA bzw. dessen Fingerprint im Rahmen seiner (persönlichen) Registrierung und Ausstellung seines Teilnehmerzertifikats üblicherweise mit ausgehändigt, z.B. mit seiner Software- oder Hardware-PSE. Teilweise ist das Root CA-Zertifikat bereits fest in der Anwendungssoftware integriert und wird zusammen mit ihr ausgeliefert und installiert.

Durch die persönliche Übergabe des Zertifikats oder des Fingerprints im Rahmen der Nutzerregistrierung oder aber durch gesicherten Transport auf einem geeigneten Medium (Floppy, Chipkarte, CD) zum Nutzer wird die Authentizität des Root CA-Zertifikats sichergestellt. Da der persönliche Kontakt bzw. die gesicherte Übertragung oder das Ausrollen des Zertifikats im Rahmen einer Software-Installation mit hohem personellen, organisatorischen und zeitlichen Aufwand für die Teilnehmer verbunden ist, ist man bestrebt, diesen Vorgang so selten wie möglich (d.h. idealerweise nie) wiederholen zu müssen.

Welche Probleme sind beim Zertifikatswechsel der Root CA zu lösen ?

Es stellt sich das Problem, wie man dem Nutzer bei einem Zertifikatswechsel der Root CA das Zertifikat bzw. dessen Fingerprint möglichst automatisiert und ohne aufwendige Nutzerinteraktion authentisch bereitstellen kann. Die Bereitstellung umfasst die Verteilung des Zertifikats, die Prüfung seiner Authentizität und die Installation in den PKI-nutzenden Anwendungen. Sie sollte ohne Störungen bei der Handhabung der Anwendungen weitgehend transparent für den Nutzer (mit Ausnahme der möglichst expliziten Authentizitätsprüfung) durchführbar sein und ausgeführt werden können, ohne dass der Nutzer hierfür speziell geschult werden oder intensiven IT-Support in Anspruch nehmen müsste.

Sobald der aktuelle Vertrauensanker nicht mehr verfügbar oder durch Zeitablauf oder Widerruf nicht mehr gültig ist, kann er nicht mehr zur authentischen Bereitstellung eines neuen Vertrauensankers verwendet werden. (Im Notfall-Konzept sind für diese Situationen entsprechend geeignete Reaktionen vorzusehen.) Daher ist in dieser Situation der gleiche Aufwand wie bei der initialen Bereitstellung zu betreiben, sofern die Client- und PKI-Core-Software nicht alternative Bereitstellungsmechanismen unterstützt. Letzteres ist heutzutage meist nicht gegeben, da diese Probleme und der damit verbundene Aufwand bisher (zu) wenig beachtet wurden. Damit ist oft ein vollständiges Ausrollen (Verteilung und Installation) des neuen Root CA-Zertifikats oder von neuer Client-Software erforderlich. Dies ist in einer geschlossenen Umgebung – wenn auch mit entsprechendem Aufwand – möglich; in einer *offenen* PKI, bei der die Teilnehmer nicht der direkten Kontrolle der PKI unterliegen, gestaltet sich das Ausrollen jedoch erheblich schwieriger, zumal die Teilnehmer eventuell gar keine Software des PKI-Betreibers installiert haben. Hinsichtlich dieses Punktes unterscheiden sich die vorgestellten Lösungsansätze erheblich in ihrer Anwendbarkeit.

Ist ein Zertifikatswechsel der Root-CA aufgrund einer Kompromittierung des Root-CA-Schlüssels oder eines der zugrundeliegenden mathematischen Verfahren erforderlich, so kann der kompromittierte Schlüssel trotzdem noch zur Sperrung des zugehörigen Root-Zertifikats benutzt werden. Wird der Root-Schlüssel hingegen durch Zeitablauf ungültig oder ist er durch Verlust nicht mehr verfügbar, so besteht diese Möglichkeit nicht.

Sofern der Nutzer zur Zertifikatsübergabe persönlich erscheinen muss oder neue Software installiert werden muss, ist ein hoher **organisatorischer und administrativer Aufwand** für

die authentische Verteilung eines neuen Root CA-Zertifikats erforderlich. Dieser reduziert sich etwas, sofern der Nutzer das Zertifikat elektronisch übermittelt bekommt, z.B. per E-Mail oder per Download von einem Web-Server. In diesem Fall muss allerdings die Überprüfung der Authentizität des Zertifikats sowie dessen Bereitstellung für die Client-Software gelöst werden. Idealerweise würde die Authentizität des Zertifikats von der Software automatisch ohne Nutzerinteraktion überprüft, da dann der organisatorische Aufwand sehr gering wäre.

Ferner sind **technische Probleme** zu bewältigen, sofern die Client-Software während einer Übergangsphase parallel sowohl auf das alte wie auch das neue Root CA-Zertifikat als Vertrauensanker zugreifen können soll, z.B. während eines geplanten Zertifikatswechsels, bei dem der laufende Betrieb der CA nicht beeinträchtigt werden soll. Dieses Problem verschärft sich, sofern für die Root CA mehrere Zertifikate unter gleichem Namen ausgestellt werden, da dieses zu Beeinträchtigungen der Prüffunktion führen kann, sofern diese den Namen des Ausstellers zur Verknüpfung der Zertifikate benutzt.

Oft kann auch die **Ausstellung** eines neuen **Root CA-Schlüssels** selbst bereits ein erhebliches Problem darstellen, wenn dieser Schlüssel unter entsprechenden Hochsicherheitsanforderungen generiert, installiert und archiviert werden soll. So kann es sein, dass zur Schlüsselerzeugung mehrere Security Officer an einem speziell gesicherten Ort (z.B. Hochsicherheitstrakt) zusammenkommen müssen, um gemeinsam die Schlüsselerzeugung durchzuführen – etwa mit einem Split-Knowledge-Verfahren zur Durchsetzung des Mehr-Augen-Prinzips (auch *Key Signing Ceremony* genannt). Im Fall einer Schlüsselkompromittierung müssen alle diese Personen kurzfristig verfügbar sein. Um hier die Koordinierung zu vereinfachen, wäre es vorteilhaft, wenn der Wechsel rechtzeitig vorbereitet werden kann.

In Kapitel 4 werden verschiedene Lösungsansätze vorgestellt und beschrieben, wie ein Wechsel des Root CA-Zertifikates durchgeführt werden kann. Die oben geschilderten Probleme infolge eines Root-Zertifikatswechsels werden in Kapitel 5 näher untersucht, und es wird aufgezeigt, inwieweit die in Kapitel 4 vorgestellten Lösungsansätze diese Probleme jeweils zu lösen vermögen.

3 Grundlagen

Dieses Kapitel beschreibt Grundlagen der X.509-Zertifikate sowie des hierarchischen Vertrauensmodells. Ferner werden alternative Gültigkeitsmodelle und Möglichkeiten zur Definition einer Verknüpfungsrelation aufgezeigt.

3.1 Zertifikate nach X.509

Wesentliche Bestandteile eines Zertifikats nach X.509 [ITUT00] sind

```
Certificate                          ::=   SIGNED { SEQUENCE {
  version                      [0]   Version DEFAULT v1,
  serialNumber                       CertificateSerialNumber,
  signature                          AlgorithmIdentifier,
  issuer                             Name,
  validity                           Validity,
  subject                            Name,
  subjectPublicKeyInfo               SubjectPublicKeyInfo,
  issuerUniqueIdentifier       [1]   IMPLICIT UniqueIdentifier OPTIONAL,
                                     -- if present, version must be v2 or v3
  subjectUniqueIdentifier      [2]   IMPLICIT UniqueIdentifier OPTIONAL,
                                     -- if present, version must be v2 or v3
```

```
extensions              [3]   Extensions OPTIONAL
                              -- If present, version must be v3 -- } }
```

Veränderungen (Hinzufügen, Löschen oder Modifizieren) oder Ungültigwerden eines oder mehrerer dieser Bestandteile erfordert die Ausstellung eines neuen Zertifikats.

Als Zertifikats-Erweiterungen sind folgende sieben Standard-Erweiterungen nach X.509 vorgesehen:

a) *Key usage*; kann im Laufe der Umstrukturierung einer PKI geändert werden, einzelne Anwendungszwecke (z.B. Verschlüsselung) können nachträglich gelöscht oder hinzugefügt werden.

b) *Extended key usage*; kann anwendungsspezifische Nutzungszwecke enthalten, die sich im Laufe der Zeit ändern oder ergänzt werden müssen.

c) *Private key usage period*; Gültigkeitszeitraum für die Verwendung des privaten Schlüssels, läuft entweder früher oder spätestens zusammen mit der Zertifikatsgültigkeit aus und führt zu einer Neuausstellung des Zertifikats, sofern mit dem privaten Schlüssel noch kryptographische Operationen (insbesondere Zertifizierungen anderer Schlüssel) vorgenommen werden sollen.

d) *Certificate policies*; können sich im Laufe der Zeit ändern, z.B. durch Einführung neuer Vertrauensstufen (trust level) oder nach erfolgter Cross-Zertifizierung.

e) *Policy mappings*; können sich nach Cross-Zertifizierung der Root CA mit einer anderen CA ändern bzw. müssen dann u.U. neu definiert werden.

f) *Authority key identifier*; dient als eindeutige Referenz auf den Schlüssel der ausstellenden CA, sofern diese nicht bereits am Issuer DN eindeutig erkannt werden kann. Kann zur technischen Lösung der parallelen Gültigkeit zweier Root CA Zertifikate als Unterscheidungsmerkmal herangezogen werden.

```
AuthorityKeyIdentifier ::= SEQUENCE {
  keyIdentifier             [0] KeyIdentifier             OPTIONAL,
  authorityCertIssuer       [1] GeneralNames              OPTIONAL,
  authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL }
  ( WITH COMPONENTS         {..., authorityCertIssuer     PRESENT,
                                  authorityCertSerialNumber PRESENT} |
   WITH COMPONENTS          {..., authorityCertIssuer     ABSENT,
                                  authorityCertSerialNumber ABSENT} )
```

g) *Subject key identifier*; eindeutige Referenz auf den privaten Schlüssel der zertifizierten Instanz (subject), sofern der Subject DN nicht bereits eindeutig ist. Im Falle eines selbstsignierten Root CA-Zertifikats ist Subject DN = Issuer DN.

3.2 Hierarchisches Vertrauensmodell

Zertifikate können nach dem X.509-Standard [ITUT00] hierarchisch ausgestellt werden. Zunächst stellt eine Wurzel-Zertifizierungsinstanz Zertifikate für nachgeordnete Zertifizierungsstellen aus, die dann ihrerseits wiederum weitere Zertifizierungsstellen zertifizieren können oder Teilnehmerzertifikate ausstellen. Bei der Prüfung des Teilnehmerzertifikats werden die Zertifikate der Zertifizierungsstellen bis hin zur Wurzel-Zertifizierungsinstanz einbezogen, wobei lediglich der Wurzel-Instanz explizit vertraut werden muss und das Vertrauen in die dazwischenliegenden Instanzen implizit durch erfolgreiche Prüfung der Zertifikatkette etabliert wird.

3.3 Verteiltes Vertrauensmodell (Web-of-Trust)

Ein alternatives Vertrauensmodell ist das Web-of-Trust, dessen bekanntestes Anwendungsbeispiel das Verschlüsselungsprogramm „Pretty Good Privacy“ (PGP) ist. Dabei entscheidet jeder Nutzer individuell, welchen anderen Nutzern (d.h. an der Zertifizierungsstruktur Beteiligten) er vertraut. Dies können natürliche Personen, aber auch Institutionen sein. Öffentliche Schlüssel, die von für ihn vertrauenswürdigen Teilnehmern signiert bzw. zertifiziert wurden, betrachtet der Teilnehmer in diesem Vertrauensmodell ohne weitere Kontrollen als authentisch.

Im Web-of-Trust (WoT)-Ansatz findet keine Über- bzw. Unterordnung zwischen Teilnehmern statt: Ein Teilnehmer (bzw. sein Schlüssel) kann von anderen Teilnehmern zertifiziert werden und gleichzeitig selbst Schlüssel anderer Teilnehmer zertifizieren. Teilnehmer können ihre Schlüssel gegenseitig zertifizieren. Das resultierende Zertifizierungs„netz“ ist dadurch im Normalfall weniger strikt strukturiert und nicht notwendigerweise vollständig verbunden wie bei einem hierarchischen Vertrauensmodell.

Verschiedene Nutzer können in diesem Modell völlig unterschiedliche Teilnehmer als vertrauenswürdig und insofern als „Vertrauenanker“ oder individuelle Wurzel-„Instanz“ betrachten; es gibt nicht (bzw. nicht in jedem Fall) eine einzelne, exponierte Vertrauensinstanz für alle Teilnehmer. Ein Teilnehmer kann im Unterschied zu hierarchischen Ansätzen auch *mehrere* andere Teilnehmer des Web-of-Trust für sich als Vertrauensstellen ansehen. Anders als im streng hierarchischen Vertrauensmodell kann es im Web-of-Trust mehrere Vertrauenspfade (Zertifikatketten) von Vertrauensankern zu ein- und demselben Teilnehmerschlüssel geben. Damit tritt das Problem des Zertifikatswechsels „der“ Root CA in diesem Modell nicht in der Form auf wie in hierarchischen Vertrauens- oder Zertifizierungsmodellen.

Das Vertrauensmodell des Web-of-Trust wird in Kapitel 5 mit den Lösungsansätzen für das hierarchische Modell verglichen.

3.4 Gültigkeitsmodell Zertifikatsprüfung

Zur technischen Gültigkeitsprüfung[3] eines Teilnehmerzertifikats muss neben der Prüfung der digitalen Signatur des Zertifikats auch das übergeordnete Zertifikat der ausstellenden Zertifizierungsinstanz geprüft werden. Diese Prüfung wird rekursiv fortgesetzt bis zur Prüfung des Zertifikats der Wurzel-Instanz. Das Root CA-Zertifikat bildet den Sicherungsanker, es muss dazu in authentischer Form vorliegen. Die Verteilung und Nutzung des authentischen Root CA-Zertifikats ist daher *essentiell* für die korrekte Zertifikatsprüfung.

Das Prüfergebnis hängt vom gewählten *Gültigkeitsmodell* sowie von der Bestimmung der Zertifikatkette auf dem Zertifizierungspfad, d.h. der gewählten *Verknüpfungsrelation* zwischen den Zertifikaten ab. Je nach gewähltem Modell können sich unterschiedliche Prüfergebnisse ergeben. In diesem Whitepaper wird ausschließlich die Gültigkeitsprüfung in der Gegenwart betrachtet, nicht die Prüfung eines in der Vergangenheit liegenden Zertifizierungszeitpunktes, der z.B. mittels eines Zeitstempels bestätigt wurde.

[3] zu allgemeinen Prüfbedingungen siehe [ITUT00], [RFC2459], den Draft des Nachfolger-RFCs [PKIX01] und [BSI 00]

3.4.1 Kettenmodell

Unter der Gültigkeitsregel des *Kettenmodells*[4] ist eine Zertifikatkette technisch gültig, wenn unter anderem jedes Zertifikat der Kette innerhalb des Gültigkeitszeitraums des jeweiligen übergeordneten Zertifikats ausgestellt wurde [BSI 00].

3.4.2 Schalenmodell

Unter der Gültigkeitsregel des *Schalenmodells*[5] ist eine Zertifikatkette technisch gültig, wenn unter anderem jedes Zertifikat der Kette vom Gültigkeitszeitraum des übergeordneten Zertifikats vollständig eingeschlossen wird.

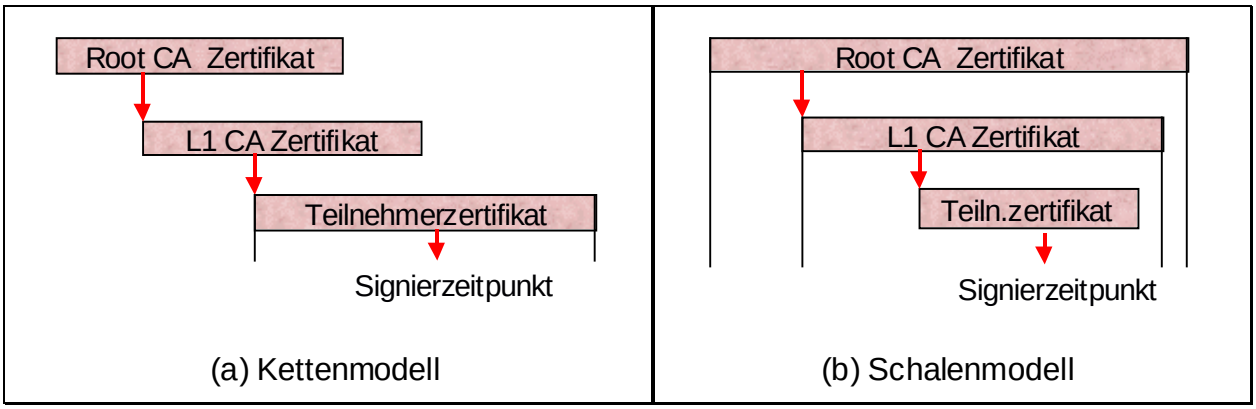

Abb. 2: Gültigkeitsmodelle zur Zertifikatsprüfung

3.4.3 Verknüpfungsrelation

Zur Gültigkeitsprüfung eines Zertifikats ist neben seiner technischen Gültigkeit ebenfalls die gesamte Zertifikatkette bis zum Vertrauensanker, dem Root CA-Zertifikat, zu prüfen. Dabei können unterschiedliche Relationen zur Bestimmung des jeweils übergeordneten Zertifikats benutzt werden [Hamm99]:

- Die **Zertifizierungsinstanz-Relation**: „Issuer zertifiziert Subject“. Die in der Menge der Zertifikate enthaltenen Paare (issuer, subject) bestimmen einen Graphen. Dieser Relation liegt in der Regel die Vorstellung der rechtlich-organisatorischen Zuständigkeiten zugrunde.
- Die **Zertifizierungsrelation**: „Schlüssel **X** wird zum Prüfen des Zertifikats **Y** benötigt“. Die Struktur des entsprechenden Graphen folgt dem Graphen der Zertifizierungsinstanz-Relation, die Relation ist aber präziser, da sie den jeweils vom Aussteller beim Signieren verwendeten *Schlüssel* referenziert und nicht bloß den Aussteller(namen). Technisch kann diese Relation über den **Authority Key Identifier** hergestellt werden.

[4] auch „Zertifikat-Gültigkeit“-Regel genannt [BSI 00]

[5] auch „Zertifizierungspfad-Gültigkeit“-Regel genannt [BSI 00]

4 Lösungsansätze

Als „Störung“ werden im folgenden vorhersehbare und unvorhersehbare Ereignisse wie der Ablauf der Gültigkeit, Schlüsselverlust oder -kompromittierung sowie die Zertifikatskompromittierung bezeichnet.

Die nachfolgende Tabelle gibt einen Überblick, unter welchen Voraussetzungen die vorgestellten Lösungsansätze geeignet sind, einen Zertifikatswechsel der Root CA unter Aufrechterhaltung des Wirkbetriebs der PKI zu ermöglichen.

Anwendbarkeit des Lösungsansatzes / **Lösungsansatz**	Neue PKI aufsetzen	über Produktzyklus	Reservezertifikat	Mehrere Vertrauensanker	Verlängerung Root CA	Lange Gültigkeitsdauer	Cross-Zertifikat	Web-of-Trust
• vor Ablauf des Root CA-Zertifikats	+	+	+	+	+	+	+	+
• nach Ablauf des Root CA-Zertifikats	o	o	+	+	o		(+)[6]	+
• nach Verlust des Root CA privaten Schlüssels	o	o	+	+[7]				o
• nach Kompromittierung des privaten Schlüssels	-	-	+	+[7]				-
• nach Kompromittierung des Signaturverfahrens	-	-	o	+[8]				

Tabelle 1: Eignung der Lösungsansätze
(Eignung: +: gut, o: mittelmäßig, -: schlecht, leer: ungeeignet)

4.1 Neue PKI aufsetzen

Bei diesem Ansatz wird bei Eintritt einer Störung die PKI neu aufgesetzt, d.h. alle Abläufe mit Ausnahme der Nutzerregistrierung müssen erneut stattfinden (Ausstellung des Root CA-Zertifikats, Zertifizierung nachgeordneter CAs und von Teilnehmerzertifikaten, authentische Verteilung der Zertifikate). Diese Lösung verursacht einen ähnlich hohen Aufwand wie das initiale Ausrollen der PKI-Infrastruktur. Damit kann bei Eintritt einer unvorhergesehenen Störung (d.h. der Schlüsselkompromittierung oder des Schlüsselverlustes) nicht unmittelbar reagiert werden, und es ist damit zu rechnen, dass die Infrastruktur für einige Zeit nicht zur Verfügung stehen wird.

Ein Vorteil dieser Lösung besteht darin, dass sie nicht bereits im Vorfeld vorbereitet werden muss, d.h. dass sie auch nachträglich, nach Eintreten einer Störung, durchgeführt werden kann. Ferner erlaubt sie den Wechsel der Algorithmen und Schlüssellängen sowie Attributs- oder Policy-Änderungen, sofern dieses erforderlich ist.

[6] abhängig vom Gültigkeitsmodell und dem Erzeugungszeitpunkt der Cross-Zertifikate

[7] sofern hiervon nicht alle Vertrauensanker betroffen sind

[8] sofern diese unterschiedliche Verfahren und/oder Schlüssellängen verwenden

4.2 Zertifikatswechsel über Produktzyklus

Bei diesem Ansatz wird davon ausgegangen, dass die Zertifikate zusammen mit den Applikationen an die Nutzer verteilt werden bzw. bereits fest in diesen installiert sind. Die Gültigkeit des Root CA-Zertifikats wird so gewählt, dass der Software-Produktzyklus im allgemeinen kürzer als die Gültigkeitsdauer des Zertifikats ist, so dass durch Update oder Neuinstallation der Applikation das Zertifikat rechtzeitig mit ausgewechselt wird. Bei einer unvorhergesehenen Störung, bei dem ein Zertifikat revoziert werden muss, ist die Lösung nicht praktikabel. Hier ist damit zu rechnen, dass die Infrastruktur für einige Zeit ausfällt, da zunächst die Applikation neu ausgerollt werden muss, was in der Regel mit hohem organisatorischen Aufwand verbunden ist.

Die Applikation sollte nach dem Zertifikatswechsel in der Lage sein, zwei (oder ggf. mehrere) Vertrauensanker zu verwalten, da die Teilnehmerzertifikate nicht automatisch mit ausgetauscht werden. Somit müssen alte Teilnehmerzertifikate unter dem bisherigen Vertrauensanker geprüft werden können, während neu ausgestellte Teilnehmerzertifikate bereits das neue Root CA-Zertifikat zur Gültigkeitsprüfung voraussetzen.

Beispiel: Vorinstallierte Root-Zertifikate in Web-Browsern

4.3 Reservezertifikat vorbereiten

Dieser Ansatz basiert darauf, frühzeitig Reservezertifikate für andere Schlüsselpaare vorzubereiten und authentisch – bevorzugt beim initialen Rollout oder nachträglich unter Verwendung der aktuell gültigen Zertifikate – zu verteilen. Hierzu kann entweder der Hashwert des öffentlichen Reserveschlüssels bereits initial verteilt werden oder er kann Teil des aktuellen Zertifikats sein.

Sobald eine Störung auftritt, kann das aktuell gültige Root CA-Zertifikat widerrufen werden, und es kann auf das zuvor authentifizierte Reservezertifikat gewechselt werden (sofern nicht das Signaturverfahren kompromittiert wurde und das Reservezertifikat die gleichen Algorithmen und Schlüssellängen verwendet). Die Client-Software muss diesen Wechsel des Root CA-Zertifikats unterstützen und hierauf entsprechend vorbereitet sein.

Das Reservezertifikat sollte möglichst bereits vor dem Ausrollen der PKI vorbereitet werden, damit seine authentische Verteilung (z.B. über Einbettung des Hashwertes in das aktuelle Root CA-Zertifikat) effizient erfolgen kann. Wird es erst im laufenden Betrieb vor Eintritt der Störung ausgestellt, kann zwar auch das aktuelle Root CA-Zertifikat – ähnlich wie bei einer Cross-Zertifizierung – zur Authentizitätssicherung verwendet werden, die Client-Software muss jedoch das nachträgliche Einbringen des neuen Zertifikats unterstützen.

Das Verfahren eignet sich für eine automatisierte Einsatzumgebung, in der bei einer Störung automatisch auf ein neues Root CA-Zertifikat gewechselt wird. Die Verteilung, Authentizitätsprüfung und Installation des neuen Zertifikats kann hierbei transparent für den Nutzer erfolgen, sofern dieses gewünscht wird.

Beispiel: PKI-Assessment Guide der American Bar Association [ABA 01].

4.4 Mehrere Vertrauensanker

Dieser Ansatz basiert darauf, dass mehrere Vertrauensanker gleichzeitig parallel betrieben werden und ein Wegfall eines Vertrauensanker durch die verbliebenen übrigen Vertrauensanker (temporär) aufgefangen wird. Gegebenenfalls wird sogar die komplette PKI – bis hin zur mehrfachen Ausstellung von Schlüsseln und Zertifikaten für Endanwender – parallel vor-

gehalten. Es bietet sich für diesen Ansatz an, die parallelen PKI-Strukturen auf unterschiedlichen kryptographischen Verfahren aufzusetzen oder zumindest unterschiedliche Schlüssellängen zu wählen, um auf Angriffe auf Algorithmen reagieren zu können (der Ansatz FlexiPKI fokussiert auf diesen Aspekt, siehe [HaMa01]).

Eine PKI-Architektur nach diesem Ansatz wird idealerweise vor dem Ausrollen aufgebaut und in Betrieb genommen, um die multiplen Sicherungsanker „in einem Schritt" initial an die Teilnehmer zu verteilen. Nach einer Störung sind keine besonderen Maßnahmen zur Erzeugung und Verteilung neuer Sicherungsanker notwendig, wenn noch ausreichend Sicherungsanker verfügbar sind und diese nicht gleichzeitig kompromittiert wurden. (Das könnte beispielsweise geschehen, wenn die privaten Schlüssel für die verschiedenen verwendeten Verfahren auf derselben Hardware-PSE gespeichert waren und gleichzeitig entwendet wurden.) Die Verteilung, Authentizitätsprüfung und Installation des Zertifikats kann automatisch erfolgen, sofern die Applikationssoftware diese Prozesse unterstützt.

Es ist bei diesem Ansatz möglich, Root-CA Zertifikate mit überlappenden Gültigkeitszeiträumen auszustellen und diese beim initialen Ausrollen authentisch an die Teilnehmer zu verteilen. So kann beim Auslaufen eines Root CA-Zertifikats ein anderes, noch gültiges genutzt werden, um das abgelaufene auszutauschen und damit ein erneutes bzw. weiteres Ausrollen eines Root-Zertifikats zu vermeiden.

Eine Besonderheit dieser Lösung ist die Notwendigkeit für die Applikationen, mehrere Sicherungsanker mit gegebenenfalls unterschiedlichen kryptographischen Verfahren gleichzeitig verwalten und nutzen zu können. Dieses unterstützen die in der Praxis verfügbaren Lösungen heutzutage aber in der Regel noch nicht.

4.5 Verlängern des Root CA-Zertifikats

Bei diesem Ansatz wird ein Root CA-Zertifikat vor dem Ende seiner Gültigkeit rechtzeitig „verlängert" (d.h. es wird mit verändertem Gültigkeitszeitraum neu ausgestellt) und das verlängerte Zertifikat an die Teilnehmer verteilt. Die Inhalte eines Zertifikats sollten bei einer Verlängerung weitestgehend unverändert, bis auf die Gültigkeitsdauer und die Seriennummer, in das neue Zertifikat übernommen werden. Die Authentizitätsprüfung bei den Teilnehmern erfolgt anhand des bereits vorhandenen Sicherungsankers, z.B. durch Vergleich des Hashwertes des öffentlichen Schlüssels mit dem Hashwert des schon als authentisch bekannten öffentlichen Schlüssels und Überprüfung des selbst-signierten Root CA-Zertifikats. Einige CA-Produkte erlauben die Verlängerung von Root CA-Zertifikaten, so dass dieser Ansatz in der Praxis gelegentlich zu finden ist.

Die Gültigkeit des neuen Zertifikats sollte die Gültigkeit des bisherigen Zertifikats vollständig umfassen, sofern das Schalenmodell zur Gültigkeitsprüfung eingesetzt wird, da ansonsten alle nachgeordneten Zertifikate neu ausgestellt werden müssten. Die dafür erforderliche Rückdatierung des Gültigkeitsbeginns ist jedoch nicht bei allen PKI-Produkten möglich. Auch bei einer Prüfung nach dem Kettenmodell sollten sich die Gültigkeitszeiträume zumindest mit dem bisherigen Zertifikat um einige Zeit überlappen, damit das „verlängerte" Zertifikat rechtzeitig vor Auslaufen des alten Zertifikats ausgestellt werden kann. Sofern zur Bildung der Zertifikatkette der **keyIdentifier** für die Verknüpfungsrelation benutzt wird, ist dies der einzige Lösungsansatz, bei dem keine Austauschzertifikate für nachgeordnete Zertifizierungsinstanzen oder Teilnehmer ausgestellt werden müssen, da das Schlüsselpaar des Verlängerungszertifikates identische mit dem des ursprünglichen Root CA-Zertifikates ist und somit die Relation über den **keyIdentifier** erhalten bleibt.

Bei unvorhergesehenen Störfällen, z.B. dem Schlüsselverlust oder der Schlüsselkompromittierung ist dieser Ansatz nicht anwendbar – das aktuelle Root CA-Zertifikat ist in diesen Fäl-

len nach Möglichkeit zu sperren und ein neuer Sicherungsanker zu etablieren (vgl. Kapitel 4.1).

4.6 Lange Gültigkeitsdauer

In letzter Zeit tauchen verstärkt Root CA-Zertifikate mit sehr langen Gültigkeitsdauern auf. Beispielsweise hat das „Class 3 Public Primary CA“-Zertifikat (Variante G3) von VeriSign eine Laufzeit von 50 Jahren, andere CA-Zertifikate von VeriSign haben eine durchschnittliche Laufzeit von 10 bis 30 Jahren (siehe [Veri99]). Die einfache Strategie hinter diesem Ansatz ist es, einen Root CA-Zertifikatswechsel nach Möglichkeit ganz zu vermeiden.

Ein Wechselkonzept für das Auslaufen des Root-CA-Zertifikats ist hier nicht erforderlich, da der Wechsel über sehr lange Zeit vermieden wird. Das Konzept kann mit dem Wechselkonzept über den Produktzyklus kombiniert werden, da der Software-Lebenszyklus im allgemeinen sehr viel kürzer sein wird als die Gültigkeit eines langlebigen Root CA-Zertifikats (siehe Kap. 3.2). Bei einigen Störfällen, z.B. der Kompromittierung oder dem aufgrund der langen Laufzeit vorhersehbaren Fortschritt bei der Kryptoanalyse der zugrundeliegenden kryptographischen Verfahren, aber auch bei Policy-Änderungen, bietet dieser Ansatz allerdings keine Möglichkeiten zur Aufrechterhaltung des PKI-Betriebs – hier muss in der Regel die PKI komplett neu aufgesetzt und eine Sperrliste für die (potentiell sehr lange) Restlaufzeit des ausgetauschten Zertifikats authentisch vorgehalten werden, wodurch dieser Ansatz nicht sehr attraktiv ist.

4.7 Cross-Zertifikate

Das Ziel, einen Wechsel des Root-CA-Zertifikats möglich automatisch durchführen zu können, wird mit dem Ansatz der Cross-Zertifizierung unterstützt. Rechtzeitig vor Ablaufen eines Root CA-Zertifikats wird ein neues Root CA-Zertifikat ausgestellt und mit dem aktuellen Zertifikat cross-zertifiziert (siehe Abb. 1). Der neue Sicherungsanker und die beiden Cross-Zertifikate werden an die Teilnehmer verteilt, die automatisierte Authentizitätsprüfung beim Teilnehmer ist dann mit dem alten Root-CA-Zertifikat möglich.

Dieser Ansatz wird in einigen aktuellen Standards (z.B. PKIX [RFC2510]) bevorzugt, da er für auslaufende Root CA-Zertifikate eine vollautomatische Authentisierung des neuen Root CA-Zertifikates im Rahmen der beim Client ohnehin unterstützten Zertifikatkettenprüfung erlaubt. Eine aufwendige und fehleranfällige Nutzerinteraktion wird so entbehrlich.

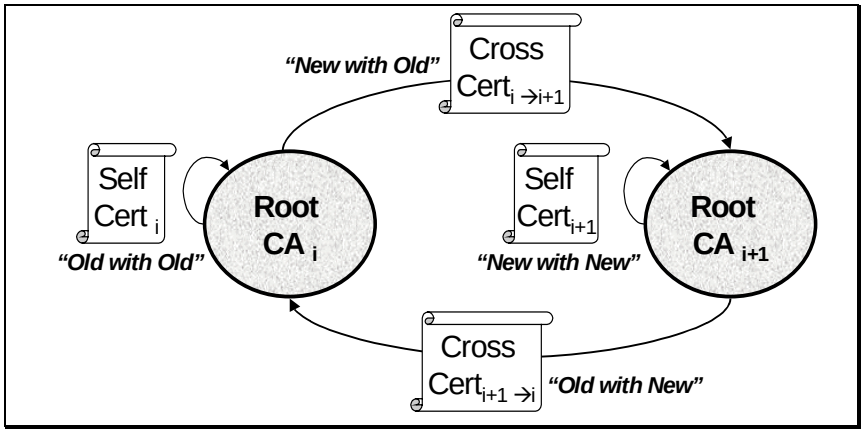

***Abb. 1**: Cross-Zertifizierung nach dem PKIX-Modell*

In Abbildung 2 wird das PKIX-Modell des Root CA-Zertifikatswechsels (nach [RFC2510]) skizziert: Eine neue Root CA wird aufgesetzt, stellt sich ein selbstsigniertes Root CA-Zertifikat aus (Wurzelzertifikat $_{i+1}$, „NewWithNew“) und zertifiziert sich mit der aktuellen Root CA über Kreuz (Cross-Zertifikat$_{i\rightarrow i+1}$, „NewWithOld“, und Cross-Zertifikat$_{i+1\rightarrow i}$, „OldWithNew“). Dieser Zertifikatssatz von drei Zertifikaten kann mittels der PKIX-Management-Nachricht „CA Key Update Announcement“ [RFC2510] an die untergeordneten PKI-Instanzen gemeldet werden, die diese Information an ihre untergeordneten Instanzen weiterzumelden haben. Letztendlich gelangt dieser Zertifikatssatz zu den Teilnehmern, wo er – idealerweise vollautomatisiert – anhand des dort bereits als Vertrauensanker vorliegenden aktuellen Root CA-Zertifikats („OldWithOld“) geprüft und authentisch übernommen werden kann.

Eine PKI-Architektur nach diesem Ansatz besitzt typischerweise einen Sicherungsanker, der initial an die Teilnehmer ausgerollt wird. Bevor das aktuell verwendete Root CA-Zertifikat ausläuft, wird rechtzeitig ein weiterer Sicherungsanker erzeugt (Zertifikatssatz von drei Zertifikaten, s.o.) und an die Teilnehmer verteilt. Dieser muss einen überlappenden Gültigkeitszeitraum zum bisherigen Zertifikat haben, damit alle drei Zertifikate nach der Verteilung gültig sind. Attribut- oder Policy-Änderungen, die das Root CA-Zertifikat betreffen, lassen sich mit diesem Verfahren an die Teilnehmer ausrollen. Gegebenenfalls müssen die Cross-Zertifikate hierzu ein entsprechendes Policy-Mapping enthalten.

Bei einigen Störfällen, z.B. bei einer Schlüsselkompromittierung und dem Verlust des aktuellen Sicherungsankers, bietet dieser Ansatz keine Vorteile: Ein nach einer Kompromittierung erzeugter neuer Sicherungsanker ist nicht mehr via Cross-Zertifizierung mit dem alten, kompromittierten Sicherungsanker authentisierbar, da die Authentizität der Cross-Zertifikate nicht mehr sichergestellt werden kann. Auch bei Schlüsselverlust ist die Lösung nicht einsetzbar, da das notwendige Cross-Zertifikat „NewWithOld“ nicht mehr erzeugt werden kann.

Eine Besonderheit tritt auf, wenn das alte Zertifikat innerhalb seines Gültigkeitszeitraumes, aber nach Ausstellung des Cross-Zertifikats „OldWithNew“ kompromittiert wurde und daher widerrufen werden muss. In diesem Fall muss nicht nur das alte selbstsignierte Root CA-Zertifikat „OldWithOld“, sondern auch das Cross-Zertifikat „OldWithNew“ widerrufen werden, um sicherzustellen, dass keine gültige Zertifikatkette zum neuen Vertrauensanker über den alten, widerrufenen Anker hergestellt werden kann.

Je nach Implementierung der Lösung kann es erforderlich sein, dass die Applikationen mehrere Sicherungsanker gleichzeitig verwalten können müssen. Da diese Eigenschaft aber bei den meisten gängigen Client-Produkten gegeben ist, stellt dies keine wirkliche Einschränkung dar. Weniger verbreitet ist hingegen noch die Fähigkeit, Cross-Zertifikate automatisch zu verarbeiten, was die Anwendung dieses Lösungsansatzes meist noch verhindert.

4.8 Web-of-Trust

Eine Zertifizierungsinfrastruktur nach dem Modell eines Web-of-Trust (WoT) ist im allgemeinen flexibler als streng hierarchische Ansätze, da im WoT u.U. alternative Vertrauenspfade (Zertifizierungspfade) zwischen zwei Knoten existieren können und sich auf diese Weise „Ausfälle“ im Vertrauensnetz „umgehen“ lassen [Elli01]. In dieser Hinsicht kann das WoT als Ganzes unempfindlicher gegenüber dem Ausfall einzelner Knoten sein als ein hierarchisches Modell. Allerdings kann es auch im WoT exponierte Teilnehmer geben, denen viele andere Teilnehmer vertrauen und deren Ausfall sich im WoT deutlich bemerkbar macht.

Das WoT kann, je nach konkreter Ausprägung und je nach individueller Vertrauensentscheidung der einzelnen Teilnehmer, die ganze Bandbreite – einschließlich Mischformen – zwischen einer rein hierarchischen Struktur und einer vollständigen Vernetzung aller Teilnehmer umfassen.

Typischerweise gibt es, anders als in den anderen Ansätzen, im WoT nicht „das“ *eine* Root-Zertifikat, das von einem Störfall im Sinne der Beschreibung eingangs dieses Kapitels betroffen sein kann. Vielmehr kann potentiell *jeder* Teilnehmer für einen anderen einen Vertrauensanker darstellen. Ein Störfall eines Teilnehmerzertifikates oder -schlüssels betrifft dann nur diejenigen anderen Teilnehmer des WoT, die den jeweiligen Schlüsselinhaber als vertrauenswürdig ansehen und sich (auch) auf seine Zertifizierungen verlassen. Insofern ist von einem Störfall innerhalb des WoT immer nur eine Teilmenge seiner Teilnehmer betroffen (sofern nicht der Fall vorliegt, dass das WoT de-facto eine streng hierarchische Struktur hat und der betroffene Teilnehmer die Wurzel dieser Struktur darstellt).

Ebenso gibt es im WoT im allgemeinen keine einheitliche Zertifizierungspolicy. Stattdessen kann jeder Teilnehmer nach individuell wählbaren, in vielen Fällen nicht explizit dokumentierten und insofern für Dritte häufig nicht nachvollziehbaren Regeln (oder sogar völlig willkürlich) seine Zertifizierungen vornehmen.

Die Verwendung eines WoT-basierten Ansatzes innerhalb einer PKI setzt in der Regel voraus, dass bereits vor dem Rollout eine Entscheidung für diese spezielle Variante getroffen wurde, da dies bereits die Produktauswahl maßgeblich mitbestimmt. Allerdings ist das WoT typischerweise dezentral organisiert und strukturiert, so dass es „den“ Rollout als eine zentral geplante, vorbereitete und koordinierte Aktion im WoT kaum gibt. Aufgrund dieser Struktur und mangels einer einheitlichen Zertifizierungspolicy gibt es bei einem WoT-Ansatz häufig auch keine einheitliche Handhabung hinsichtlich der Sperrung von Schlüsseln oder Zertifikaten.

Vor einem absehbaren Störfall, z.B. dem Auslaufen eines Zertifikats, können im WoT die „bedrohten“ Zertifikate einer Vertrauensstelle mit eigenen Zertifikaten bzw. durch den vertrauenswürdigen Teilnehmer selbst ersetzt werden, indem er mit einem zusätzlichen (neuen) Schlüssel diejenigen Zertifizierungen wiederholt oder erneuert, die in Gefahr sind, ungültig zu werden.

Der Verlust eines Schlüssels ist im WoT für die PKI als Ganzes eher unkritisch, da potentiell jeder andere Teilnehmer als Ersatz einspringen und neue Zertifikate ausstellen kann. (Im allgemeinen gibt es im WoT keine vergleichbar exponierten Teilnehmer, wie es die CAs in einer hierarchischen PKI sind.) Aufgrund fehlender oder nicht ausreichend etablierter/einheitlicher Sperrmechanismen ist es allerdings in dieser Situation schwierig, die Information über den Verlust an andere PKI-Teilnehmer zu kommunizieren, damit diese nicht mehr an den zugehörigen Public-Key verschlüsseln. Für den unmittelbar betroffenen Schlüsselinhaber bedeutet dieser Fall, dass er die anderen PKI-Teilnehmer informieren muss, dass sein alter Schlüssel nicht mehr verfügbar ist (dies ist nur für den Fall bedeutsam, dass der Schlüssel zum Entschlüsseln eingesetzt wurde).

Nach Eintreten eines Störfalls muss im WoT ein Ersatzschlüssels auf dem sonst auch benutzten Weg authentisch verteilt werden, d.h. mittels direkter persönlicher Übergabe oder durch Überprüfung des öffentlichen Schlüssels z.B. via Telefon oder Nennung auf der Visitenkarte. Auf diese Weise erfolgt somit die Integration des neuen Schlüssels in das trotz des Störfalls verbliebene „Rest-WoT“. Hinsichtlich der Sperrung gilt das gleiche wie im Falle eines Schlüsselverlustes, mit der Verschärfung, dass in jenem Fall nur eine Verzögerung der Kommunikation eintritt und diese u.U. etwas umständlicher wird, bei einer Kompromittierung hingegen der Verlust von Vertraulichkeit, Integrität und Authentizität der Kommunikation droht, wenn die Kompromittierung anderen Teilnehmern nicht geeignet signalisiert werden kann.

5 Bewertung

Die folgenden Tabellen bewerten die Charakteristika Vorbereitbarkeit, Anwendbarkeit und technischer Aufwand der Lösungsansätze zum Wechsel bzw. Ersatz eines Root-Zertifikats.

Vorbereitung des Lösungsansatzes	**Lösungsansatz Nr.**	Neue PKI aufsetzen	über Produktzyklus	Reservezertifikat	Mehrere Vertrauensanker	Verlängerung Root CA	Lange Gültigkeitsdauer	Cross-Zertifikat	Web-of-Trust
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
• vor Rollout		+	+	+	+	+	+	+	+
• nach Rollout, vor Störung		+	+	o	o	+		+	+
• nach Störung		o	o						o

Tabelle 2: Vergleich der Lösungsansätze hinsichtlich ihrer Vorbereitbarkeit
(Eignung: +: gut, o: mittelmäßig, -: schlecht, leer: ungeeignet)

Die beiden Ansätze „Reservezertifikat“ und „Mehrere Vertrauensanker“ sollten möglichst vor dem initialen Rollout vorbereitet werden, da es bei der nachträglichen Verteilung und Installation des neuen, zusätzlichen Sicherungsankers zu Problemen kommen kann. Alle anderen Lösungsansätze – mit Ausnahme der „langen Gültigkeitsdauer“ – erlauben es, den Root-CA-Zertifikatswechsel nach dem Rollout aber vor der Störung (d.h. dem Auslaufen der Gültigkeit bzw. der Sperrung des Wurzelzertifikats) vorzubereiten. Dies ist grundsätzlich zu empfehlen, um einen zügigen und sicheren Wechsel des Sicherungsankers vornehmen zu können. Ist die Störung eingetreten, so ist der Rollout des neuen Wurzelzertifikats nur noch mittels eines der beiden ersten Lösungsansätze zu bewerkstelligen. Sofern keine Vorbereitungen getroffen wurden und das Root CA-Zertifikat hierbei gesperrt wurde, führt dies jedoch im allgemeinen zu einem längeren Ausfall der PKI, da das alte Zertifikat nicht mehr zur authentischen Verteilung des neuen Root CA-Schlüssels genutzt werden kann.

Anwendbarkeit des Lösungsansatzes	**Nr.**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Org. Aufwand zum Ausrollen des neuen Root-Zertifikats		-	+	+	+	o	+	o	
automatisierte Einsatzumgebung			-	+	+	o		o	
Prüfung von Zertifikaten unter alter Root möglich		o	o	o	-	+		+	o
Attribut-/Policy-Änderung für neues Zertifikat möglich		+	+	-				o	+

Tabelle 3: Vergleich der Lösungsansätze hinsichtlich der Anwendbarkeit
(Eignung: +: gut, o: mittelmäßig, -: schlecht, leer: ungeeignet, schattiert: nicht anwendbar)

Es fällt auf, dass die Beurteilung hinsichtlich des Aufwands zum Ausrollen des neuen Root-Zertifikats und ihrer Eignung für eine automatisierte Einsatzumgebung beim Nutzer bei den Lösungsansätzen Nr. 3 bis 5 und Nr. 7 jeweils gleich ausfällt. . So sind die Lösungsansätze „Reservezertifikat“ und „mehrere Vertrauensanker“ z.B. leicht anzuwenden, da das neue Zertifikat bereits zeitgleich mit dem alten Zertifikat ausgerollt wird und damit kein Zusatzaufwand für dessen Verteilung erforderlich ist.

Die Ansätze „Verlängerung der Root CA“ und „Cross-Zertifikate“ verursachen geringen Aufwand, sofern das alte Root CA-Zertifikat nicht widerrufen wurde und noch zur Authentizitätsprüfung herangezogen werden kann. Die Client-Software muss im Falle der Verlängerung die entsprechende Prüfung (neues Root-Zertifikat mit Unterschriftenschlüssel des alten, bzw. mit dem alten Schlüssel signiertes Crosszertifikat für den neuen Key) unterstützen.

Der Ansatz „neue PKI“ verursacht den gleichen organisatorischen Aufwand wie das initiale Rollout (mit der Ausnahme, dass ggf. die Client-Software nicht installiert werden muss) und ist für eine automatisierte Einsatzumgebung ungeeignet. Der Ansatz „über Produktzyklus“ verursacht geringen organisatorischen Zusatzaufwand, da im Rahmen des Produkt-Rollouts das Root CA-Zertifikat mit ausgerollt werden kann. Lediglich die Authentizitätsprüfung muss manuell durchgeführt werden und ist nur mit größerem Aufwand automatisierbar.

Die Prüfung von Zertifikaten/-ketten unter der alten Root-CA ist bei den zwei Lösungsansätzen Nr. 5 und Nr. 7 mit nur einem Sicherungsanker im Client möglich. Die anderen Ansätze setzen voraus, dass die Clients mehrere Sicherungsanker gleichzeitig verwalten können. Dies stellt technische Anforderungen an die Client-Software, die in der Praxis nicht immer erfüllt werden.

Manchmal ist es wünschenswert, mit einem Root-CA-Zertifikatswechsel auch einen Wechsel der Policy durchführen zu können. Dies ist bei den beiden ersten Ansätzen trivialerweise möglich, beim Lösungsansatz „Cross-Zertifikate“ sollte die neue mit der bisherigen Zertifizierungspolicy kompatibel sein und mittels Policy-Mapping im Cross-Zertifikat abgebildet werden. Ein Reservezertifikat kann theoretisch ebenfalls unter einer anderen Policy ausgestellt werden, je nach Ausstellzeitpunkt dieses Zertifikats muss diese jedoch u.U. bereits initial bekannt sein, was den Nutzen stark einschränkt.

Technischer Aufwand **Nr.**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Re-Zertifizierung nachgeordneter CAs / TN bei Verknüpfung über Keyldentifier erforderlich	J	J	N	N	N		J	
Unterstützung durch Client-Software erforderlich	N	J/N	J	J	J/N	N	J	J

Tabelle 4: Vergleich der Lösungsansätze hinsichtlich des technischen Aufwands

Die Re-Zertifizierung nachgeordneter CAs bzw. der Teilnehmer ist bei den Lösungsansätzen „neue PKI“, „Produktzyklus“ und „Cross-Zertifizierung“ im allgemeinen notwendig, was einen hohen technischen und organisatorischen Aufwand verursacht.

Die Ansätze „Reservezertifikat“, „Mehrere Vertrauensanker“ und „Cross-Zertifikat“ erfordern eine spezielle Unterstützung durch die Anwender-Software, die in der Praxis oft nicht gegeben ist. (Gleiches gilt für den Sonderfall Web-of-Trust.) Bei den Ansätzen „Produktzyklus“ und „Verlängerung Root CA“ ist die Unterstützung durch die Anwender-Software erforderlich, sofern die Ansätze in einer automatisierten Einsatzumgebung verwendet werden sollen, in der die Authentizitätsprüfung des neuen Root-Zertifikats automatisch erfolgt.

5.1 Kombination der Lösungsansätze

Die folgende Tabelle zeigt, welche Lösungsansätze gewinnbringend miteinander kombiniert werden können. Dies ist insbesondere sinnvoll, wenn hierdurch zusätzliche Eigenschaften erreicht werden können, wie z.B. eine Vorbereitung nach Ausrollen der Teilnehmerzertifikate oder die erweiterte Anwendbarkeit der Lösung.

Kombinierbarkeit der Ansätze **Lösungsansatz**	Neue PKI aufsetzen	über Produktzyklus	Reservezertifikat	Mehrere Vertrauensanker	Verlängerung Root CA	Lange Gültigkeitsdauer	Cross-Zertifikat	Web-of-Trust
neue PKI aufsetzen		x				x		x
über Produktzyklus	x		x	x	x	x	x	
Reservezertifikat		x		x			x	x
mehrere Vertrauensanker		x	x		x	x	x	x
Verlängerung Root CA-Zertifikat		x		x		x		x
lange Gültigkeitsdauer	x	x		x	x			x
Cross-Zertifikate		x	x	x				x
Web-of-Trust	x		x	x		x	x	

Tabelle 5: Kombinierbarkeit der Lösungsansätze

So lässt sich beispielsweise der Ansatz „mehrere Sicherheitsanker“ gut mit den Ansätzen „Produktzyklus“ und „Cross-Zertifizierung“ verbinden, um für viele Ursachen, die einen Zertifikatswechsel der Root CA erzwingen können, gewappnet zu sein (vgl. Tabelle 1).

Der Lösungsansatz „über Produktzyklus“ kann mit allen anderen Lösungsansätzen kombiniert werden. Er kann, sofern sinnvoll, mit dem Ansatz „Verlängerung Root CA“ kombiniert werden, um das in Kapitel 4.2 adressierte Problem der Gültigkeitsprüfung unter mehreren gleichzeitig gültigen Vertrauensankern zu entschärfen.

5.2 Übergeordnete Aspekte

In diesem Abschnitt wird der Einfluss des gewählten Gültigkeitsmodells sowie der Verknüpfungsrelation zwischen den Zertifikaten beschrieben, die für alle Lösungsansätze gelten. Das Gültigkeitsmodell hat Einfluss darauf, wann ein Zertifikatswechsel der Root CA spätestens vorgenommen werden sollte; die Verknüpfungsrelation beeinflusst, wie hoch der organisatorische Aufwand zum Austausch nachgeordneter Zertifikate ist.

Gültigkeitsmodell

Sofern im *Kettenmodell* die Gültigkeit des Root CA-Zertifikats ausläuft, beeinträchtigt dies den laufenden Betrieb bis zu dem Zeitpunkt nicht, an dem die Root CA weitere Zertifikate ausstellen muss, sie etwa nachgeordnete CAs oder Teilnehmer zertifizieren oder Sperrungen anderer Zertifikate vornehmen muss. Kann diese Funktion von nachgeordneten Zertifizierungsinstanzen weiterhin wahrgenommen werden, braucht der Zertifikatswechsel für die Root CA nicht unmittelbar nach Ablauf der Gültigkeit des alten Root-Zertifikats zu erfolgen.

Läuft im *Schalenmodell* die Gültigkeit des Root CA-Zertifikats aus, so ist keine Signatur mehr als technisch gültig prüfbar, sofern keine Zeitstempel eingesetzt werden. Damit ist ein Zertifikatswechsel der Root CA zum Weiterbetrieb der Infrastruktur zwingend erforderlich. Dieser zieht in der Praxis zwangsläufig einen Wechsel aller nachgeordneten Zertifikate nach sich, da deren Gültigkeit durch die Gültigkeit des Root CA-Zertifikats begrenzt wird.

Verknüpfungsrelation

Je nach implementierter Verknüpfungsrelation zur Bestimmung der Zertifikatkette ergeben sich unterschiedliche Anforderungen und Probleme hinsichtlich überlappender Gültigkeitszeiträume oder der Fragestellung, ob beim Zertifikatswechsel der private Schlüssel ebenfalls erneuert werden muss.

Wird der **Authority Key Identifier** zur Erstellung der Zertifizierungsrelation verwendet, so lässt X.509 zwei Möglichkeiten zu, mittels diesem die Zertifikate zu referenzieren:

1. mittels **AuthorityCertIssuer** und **AuthorityCertSerialNo**, die gemeinsam das Zertifikat der ausstellenden Instanz eindeutig referenzieren, bzw.
2. mittels **KeyIdentifier**, der den öffentlichen Schlüssel der ausstellenden Instanz eindeutig referenziert. Er kann z.B. als Hash über den Public Key realisiert werden.

Im ersten Fall müssen bei einem Zertifikatswechsel der Root CA alle nachgeordneten Zertifikate ebenfalls ausgetauscht werden, da diese jeweils auf ein eindeutig bestimmtes Zertifikat referenzieren, das ersetzt worden ist; im zweiten Fall ist aufgrund der Referenzierung des *Schlüssels* keine Neu-Zertifizierung wegen der Verknüpfungsrelation erforderlich.

6 Hinweise für die Praxis

Zusätzlich zu den theoretischen Überlegungen aus den vorangegangenen Kapiteln folgen nun einige Hinweise für die Praxis des Root CA-Zertifikatswechsels.

- **Schlüsselwechsel bei Zertifikatswechsel?** Bei jedem Zertifikatswechsel stellt sich grundsätzlich die Frage, ob das dazugehörige Schlüsselpaar ebenfalls gewechselt werden soll oder beibehalten werden kann. Der Schlüsselwechsel ist obligatorisch für den Fall, dass der mit dem Zertifikat assoziierte private Schlüssel kompromittiert wurde oder das zugrundeliegende Verfahren oder die verwendete Schlüssellänge mit der Zeit zu „schwach“ geworden ist. In vielen Fällen ist dies aber nicht so eindeutig, zumal ein Zertifikatswechsel *ohne* Schlüsselwechsel oft mit weniger Aufwand verbunden ist, da keine neuen Schlüssel erzeugt werden müssen.
  Es wird empfohlen, stets – bis auf wenige Ausnahmen[9] – einen expliziten Schlüsselwechsel beim Root CA-Zertifikatswechsel vorzusehen. Insbesondere wenn die Policy bzw. Attribute im Zertifikat verändert wurden, ist ein Schlüsselwechsel angezeigt. Beispielsweise kann sonst der Fall auftreten[10], dass bei der Validierung der Zertifikatskette unklar ist, welches der vorhandenen Root CA-Zertifikate – das alte oder das neue – als Sicherungsanker verwendet werden soll. Dies führt zu unterschiedlichen Ergebnissen hinsichtlich der zugrunde liegenden Policy bzw. der weiteren Zertifikatsattribute.
- **Aufwand des Zertifikatswechsels reduzieren!** Der Zertifikatswechsel der Root CA ist i.d.R. sehr aufwendig, daher sollte jede Gelegenheit genutzt werden, den Betroffenen neue Zertifikate authentisch zu übergeben. So können Endanwendern bei jedem Besuch der Registrierungsstelle den aktuellen Satz an Root CA Zertifikaten erhalten. Falls das Unternehmen automatische Remote-Softwarewartung unterstützt, können auch auf die-

9 Solche Ausnahme könnte z.B. vorliegen, wenn sich die wesentlichen Attribute des Zertifikats sowie die zugrundeliegende Policy nicht ändern, beispielsweise wenn nur die Gültigkeitsdauer verlängert wird. Dies ist z.B. im Ansatz „Verlängern des Root CA-Zertifikats“ der Fall.

10 Insbesondere dann, wenn nicht der **Authority Key Identifier** (bzw. **AuthorityCertIssuer** und **AuthorityCertSerialNo**) zur eindeutigen Referenzierung des Root CA-Zertifikats verwendet wird.

sem Wege die Zertifikate vollautomatisch und authentisch an die Teilnehmer verteilt werden (siehe hierzu auch den Praxishinweis zum Einsatz von Standardprodukten). Andererseits könnte der Aufwand, den die explizite Überprüfung und Vertrauenszuweisung beim Import eines neuen Root CA-Zertifikats durch die Anwender verursacht, auch gewollt sein, um sie für *Ihren* Beitrag für die Sicherheit im Unternehmen zu sensibilisieren.

- **Möglichen Aufwand für sich selbst und Dritte berücksichtigen!** Ein Root CA-Zertifikatswechsel kann zeitkritisch und sehr „voluminös" sein. Es ist daher wichtig, den Aufwand rechtzeitig zu bestimmen, der für die Root CA, aber auch für die *anderen* Teilnehmer der PKI – untergeordnete CAs und Endanwender – entsteht. Falls möglich sollten betroffene Dritte rechtzeitig über einen Root CA-Zertifikatswechsel informiert und unterstützt werden. Für die Notfallvorbereitung wird empfohlen, für sich und ggf. auch für die untergeordneten Teilnehmer Notfallpläne bereitzuhalten, die zielgruppengerecht über die notwendigen Schritte beim Zertifikatswechsel informieren.
- **Den Zeitpunkt des Wechsels richtig wählen!** Oft laufen Root CA-Zertifikate zu „runden" Terminen aus, z.B. zum 31.12. eines Jahres. Auf derartige Termine fallen aber oft auch andere besondere Ereignisse (Beispiele aus der Vergangenheit sind die Euro-Umstellung und der Jahrtausendwechsel), so dass es durch eine mögliche Ereignishäufung zu Problemen oder Engpässen kommen kann. Auch ist es beispielsweise für einen E-Shop-Betreiber sicherlich ungünstig, wenn etwa in der umsatzträchtigen Weihnachtszeit die SSL-Root-Zertifikate auslaufen und die Kunden dann nicht in gewohnter Weise auf die Server zugreifen können. Es wird daher empfohlen, für das Auslaufen von Root CA-Zertifikaten vorbeugend entsprechend „unkritische" Zeitpunkte auszuwählen.
- **Funktionalität der Produkte berücksichtigen und rechtzeitig überprüfen!** Es wird empfohlen, bei der Produktauswahl Aspekte des Root CA-Zertifikatswechsels explizit zu berücksichtigen und hinsichtlich der eigenen Anforderungen zu evaluieren. Beispielsweise unterstützen viele Standardprodukte keine Cross-Zertifikate; werden solche Produkte in einem Unternehmen obligatorisch eingesetzt, macht es keinen Sinn, diesen Lösungsansatz für den Zertifikatswechsel anzustreben. Andererseits müssen die Anwender die Vorgaben, die die Root CA macht, ggf. bei ihrer Produktauswahl berücksichtigen.
- **Der unbedachte Einsatz von Standardprodukten kann risikoträchtig sein!** Webbrowser und –server sowie andere Standardprodukte, die Zertifikate verwenden, werden häufig von Hause aus mit einem Satz an Root CA-Zertifikaten ausgeliefert, über deren Authentizität und Vertrauenswürdigkeit beim Anwender oft Unklarheit besteht. Oft werden solche Produkte auf öffentlichen Servern bereitgestellt, und es ist somit grundsätzlich möglich, dass dort von unbekannten Dritten gefälschte Zertifikate hinzugefügt wurden – der Anwender kann dies mit einfachen Mitteln nicht mehr erkennen. Wenn auf diesem Wege entsprechende nicht-vertrauenswürdige Anwendungen unerkannt zum Einsatz kommen, kann dies die Sicherheit des gesamten Unternehmens gefährden! Es wird daher für den Einsatz im Unternehmen dringend empfohlen, aus Standardprodukten alle nicht benötigten bzw. alle nicht vertrauenswürdigen oder unbekannten Zertifikate explizit zu entfernen und den Anwendern entsprechend für den Unternehmenseinsatz vorbereitete Produktversionen bereitzustellen, die nur überprüfte und als vertrauenswürdig akzeptierte Zertifikate enthalten. In diese modifizierten Produktversionen können dann auch die eigenen Root CA-Zertifikate aufgenommen und im Unternehmen ausgerollt werden.
- **Externe Anforderungen an den Root CA-Zertifikatswechsel!** Strebt eine Root CA eine spezielle Zertifizierung z.B. unter WebTrust oder nach dem Signaturgesetz an oder sollen spezielle Anwendungen innerhalb der PKI unterstützt werden (z.B. DNSSEC oder WPKI), sind damit oft auch Vorgaben an den Root CA-Zertifikatswechsel verbunden. Es

wird dringend empfohlen, die Vorgaben der relevanten Spezifikationen rechtzeitig bei der Planung der Root CA bzw. der PKI zu berücksichtigen und umzusetzen.

- **Rechtzeitige Vorbereitung des Verzeichnisdienstes!** Das Einstellen mehrerer Root CA-Zertifikate einer CA in einem Verzeichnis muss rechtzeitig vorbereitet werden, z.B. durch die Konfiguration des entsprechenden Eintrags als „multiple entry“. Darüber hinaus müssen ggf. Einträge für Cross-Zertifikate im Verzeichnis vorgesehen werden.
- **Cross-Zertifikate zu anderen PKIs erneuern!** Falls die Root CA mit anderen PKIs cross-zertifiziert ist, sind bei einem Root CA-Zertifikatswechsel auch die entsprechenden Cross-Zertifikate zu erneuern und die alten Cross-Zertifikate gegebenenfalls zu widerrufen (abhängig vom Wechselgrund).

7 Ausblick

Bereits der Wirbel um das Auslaufen einiger Root CA-Zertifikate der Firma VeriSign im Dezember 1999, die in älteren Versionen einiger Internet-Browser verwendet wurden, hat gezeigt, dass das Problem des Root CA-Zertifikatswechsels nicht abstrakt in ferner Zukunft liegt. Hier wurde seinerzeit der Lösungsansatz „über den Produktzyklus“ propagiert, d.h. der manuelle Wechsel zu einer neueren Browser-Version, da die Browser keine anderen, benutzerfreundlichen Ansätze zum Zertifikatswechsel unterstützten. Dies hat sich bis heute nicht geändert.

Dieses Whitepaper hat verschiedene Lösungsansätze zum Zertifikatswechsel der Root CA miteinander verglichen. Dabei zeigt sich, dass die in der Praxis hinsichtlich ihrer Vorbereitungszeit und ihrer Anwendbarkeit nach Ablauf oder Kompromittierung des Root CA-Schlüssels tauglichsten Verfahren derzeit in den PKI-unterstützenden Applikationen technisch nicht vorbereitet sind. Hier sind insbesondere die Produkthersteller gefordert, diese Lösungsansätze in zukünftigen Produktversionen zu unterstützen. Solange es jedoch noch keine einheitlichen, etablierten Standards für den Wechsel des Root CA-Zertifikates gibt, wird eine entsprechende Anpassung oder Entwicklung der Produkte wohl noch einige Zeit auf sich warten lassen.

Die Auswahl eines geeigneten Lösungsansatzes hängt wesentlich vom Risk-Management des PKI-Betreibers ab: Ist der durchgehende Betrieb der PKI geschäftskritisch, so ist ein schneller Wechsel erforderlich und damit wird i.A. auch ein hoher Aufwand bei der Vorbereitung der notwendigen Maßnahmen in Kauf genommen. Ist die Störung hingegen verkraftbar und die Wahrscheinlichkeit ihres Auftretens hinreichend gering, so wird der Aufwand, der in die Vorbereitung des Wechselprozesses investiert wird, eher gering ausfallen.

8 Literatur

[ABA 01] American Bar Association: PKI Assessment Guidelines – Guidelines to help assess and facilitate interoperable trustworthy public key infrastructures, Draft Version 0.3, 18.06.2001 http://www.abanet.org/scitech/ec/isc/pag/pag.html

[BSI 00] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV – SigI Abschnitt A6 Gültigkeitsmodell, Version 1.1a, Bonn, 2000.

[CaPeSt02] Camphausen, I.; Petersen, H.; Stark, C.: „Konzepte zum Root-CA Zertifikatswechsel". In: Horster (Hrsg.): *Enterprise Security*, IT Verlag für Informationstechnik, 2002, S. 198-212.

[Elli01] Ellison, C.: „SPKI/SDSI and the Web of Trust", 2001. Online-Dokument, April 2001. http://world.std.com/~cme/html/ web.html

[Hamm99] Hammer, V.: *Die 2. Dimension der IT-Sicherheit – Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen*, Vieweg Verlag, 1999.

[HaMa01] Hartmann, M.; Maseberg, S.: „Fail-Safe-Konzept für FlexiPKI", in: Horster, P. (Hrsg.): *Kommunikationssicherheit im Zeichen des Internet*, Vieweg Verlag, 2001, S. 128ff.

[ITUT00] International Telecommunication Union – Telecommunication sector: ITU-T X.509 – Draft Recommendation X.509 – Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, 2000.

[RFC3280] Housley, R.; Ford, W.; Polk, W.; Solo, D.: Internet X.509 Public Key Infrastructure – Certificate and CRL Profile, RFC 3280, 2002.

[RFC2510] Adams, C.; Farell, S.: Internet X.509 Public Key Infrastructure Certificate Management Protocols, RFC 2510, 1999.

[RFC2541] Eastlake, D.: DNS Security Operational Considerations, RFC 2541, 1999.

[Veri99] VeriSign: VeriSign Key Hierarchy, 21.12.1999. http://www.verisign.com/repository/hierarchy/hierarchy.pdf

[WPKI00] Wireless Application Forum: WPKI – Wireless Application Protocol Public Key Infrastructure Definition, WAP-217-PKI, 2000. http://www1.wapforum.org/ tech/terms.asp?doc=WAP-217-WPKI-20010424-a.pdf