DuD
Datenschutz und Datensicherheit

Konzepte zum Root CA-Zertifikatswechsel

Ingmar Camphausen, Holger Petersen, Claus Stark

Im vorliegenden Beitrag diskutieren die Autoren – vor dem Hintergrund der zahlreichen Gründe, die zu einem Zertifikatswechsel der Root CA führen können – die damit verbundenen organisatorischen und technischen Probleme und stellen verschiedene mögliche Lösungsansätze vergleichend gegenüber.[41]

Ingmar Camphausen

Projektleiter IT-Sicherheit, Fachbereich Mathematik und Informatik der Freien Universität Berlin

E-Mail: ingmar@inf.fu-berlin.de

Dr. Holger Petersen

Security Consultant, Secorvo Security Consulting GmbH, Arbeitsschwerpunkt: Sicherheitsanalysen und –konzepte

E-Mail: petersen@secorvo.de

Claus Stark

Berater im Bereich IT-Risikomanagement der DB Systems GmbH, Frankfurt

E-Mail: Claus.Stark@bahn.de

[41] Der Beitrag ist erschienen im Tagungsband „Enterprise Security“, IT Verlag für Informationstechnik GmbH, 2002.

Einleitung

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 Lösungen sparen die Probleme, die sich aus dem Wechsel des Root CA-Zertifikats ergeben, aus, verbunden mit der Hoffnung, dass das Problem technisch gelöst sein werde, bevor es „in einigen Jahren“ auftritt. Damit gibt es oft keinen wirksamen Notfallplan im Fall, dass ein vorzeitiger Zertifikatswechsel notwendig wird.

1 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, unbefugten Zugang zum privaten Schlüssel (beispielsweise durch Entwenden einer Hardware-PSE[42] oder „Hacken“ der Software-PSE) oder aufgrund von Schwächen des mathematischen Problems, auf dem die Sicherheit des privaten Schlüssels beruht,
- *Kompromitterung des Signaturverfahrens*, mit dem das Root CA-Zertifikat signiert wurde; z. B. durch Schwächen der kryptographischen Algorithmen (Hash- oder Signaturverfahren) oder zu geringer 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 Policy, unter der das Zertifikat ausgestellt wurde[43], 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. ein Wechsel des Zertifizierungsdiensteanbieters oder vorfristiger CA-Schlüsselwechsel als „Sperrlistenersatz“, falls keine Sperrung von nachgeordneten Zertifikaten möglich ist, siehe 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

[42] PSE = Personal Security Environment

[43] 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.

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.

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 erfolgt die initale authentische Verteilung des Root CA-Zertifikats?
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 unterstützen. 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 zu Grunde liegenden 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.

2 Grundlagen

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

2.1 Zertifikate nach X.509

Wesentliche Bestandteile eines Zertifikats nach X.509 [ITUT00] sind seine Seriennummer (**serialNumber**), der Aussteller (**issuer**), der Empfänger (**subject**), die Gültigkeit (**validity**), die Information über den öffentlichen Schlüssel des Empfängers (**subjectPublicKeyInfo**), die eindeutigen Schlüsselidentifikatoren (**issuerUniqueIdentifier**, **subjectUniqueIdentifier**) sowie

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

2.2 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.

2.3 Gültigkeitsmodell

Zur technischen Gültigkeitsprüfung[47] 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 Beitrag 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.

- **Kettenmodell:** Unter der Gültigkeitsregel des *Kettenmodells*[48] ist eine Zertifikatkette technisch gültig, wenn unter anderem jedes Zertifikat der Kette innerhalb des Gültigkeitszeitraums des jeweiligen übergeordneten Zertifikats ausgestellt wurde [BSI 00].
- **Schalenmodell**: Unter der Gültigkeitsregel des *Schalenmodells*[49] ist eine Zertifikatkette technisch gültig, wenn unter anderem jedes Zertifikat der Kette vom Gültigkeitszeitraum des übergeordneten Zertifikats vollständig eingeschlossen wird.

2.4 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.

3 Lösungsansätze

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

Tabelle 1 gibt einen Überblick, unter welchen Voraussetzungen die vorgestellten Lösungsansätze geeignet sind, einen Zertifikatswechsel der Root CA unter Aufrechterhaltung des Wirkbetriebs der PKI zu ermöglichen.

Zertifikatwechsel Root CA / **Lösungsansatz**	Neue PKI aufsetzen	über Produktzyklus	Reservezertifikat	Mehrere Vertrauensanker	Verlängerung Root CA	Lange Gültigkeitsdauer	Cross-Zertifikat
Anwendbarkeit des Lösungsansatzes ...							
vor Ablauf des Root CA-Zertifikats	+	+	+	+	+	+	+
nach Ablauf des Root CA-Zertifikats	o	o	+	+	o		(+)[44]
nach Verlust des privaten Schlüssels der Root CA	o	o	+	(+)[7]			
nach Kompromittierung des privaten Schlüssels	-	-	+	(+)[45]			
nach Kompromittierung des Signaturverfahrens	-	-	o	(+)[46]			

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

3.1 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, durchge-

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

[45] sofern hiervon nicht alle Vertrauensanker betroffen sind

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

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

[48] Auch „Zertifikat-Gültigkeit“-Regel genannt [BSI 00]

[49] Auch „Zertifizierungspfad-Gültigkeit“-Regel genannt [BSI 00]

führt werden kann. Ferner erlaubt sie den Wechsel der Algorithmen und Schlüssellängen sowie Attributs- oder Policy-Änderungen, sofern dieses erforderlich ist.

3.2 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.

3.3 Reservezertifikat

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 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.

3.4 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 vorgehalten. Es bietet sich für diesen Ansatz an, die parallelen PKI-Strukturen auf unterschiedlichen kryptografischen 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] und den Beitrag von Sönke Maseberg in diesem Heft).

Eine PKI-Architektur nach diesem Ansatz wird idealer Weise 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 kryptografischen Verfahren gleichzeitig verwalten und nutzen zu können. Dieses unterstützen die in der Praxis verfügbaren Lösungen heutzutage aber in der Regel noch nicht.

3.5 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 Fällen nach Möglichkeit zu sperren und ein neuer Sicherungsanker zu etablieren (vgl. Kapitel 3.1).

3.6 Lange Gültigkeit

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.

3.7 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 crosszertifiziert (siehe Abb. 1). Der neue Sicherungsanker und die beiden Cross-Zertifikate werden an die Teilnehmer verteilt, die automatisierte Authentitätsprüfung beim Teilnehmer ist dann mit dem alten Root-CA-Zertifikat möglich.

Dieser Ansatz wird in einigen aktuellen Standards (z. B. PKIX [RFC2510]) präferiert, 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 aufwändige und fehleranfällige Nutzerinteraktion wird so entbehrlich.

In Abbildung 1 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 – idealer Weise 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.

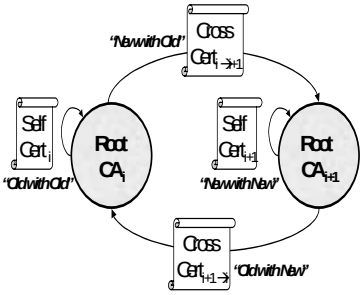

Abb. 1: Cross-Zertifizierung nach dem PKIX-Modell

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.

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

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

4 Bewertung

Die Tabellen 2 bis 4 bewerten die Charakteristika Vorbereitbarkeit, Anwendbarkeit und technischer Aufwand der Lösungsansätze.

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
Org. Aufwand zum Ausrollen des neuen Root-Zerts		-	+	+	+	o	+	o
automatisierte Einsatzumgebung			-	+	+	o		o
Prüfung von Zertifikaten unter alter Root möglich		o	o	o	-	+		+
Attribut-/Policy-Änderung für neues Zertifikat möglich		+	+	-				o

Tabelle 3: Vergleich der Lösungsansätze hinsichtlich der Anwendbarkeit

Hinsichtlich des organisatorischen Aufwands zum Ausrollen des neuen Root CA-Zertifikats und der automatisierten Einsatzumgebung beim Nutzer verhalten sich die letzten fünf Ansätze jeweils gleich. So sind die Lösungsansätze „Reservezertifikat“, „mehrere Vertrauensanker“ und „lange Gültigkeit“ gut geeignet, da das neue Zertifikat bereits zeitgleich mit dem alten Zertifikat ausgerollt wird und damit kein Zusatzaufwand entsteht.

Die Ansätze „Verlängerung der Root CA“ und „Cross-Zertifikate“ verursachen geringen Aufwand, sofern das alte Root CA-Zertifikat nicht widerrufen wurde und zur Authentitätsprüfung herangezogen werden kann. Die Client-Software muss im Falle der Verlängerung die entsprechende Prüfung 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 CA Root ist bei zwei Lösungsansätzen 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.

Die Rezertifizierung 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. Bei den Ansätzen „Produktzyklus“ und „Verlängerung Root CA“ ist diese erforderlich, sofern sie in einer automatisierten Einsatzumgebung eingesetzt werden sollen, in der die Authentizitätsprüfung des neuen Root-Zertifikats automatisch erfolgt.

5 Übergeordnete Aspekte

Abschließend soll der Einfluss des gewählten Gültigkeitsmodells sowie der Verknüpfungsrelation zwischen den Zertifikaten

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

Tabelle 4: Vergleich der Lösungsansätze hinsichtlich des technischen Aufwands

beschrieben werden, 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.

5.1 Gültigkeitsmodell

Sofern im *Kettenmodell* die Gültigkeit des Root CA-Zertifikats ausläuft, beeinträchtigt dies den laufenden Betrieb nicht, bis zu dem Zeitpunkt, zu dem die Root CA weitere Zertifikate ausstellen muss, 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 technisch als 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.

5.2 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 eindeutig zu referenzieren:

- mittels **AuthorityCertIssuer** und **AuthorityCertSerialNo**, die gemeinsam das Zertifikat der ausstellenden Instanz eindeutig referenzieren, bzw.
- 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 Fazit

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

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.

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.

[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.

[PKIX01] Housley, R.; Ford, W.; Polk, W.; Solo, D.: Internet X.509 Public Key Infrastructure – Certificate and CRL Profile, Internet Draft (work in progress) <draft-ietf-pkix-new-part1-11.txt>, PKIX Working Group, Oktober 2001.

[RFC2459] Housley, R.; Ford, W.; Polk, W.; Solo, D.: Internet X.509 Public Key Infrastructure – Certificate and CRL Profile, RFC 2459, 1999.

[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