Herausforderungen bei der Cross-Zertifizierung

Secorvo White Paper

Version 1.0
Stand 15. März 2002

Dr. Volker Hammer, Dr. Holger Petersen

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

ARL	Authority Revocation List
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CMC	Certificate Management Protocol using CMS
CMP	Certificate Management Protocol
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DFN	Deutsches Forschungsnetz
DMZ	Demilitarisierte Zone
ITU	International Telecommunication Union
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PCA	Policy Certification Authority
PEM	Privacy Enhanced Mail
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Internet X.509 Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
S/MIME	Secure/Multipurpose Internet Mail Extension
SigG	Signaturgesetz
XML	Extended Markup Language

Historie

Version	Datum	Status/Änderung	Autor
1.0	15.3.02	Erste veröffentlichte Fassung	Dr. Holger Petersen, Dr. Volker Hammer

1 Zusammenfassung

Die Einführung von Public-Key Infrastrukturen (PKI) im Unternehmensbereich, in der öffentlichen Verwaltung sowie über den Betrieb von Trustcentern für den breiten Massenmarkt schreitet zügig voran. Dabei entstehen derzeit überwiegend Insellösungen, innerhalb derer die Benutzer gesichert in ihren eigenen „Trust-Domain“ kommunizieren können. Im Zuge der Entwicklung von E-Business Aktivitäten sowohl zwischen Firmen (B2B/G2B) als auch zwischen Firmen und Privatkunden (B2C/G2C) wird dabei die Möglichkeit einer Cross-Zertifizierung zwischen diesen Insellösungen immer wichtiger, um die Vorteile PKI-basierter Transaktionen zur Sicherstellung von Vertraulichkeit, Integrität und Authentizität der übermittelten Daten auch über Unternehmens-/Behördengrenzen hinweg nutzen zu können. Das vorliegende White Paper[1] widmet sich wichtigen Herausforderungen der Cross-Zertifizierung, zeigt dabei wesentliche Problemfelder auf und diskutiert Lösungsansätze.

2 Einleitung

Das White Paper gibt zunächst eine kurze Einführung in Cross-Zertifikate, ihre Verwendungsmöglichkeiten und die grundlegenden technischen Konzepte. Anschließend werden eine Reihe von Fragestellungen und Diskussionspunkten formuliert und Lösungsalternativen vorgestellt.

Gegenwärtig werden Public Key Infrastrukturen in Insellösungen (einzelnen Domains) aufgebaut und in ersten produktiven Anwendungen eingesetzt. Es ist aber absehbar, dass der Aufwand für Zertifizierung und Zertifikatverwaltung zu hoch ist, um immer alle möglichen Teilnehmer und Partner innerhalb einer Domain jeweils selbst zu zertifizieren. Vielmehr versprechen Verknüpfungen der "Inseln" mit Hilfe von Cross-Zertifikaten erhebliche Synergieeffekte – damit zugleich einen früheren Return of Investment – und zugleich einen höheren Business-Value für die unterstützten PKI-Anwendungen. Auch bei der Fusion zweier Unternehmen mit jeweils eigener Zertifizierungshierarchie können Cross-Zertifikate eine Möglichkeit zur Verknüpfung der Infrastrukturen bieten.

Vor einer Cross-Zertifizierung ist jedoch die Frage zu beantworten, ob das Vertrauen, das einer "fremden" Infrastruktur mit Cross-Zertifikaten ausgesprochen wird, auch domainübergreifend gerechtfertigt ist. Die Antworten sollten technisch abgebildet werden. Schließlich müssen auch die Prüffunktionen der Anwendungen Cross-Zertifikate auswerten können.

Die genannten Aspekte werden aus der Perspektive digitaler Signaturen betrachtet. Die Betrachtungen lassen sich jedoch ohne wesentliche Änderungen auf andere Nutzungszwecke (z.B. die Verschlüsselung) übertragen.

Cross-Zertifikate sind Gegenstand der Standards X.509 (Definition, Format) und PKIX sowie einigen weiteren Internet Drafts (Nutzung) [ITUT00, PKIX99a, PKIX99b].

2.1 Definition von Cross-Zertifikaten

Öffentliche Schlüssel können in mehr als einem Zertifikat bestätigt werden. Ist dies der Fall, wird allgemein von **Mehrfachzertifikaten** für einen öffentlichen Schlüssel gesprochen ([Ham95a], [Ham95b]).

---

1 Dieses White Paper ist eine überarbeitete Version des Konferenzbeitrags auf dem 7. Deutschen IT-Sicherheitskongress des BSI, der vom 14.-16.Mai 2001 in Bonn/Bad Godesberg stattfand. Der Beitrag wurde mit dem „Best Paper Award“ des BSI prämiert [HaP01b].

Es lassen sich die folgenden Arten von Mehrfachzertifikaten unterscheiden:

- **Verlängerungszertifikate**: Verlängerungszertifikate unterscheiden sich vom ursprünglichen Zertifikat nur in Gültigkeitszeitraum, Seriennummer und Signatur.
- **Austauschzertifikate**: issuer *dn*, *subject dn* und bestätigter öffentlicher Schlüssel sind in Austauschzertifikaten identisch mit dem ursprünglichen Zertifikat, aber alle anderen Attributwerte können abweichen.
- **Cross-Zertifikate**: Ein öffentlicher Schlüssel wird bereits durch eine Zertifizierungsinstanz bestätigt (primäre Zertifizierungsrelation).[2] Zu einem bereits von einer Zertifizierungsinstanz bestätigten öffentlichen Schlüssel (primäre Zertifizierungsrelation) kann eine andere Zertifizierungsinstanz (mit anderem *issuer dn*) ein weiteres Zertifikat (Cross-Zertifikat) ausstellen. Der Sonderfall, dass die primäre Zertifizierungsinstanz ihren Namen wechselt und daraufhin neu zertifiziert, wird eingeschlossen.

Cross-Zertifikate liegen nach dieser Definition vor, wenn mehr als ein *issuer dn* einen *subject dn* zertifiziert.

Cross-Zertifikate (auch Mehrfachzertifikate im allgemeinen) können vom Schlüsselinhaber nicht verhindert werden, da der öffentliche Schlüssel jedem zugänglich ist und deshalb von jedem Inhaber eines Schlüsselpaares ein Zertifikat ausgestellt werden kann, das diesen Schlüssel enthält.

Durch die Ausstellung von Zertifikaten entstehen mehrere Relationen zwischen den Ausstellern und Inhabern der Zertifikate. Zum Verständnis von Cross-Zertifikaten sind vor allem zwei dieser Relationen relevant:

1. Die **Zertifizierungsinstanz-Relation**: "Aussteller zertifiziert Inhaber".
   Die in der Menge der Zertifikate enthaltenen Paare (*issuer dn, subject dn*) bestimmen einen Graphen. In "klassischen" Zertifizierungshierarchien bildet dieser einen Baum. Diese Relation lehnt sich häufig an die rechtlich-organisatorischen Zuständigkeiten an.
2. Die **Zertifizierungsrelation**: "Schlüssel **X** wird zum Prüfen des Zertifikats **Y** benötigt".
   Im entsprechenden Graphen wird erkennbar, ob eine Zertifizierungsinstanz mit wechselnden Schlüsseln Zertifikate für ein Schlüsselpaar eines nachgeordneten Inhaber ausstellt.

Cross-Zertifikate beeinflussen die Struktur beider Graphen. Während mit Verlängerungszertifikaten und Austauschzertifikaten die Baumstruktur der Zertifizierungsinstanz-Relation erhalten bleibt, entstehen mit Cross-Zertifikaten beliebige Graphen für diese Relation.

2.2 Verwendungsmöglichkeiten für Cross-Zertifikate

Für Cross-Zertifikate nach der obigen Definition gibt es zwei vorrangige Verwendungszwecke: Verknüpfung von Zertifizierungshierarchien und Verkürzungen von Zertifikatketten.

Der geläufigste Zweck ist die Verknüpfung von Zertifizierungshierarchien, insbesondere auf der Ebene der Wurzel-Zertifizierungsinstanzen. In diesem Fall stellen sich die beiden Root-

---

2 [ITUT00] formuliert allgemeiner: "Cross certificate – This is a certificate where the issuer and the subject are different CAs." Da diese Definition alle zwischen unterschiedlichen CAs ausgestellten Zertifikate umfasst, wird im Kontext dieses White Papers die oben angegebene engere Definition verwendet.

CAs gegenseitig Zertifikate aus. Dieser Fall wird im weiteren auch als Verknüpfung von Domänen bezeichnet.

Nach der obigen Definition liegt aber auch ein (einseitiges) Cross-Zertifikat vor, wenn nur eine Root das Wurzel-Zertifikat einer anderen Zertifizierungshierarchie bestätigt.

Schließlich können sich auch nachgeordnete Zertifizierungsinstanzen unterschiedlicher Domänen gegenseitig zertifizieren.

Mit Cross-Zertifikaten können demnach sowohl innerhalb einer Zertifizierungshierarchie als auch zwischen Zertifizierungshierarchien neue Relationen erzeugt werden. Die entstehenden "Querverbindungen" können zu kürzeren Zertifikatketten für Signaturprüfungen führen [ITUT00].

3 Aufbau, Erzeugung und Bereitstellung von Cross-Zertifikaten

Cross-Zertifikate sind ihrem Aufbau nach "Standard"-Zertifikate gemäß X.509. Sie können allerdings bestimmte, weitergehende Extensions enthalten, um ihre Verwendung zu steuern:

- **policyMappings: als SEQUENCE OF {issuerDomainPolicy, subjectDomainPolicy}.** Semantik: Der Aussteller des Cross-Zertifikats erklärt, dass die **issuerDomainPolicy** äquivalent zur **subjectDomainPolicy** ist.
- **policyConstraints:** steuern, ob und ab welcher Position in der zu prüfenden Zertifikatkette Policies ausgewiesen sein müssen (Attribut **requireExplicitPolicy**) und ob die Policies direkt bekannt sein müssen oder ob eine Referenz über "**policyMapping**" ausreichend ist (Attribut **inhibitPolicyMapping**). Mit **inhibitAnyPolicy** kann außerdem der Wert "**anyPolicy**" für Policy Identifier unterbunden werden.
- **nameConstraints:** kann zur Einschränkung der Namen verwendet werden, die von der zertifizierten CA verwendet werden dürfen (im Sinne von Cross-Zertifikaten: für die das Cross-Zertifikat Gültigkeit hat).

Weitere Attribute können für den Einsatz von Cross-Zertifikaten hilfreich sein, z. B**. pathLenConstraints**. Im allgemeinen Fall kann aber *nicht* davon ausgegangen werden, dass ein Cross-Zertifikat von einem "normalen" Hierarchie-Zertifikat unterschieden werden kann, denn die genannten Attribute können auch in "normalen" Zertifikaten enthalten sein oder in Cross-Zertifikaten fehlen.

Da nach der hier verwendeten Terminologie Cross-Zertifikate nur für bereits existierende Schlüsselpaare ausgestellt werden, kommen für die technische Erzeugung solcher Zertifikate nur Lösungen in Frage, die auf einer Übertragung des öffentlichen Schlüssels an die CA beruhen. Es können beispielsweise Zertifikat-Management-Protokolle nach PKIX (CMP, CMC), oder die Formate PKCS# 10 / PKCS# 7 verwendet werden.

Cross-Zertifikate können über Directories bereitgestellt oder in Nachrichten direkt mit versandt werden. Im Directory ist in Einträgen von Zertifizierungsinstanzen (jetzt Object Class **pkiCA**, [ITUT00, Kap. 11.1.2]) ein Attributtyp "**crossCertificatePair**" vorgesehen. Dieser kann ein Vorwärts- und ein Rückwärts-Cross-Zertifikat (von bzw. für eine gegenseitig zertifizierte Zertifizierungsinstanz) enthalten. Im Directory können daher beide CA-Einträge jeweils beide Zertifikate enthalten.

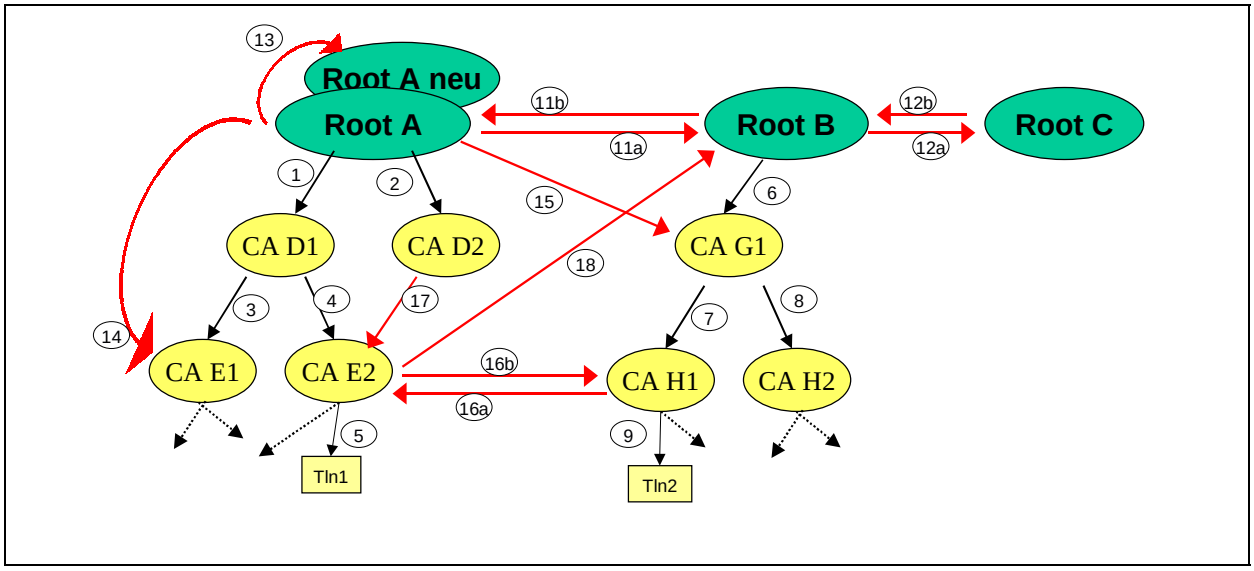

Abb. 1: Graph einer Zertifizierungsinstanz-Relation. Cross-Zertifikate haben Kantennummern >= 1. Die Kantennummern werden in den weiteren Beispielen verwendet.

4 Ausstellen von Cross-Zertifikaten

Da durch Cross-Zertifikate Vertrauen in Zertifikate einer anderen Hierarchie (und in der Regel auch vollständig unabhängigen Zertifizierungsinfrastruktur) ausgesprochen wird, sind die Informationen in Zertifikaten insbesondere unter dem Blickwinkel des Sicherheitsniveaus zu betrachten, unter dem die jeweiligen Zertifizierungshierarchien betrieben werden. Dabei können in einer Zertifizierungshierarchie durchaus unterschiedliche Sicherheitsklassen definiert sein, die sich in den jeweils referenzierten Certification Policies unterscheiden. Die Menge der Sicherheitsklassen einer Zertifizierungshierarchie und die Regeln für ihre Verwendung wird im folgenden als Domain-Policy bezeichnet.

Im weiteren wird modellhaft angenommen, dass für zwei gegebene Zertifizierungs(teil-)hierarchien, für die eine Cross-Zertifizierung geplant ist, jeweils eine Domain-Policy definiert ist. Außerdem wird angenommen, dass die Teilnehmer einer Zertifizierungshierarchie (Zertifikatinhaber und Empfänger von Zertifikaten) über Clients verfügen, die die jeweilige Domain-Policy auswerten können.

4.1 Notwendigkeit von Cross-Zertifikaten

Cross-Zertifikate sind nicht der einzige Weg, um getrennte Zertifizierungshierarchien miteinander zu verbinden. Alternativ zum Einsatz von Cross-Zertifikaten mit Angaben zum Policy

Mapping könnten für bestimmte Sicherheitsklassen unterschiedliche übergeordnete Wurzelinstanzen eingeführt werden. Dies entspricht dem PEM-Modell von Policy-CAs. Möglicherweise ist dies der pragmatischere und anwenderfreundlichere Ansatz. Anstatt an zentraler Stelle per Cross-Zertifikat zu entscheiden, welchen Infrastrukturen Vertrauen entgegengebracht werden soll, kann als weitere Alternative diese Aufgabe dem Anwender übertragen werden, indem er mehrere unabhängige Wurzelzertifikate als Sicherungsanker in seinem lokalen Zertifikatsverzeichnis aufnimmt.

Die Wahl zwischen diesen drei Verknüpfungsmöglichkeiten von Zertifizierungshierarchien oder ihre geschickte Kombination hängt von vielen Randbedingungen ab. Dazu gehören Kosten- und Nutzengesichtspunkte, "politische" Fragen, z. B. Branding", Sicherheitsaspekte, Anforderungen an und technische Realisierbarkeit von Gültigkeitsmodellen, und schließlich die Beherrschbarkeit für die Teilnehmer. So können Teilnehmer beim Akzeptieren unabhängiger Root-Zertifikate die akzeptierte Zertifikatmenge selbst kontrollieren. Der Preis dafür ist allerdings, dass sie Wurzelzertifikate "manuell" prüfen und das jeweilige CPS selbst bewerten müssen. Im Falle von Cross-Zertifikaten übernimmt dies eine zentrale Instanz für sie. Ob dadurch allerdings das Verständnis der entstehenden Zertifizierungsgraphen für die Teilnehmer und ihr Vertrauen in die PKI erhöht wird, muss sich erst zeigen.

4.2 Interdomain-Vertrauen

Eine wesentliche, der technischen Umsetzung vorgelagerte grundsätzliche Frage ist, ob ein "Interdomain-Vertrauen" der Zertifikatsnutzer einer Domaine über Cross-Zertifikate erzwungen werden kann. Schließlich könnte ein Zertifikatsnutzer mit der Beantragung seines Zertifikats in einer PKI erwarten, dass er sich mit der Anerkennung des Wurzelzertifikats "seiner" PKI auch nur in deren Domain bewegt und Zertifikate anderer Domains ausgeschlossen sind.

Grundsätzlich sind hier zwei Sichtweisen möglich:

- Mit der Anerkennung eines Wurzelzertifikats delegiert der Teilnehmer das "Vertrauensmanagement" seiner Domaine. Da der Teilnehmer mit der Ausstellung seines Zertifikats einer bestimmten Vertrauens-Domäne beitritt und die Policy der Wurzel-Zertifizierungsinstanz anerkennt, muss er auch akzeptieren, dass die Zertifizierungsinstanzen Cross-Zertifikate ausstellen, wenn sie sich an die Certification Policy halten und hinreichende Äquivalenz zwischen den Policies der Domains sicherstellen. Schließlich muss er auch akzeptieren, dass innerhalb seiner Domaine weitere Zertifizierungsinstanzen eingerichtet und Nutzerzertifikate ausgestellt werden.
- Will der Teilnehmer die Vertrauensgewährung hingegen selbst kontrollieren, würde er eine Cross-Zertifizierung nicht unbesehen akzeptieren. Er würde sie in diesem Fall unter den Vorbehalt einer expliziten Anerkennung der anderen Domain stellen und sich gegebenenfalls sogar eine Entscheidung für einzelne Teilnehmerzertifikate vorbehalten.

Da eine explizite Kennzeichnung von Cross-Zertifikaten nach dem Standard nicht vorgesehen ist, müsste zur Unterstützung des zweiten Falles ein spezifische Regelung innerhalb der Domain festgelegt werden. Diese wäre bei der Cross-Zertifizierung von den Zertifizierungsinstanzen zu beachten und müsste von den Clients der Teilnehmer bei der Zertifikatsprüfung unterstützt werden. Eine Kennzeichnung von Cross-Zertifikaten könnte auch durch Nutzung von Standard-Extensions im Zertifikatsformat erfolgen.[3]

[3] Vgl. dazu auch "Gültigkeitsmodell".

4.3 Vergleichbarkeit von Certificate Policies

In einem Zertifikat können über sogenannte Policy-OIDs, das sind weltweit eindeutige Object Identifier, die auf eine zugehörige Certificate Policy der CA verweisen, Informationen zum Sicherheitsniveau oder Hinweise zur Eignung ausgedrückt werden. Certificate Policies können dazu eine Fülle von Parametern enthalten und über Zusicherungen, Begrenzungen und Service-Qualitäten für das ausgestellte Zertifikat informieren.

Für die konkrete Realisierung der zugesicherten Eigenschaften gibt es in vielen Fällen eine Reihe von Alternativen. Die in einer PKI ausgewählten Varianten werden in der Regel in einem von der CA veröffentlichten Certification Practice Statement (CPS) beschrieben. Aus praktischen Gründen [DF1]abstrahieren Certificate Policies jedoch von vielen Details eines Certification Practice Statement. Doch auch die Certification Practice Statements zweier Domains können sich in ihrem Detaillierungsgrad unterscheiden. Außerdem hat die Erfahrung gezeigt, dass in vielen PKIs mit der Zeit unterschiedliche Trust Level eingeführt werden, die die Vergleichbarkeit von Certificate Policies weiter erschweren.

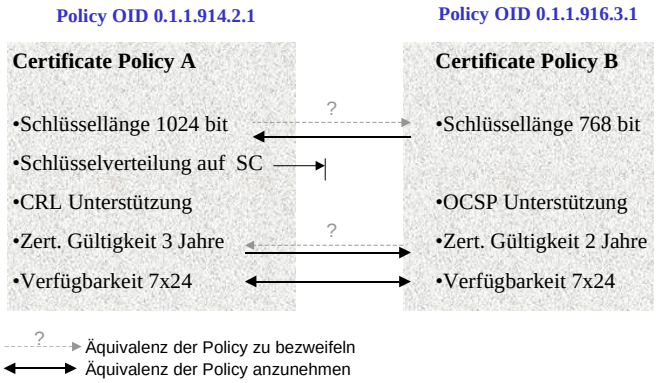

Abb. 2. Bereits Standard-Parameter von Policies weisen häufig Unterschiede auf.

Hingegen ist es *technisch* sehr leicht, unterschiedliche Certification Policies einander gleich zu stellen: So wird im ITU-Standard X.509 spezifiziert, wie die Äquivalenz von Certificate Policies in (Cross-)Zertifikaten definiert werden kann (**policyMapping,** [ITUT00, Kap. 18.2.1.]). Für diese Art des Policy-Mapping in Cross-Zertifikaten ergeben sich jedoch zwei *praktische* Problembereiche:

- Selbst in sehr einfachen PKI-Strukturen wird es vermutlich keine zwei exakt gleichen Certificate Policies für unterschiedliche Domänen geben: Certification Policies unterscheiden sich in der Praxis oft in Details. Damit stellt sich die Frage, ob der Mechanismus des Policy-Mapping überhaupt verwendet werden sollte, da er den Anwender unter Umständen in dem trügerischen Glauben lässt, zwei unterschiedliche Policies seien inhaltlich in jedem Punkt äquivalent?
- Selbst wenn in Certificate Policies unterschiedlicher PKIs die gleichen Festlegungen getroffen werden, stellt sich die Frage, ob sie auch dann als äquivalent angesehen werden können, wenn sich die zugehörigen Certification Practice Statements der einzelnen PKIs unterscheiden?

Für den praktischen Einsatz von Policy-Mapping werden deshalb allgemeine und klare Regeln benötigt. Sie müssen bestimmen, welche Parameter in welchen Toleranzen übereinstimmen müssen, damit

- Policy Mapping überhaupt beim Zertifizieren genutzt werden kann und
- die Mapping-Aussagen in verschiedenen Anwendungen bei der Zertifikatsprüfung *sinnvoll* verwendet werden können.

Für eine vertrauenswürdige Interdomain Cross-Zertifizierung wird es deshalb regelmäßig erforderlich sein, einen umfangreicheren Zertifizierungsprozess durchzuführen. In dessen Verlauf sind eine Vielzahl von Prüfungen und Abstimmungen vorzunehmen, wie z.B.:[4]

- Stimmen die geforderten Mindestschlüssellängen überein?
- Unterscheidet sich die maximale Gültigkeitsdauer der Zertifikate?
- Sind die Verfahren zur Auslieferung von Schlüsseln (Schlüsselträgern) und Zertifikaten vergleichbar sicher?
- Garantieren die bei CAs und RAs getroffenen Sicherheitsmaßnahmen in gleichwertiger Weise den Schutz der geheimen Schlüssel?
- Sorgen die Abläufe im Falle einer Sperrung (Erreichbarkeit des Sperrdienstes, Reaktionszeiten, Publikation von Rückruflisten) für ein einheitliches Sicherheitsniveau?
- Sind die Haftungsgarantien identisch?

Nur durch einen derartigen Detailvergleich der Festlegungen in CP und CPS ist eine hinreichende Äquivalenz von Policy-Elementen sicherzustellen.

Da Certification Practice Statements im allgemeinen nicht statisch sind, ist außerdem bei jeder Änderung eines CPS, einer Certificate Policy und einer Domain Policy zu prüfen, ob und welche Konsequenzen sich daraus für das Cross-Zertifikat ergeben. Es ist daher zu erwarten, dass die Verbindung zwischen unterschiedlichen Domains kontinuierlich beobachtet und gepflegt werden muss – und auch der Rückruf einer Cross-Zertifizierung bei einseitigen substantiellen Veränderungen eines CPS bzw. einer Certification Policy grundsätzlich nicht ausgeschlossen werden kann.

Mit der X.509-Konstruktion wird immer die gesamte Policy auf eine andere Policy abgebildet. Eine Alternative bestünde darin, einzelne Policy-Elemente mit einem Wert anzugeben. In der Prüffunktion könnte dann eine differenzierte Bewertung der einzelnen Elemente vorgenommen werden. Ob dies zu einer Vereinfachung des Vergleichs von Policies unterschiedlicher Zertifizierungsinstanzen führt, hängt dabei vor allem von der Zahl und der "diskreten" Darstellbarkeit der als relevant erachteten Parameter ab. Im Prinzip können alle Aspekte angesprochen werden, beispielsweise im Detaillierungsgrad von [RFC2527]. Im Standard X.509 wird eine solche "parameter-basierte" Variante bisher nicht unterstützt. Ein Vorschlag für XML findet sich in [GPS00].

4.4 Transitive Cross-Zertifizierung

Spezielle Probleme treten auf, wenn in einer Zertifikatkette mehrere Cross-Zertifikate enthalten sind. Durch Cross-Zertifikate können

- mehrere Zertifizierungshierarchien miteinander verknüpft werden. Hier stell sich die Frage, wie die entsprechenden Mapping-Regeln vom Client berücksichtigt werden sollen. Muss die cross-zertifizierende CA grundsätzlich mit **inhibitPolicyMapping** festlegen, dass nach dem von ihr ausgestellten Cross-Zertifikat keine weitere Mapping-Regeln mehr akzeptiert werden dürfen? Da mit weiteren Cross-Zertifizierungen die im Rahmen der ersten Cross-Zertifizierung durchgeführte Prüfung der Vertrauenswürdigkeit implizit wird, d.h. ohne Beteiligung der Partner-CA auf weitere PKIs ausgedehnt wird, erscheinen verkettete Cross-Zertifikate grundsätzlich problematisch.

4 Vgl. dazu auch die Vorschläge in [GCPKI99].

- Zertifizierungshierarchien "rückverknüpft" sein, wenn eine nachgeordnete CA einer cross-zertifizierten Zertifizierungshierarchie wiederum ein Cross-Zertifikat für die erste Zertifizierungshierarchie ausstellt (z. B. Pfad 11a, 6, 7, 16a in Abb. 1). Hier stellt sich die Frage, ob solche "Rückverknüpfungen" bei der Prüfung einer Zertifikatkette verwendet werden dürfen?

Die Begrenzung der Pfadlänge über die **basicConstraints** hilft dabei nur in einfachen Fällen (PKIs mit wenigen Hierarchieebenen). **nameConstraints** oder **inhibitPolicyMapping** nutzen nur etwas, wenn die anderen Zertifizierungshierarchien andere Namensräume bzw. auch weltweit einheitliche Policy-OIDs verwenden.

5 Konsequenzen für das Gültigkeitsmodell

Für die praktische Nutzung von Cross-Zertifikaten ist es wesentlich, dass die Prüffunktionen für Zertifikate in einzelnen Anwendungen die angeführten speziellen Attribute in Zertifikatketten mit Cross-Zertifikaten korrekt auswerten. Im folgenden werden Aspekte der Gültigkeitsprüfung von Zertifikatketten, die Cross-Zertifikate enthalten, angesprochen, die über Gültigkeitsprüfungen von "normalen" Zertifikaten hinausgehen.[5]

Dabei müssen grundsätzlich zwei Aufgaben gelöst werden:

- Zum einen ist die zur Prüfung zu verwendende Zertifikatkette zu bestimmen. Dies kann aus der Sicht des Signierenden wie auch des Prüfenden erfolgen.
- Zum zweiten muss der "Policy-Wert" des Prüfergebnisses festgestellt werden.
- Da bei Cross-Zertifikaten mehrere Zertifikate den gleichen öffentlichen Schlüssel bestätigen, können unterschiedliche Zertifikatketten geprüft werden. Will Tln1 aus Abb. 1 ausgehend von Root A das Zertifikat von Tln2 prüfen, kann er unterschiedlichen Pfaden des Zertifizierungsgraphen folgen (vgl. Abb. 3).

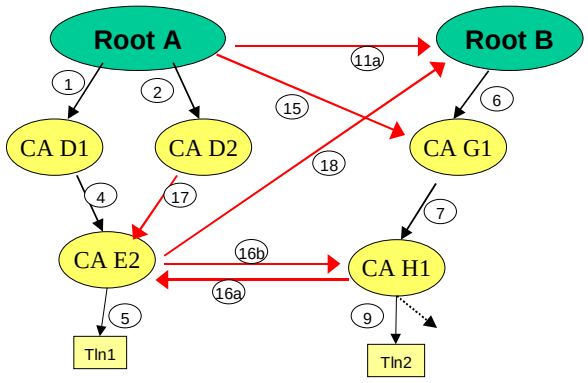

Abb. 3: Ausschnitt des Zertifizierungsgraphen aus Abb. 1 für die Prüfung von Tln2 durch Tln1. Ausgehend von Root A sind z.B. der Pfad 11a, 6, 7, 9, der Pfad 15, 7, 9, oder der Pfad 2, 17, 16b, 9 geeignet.

Der Austausch der Zertifikatkette kann allerdings zu unterschiedlichen Prüfergebnissen führen. Daher müssen Regeln definiert sein, nach denen "die richtige" Zertifikatkette ausgewählt wird. Die Entscheidung hierüber kann dem Signierenden wie auch dem Prüfenden obliegen.

5 Zu allgemeinen Prüfbedingungen siehe [ITUT-00], [RFC2459], den Draft des Folge-RFCs und [BSI00].

5.1 Bestimmen der Zertifikatkette durch den Signierenden

Soll sichergestellt werden, dass alle Prüfenden zum gleichen Ergebnis kommen, wie dies beispielsweise im Kontext des SigG gefordert ist, kann beispielsweise in jedem digital signierten Dokument[6] vom Signierenden ein Verweis auf das Zertifikat (oder die Zertifikate) angegeben werden, das (bzw. die) zum Prüfen zu verwenden ist (sind). Dies kann erreicht werden, indem der Signierende zum digital signierten Dokument ein Attribut wie **authorityKeyIdentifier** nach [ITUT00] mit den Angaben für **issuer** und **serialNumber** des Zertifikats der ausstellenden Zertifizierungsinstanz hinzufügt.[7] Die Prüffunktion muss dann genau die durch die Referenz bezeichneten Zertifikate für die Prüfung heranziehen.[8] Für Anwendungen, die einen hohen Beweiswert erbringen sollen, ist diese Variante dringend zu empfehlen.

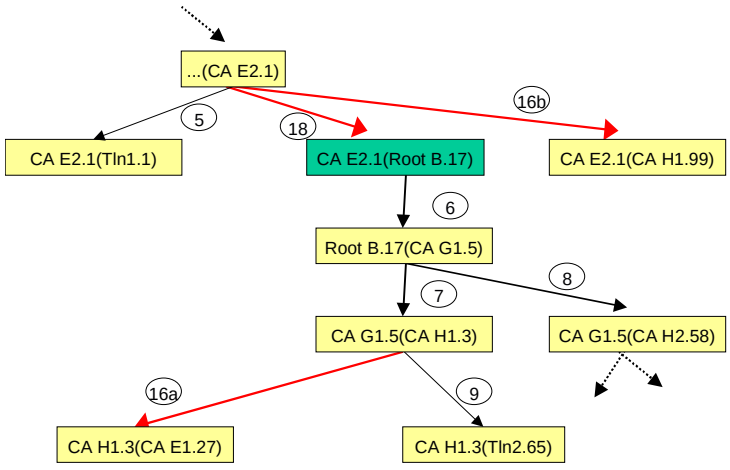

Abb. 4: Angenommene Zertifikat-Relation für einen Ausschnitt aus Abb. 1.
***Legende:** "CA H1.3(CA E1.27)" bedeutet Zertifikat von CA H1 für CA E1. Die Zahl nach dem Punkt vor der Klammer entspricht der Seriennummer des Zertifikats, auf das im Zertifikat verwiesen wird, die Zahl nach dem Punkt in der Klammer der Seriennummer des ausgestellten Zertifikats.*
Die Cross-Zertifikate (16a, 16b und 18) sind jetzt Teil eines Baums.

Da in diesem Fall Zertifikate beim Prüfprozess nicht ausgetauscht werden dürfen, stellt sich allerdings das Problem, ob und wie der Signierende die durch Cross-Zertifikate möglichen alternativen Zertifikatketten für den Prüfenden zulassen kann.

Die Verweise in Zertifikaten auf das jeweils übergeordnete Zertifikat bildet dabei die Zertifikat-Relation. Betrachtet man den Graphen der Zertifikat-Relationen in Abb. 3, hat der Tln2 nur ein Zertifikat (9). Nach den in SigI spezifizierten Anforderungen muss die Zertifizierungsinstanz im Teilnehmerzertifikat auf eines ihrer eigenen Zertifikate verweisen. Wenn nur das jeweils übergeordnete Zertifikat referenziert wird, legt die Zertifizierungsinstanz H1 fest, welche der Zertifikatketten weiter zu verfolgen ist. Beschränkt sich jede Zertifizierungsinstanz auf die Angabe *eines* übergeordneten Zertifikats, entsteht wieder ein baumartiger Graph (Abb. 4). Die Pfade in diesem Graphen sind für die Prüffunktion eindeutig, wenn letztere sich an die Verweise hält, die in den Zertifikaten eingeschlossen sind. Allerdings wird der für die Prüfung zulässige Pfad durch die Zertifizierungsinstanzen bestimmt: Aus der Sicht des Zertifikatsinhabers ist der Pfad mit der Ausstellung seines Zertifikats bereits festgelegt.

---

6 Darunter fallen auch Zertifikate.

7 Vgl. zu entsprechenden Vorschlägen [Ham95a] und [BSI99].

8 Vgl. z. B. [BSI00] und [HAM00].

Alternativ könnte der Signierende nicht nur das Teilnehmerzertifikat, sondern den gesamten Pfad (oder mehrere alternative) über entsprechende Verweise[9] im digital signierten Dokument festlegen. In diesem Fall würden die Zertifikatketten, die zum Prüfen verwendet werden dürfen, erst zum Signierzeitpunkt festgelegt. Sie würden außerdem vollständig *vom Signierenden* definiert. Dadurch entsteht für ihn einerseits eine größere Flexibilität, aber möglicherweise auch eine höhere Komplexität in der Anwendung von digitalen Signaturen.

5.2 Bestimmen der Zertifikatkette durch den Prüfenden

Ist die bei der Prüfung zu verwendende Zertifikatkette durch Signatur und Zertifikate nicht festgelegt und stehen dem prüfenden Empfänger unterschiedliche Zertifikate zur Verfügung, so muss (kann) er die Zertifikatkette selbst auswählen. Dazu kann er versuchen, den Zertifizierungsgraphen zu reduzieren, um eine möglichst einfache und kurze Zertifikatkette zu finden.[10] Welche Bedingungen dazu während des Traversierens des entstehenden Graphen herangezogen werden, hängt von den jeweils unterstützten Zertifikat-Attributen und dem Anwendungszweck ab.

- Zunächst werden die Zertifikate bestimmt, die in der transitiven Hülle der (gültigen) Wurzelzertifikate liegen, die selbst direktes Vertrauen genießen.
- Aus dieser Menge werden alle abgelaufenen Zertifikate, alle Zertifikate mit dem Status "revoked" oder "suspended" und solche, zu denen keine Statusinformation verfügbar ist, entfernt.
- Akzeptiert werden nur Zertifikate, die folgenden Bedingungen genügen:
  - das Zertifikat zum ausstellenden Schlüssel ist ein Zertifikat für die Zertifizierung ("**keyUsage**" = "**keyCertSign**" oder "**basicConstraints.cA**" = "**true**") und
  - die "**pathLenConstraint**" aller in der Kette enthaltenen Zertifikate wird eingehalten.
- In Zertifizierungsgraphen können Zyklen auftreten. Um in solchen Fällen ein Terminieren der Zertifikatsprüfung sicherzustellen, kann der Prüfvorgang abgebrochen werden, wenn ein Zertifikate in einer Kette zum zweiten Mal auftritt. Alternativ kann durch Längenbegrenzungen sichergestellt werden, dass die Prüfung der Zertifikatkette terminiert. Auch die Bedingung, dass ein nachgeordnetes Zertifikat nach dem Beginn des Gültigkeitszeitraums ("**notBefore**") des übergeordneten Zertifikats ausgestellt sein muss, kann ein Abbruchkriterium liefern.
- Bleiben nach Anwendung der angeführten Kriterien schließlich noch alternative Zertifikatketten für die Prüfung eines digital signierten Dokuments übrig, erfolgt die Auswahl einer Kette (sei es durch eine explizite Entscheidung des Prüfenden oder automatisch) nach einem der folgenden Kriterien:
  - minimale Länge der Kette,
  - "maximale Minimal-Policy", die von allen Zertifikaten erfüllt wird,
  - es wird kein Policy Mapping benötigt oder
  - "günstigste" Naming-Constraints.

---

9 Auch hierfür bieten sich **issuer** und **serialNumber** als eindeutige Referenzen an. Eine Folge von solchen Angaben würde dann alle Zertifikate der Kette bestimmen.

10 Siehe dazu auch einige Hinweise in [Zie96].

Die Ergebnisse einer solchen Analyse können teilweise wieder verwendet bzw. kontinuierlich fortgeschrieben werden. Dadurch sollte sich der Aufwand zumindest für die (halb-) automatische Auswahl einer geeigneten Zertifikatkette in vertretbarem Rahmen halten lassen.

5.3 Feststellen der Pfad-Policies

Im Rahmen der Prüfung einer Zertifikatkette muss eine "Gesamt-Policy" für die Kette bestimmt werden.[11] Durch alternative Zertifikatketten können sich dabei jedoch unterschiedliche Gesamt-Policies ergeben. Für das Gültigkeitsmodell muss daher grundsätzlich entschieden werden,

- ob alternative Gesamt-Policies zu bestimmen sind,
- welche der alternativen Gesamt-Policies für das Prüfergebnis berücksichtigt wird, also beispielsweise die minimale oder die maximale.
- ob so lange geprüft wird, bis eine Zertifikatkette gefunden wird, die einer der initial geforderten (Mindest-)Policies genügt.

Bei der Prüfung muss außerdem beachtet werden, auf welchem Niveau Mapping-Regeln angegeben werden. Beispielsweise muss der Prüfprozess erkennen, wenn eine CA mit einer niedrigen Policy ein weiteres CA-Zertifikat ausgestellt hat, in dem ein Mapping auf ein "höheres" Sicherheitsniveau festgelegt wurde.

Prüffunktionen dürfen diese Regeln allerdings nicht dauerhaft speichern, denn Policy-Mapping und policyConstraints sind insofern dynamisch, als sie mit der Sperrung oder dem Auslaufen der zugehörigen Zertifikate nicht mehr als Regeln gelten. Daher müssen sie sich in Abhängigkeit von der jeweils verwendeten Zertifikatkette über die Anwendbarkeit der Regeln vergewissern.

5.4 Prüfung im Schalenmodell

In diesem Abschnitt wird die Gültigkeitsdauer der Cross-Zertifikate im so genannten Schalenmodell betrachtet. Das "Schalenmodell" ist ein weit verbreitetes Gültigkeitsmodell, das bereits im PEM-Standard [RFC1422] beschrieben und in [RFC2459] erneut zu Grunde gelegt wurde. Die Gültigkeit von Schlüsseln und Zertifikaten ist in diesem Modell wie folgt definiert:

- Ein Schlüssel(-paar) ist zu einem bestimmten Zeitpunkt genau dann gültig, wenn zu diesem Zeitpunkt der zugehörige Zertifizierungspfad gültig ist.
- Ein Zertifizierungspfad ist zu einem bestimmten Zeitpunkt genau dann gültig, wenn alle in ihm enthaltenen Zertifikate zu diesem Zeitpunkt gültig sind.
- Ein Zertifikat ist zu einem bestimmten Zeitpunkt genau dann gültig, wenn
  - die Signatur des Zertifikates gültig ist,
  - der fragliche Zeitpunkt innerhalb des Gültigkeitszeitraums des Zertifikates liegt,
  - das Zertifikat in der zum Zeitpunkt der Prüfung aktuellen Sperrliste der ausstellenden Zertifizierungsstelle nicht oder mit einem späteren Sperrzeitpunkt enthalten ist.

[11] Siehe dazu die Algorithmen in [ITUT00] und [PKIX00].

Bezogen auf den Gültigkeitszeitraum der Zertifikate einer Kette ergibt sich damit, dass eine erfolgreiche Prüfung nur dann möglich ist, wenn der Zeitpunkt, für den die Prüfung durchgeführt wird, in der Schnittmenge aller Gültigkeitszeiträume der betroffenen Zertifikate liegt.

Um Problemen bei der Prüfung vorzubeugen, sollte eine der beiden folgenden Vorgehensweisen gewählt werden:

- Ein CA-Zertifikat, das ausläuft und noch gültige nachgeordnete Zertifikate besitzt, muss rechtzeitig verlängert werden. Das ausgelaufene Zertifikat kann dann im Prinzip in Zertifikatketten durch das neue Zertifikat ausgetauscht werden. Zwei Rahmenbedingungen müssen aber gelten: Zum einen muss das Schlüsselpaar beibehalten werden, weil sonst mit dem ausgetauschten Zertifikat das nachgeordnete nicht mehr erfolgreich geprüft werde kann.[12] Zum anderen dürfen eventuell in den Zertifikaten enthaltene Verweise auf übergeordnete Zertifikate (**authorityKeyIdentifier**) nur als Verweise auf den öffentlichen Schlüssel, nicht aber im Format "**Issuer**, **SerialNumber**" enthalten sein. Die Seriennummer referenziert nämlich genau das alte Zertifikat und verbietet damit den Austausch.
- Die Gültigkeitszeiträume der Zertifikate sind von der Wurzelinstanz zum Nutzerzertifikat "überdeckend", d. h., dass der Gültigkeitszeitraum des jeweils nachgeordneten Zertifikats später beginnt und früher endet als der des übergeordneten. Diese Anforderung an die Gültigkeitszeiträume wird gemäß [BSI00] auch von der RegTP empfohlen. Mit dieser Regel erübrigt es sich, Verlängerungzertifikate auszustellen, da die nachgeordneten Zertifikate eher auslaufen als die der übergeordneten Zertifizierungsinstanzen. Die Variante ist deshalb auch geeignet für Zertifikate mit Verweise auf übergeordnete Zertifikate (**authorityKeyIdentifier**) im Format "**Issuer**, **SerialNumber**".

In der zweiten Variante sollte das Cross-Zertifikat von A für B sinnvollerweise nicht über das Gültigkeitsende des Root-Zertifikats von A hinaus gültig sein, da eine (positive) Prüfung nach diesem Zeitpunkt im Schalenmodell nicht möglich wäre. Für das Crosszertifikat von B für A gilt dies entsprechend.

In der ersten Variante kann ein langer Gültigkeitszeitraum eines Cross-Zertifikats dagegen durch Verlängerungszertifikate für die Wurzel-Zertifizierungsinstanz sinnvoll genutzt werden, die eine Überprüfung des Cross-Zertifikats unter dem verlängerten Root-Zertifikat erlauben.

Die Gültigkeitsregel des Schalenmodells wird ebenfalls im PKIX Standard [RFC2510] berücksichtigt, in dem Cross-Zertifikate für einen Zertifikatswechsel einer Root-CA eingesetzt werden. Für die Cross-Zertifikate, die das alte und das neue Self-Signed-Zertifikat einer Root-CA verbinden, ergibt sich daraus, dass sie nur bis zum Ende des Gültigkeitszeitraums des ersten Wurzelzertifikats akzeptiert werden.

6 Sperrung von Cross-Zertifikaten

Cross-Zertifikate können, wie andere Zertifikate auch, gesperrt werden. Die Seriennummer des gesperrten Cross-Zertifikats wird dazu in den entsprechenden CRLs wie auch ARLs aufgenommen und erst gelöscht, wenn die Gültigkeit des Cross-Zertifikats abgelaufen ist.[13] Diese Möglichkeit ist ein wesentlicher Vorteil gegenüber einer direkten Anerkennung eines Root-

12 Eine solche "Zertifikatsverlängerung", d. h. die Ausstellung eines neuen Zertifikats mit geändertem Gültigkeitszeitraum zu einem bereits genutzten Schlüsselpaar ist in vielen heute erhältlichen CA-Lösungen nicht vorgesehen.

13 Auf Differenzierungsmöglichkeiten, die nach [ITUT00] gegenüber diesen Basis-Listen möglich sind, kann an dieser Stelle nicht eingegangen werden.

Zertifikats (oder eines CA-Zertifikats) einer anderen Domain durch den Nutzer. Im letzteren Fall muss jener nämlich nicht nur die Informationen seiner primären Domain, sondern auch die der anderen darauf hin verfolgen, ob der Root-Schlüssel zurück gerufen wurde. Im Falle von Cross-Zertifikaten sollte diese Prüfung von der primären Domain durchgeführt werden und gegebenenfalls zu einem Rückruf des Cross-Zertifikats führen.

Wie bereits erwähnt, müssen unter anderem wegen der Möglichkeit eines Zertifikat-Rückrufs die Zertifikatkette und ihre Policy während der Gültigkeitsprüfung jeweils neu bestimmt oder zumindest überprüft werden. Treten in der Zertifikatkette Cross-Zertifikate auf, müssen darüber hinaus die folgenden weiteren Fälle berücksichtigt werden:

- In einer strikten Baum-Hierarchien ist es möglich, durch die Sperrung eines übergeordneten Zertifikats die gesamte Teilhierarchie implizit mit zu sperren.[14] Dies ist insbesondere als Reaktion auf eine Schlüsselkompromittierung eines CA-Schlüssels sinnvoll. Mit Cross-Zertifikaten existieren jedoch mehrere Zertifikate für ein Schlüsselpaar. Daraus ergeben sich im Falle einer Sperrung Probleme:
  - Zur Sperrung berechtigte Stellen müssen entscheiden, ob sie das Schlüsselpaar für alle Anwendungen sperren oder ob sie lediglich ein einzelnes Zertifikat sperren lassen wollen. Im ersten Fall muss die Zertifikatverwaltung (oder ein Service Provider) eine Übersicht über die existierenden Zertifikate zu einem Schlüssel haben.
  - Für Zertifikate von Zertifizierungsinstanzen kann es im Zertifizierungsgraphen "Umwege" um gesperrte Knoten herum geben, die trotz Zertifikatsperrung eine gültige Zertifikatkette liefern. Soll eine Teilhierarchie eines Zertifizierungsbaums gesperrt werden, beispielsweise weil in einer Zertifizierungsinstanz schwerwiegende Unregelmäßigkeiten aufgetreten sind (sei in Abb. 3 die CA G1 "compromised"), muss der Graph auf weitere gültige Zertifikatketten untersucht werden. Dazu ist es erforderlich, dass einer geeigneten Stelle die Informationen über alle Zertifizierungsrelationen zur Verfügung stehen. Diese kann entweder die notwendigen Sperrungen selbst veranlassen oder alternativ alle Zertifizierungsinstanzen des Graphen geeignet informieren, so dass diese ihrerseits die Zertifikate sperren, die sie beispielsweise für die CA G1 ausgestellt haben.
- Für die Sperrung von Zertifizierungsinstanz-Zertifikaten werden Regeln benötigt, die festlegen, wie weit die Sperrung transitiv "weitergegeben" werden muss, also welche der CA G1 im Graphen nachgeordneten Zertifikate ebenfalls zu sperren sind. Etwa könnte es bei Schwachstellen in der Schlüsselgenerierung notwendig sein, auch alle weiteren Zertifikate für die von CA G1 erzeugten Schüssel zu sperren, während im Fall von Schlüsseln, die von einer nachgeordneten Zertifizierungsinstanz oder den Nutzern selbst erzeugt wurden, nur die von CA G1 ausgestellten Zertifikate, nicht aber Mehrfachzertifikate anderer Zertifizierungsinstanzen zu sperren wären.

Konzepte, die diese im Rahmen der Gültigkeitsprüfung anfallenden Aufgaben auf den Prüfenden verlagern, dürften die Effizienz von PKI-Anwendungen wesentlich verringern und die Nutzer erheblich überfordern.

Eine weitere wichtige Rahmenbedingung soll an dieser Stelle nicht unerwähnt bleiben: Die Sperrlisten der cross-zertifizierten Domain müssen auch den Teilnehmern der jeweils ande-

---

14 Hier unterscheiden sich allerdings verschiedene Gültigkeitsmodelle, vgl. z. B. [RFC2459] im Unterschied zu [BSI00]. Zur Forderung nach differenzierten Sperrstrategien siehe [Ham99, 536 ff.].

ren Domains zugänglich gemacht werden. Dazu sind entweder Leserechte für die betroffenen Directories einzurichten oder aber geeignete Replikationsmechanismen aufzusetzen.

7 Praxisbeispiele

Hinsichtlich der Erzeugung und Bereitstellung von Cross-Zertifikaten sollten in der Praxis keine Hürden mehr zu erwarten sein. Für Prüffunktionen kann sich ein etwas anderes Bild ergeben, wenn der Zugriff auf Cross-Zertifikate über das oben genannte Attribut [DF2]und die Verarbeitung der notwendigen Extensions in Client-Komponenten noch nicht unterstützt wird.

Beispiele für produktiv eingesetzte Cross-Zertifikate lassen sich derzeit nur wenige finden:

- Auf der Basis von PGP wurde von einigen Zertifizierungsinstanzen eine Cross-Zertifizierung durchgeführt, z. B. der DFN-PCA, der c't-CA und TC Trustcenter.[15]
- In der Literatur wird gelegentlich unter dem Stichwort "Cross-Zertifikat" auch die Verknüpfung von Root-Schlüsseln einer Zertifizierungshierarchie verstanden (Abb. 1 Kante 13). Praktisch umgesetzt wurde dieses Verständnis von der Regulierungsbehörde für Telekommunikation und Post in der PKI nach SigG. Dabei wechseln sogar die Namen der Wurzel-Zertifizierungsinstanzen, obwohl der Betreiber gleich bleibt.[16]
- Die Sphinx-PCA beabsichtigt, Cross-Zertifikate anzubieten.
- Die Bridge-CA[17] der Deutschen Bank, Telesec und TeleTrust Deutschland e.V. plant, in einer späteren Projektphase ebenfalls CAs der beteiligten Unternehmen und Behörden über Cross-Zertifikate mit der Bridge-CA zu verbinden.

Inwieweit andere Akteure Cross-Zertifikate einsetzen werden, wird sich im Laufe der Zeit zeigen.

Im Unterschied dazu wird mit der PCA-1-Verwaltung des BSI ein hierarchisches Zertifizierungsmodell für nachgeordnete CAs von Bundeseinrichtungen, Ländern und Kommunen verfolgt. Für diesen Anwendungsbereich wird gegenwärtig ein Verzeichnisdienstkonzept entwickelt, das wertvolle Erfahrungen für die Directory-Integration im Kontext von Cross-Zertifizierung liefern wird.

In Kanada haben verschiedene Behörden ihre Public Key Infrastrukturen mit der "Government of Canada PKI" cross-zertifiziert,[18] unter anderem "Health Canada", die "Royal Canadian Mounted Police", das "Department of Foreign Affairs and International Trade" und "Public Works". Für zwei weitere PKIs wird der Prozess der Cross-Zertifizierung gegenwärtig durchgeführt. Dies sind "Industry Canada" und "Canada Customs and Revenue Agency".

In den USA wurde im Rahmen eines Demonstrations-Projekts zu einer "US DOD Bridge Certification Authority" gezeigt, dass Cross-Zertifizierung und Directory-Integration mit dem

---

15 Vgl. www.pca.dfn.de/dfnpca/certify/pgp/infrapgp.html oder www.heise.de/ct/pgpCA/keys.s-html#xcert. Die Cross-Zertifikate beziehen sich allerdings teilweise auf nicht mehr verwendete Schlüsselpaare.

16 Vgl. z. B. die Zertifikate für "4R-CA" und "5R-CA", abrufbar unter www.regtp.de bzw. www.nrca-ds.de.

17 Vgl. Homepage der Bridge CA Initiative: www.brigde-ca.org

18 Laut E-Mail vom 18.12.2000.

Stand der Technik realisierbar sind ([USBCA01]). Für die ausgewählten Produkte des Projekts konnte Interoperabilität nachgewiesen werden.

8 Ausblick

Dem Thema Cross-Zertifizierung wurde bisher nur unzureichend Beachtung geschenkt. Cross-Zertifikate bieten die Möglichkeit, unabhängige Zertifizierungshierarchien zu verknüpfen, Pfade in Zertifizierungshierarchien zu optimieren, Wurzelzertifikate einer Root zu verketten und gegebenenfalls in Störfällen Handlungsvarianten zur Begrenzung des Schadens[19] zu eröffnen. Bezüglich der Verknüpfung unabhängiger Zertifizierungshierarchien konkurriert der Ansatz mit übergeordneten Roots, die eine einheitliche Policy durchsetzen, sowie dem Ansatz der individuellen Anerkennung unabhängiger Wurzel-Zertifizierungsinstanzen.

Interdomain-Cross-Zertifikate können nur unter bestimmten Bedingungen von einem Nutzer erkannt werden. Daraus ergeben sich zwei Konsequenzen:

- Zum einen wird Zertifizierungsinstanzen empfohlen, eine geeignete Kennzeichnung von Cross-Zertifikaten vorzunehmen.
- Zum anderen sollten Client-Implementierungen die Auswertung der relevanten Attribute unterstützen und dem Nutzer die Möglichkeit geben, einen "Domain-Wechsel" zu erkennen und ggf. zu unterbinden, wenn er dies möchte. Denkbar wäre beispielsweise auch, dafür in Cross-Zertifikaten eine private Extension zur Markierung der Domain-Grenze einzusetzen. Dieses Attribut muss dann allerdings auch von den Clients unterstützt werden.

Wenn eine Zertifizierungsinstanz ein Interdomain Cross-Zertifikat ausstellt, hat sie die prinzipielle Möglichkeit, darin (genauer: über ihre Policy oder das CPS) Zusicherungen und Verpflichtungen für die Nutzer der cross-zertifizierten Domain auszudrücken, ohne dass die Nutzer zugestimmt hätten. Auf diese Zusicherungen könnten andere Nutzer fälschlich vertrauen. Für solche Fälle muss sichergestellt sein, dass der Aussteller des Cross-Zertifikats die Verantwortung trägt. Zu klären wäre daher, ob das bestehende Haftungsrecht und die geplanten Regelungen im novellierten SigG dieses Problem hinreichend abdecken.

Die bisher nur geringe Nutzung von Cross-Zertifikaten ist nicht zuletzt auch darin begründet, dass noch eine Reihe von organisatorischen, rechtlichen und technischen Problemen zu lösen sind. Cross-Zertifizierung wird jedoch in naher Zukunft an Bedeutung gewinnen, sobald die Verbreitung von "PKI-Insellösungen" zunimmt, nicht zuletzt weil dadurch auch der Business-Value der bereits etablierten Lösungen steigt.

Bis dahin sollten die in diesem White Paper angesprochenen Aspekte der Cross-Zertifizierung jedoch noch weiter untersucht und für ein gemeinsames Verständnis dieser Problematik unter Policy-Verantwortlichen, Entwicklern von PKI Komponenten und Nutzern gesorgt werden. Dieses gemeinsame Verständnis ist Voraussetzung für begründete Cross-Zertifizierung und damit mittelbar notwendig, damit das gewünschte hohe Vertrauen in PKI-Leistungen erreicht bzw. erhalten werden kann.

19 [Ham99, 536 ff.].

Anhang A: Praktische Aspekte

In diesem Anhang werden einige Anforderungen an CA- und Client-Komponenten beschrieben, die diese zur Unterstützung von Cross-Zertifikaten erfüllen sollten. Ferner werden praktische Schwierigkeiten skizziert, die bei Produktevaluierungen im Rahmen unterschiedlicher Projekte aufgefallen sind.

A.1 Anforderungen an CA-Komponenten

CA-Komponenten müssen folgende Anforderungen erfüllen, um Cross-Zertifikate ausstellen zu können und für ihre Anwender nutzbar zu machen:

- Die eingesetzten CA-Produkte sollten die Generierung eines (self-signed) Zertifizierungsrequest (**CertReqest**) im PKCS#10-Format unterstützen.
- Die eingesetzten CA-Produkte sollten PKCS#10-Requests verarbeiten können.
- Falls CAs Informationen über zurückgerufene Zertifikate bereitstellen sollen, muss hierfür ein Konzept entwickelt werden, das allen Client-Komponenten den Zugriff auf die Rückrufinformationen ermöglicht.
- Der Sicherheitsanker ist auszutauschen, wenn
  - vom Feld **pathLenConstraint** der Zertifikatsweiterung **BasicConstraints** Gebrauch gemacht wurde, um die Länge des Zertifizierungspfades zu begrenzen und
  - der Wert im Feld **pathLenConstraint** nicht mindestens so groß ist wie die maximale Tiefe des durch die Cross-Zertifizierungen entstehenden Zertifizierungsbaums.
- CAs, die in den von ihnen ausgestellten Zertifikaten von der Erweiterung **AuthorityKeyIdentifier** Gebrauch machen und auf ihr Zertifikat durch Angabe von Aussteller und Seriennummer verweisen, müssen zusätzliche nachgeordnete Zertifikate neu ausstellen, die einen Verweis auf das Cross-Zertifikat enthalten. Nur so ist eine Prüfung der Zertifikatkette über ihr Zertifikat hinaus mittels des Cross-Zertifikats möglich (vgl. Kapitel 5.1 und 5.4).

A.2 Anforderungen an Client-Komponenten

Für Client-Komponenten, die Cross-Zertifikate unterstützen sollen, ergeben sich die folgenden Anforderungen:

- Der Client sollte unterschiedliche Zertifikatsformate zum Import unterstützen (z.B. Direktes Zertifikat, p7-Format, Mehrfach-Zertifikate im p7-Format)
- Die Suchstrategie für die Suche nach Zertifikaten (und CRLs) sollte einstellbar sein.

Clients, die Zertifikatketten prüfen sollen, die ein Cross-Zertifikat enthalten, benötigen die Sperrlisten aus den beiden (und ggf. weiteren) Domänen, die durch die Cross-Zertifikate verknüpft wurden. Sperrlisten werden üblicherweise über Directories bereitgestellt. Häufig stößt aber die externe Nutzung von Directories über Domänen-Grenzen hinweg aus unterschiedlichen Gründen auf größere Probleme als die "eigentliche" Cross-Zertifizierung, denn

- Unternehmens-Directories enthalten in der Regel nicht nur Zertifikate und Sperrlisten, sondern sensible unternehmensinterne Daten, die nicht von extern zugänglich sein sollen. Daher ist eine Konfigurationen oder Replikation des Directories erforderlich, die nur ausgewählte Inhalte sichtbar macht.

- der Zugriff der Client-Komponenten im Rahmen der Zertifikatsprüfung auf externe Directories stellt zusätzliche Anforderungen an deren Verfügbarkeit. Auch hier können Replikationslösungen sinnvoll sein.
- die Schaffung eines externen Zugangs zu einem unternehmensinternen Directory erfordert eine geeignete Konzeption und Konfiguration der Sicherheitskomponenten (Protokollfreigaben, Replikation in DMZ etc.).

Ist eine geeignete Kopplung von Directories noch nicht erfolgt, müssen folgende Voraussetzungen erfüllt sein, damit ein reibungsloser Zugriff der Clients auf Sperrinformationen möglich ist:

- Die Clients können auf alle relevanten Directories zugreifen. Für unterschiedliche Domänen bedeutet dies in der Regel, dass sie über Firewalls hinweg zugänglich sind.
- Die eingesetzten Client-Produkte erlauben die Konfiguration und den parallelen Zugriff auf mehrere Directories.

A.3 Praktische Schwierigkeiten

Mit Cross-Zertifikaten erhöhen sich die Anforderungen an die Verwaltung von Zertifikaten durch den Client, denn für die Schlüssel der Wurzel-Zertifizierungsinstanzen existieren nun nicht nur self-signed Zertifikate, sondern auch die Cross-Zertifikate. Diese Zertifikate können in S/MIME-Nachrichten mitgeschickt werden. Clients müssen die Zertifikat-Typen für den gleichen Inhaber (Distinguished Name) geeignet unterscheiden können und dürfen sie beispielsweise nicht in einer lokalen Zertifikat-Datenbank ersetzten. Auch darf der Nutzer nicht durch die vermeintliche "Doppelung" eines Schlüssels dazu verleitet werden, Wurzelzertifikate zu löschen.

Weitere Probleme können auftreten, wenn in Zertifikaten die Erweiterung **authorityInformationAccess**[20] enthalten ist und die eingetragene Adresse einen Servernamen enthält. In diesem Fall muss der angegebenen Server extern zugänglich sein, da Clients sonst nicht auf die dort bereitgestellten CA-Zertifikate und Sperrlisten zugreifen können. Zudem wird diese Zertifikatserweiterung bisher nur von wenigen CA-Produkten[DF3]unterstützt.

Ferner ist zu beachten, dass einige Client-Komponenten im Rahmen der Gültigkeitsprüfung eines Zertifikats, in dem eine explizite Policy ausgewiesen ist, prüfen, ob diese Policy durch den Nutzer akzeptiert wurde. Hierbei besteht das Problem, dass sich durch die Cross-Zertifizierung der Zertifizierungspfad ändern kann. So können Zertifizierungspfade entstehen, bei denen einige, aber nicht alle Zertifikate Policy-OIDs ausweisen. Auf den betroffenen Client-Komponenten führt dies in der Regel dazu, dass das Prüfergebnis für solche Zertifizierungspfade stets negativ ist.

Um dies zu vermeiden, müssten die betroffenen Client-Komponenten alle Nutzer-Zertifikate, bei denen der Zertifizierungspfad ungültig geprüft wird, als vertrauenswürdig anerkennen. Leider relativiert sich dadurch der wesentliche Vorteil der Cross-Zertifizierung, dass nur dem Wurzelzertifikat vertraut werden muss. Das Verhalten der Prüfprozeduren der Client-Komponenten sollte bei der Entscheidung darüber, ob bzw. welche OIDs in die von den cross-zertifizierenden CAs ausgestellten Zertifikate eingetragen werden, wenn möglich berücksichtigt werden, um die Probleme zu vermeiden.

20 In [RFC2459] definiert.

Literatur

[BSI00] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2000): *Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV - SigI Abschnitt A6 Gültigkeitsmodell*, BSI, Bonn 2000, Version 1.1a.

[BSI99] Bundesamt für Sicherheit in der Informationstechnik (1999): *Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV - SigI Abschnitt A2 Signatur*, BSI, Bonn, 1999, Version 6.1.

[GCPKI99] Government of Canada Public Key Infrastructure (2000): *Cross-Certification Methodology and Criteria*, Draft, Version of September 22, 1999; http://www.cio-dpi.gc.ca/pki/Documents/documents_e.html.

[GPS00] Greuer-Pollmann, C. / Schweitzer, N. (2000): *Vergleichbarkeit von Policies mittels XML*, DuD 10/2000, 578 ff.

[Ham00] Hammer, V. (2000): *Signaturprüfungen nach SigI*, DuD 2/2000, 97 ff.

[Ham95a] Hammer, V. (1995): *Digitale Signaturen mit integrierter Zertifikatkette – Gewinne für den Urheberschafts- und Autorisierungsnachweis*, in: Brüggemann, H. H. / Gerhardt-Häckl, W. (Hrsg.): Verläßliche IT-Systeme – Proceedings der GI-Fachtagung VIS '95, Braunschweig/Wiesbaden, 1995, 265 ff.

[Ham95b] Hammer, V. (1995): *Vor- und Nachteile von Mehrfachzertifikaten für öffentliche Schlüssel*, in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Fachvorträge 4. Deutscher IT-Sicherheitskongreß 1995, Bonn, 1995.

[Ham99] Hammer, V. (1999): *Die 2. Dimension der IT-Sicherheit – Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen*, Braunschweig/ Wiesbaden, 1999.

[HaP01a] Hammer, V. / Petersen, H. (2001): *Aspekte der Cross-Zertifizierung*, in: Proceedings der Arbeitskonferenz Kommunikationssicherheit 2001, P. Horster (Hrsg.), DuD-Fachbeiträge, Vieweg-Verlag, 2001, S.192 ff.

[HaP01b] Hammer, V. / Petersen, H. (2001): *Aspekte der Cross-Zertifizierung*, in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Tagungsband 7. Deutscher IT-Sicherheitskongreß des BSI, 2001, S.281 ff.

[Herf99] Herfert, M. (1999): *Crosszertifizierung nach Wechsel des Sicherheitsankers einer Public-Key Infrastruktur*, in: Beiersdörfer, K. / Engels, G. / Schäfer, W.: Informatik überwindet Grenzen – Jahrestagung der Gesellschaft für Informatik 1999, Berlin, Heidelberg, 1999, 119 ff.

[ITUT00] International Telecommunication Union – Telecommunication sector (2000): *ITU-T X.509 – Draft Recommendation X.509 – Information Technology – Open Systems Interconnection – The Directory: Authentication Framework* (= ISO/IEC 9594-8), 2000

[PKIX00] Housley, R. / Ford, W. / Polk, W. / Solo, D.: *Internet X.509 Public Key Infrastructure – Certificate and CRL Profile*, November 2000, in "draft-ietf-pkix-new-part1-03.txt" z.B. unter ftp.nordu.net/internet-drafts

[RFC2422] Kent, S., (1993): *RFC 1422 – Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management*, Februar 1993

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

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

[RFC2527] Chokhani, S. / Ford, W. (1999): *RFC 2527 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*

[SigI98] Bundesamt für Sicherheit in der Informationstechnik: *Schnittstellenspezifikation für die Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV*, 1998-2000.

[USBCA01] US DOD: *Bridge Certification Authority Final Report*, http://www.anassoc.com/BCA.html.

[Zie96] Zieschang, T. (1996): *Security Properties of Key Certification Infrastructures*, in: Horster, P. (Hrsg.): Digitale Signaturen – Grundlagen, Realisierungen, Rechtliche Aspekte, Anwendungen, Braunschweig/Wiesbaden, 1996, 109 ff.