DuD
Datenschutz und Datensicherheit

Cross-Zertifikate verbinden

Volker Hammer

Einzelne Zertifizierungshierarchien bilden noch keine effiziente Infrastruktur für Public Key Anwendungen. Über Cross-Zertifikate können bislang getrennte Domains aber verbunden werden. Der Beitrag gibt eine kurze Einführung in Cross-Zertifikate, ihre Verwendungsmöglichkeiten und Fragestellungen bei ihren Einsatz.[1]

Dr.
Volker Hammer

Secorvo Security Consulting GmbH.
Arbeitsschwerpunkt: Public Key Infrastrukturen, digitale Signaturen, Anforderungsanalyse, Technikgestaltung
E-Mail: hammer@secorvo.de

[1] *Der Aufsatz ist eine gekürzte Fassung von [HaPe01].*

1 Einleitung

Gegenwärtig werden Public Key Infrastrukturen in Insellösungen (einzelnen Domains) aufgebaut und in ersten produktiven Anwendungen eingesetzt. Es ist aber absehbar, dass der Aufwand zur Zertifizierung und Zertifikatverwaltung zu hoch ist, um immer alle möglichen Teilnehmer und Partner einer Domain innerhalb dieser Domain selbst zu zertifizieren. Vielmehr versprechen Verknüpfungen der „Inseln“ mit Hilfe von Cross-Zertifikaten erhebliche Synergieeffekte und dementsprechend einen höheren Business-Value für die PKI Anwendungen. Auch wenn zwei Unternehmen mit jeweils eigener Zertifizierungshierarchie fusionieren, können Cross-Zertifikate eine Möglichkeit zur Verknüpfung bieten. Vor einer Cross-Zertifizierung ist jedoch die Frage zu beantworten, ob das Vertrauen, das mit Cross-Zertifikaten ausgesprochen wird, auch domainübergreifend gerechtfertigt ist. Die „Antworten“ auf diese Frage sind technisch abzubilden. Schließlich müssen Prüffunktionen Cross-Zertifikate verwenden können.

Cross-Zertifikate werden im Standard X.509 definiert und in PKIX sowie einigen Internet Drafts angesprochen [ITUT00, PKIX99a, PKIX99b].

2 Grundlagen

2.1 Cross-Zertifikate und andere Zertifikat-Typen

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:

- Die Zertifizierungsinstanz-Relation: „Issuer zertifiziert Subject“. Die in der Menge der Zertifikate enthaltenen Paare (*issuer dn, subject dn*) bestimmen einen Graphen. In „klassischen“ Zertifizierungshierarchien bildet dieser einen Baum. Dieser Relation liegt in der Regel die Vorstellung der rechtlich-organisatorischen Zuständigkeiten zugrunde.
- Die Zertifizierungsrelation: „Schlüssel X wird zum Prüfen des Zertifikats Y benötigt“. In der Struktur des entsprechenden Graphen kann allerdings jede Kante im Graphen der Zertifizierungsinstanz-Relation aus mehreren Kanten bestehen.

Cross-Zertifikate beeinflussen die Struktur beider Graphen.

Öffentliche Schlüssel können – wie der Name sagt – als öffentliche Informationen verwendet werden. Sie können daher in mehr als einem Zertifikat bestätigt werden. Ist dies der Fall, kann allgemein von Mehrfachzertifikaten für einen öffentlichen Schlüssel gesprochen werden [Ham95a, Ham95b].

Beispiele für Mehrfachzertifikate sind:

- **Verlängerungszertifikate**: es unterscheiden sich nur Gültigkeitszeitraum, Seriennummer und Signatur.
- **Austauschzertifikate**: *issuer dn*, *subject dn* und bestätigter öffentlicher Schlüssel sind gleich, aber alle anderen Attributwerte können sich ändern.
- **Cross-Zertifikate**: Ein öffentlicher Schlüssel wird bereits durch eine Zertifizierungsinstanz bestätigt (primäre Zertifizierungsrelation).[2] Zu diesem öffentlichen Schlüssel stellt eine Zertifizierungsinstanz mit anderem *issuer dn* als das der primären Zertifizierungsinstanz ein weiteres Zertifikat, ein Cross-Zertifikat, aus. Der Sonderfall, dass die primäre Zertifizierungsinstanz ihren Namen wechselt und daraufhin neu zertifiziert, wird eingeschlossen.

Während mit Verlängerungszertifikaten und Austauschzertifikaten eine bestehende Baumstruktur der Zertifizierungsinstanz-Relation erhalten bleibt, entstehen mit Cross-Zertifikaten beliebige Graphen für diese Struktur. Cross-Zertifikate liegen nach

[2] [ITUT00, Kap. 7] 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 Beitrags die oben angegebenen engere Definition verwendet.

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 ein Zertifikat ausgestellt werden kann, das diesen Schlüssel enthält.

2.2 Verwendungsmöglichkeiten für Cross-Zertifikate

Für Cross-Zertifikate nach der obigen Definition können zwei vorrangige Verwendungszwecke identifiziert werden.

Verknüpfung von Zertifizierungshierarchien: Der geläufigste Zweck ist die Verknüpfung von Zertifizierungshierarchien, insbesondere auf der Ebene der Wurzel-Zertifizierungsinstanzen. Die beiden Root-CAs können sich gegenseitig Zertifikate ausstellen. 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 die Wurzel-Zertifizierungsinstanz einer anderen Zertifizierungshierarchie bestätigt, wenn diese bereits über ein Selbstzertifikat verfügt.

Verkürzungen von Zertifikatketten: Es können sich auch nachgeordnete Zertifizierungsinstanzen der gleichen oder unterschiedlicher Domänen cross-zertifizieren. Dadurch können sowohl innerhalb einer Zertifizierungshierarchie als auch zwischen Zertifizierungshierarchien zusätzliche „Wege“ erzeugt werden. Die entstehenden „Querverbindungen“ können zu kürzeren Zertifikatketten z.B. für Signaturprüfungen führen [ITUT00, Kap. 18.2.1].

2.3 Aufbau, Erzeugung und Bereitstellung von Cross-Zertifikaten

Cross-Zertifikate sind nach X.509 „Standard“-Zertifikate. Sie können allerdings bestimmte Extensions enthalten, um ihre Verwendung zu steuern:

- **policyMappings**: als **SEQUENCE OF {issuerDomainPolicy, subjectDomainPolicy}.** Semantik: Der Issuer des Cross-Zertifikat erklärt, dass die issuerDomainPolicy äquivalent zur subjectDomainPolicy ist.

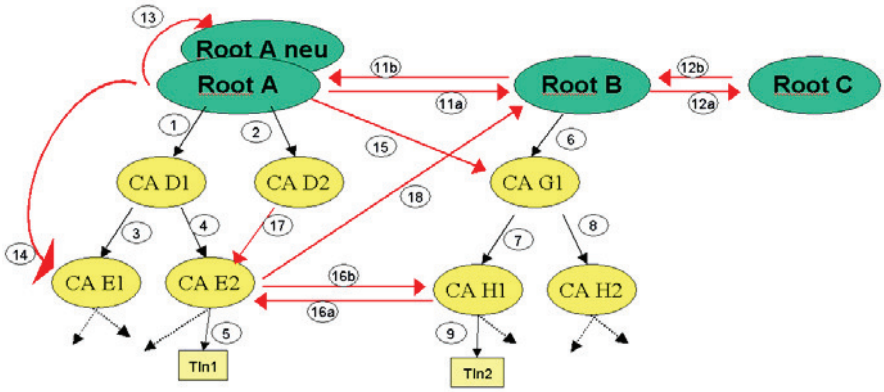

Abb. 1: Graph einer Zertifizierungsinstanz-Relation. Cross-Zertifikate haben Kantennummern >= 1.

- **policyConstraints:** steuern, ob und ab welcher Position in der zu prüfenden Zertifikatkette Policies ausgewiesen (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. 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 Erzeugung nur Lösungen in Frage, die auf einer Übertragung des öffentlichen Schlüssels an die CA beruhen. Es können bspw. Zertifikat Management Protokolle nach PKIX (CMP, CMC) oder PKCS# 10 / PKCS# 7 verwendet werden.

Cross-Zertifikate können über Directories bereitgestellt oder direkt in Nachrichten mit versandt werden. Im Directory ist in Einträgen von Zertifizierungsinstanzen (jetzt ObjectClass **pkiCA**, [ITUT00, Kap. 11.1.2]) ein Attributtyp „**crossCertificatePair**“ vorgesehen. Dieser kann Vorwärts- und Rückwärts-Cross-Zertifikate enthalten. Im Directory können daher beide CA-Einträge jeweils beide Zertifikate enthalten.

3 Aspekte beim Ausstellen von Cross-Zertifikaten

Die Informationen in Zertifikaten sind insbesondere unter dem Blickwinkel des Sicherheitsniveaus zu betrachten, unter dem die Zertifizierungshierarchie betrieben wird. Dabei können in einer Zertifizierungshierarchie durchaus unterschiedliche Sicherheitsklassen definiert sein, die durch Policy-Angaben unterschieden werden. Die Menge der Sicherheitsklassen einer Zertifizierungshierarchie und die Regeln für Ihre Verwendung wird im folgenden als Domain-Policy bezeichnet.

An dieser Stelle wird angenommen, dass für zwei 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 Zertifikat-User) über Clients verfügen, die die jeweilige Domain-Policy beherrschen.

Im folgenden werden einige Aspekte diskutiert, die beim Einsatz von Cross-Zertifikaten beachtet werden sollten.

3.1 Notwendigkeit von Cross-Zertifikaten

Alternativ zum Einsatz von Cross-Zertifikaten mit Angaben zum Policy Mapping könnten übergeordnete Roots für bestimmte Sicherheitsklassen gebildet werden (entspricht dem PEM-Modell von PCAs). Möglicherweise ist dies der pragmatischere und anwenderfreundlichere Ansatz. Als weitere Alternative kann der Anwender in seiner

Prüffunktion mehrere unabhängige Wurzelzertifikate als Sicherungsanker aufnehmen.
Die Wahl zwischen diesen drei Verknüpfungsmöglichkeiten von Zertifizierungshierarchien oder ihre geschickte Kombination unterliegt vielen Einflussfaktoren. 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 nach Hierarchien kontrollieren. Der Preis dafür ist allerdings, dass sie Wurzelzertifikate „manuell" prüfen und das jeweilige CPSs selbst bewerten müssen. Im Falle von Cross-Zertifikaten übernimmt dies ihre Root für sie. Ob dadurch allerdings das Verständnis der entstehenden Zertifizierungsgraphen für die Teilnehmer und ihr Vertrauen in die PKIs erhöht wird, muss sich erst zeigen.

3.2 Interdomain-Vertrauen

Eine der technischen Umsetzung vorgelagerte Fragestellung ist, inwieweit die Teilnehmer Interdomain Cross-Zertifikaten vertrauen müssen. Schließlich könnte der Teilnehmer zum Zeitpunkt seines Eintritts in eine PKI annehmen wollen, dass er sich mit der Anerkennung des Wurzelzertifikats „seiner" PKI auch nur in deren Domain bewegt und Zertifikate anderer Domains ausgeschlossen sind. Grundsätzlich können hier zwei Positionen bezogen werden:

- Nach der einen Position delegiert der Teilnehmer Vertrauen weitgehend: Da der Teilnehmer einer bestimmten Vertrauens-Domäne beitritt und die Policy der Wurzel-Zertifizierungsinstanz anerkennt, muss er auch akzeptieren, dass die Zertifizierungsinstanzen Interdomain Cross-Zertifikate ausstellen, wenn sie sich an die Policy halten und hinreichende Policy-Äquivalenz zwischen den Domains sicherstellen.
- Nach der zweiten Position will der Teilnehmer die Vertrauensgewährung selbst kontrollieren. In diesem Fall würde er die Crosszertifizierung nicht unbesehen akzeptieren, sondern unter den Vorbehalt einer expliziten Anerkennung der anderen Domain stellen, sich gegebenenfalls sogar eine Entscheidung für einzelne Teilnehmerzertifikate vorbehalten.

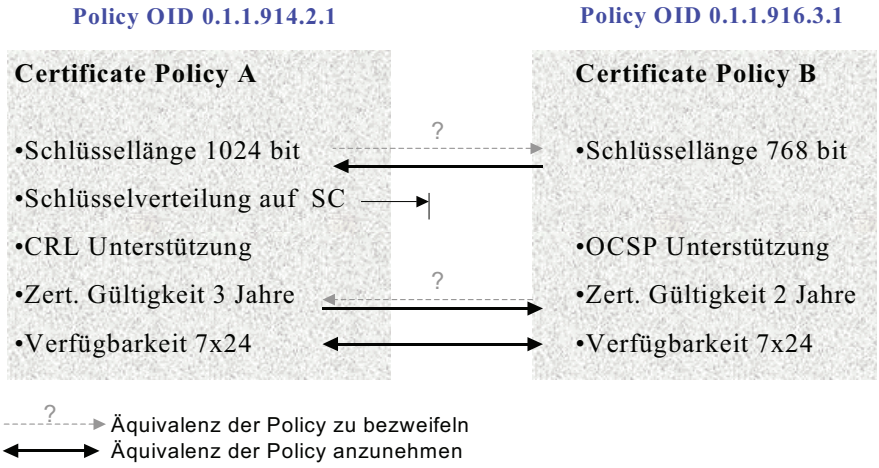

Abb. 2. Bereits Standard-Parameter von Policies weisen häufig Unterschiede auf.

Da eine explizite Kennzeichnung von Cross-Zertifikaten nach dem Standard nicht vorgesehen ist, müsste zur Unterstützung des zweiten Falles ein spezifische Regelung innerhalb der Teilnehmer-Domain festgelegt werden. Diese wäre bei der Zertifizierung von den Zertifizierungsinstanzen zu beachten und müsste von den Clients der Teilnehmer unterstützt werden. Es könnte allerdings auf Standard-Extensions zurückgegriffen werden.[3]

3.3 Gleichheit von Certificate Policies

In einem Zertifikat können über sogenannte Policy-OIDs Informationen zum Sicherheitsniveau oder Hinweise zur Eignung ausgedrückt werden (Certificate Policies). Certificate Policies adressieren dazu eine Fülle von Parametern und informieren über Zusicherungen, Begrenzungen und Service Qualitäten für das ausgestellte Zertifikat.
Für das Erbringen der zugesicherten Eigenschaften bestehen in vielen Fällen eine Reihe von Alternativen. Die in einer PKI ausgewählten Varianten werden z. B. in einem Certification Practice Statement (CPS) beschrieben. Aus praktischen Gründen abstrahieren Certificate Policies jedoch von vielen Details eines Certification Practice Statement. Trotzdem zeigt sich, dass es in jeder PKI eine Menge von Trust Level geben kann, die gegebenenfalls erst im Laufe der Zeit durch graduelle Veränderungen entstehen.

Technisch wird in X.509 spezifiziert, wie in (Cross-)Zertifikaten zu definieren ist, dass bestimmte Certificate Policies äquivalent seien (**policMapping,** [ITUT00, Kap. 18.2.1.]). Für das Policy-Mapping in Cross-Zertifikaten ergeben sich zwei Problembereiche:

- Selbst bei sehr einfachen und klaren Modellen wird es vermutlich keine zwei exakt gleichen Certificate Policies in unterschiedlichen Domänen geben. Damit stellt sich die Frage, ob Policy-Mapping überhaupt verwendet werden kann oder den Anwender unter Umständen in trügerischer Sicherheit wiegt.
- Selbst wenn für Certificate Policies die gleichen Aussagen getroffen werden, stellt sich die Frage, ob sie als äquivalent anzusehen sind, wenn sich die dahinter liegenden Certification Practice Statements unterscheiden.

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

- Policy Mapping überhaupt beim Zertifizieren genutzt werden kann und
- die Mapping-Aussage in verschiedenen Anwendungen von Prüfenden sinnvoll verwendet werden kann.

Da Certification Practice Statements i. A. nicht statisch sind, stellt sich ausserdem die Frage, welche Konsequenzen sich bei Veränderungen von Certification Practice Statements, Certificate Policies und Domain-Policies für das Cross-Zertifikat ergeben.

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

[3] Vgl. dazu auch unten „Gültigkeitsmodell".

Elemente vorgenommen werden. Ob dies zu einer einfacheren Vergleich von Policies unterschiedlicher Zertifizierungsinstanzen führt, hängt sehr von der Zahl der als relevant erachteten Parameter ab. Im Prinzip können alle Aspekte angesprochen werden, bspw. im Detaillierungsgrad von [RFC2527]. In X.509 wird eine solche „Parameter-basierte" Variante bisher nicht unterstützt. Ein Vorschlag für XML findet sich in [GPS00].

3.4 Transitive Cross-Zertifizierung

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

- mehrere Zertifizierungshierarchien miteinander verknüpft werden. Hier stellt sich die Frage, wie die entsprechenden Mapping-Regeln vom Client berücksichtigt werden sollen: Muss die crosszertifizierende CA grundsätzlich mit **inhibitPolicyMapping** festlegen, dass nach dem von ihr ausgestellten Cross-Zertifikat keine weitere Mapping-Regeln mehr akzeptiert werden dürfen?
- 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 fragt sich, ob solche „Rückverknüpfungen" bei der Prüfung einer Zertifikatkette verwendet werden dürfen.

Die Begrenzung der Pfadlänge über die **basicConstraints** hilft nur bedingt in einfachen Fällen. **nameConstraints** oder **inhibitPolicyMapping** nutzen nur etwas, wenn die anderen Zertifizierungshierarchien andere Namensräume bzw. andere Policy-OIDs verwenden.

4 Gültigkeitsmodell

Da die bisher genannten Attribute in Zertifikatketten mit Cross-Zertifikaten auftreten können, müssen sie von Prüffunktionen beherrscht werden. Im folgenden werden Aspekte angesprochen, die über „normale" Gültigkeitsprüfungen hinausgehen.[4] Dabei müssen zwei spezielle 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 beim Vorliegen von Cross-Zertifikaten mehrere Zertifikate den gleichen öffentlichen Schlüssel bestätigen, können unterschiedliche Zertifikatketten geprüft werden. Will Tln1 in Abb. 1 ausgehend von Root A das Zertifikat von Tln2 prüfen, kann er bspw. dem Pfad 11a, 6, 7, 9, dem Pfad 15, 7, 9, oder dem Pfad 2, 17, 16b, 9 folgen. In einem allgemeinen Zertifizierungsgraf sind mehrere Wege zwischen einer Wurzel und einem Teilnehmerzertifikat möglich. Der Austausch von Zertifikaten in einer 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.

4.1 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 in jedem digital signierten Dokument[5] ein Verweis auf das Zertifikat angegeben werden, das zum Prüfen zu verwenden ist. Dies kann erreicht werden, indem der Signierende zum digital signierten Dokument ein Attribut wie **authorityKeyIdentifier** nach [ITUT00, Kap,. 8.2.2.1] mit den Angaben für Subject und Serialnumber des Zertifikats der ausstellenden Zertifizierungsinstanz hinzufügt.[6] Die Prüffunktion würde dann genau die durch die Referenzen identifizierten Zertifikate für die Prüfung heranziehen.[7] Für Anwendungen, die einen hohen Beweiswert erbringen sollen, ist diese Variante dringend zu empfehlen.

Wenn Zertifikate beim Prüfprozess nicht ausgetauscht werden dürfen, stellt sich allerdings das Problem, welche Zertifikate der Signierende einschließen muß, um die durch Cross-Zertifikate möglichen alternativen Zertifikatketten auch für den Prüfenden zuzulassen. Nach dem Modell von [SigI98] wird in jedem digital signierten Dokument, d. h. auch in Zertifikaten, jeweils auf das zum Prüfen zu verwendende Zertifikat verwiesen. Betrachtet man den Graph in Abb. 1, hat der Tln2 nur ein Zertifikat (9). Nach den Regeln von SigI muss die Zertifizierungsinstanz im Teilnehmerzertifikat auf eines ihrer eigenen Zertifikate verweisen. Wenn nur das jeweils übergeordnete Zertifikat referenziert wird, definiert also die Zertifizierungsinstanz H1, welche der drei Zertifikatketten weiter zu verfolgen ist. Alternativ könnte der Signierende den gesamten Pfad (oder mehrere alternative) bereits im digital signierten Dokument festlegen. In diesem Fall würde die Zertifikatkette zum Prüfen erst zum Signaturzeitpunkt festgelegt und vollständig von Signierenden definiert.

4.2 Bestimmen der Zertifikatkette durch den Prüfenden

Für diese Variante nehmen wir an, dass dem prüfenden Teilnehmer eine Menge von Zertifikaten zur Verfügung steht. Die Zertifikate einer ausgewählten Teilmenge genießen als Wurzelzertifikate direktes Vertrauen. Der Prüfende muss nun eine oder mehrere Zertifikatketten bestimmen, die er zum Prüfen eines digital signierten Dokuments verwenden will. Dazu kann er versuchen, den allgemeinen Zertifizierungsgraphen zu reduzieren.[8] 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 Wurzelzertifikate liegen. Außerdem werden alle abgelaufenen Zertifikate, alle Zertifikate mit dem Status „revoked" oder „suspended" und solche, zu denen keine Statusinformation verfügbar ist, aus der Menge zulässiger Zertifikate entfernt.
- Es werden nur Zertifikate akzeptiert, die folgenden Bedingungen genügen: das Zertifikat zum ausstellenden Schlüssel ist ein Zertifikat für die Zertifizierung („**keyUsage**" = „**keyCertSign**" oder „**basicConstraints.cA**" = „**true**") und

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

[5] Darunter fallen auch Zertifikate.

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

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

[8] Siehe dazu auch einige Hinweise in [Zie96].

die „**pathLenConstraint**“ aller in der Kette enthaltenen Zertifikate wird eingehalten.
- In allgemeinen Zertifizierungsgrafen können Zyklen auftreten. Taucht ein Zertifikate in einer Kette zum zweiten mal auf, kann die Traversierung für diese Kette abgebrochen werden. Alternativ kann durch Längenbegrenzungen sichergestellt werden, dass die Traversierung terminiert. Gegebenenfalls liefert auch die Bedingung, dass ein nachgeordnetes Zertifikat nach dem „**notBefore**“ des Zertifikats zum bestätigenden Schlüssel ausgestellt sein muss, ein Abbruchkriterium.
- Es könnten Zertifikatketten entweder nur mit lokal akzeptierten (bereits bekannten) Policies oder oberhalb einer geforderten Mindest-Policy oder ohne Policy-Mapping ausgewählt werden.
- Sofern nach Anwendung der bisherigen Kriterien noch alternative Zertifikatketten für die Prüfung eines digital signierten Dokuments geeignet sind, kann z. B. eine durch Entscheidung des Prüfenden oder automatisch eine der folgenden Ketten gewählt werden: Entweder die mit der minimale Länge, der maximalen Policy, die ohne Policy Mapping oder die mit den „günstigsten“ Naming-Constraints.

Die Ergebnisse einer Analyse können teilweise wiederverwendet bzw. kontinuierlich fortgeschrieben werden. Dadurch sollte sich der Aufwand für die Auswahl von Zertifikatketten in vertretbarem Rahmen halten.

4.3 Feststellen der Pfad-Policies

Die eigentliche Prüfung setzt auf der oder den ausgewählten Zertifikatketten auf. Im Rahmen der Prüfung einer Zertifikatkette wird eine Gesamt-Policy für die Kette bestimmt.[9] Durch alternative Zertifikatketten können sich unterschiedliche Gesamt-Policies ergeben. Für das Gültigkeitsmodell muss daher 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 eine der initial geforderten (Mindest-)Policies erreicht.

Im Gültigkeitsmodell muss außerdem geprüft werden, auf welchem Niveau Mapping-Regeln angegeben werden. Beispielsweise muss erkannt werden, wenn eine CA mit einer niedrigen Policy ein weiteres CA-Zertifikat ausstellt, in dem ein Mapping auf ein „höheres“ Sicherheitsniveau festgelegt wird.

Policy-Mapping und PolicyConstraints sind insofern dynamisch, dass sie mit Sperrungen oder ausgelaufenen Zertifikaten nicht mehr als Regeln gelten. Prüffunktionen dürfen dieses Regeln daher nicht dauerhaft speichern, sondern müssen sich in Abhängigkeit von der jeweils verwendeten Zertifikatkette über ihre Anwendbarkeit vergewissern.

5 Implikationen für Sperrungen

In strikten Baum-Hierarchien ist es möglich, durch die Sperrung eines übergeordneten Zertifikats die gesamte Teilhierarchie implizit mitzusperren.[10] Dies ist insbesondere als Reaktion auf Schlüsselkompromitierung eines Zertifizierungsinstanz-Schlüssels sinnvoll. Mit Cross-Zertifikaten existieren jedoch mehrere Zertifikate für ein Schlüsselpaar. Daraus ergeben sich im Falle einer Sperrung Probleme:
- Teilnehmer oder zur Sperrung berechtigte Stellen müssen entscheiden, ob sie das Schlüsselpaar für alle Anwendungen sperren oder ob sie lediglich ein einzelnes Zertifikat sperren lassen wollen, beispielsweise weil sie eine Bankverbindung aufgegeben haben. Im ersten Fall muss ihre Zertifikatverwaltung (oder ein Service Provider) eine Übersicht über die existierenden Zertifikate zu einem Schlüssel haben.
- Für Zertifikate von Zertifizierungsinstanzen kann es je nach Struktur des Zertifizierungsgrafen „Umwege“ um gesperrte Knoten herum geben. Soll ein Teilgraf eines Zertifizierungsgrafen gesperrt werden, bspw. weil in einer Zertifizierungsinstanz schwerwiegende Unregelmäßigkeiten aufgetreten sind (sei in der ZI „G1“ „compromised“), müsste der Graf bezüglich des Sperrziels analysiert werden. Dazu ist es entweder erforderlich, dass einer geeigneten Stelle die Informationen über alle Zertifizierungsrelationen zur Verfügung stehen und sie die notwendigen Sperrungen veranlasst. Alternativ könnten alle Zertifizierungsinstanzen des Grafen geeignet informiert werden und ihrerseits die Zertifikate sperren, die sie für ZI „G1“ ausgestellt haben.
- Für die Sperrung von Zertifizierungsinstanz-Zertifikaten werden ferner Regeln benötigt, wie weit die Sperrung transitiv „weitergegeben“ werden muss, also welche der ZI „G1“ im Graphen nachgeordneten Zertifikate ebenfalls zu sperren sind. Z. B. könnte es bei Schwachstellen in der Schlüsselgenerierung notwendig sein, auch alle weiteren Zertifikate für die von ZI „G1“ erzeugten Schüssel zu sperren, während im Fall von Schlüsseln die von einer nachgeordneten Zertifizierungsinstanz selbst erzeugt wurden, nur die von ZI „G1“ ausgestellten Zertifikate, nicht aber Mehrfachzertifikate anderer Zertifizierungsinstanzen zu sperren wären.

Varianten, die diese entsprechende Aufgaben im Rahmen der Gültigkeitsprüfung auf den Prüfenden verlagern, dürften die Effizienz von PKI-Anwendungen erheblich verringern und die Teilnehmer überfordern.

6 Fazit

Cross-Zertifikate bieten die Möglichkeit, unabhängige Zertifizierungshierarchien zu verknüpfen, Pfade in Zertifizierungshierarchien zu optimieren, Wurzelzertifikate einer Root zu verketten und gegebenenfalls in Störfällen Handlungsoptionen zur Schadensbegrenzung[11] zu erschließen. Die technische Erzeugung von Cross-Zertifikaten ist ohne große Probleme möglich. Ausgebaut werden muss die Unterstützung differenzierter Gültigkeitsmodelle in den Prüffunktionen. Die „echten“ Probleme der Cross-Zertifikate liegen jedoch – wie häufig bei PKIs – eher in organisatorischen und rechtlichen Fragen und der entstehenden Komplexität für die Anwender.

Praxisbeispiele für produktiv eingesetzte Cross-Zertifikate sind für Deutschland nur auf der Basis von PGP bekannt (z. B. der

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

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

[11] [Ham99, 536 ff.].

DFN-PCA, der c't-CA und TC Trustcenter.[12]). Neuere Policy-CAs beabsichtigen allerdings, X.509 Cross-Zertifikate einzusetzen (z. B. die Sphinx-PCA oder die Initiative der Deutschen Bank mit TeleSec[13]). In Kanada sollen die PKIs einiger Departments der kanadischen Verwaltung cross-zertifiziert sein (Heath Canada, Royal Canadian Mounted Police, Department of Foreign Affairs and International Trade, ...). Die Verknüpfung von Root-Schlüsseln einer Zertifizierungshierarchie über „Cross-Zertifikate“ (Abb. 1, Kante 13) wird in der PKI nach SigG von der Regulierungsbehörde für Telekommunikation und Post angewendet.[14] Ob sich das Konzept der Cross-Zertifikate auf Dauer als tragfähig erweist, werden daher erst die Praxiserfahrungen der nächsten Jahre zeigen.

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.

[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 / Gerhardt-Häckl (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.

[HaPe01] Hammer, V. / Petersen, H. (2001): Aspekte der Cross-Zertifizierung, Proceedings der Arbeitskonferenz Kommunikationssicherheit 2001, im Erscheinen.

[Her99] 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

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

[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.

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

13 Pressemeldung, zu finden über „Suche“ nach „Telesec“ auf www.deutsche-bank.de.

[14] Dabei wechseln sogar die Namen der Wurzel-Zertifizierungsinstanzen, obwohl der Betreiber gleich bleibt.[14] Insofern trifft die hier gewählte Definition für „Cross-Zertifikate“ zu.