Erschienen in: Tagungsband 6. Deutscher IT-Sicherheitskongreß des BSI 1999, SecuMedia Verlag, 1999, S. 215-230.

Zum Problem der Gültigkeitsprüfung von Schlüsselzertifikaten

Dirk Fox[1]

Kurzfassung

Schlüsselzertifikate, die die Gültigkeit und Authentizität eines öffentlichen Schlüssels und dessen Zugehörigkeit zu einem eindeutig bezeichneten Schlüsselinhaber zuverlässig bestätigen, sind eines der wichtigsten Elemente einer Public Key-Infrastruktur. Aus diesem Grund treffen auch Signaturgesetz und Signaturverordnung vor allem Festlegungen, die eine vertrauenswürdige Ausstellung von Schlüsselzertifikaten garantieren sollen.
Schlüsselzertifikate sind naturgemäß offline-Bestätigungen. Das bedeutet, daß Mechanismen benötigt werden, die es erlauben, ein Zertifikat aus wichtigem Grund vor Ablauf der Gültigkeit zurückrufen oder sperren zu können, z.B. im Falle einer Kompromittierung oder eines Verlusts des geheimen Schlüssels.
Der vorliegende Beitrag diskutiert die Anforderungen an Sperrmechanismen für Schlüsselzertifikate und die damit verbundenen Schwierigkeiten. Es werden unterschiedliche Ansätze vorgestellt und eine spezielle Vorgehensweise empfohlen.

Abkürzungen

ARL Authority Revocation List (Sperrliste für CA-Zertifikate)

CA Certification Authority (Zertifizierungsstelle)

CRL Certificate Revocation List (Sperrliste für Nutzer-Zertifikate)

OCSP Online Certificate Status Protocol (Zertifikats-Auskunftsdienst)

LDAP Lightweight Directory Access Protocol (Zugriff auf einen Verzeichnisdienst)

SigG Signaturgesetz

SigV Signaturverordnung

1 Einführung

Schlüsselzertifikate sind von speziellen, vertrauenswürdigen Instanzen – Zertifizierungsstellen oder Certification Authorities (CAs) – ausgestellte, digital signierte Bestätigungen, daß ein ausgewiesener öffentlicher Schlüssel zu einer angegebenen eindeutigen Identität gehört. Solche Schlüsselzertifikate werden für einen im Schlüsselzertifikat angegebenen Gültigkeitszeitraum nach einem definierten Gültigkeitsmodell ausgestellt.

In Public Key-Infrastrukturen werden diese digital signierten Bestätigungen den Schlüsselinhabern ausgehändigt und in allgemein zugänglichen Verzeichnissen bekannt gemacht. Dritte, die der für die Ausstellung eines Zertifikats verantwortlichen Zertifizierungsstelle vertrauen, können durch die Prüfung der digitalen Signatur im

1 Secorvo Security Consulting GmbH, Karlsruhe

Zertifikat die Authentizität eines Schlüssels kontrollieren.

Dieser Mechanismus, der auf eine Arbeit von Kohnfelder [Kohn_78] zurückgeht, ermöglicht eine authentische Verteilung von öffentlichen Schlüsseln, ohne daß der Nutzer des Schlüssels und der Schlüsselinhaber sich persönlich kennen oder einander vertrauen.

In der Praxis kommen Schlüsselzertifikate beispielsweise beim Einsatz von Digitalen Signaturen in E-Mail-Sicherheitssystemen wie folgt zur Anwendung:

- Der Empfänger einer digital signierten Nachricht (z.B. nach dem S/MIME-Standard), der diese Signatur prüfen möchte und den öffentlichen (Prüf-) Schlüssel des Senders nicht kennt, erhält zusammen mit der signierten Nachricht das zugehörige Schlüsselzertifikat vom Sender, oder er ruft es über einen Verzeichnisdienst (z.B. über einen LDAP-Zugriff auf ein X.500-Directory) ab. Dabei müssen keine Sicherheitsanforderungen an die Übertragung des Schlüsselzertifikats gestellt werden.
- Besitzt der Empfänger den öffentlichen (Prüf-) Schlüssel der Zertifizierungsstelle, kann er durch Prüfung des Schlüsselzertifikats feststellen, ob der öffentliche Schlüssel im Schlüsselzertifikat auch zu dem Sender gehört.

Analog kann der Sender einer Nachricht, der diese mit dem öffentlichen Schlüssel des Empfängers verschlüsseln möchte, diesen aber nicht kennt, den Verschlüsselungsschlüssel durch Abfrage des Verzeichnisdienstes und Prüfung des Schlüsselzertifikats authentisch beziehen.

Die Technik des Schlüsselzertifikats reduziert die Sicherheitsanforderungen an die Verteilung asymmetrischer, öffentlicher Schlüssel: Nur der öffentliche Schlüssel der Zertifizierungsstelle muß allen Kommunikationsteilnehmern authentisch mitgeteilt werden; die Authentizität der öffentlichen Schlüssel der Kommunikationsteilnehmer wird durch die Schlüsselzertifikate sichergestellt, d.h aus der Authentizität des Schlüssels dieser allgemein als vertrauenswürdig erachteten Zertifizierungsstelle „abgeleitet“. So können auch einander nicht bekannte Kommunikationspartner eine sichere Kommunikationsverbindung aufbauen, sofern ihre Zertifikate von einer gemeinsamen „Wurzel-Instanz“ (Root CA) ausgestellt wurden.

Zugleich erfordern Schlüsselzertifikate keine Online-Verfügbarkeit der Zertifizierungsinstanz: Zertifikate werden von der Zertifizierungsstelle offline ausgestellt und können von den Kommunikationsteilnehmern selbst verteilt werden (z.B. als Teil oder Anhang einer digital signierten Nachricht verschickt). Sie erlauben eine Nutzung des öffentlichen Schlüssels ohne eine direkte Verbindung zur CA; es muß lediglich auf den Verzeichnisdienst zugegriffen werden.

Problematisch ist allerdings, daß ein Zertifikat eine „Zukunftsvermutung“ darstellt: Die Bestätigung kann z.B. durch eine Kompromittierung des Schlüssels oder einen Defekt des Datenträgers, auf dem der zugehörige geheime Schlüssel gespeichert ist, noch während der „Lebenszeit“ des Zertifikats unzuverlässig werden.

2 Prüfung von Schlüsselzertifikaten

Die Nutzung eines Schlüsselzertifikats z.B. zur Prüfung einer digitalen Signatur oder zum Verschlüsseln eines Nachrichtenschlüssels setzt die Anerkennung des Zertifikats durch den Nutzer voraus. Diese Anerkennung hängt im Kern von zwei Bedingungen ab:

1. der Gültigkeit des Schlüsselzertifikats und
2. dem Vertrauen des Nutzers in den Aussteller des Schlüsselzertifikats.

Die Gültigkeit eines Schlüsselzertifikats unterscheidet sich dabei von der Gültigkeit einer digitalen Signatur: Die Gültigkeit einer Signatur hängt nur vom Zeitpunkt der Erzeugung ab[2] – die Gültigkeit eines Schlüsselzertifikats hingegen ist abhängig von einem Bezugszeitpunkt: Ihre Gültigkeit wird für einen Referenzzeitpunkt geprüft, der bei der Prüfung vorgegeben wird.

Die Gültigkeit eines Schlüsselzertifikats zu einem gegebenen Referenzzeitpunkt hängt damit von zwei Bedingungen ab:

- vom Zeitpunkt der Zertifikatsausstellung und des im Zertifikat angegebenen Gültigkeitsintervalls, und
- davon, daß das Zertifikat nicht vorzeitig zurückgerufen, d.h. vor Ablauf des Gültigkeitsintervalls vom Aussteller für ungültig erklärt worden ist.

Das Vertrauen des Nutzers in den Aussteller des Schlüsselzertifikats kann wiederum auf der Gültigkeit eines weiteren Zertifikats einer anderen Zertifizierungsstelle bzw. einer „Kette“ von aufeinander bezogenen Zertifikaten beruhen. Eine solche Kette muß jedoch mit einem dem Nutzer authentisch bekannten, öffentlichen „Root-Schlüssel“ enden, dem der Nutzer explizit vertraut.

Das Vertrauen des Benutzers in den Aussteller des Schlüsselzertifikats kann damit abhängen:

- von der Gültigkeit aller Schlüsselzertifikate einer möglicherweise vorliegenden Zertifikatskette, sowie
- von der Gültigkeit des öffentlichen Root-Schlüssels bzw. des Schlüssels einer der Zertifizierungsinstanzen, die die Schlüsselzertifikate der Zertifikatskette ausgestellt haben und deren öffentlichen Schlüssel der Prüfer authentisch kennt.

Die Gültigkeit eines Schlüsselzertifikats können wir also wie folgt definieren:

> **Definition** (Gültigkeit von Schlüsselzertifikaten):
>
> Ein Schlüsselzertifikat nennen wir *gültig zu einem Zeitpunkt*, wenn die folgenden Bedingungen erfüllt sind:

---

[2] Da dieser Zeitpunkt vom Empfänger einer signierten Nachricht nicht immer zuverlässig festgestellt werden kann, wird hier in der Regel der Zeitpunkt des Eingangs des signierten Dokuments als „Signierzeitpunkt“ angenommen.

- Die (mathematische) Prüfung der Signatur der Zertifizierungsstelle unter dem Zertifikat liefert das Resultat „korrekt“.
- Das Zertifikat ist zum gegebenen Zeitpunkt nicht abgelaufen.
- Das Zertifikat ist zum gegebenen Zeitpunkt nicht zurückgerufen.

Um Vertrauen in ein Schlüsselzertifikat setzen zu können, ist – wie oben ausgeführt – ggf. die Prüfung der Gültigkeit weiterer Zertifikate einer vorliegenden Zertifikatskette erforderlich sowie die Existenz eines vertrauenswürdigen Root-Schlüssels, bei dem die Zertifikatskette endet.

Zur Prüfung eines Zertifikats ist nun die Gültigkeit dieser drei Bedingungen zu untersuchen. Dabei gilt im allgemeinen:

- Die Erfüllung der ersten Bedingung ist sehr leicht durch einen Rechenschritt zu überprüfen. In diesem Schritt sind ggf. noch weitere Anforderungen an das Verfahren wie eine Mindestschlüssellänge oder die Verwendung eines sicheren Hashverfahrens zu untersuchen.
- Die Erfüllung der zweiten Bedingung kann leicht überprüft werden: Der vorgegebene Zeitpunkt muß in dem im Zertifikat angegebenen Gültigkeitszeitraum liegen.
- Schwierigkeiten macht die dritte Bedingung, denn sie fordert eine Aussage über das „Nichtvorliegen“ eines Ereignisses. Eine solche Prüfung erfordert eine verläßliche Bestätigung, daß bis zu einem bestimmten Zeitpunkt kein Rückruf erfolgt ist.

In der Praxis kann die letzte Bedingung nicht objektiv festgestellt werden; es ist lediglich prüfbar, daß das Vorliegen eines Rückrufs (oder einer Sperrung) eines Zertifikats zu einem bestimmten Zeitpunkt nicht bekannt ist.

Die Prüfung, daß kein Rückruf erfolgt ist, wird immer dann vergleichsweise leicht und verläßlich durchgeführt werden können, wenn der Zeitpunkt, für den die Gültigkeit des Zertifikats geprüft wird, erheblich vor dem Zeitpunkt der Durchführung der Prüfung liegt. Dieser Fall wird allerdings in der Praxis selten auftreten; wahrscheinlich meist in einem Streitfall, der durch eine nachträgliche Prüfung der Gültigkeit eines Zertifikats entschieden werden soll.

Liegen jedoch Referenzzeitpunkt und Prüfzeitpunkt dicht beieinander – das wird die Regel sein bei der Prüfung der Gültigkeit von Schlüsselzertifikaten z. B. im Zusammenhang mit der Prüfung einer digitalen Signatur unter einer E-Mail-Nachricht –, dann erfordert die Prüfung eine verläßliche Aussage mit hoher Aktualität über das Vorliegen von Zertifikats-Rückrufen oder -Sperrungen.

Zu diesem Zweck sind verschiedene Mechanismen vorgeschlagen und standardisiert worden, die im folgenden vorgestellt und deren jeweiligen Vor- und Nachteile diskutiert werden.

3 Rückruf von Schlüsselzertifikaten

Beim praktischen Einsatz von Schlüsselzertifikaten kann es erforderlich sein, daß das

Zertifikat eines Teilnehmers in einer Public Key-Infrastruktur innerhalb des Gültigkeitszeitraums für ungültig erklärt werden muß. Dieser Vorgang wird Zertifikats-Rückruf oder -Sperrung genannt. Da der Rückruf sich nicht auf den Schlüssel, sondern die Bestätigungsaussage im Zertifikat bezieht, muß der Rückruf oder die Sperrung vom Zertifikatsaussteller vorgenommen werden.[3]

3.1 Rückrufgründe

Für einen Rückruf oder die Sperrung eines Zertifikats gibt es unterschiedliche Gründe, die sich in dringliche und weniger dringliche unterscheiden lassen. Ein dringlicher Rückrufgrund liegt vor, wenn die Gefahr besteht, daß digitale Signaturen gefälscht oder verschlüsselte Daten unberechtigt entschlüsselt werden können.

Zu den ***dringlichen Rückrufgründen*** zählen insbesondere die folgenden:

- Ein Schlüsselinhaber hat den Datenspeicher mit dem zugehörigen geheimen Schlüssel, z.B. seine Chipkarte, möglicherweise unter Preisgabe seines Paßworts verloren.
- Der Schlüssel eines Benutzers wurde kompromittiert, oder es besteht der begründete Verdacht, daß dies passiert ist.
- Der Schlüssel der Zertifizierungsstelle wurde kompromittiert, oder es besteht der begründete Verdacht, daß dies passiert ist, und daher wurden möglicherweise einzelne Zertifikate gefälscht.

Weniger dringliche Rückrufgründe liegen vor, wenn eine Nutzung der öffentlichen Schlüssel des Benutzers nicht mehr sinnvoll möglich ist, weil

- der Datenspeicher des geheimen Schlüssel eines Benutzers (Chipkarte) defekt ist,
- der Datenspeicher des geheimen Schlüssel eines Benutzers (Chipkarte) von der Registrierungsinstanz eingezogen wurde,
- der Schlüsselinhaber das Unternehmen verlassen hat, das ihm das Schlüsselpaar für Unternehmenszwecke ausgestellt hat,
- der Schlüsselinhaber seine PIN oder sein Paßwort vergessen hat, oder
- der ein-eindeutige Name des Schlüsselinhabers sich geändert hat oder geändert werden muß.[4]

In diesen Fällen ist kein dringlicher Rückruf erforderlich, weil weder der Schlüsselinhaber noch ein unberechtigter Dritter digitale Signaturen mit dem zugehörigen (geheimen) Signierschlüssel erzeugen oder für den Schlüsselinhaber verschlüsselte Daten entschlüsseln können. Zwar können nun auch mit dem öffentlichen Verschlüsselungsschlüssel des Schlüsselinhabers verschlüsselte Nachrichten von diesem selbst

---

3 Sie kann allerdings vom Schlüsselinhaber veranlaßt werden.

4 Dies kann z.B. eintreten bei einer Änderung der Unternehmensstruktur, sofern diese in den Aufbau des Distinguished Name (DN) eingeht.

nicht mehr entschlüsselt werden; er kann sie jedoch beim Sender neu anfordern.

Für den Fall eines Schlüsselrückrufs wird nun ein Mechanismus benötigt, der eine authentische vorzeitige Sperrung von Zertifikaten zuläßt. Dieser Mechanismus muß für dringliche Fälle sicherstellen, daß alle Benutzer, die einen (zwischenzeitlich zurückgerufenen) öffentlichen Schlüssel eines anderen Benutzers verwenden möchten, mit akzeptablem Aufwand oder innerhalb einer akzeptablen Zeitspanne Kenntnis vom Rückruf des Zertifikats erhalten.

3.2 Ablauf des Rückrufs

Der Rückruf eines Schlüsselzertifikats wird vom Schlüsselinhaber (bzw. einem im Zertifikat explizit ermächtigten Vertreter) oder – im Fall der Kompromittierung des CA-Schlüssels – direkt von der Zertifizierungsinstanz eingeleitet.

Im Falle eines vom Schlüsselinhaber (bzw. einem berechtigten Vertreter) veranlaßten Rückrufs sind organisatorische Abläufe erforderlich, die eine Authentisierung des Schlüsselinhabers (bzw. des Vertreters) erlauben. Dazu ist in der Regel das persönliche Erscheinen des Schlüsselinhabers bei der zuständigen Registierungsstelle zur zweifelsfreien Identifikation erforderlich, um unberechtigte Rückrufe, die Denial of Service-Angriffe darstellen, auszuschließen.

Um in dringenden Fällen eine Sperrung umgehend veranlassen zu können, sollte zwischen Schlüsselinhaber und zuständiger Registrierungsstelle ein einmalig gültiges Authentisierungs-Paßwort vereinbart werden, mit dem auch eine telefonische Sperrung über eine Sperr-Rufnummer möglich ist.[5] Diese Rückrufpaßworte werden in der Registrierungsstelle (vor unberechtigtem Zugriff geschützt) aufbewahrt.

Ein solches Authentisierungspaßwort kann auch verwendet werden, um ein elektronisches Rückrufprotokoll zwischen Schlüsselinhaber und Registrierungsstelle mit Hilfe symmetrischer Kryptoverfahren zu schützen.

Ein Zertifikatsrückruf wird von der Registrierungsstelle umgehend mit Angabe

- der laufenden Zertifikatsnummer
- des Rückrufzeitpunkts und
- ggf. des Rückrufgrunds

an die Zertifizierungsstelle gemeldet, die den Rückruf in die aktuelle Rückrufliste (s.u.) aufnimmt.

Für einen solchen Revocation Request bietet sich das PKIX-Protokoll an, das ein sicheres (authentisches und vertrauliches) Kommunikationsprotokoll CA spezifiziert. Für den Rückruf eines Zertifikats ist die folgende Datenstruktur vorgesehen [AdFa_98]:

---

5 Ein solcher Mechanismus ist beispielsweise ausdrücklich in der Signaturverordnung vorgesehen; § 9 SigV [SigV_97]

```
RevReqContent ::= SEQUENCE OF RevDetails

RevDetails ::= SEQUENCE {
        certDetails                 CertTemplate,
        -- hier werden entweder nur die Seriennummer des Zertifikats
        -- oder alle bekannten Angaben zum zurückzurufenden
        -- Zertifikat eingetragen, falls die Seriennummer nicht
        -- bekannt ist.
        revocationReason            ReasonFlags  OPTIONAL,
        -- hier kann der Rückrufgrund beschrieben werden
        badSinceDate                GeneralizedTime  OPTIONAL,
        -- falls bekannt, Zeitpunkt, zu dem die Smartcard verlorenging
        -- oder eine Kompromittierung vermutet wird
        crlEntryDetails             Extensions  OPTIONAL
        -- gewünschte Extensionen für den CRL-Eintrag }
```

Abb. 1: Revocation Request nach PKIX [AdFa_98]

Das zurückzurufende Zertifikat wird dabei in der Regel über die Seriennummer des Zertifikats der CA eindeutig bezeichnet, die das Zertifikat ausgestellt hat. Die Angabe von Rückrufgrund und vermutlichem Zeitpunkt einer Kompromittierung des Schlüssels sind dabei optional.

Die Rückruf-Anforderung wird durch ein symmetrisches oder asymmetrisches kryptographisches Verfahren geschützt und von der CA durch eine (ebenfalls in PKIX spezifizierte) Datenstruktur bestätigt.

3.3 Certificate Revocation Lists (CRLs)

Der für die Verteilung aktueller Zertifikatssperrungen üblicherweise eingesetzte Mechanismus ist die Herausgabe von Certificate Revocation Lists (CRL) durch eine Zertifizierungsstelle (CA) in regelmäßigen Zeitabständen.

Eine CRL enthält die Seriennummern und das jeweilige Rückrufdatum aller von der CA zurückgerufenen (zu von ihr ausgestellten) Schlüsselzertifikate und ist von der CA digital signiert, um die Integrität (Vollständigkeit und Korrektheit) und die Authentizität sicherzustellen. Dabei sollte von der CA ein separater, mit dem Zertifizierungsschlüssel nicht identischer CRL-Signaturschlüssel verwendet werden.[6]

Ein Format für den Aufbau der CRLs wurde spezifiziert in der Norm X.509v2; dort sind auch optionale Erweiterungen des Rückrufeintrags (z.B. um Referenzen auf eine Rückruf-Policy und die Angabe des Rückrufgrunds) vorgesehen [ITU_93].

Das CRL-Format nach X.509v2 ist dabei wie folgt spezifiziert:

```
certificateRevocationList   ATTRIBUTE    ::=          {
        WITH SYNTAX         CertificateList
        EQUALITY MATCHING RULE certificateListExactMatch
        ID                              id-at-certificateRevocationList }
```

6 Das Zertifikatsformat X.509v3 unterstützt dies mit unterschiedlichen Bits für cRLSign und keyCertSign im keyUsage-Attribut.

```
authorityRevocationList    ATTRIBUTE    ::=          {
      WITH SYNTAX          CertificateList
      EQUALITY MATCHING RULE certificateListExactMatch
      ID                   id-at-authorityRevocationList }

CertificateList            ::=    SIGNED { SEQUENCE {
      version                       Version OPTIONAL,
                                    -- wenn angegeben: version muß „v2“ sein
      signature                     AlgorithmIdentifier,
      issuer                        Name,
      thisUpdate                    Time,
      nextUpdate                    Time OPTIONAL,
      revokedCertificates           SEQUENCE OF SEQUENCE {
        userCertificate             CertificateSerialNumber,
        revocationDate              Time,
        crlEntryExtensions          Extensions OPTIONAL } OPTIONAL,
      crlExtensions          [0]  Extensions OPTIONAL }}
```

Abb. 2: CRL-Format nach X.509v2 [ITU_93]

Wesentlich ist, daß eine CRL nur von einer Zertifizierungsstelle und nur für von dieser ausgegebene Zertifikate ausgestellt werden darf. Eine CRL enthält den Zeitpunkt ihrer Veröffentlichung und den Zeitpunkt, zu dem die CRL ungültig wird und spätestens durch eine neue ersetzt sein muß.

Eine CRL muß immer die folgenden Angaben enthalten:

- eine CRL-Seriennummer,
- die Seriennummern aller seit Ausstellung der letzten CRL zurückgerufenen Zertifikate (mit Sperrzeitpunkt),
- die Seriennummern aller bisher von der CA zurückgerufenen und noch nicht abgelaufenen Zertifikate (mit Sperrzeitpunkt),
- einen Gültigkeitszeitraum.

Eine CRL nach X.509v2 enthält in minimaler Ausprägung (d.h. ohne optionale weitere Angaben z.B. zum Rückrufgrund) lediglich Referenzen auf die zurückgerufenen Zertifikate in Form der eindeutigen Zertifikats-Seriennummer der zuständigen CA sowie den Sperrzeitpunkt. Bei ASN.1-Codierung liegt der Umfang eines (minimalen) CRL-Eintrags damit bei weniger als 50 Byte.

Damit der Rückruf eines Zertifikats bei der Prüfung bewertet werden kann (z.B. eine Unterscheidung von dringlichen und weniger dringlichen Rückrufgründen möglich ist), sollten die Rückrufgründe in der CRL angegeben werden [ITU_93, HFPS_99]:

```
CRLReason ::= ENUMERATED {
      unspecified             (0),
      keyCompromise           (1),
      cACompromise            (2),
      affiliationChanged      (3),
      superseded              (4),
      cessationOfOperation    (5),
      certificateHold         (6),
      removeFromCRL           (8) }
```

Abb. 3: CRL-Rückrufgründe nach X.509v2 [ITU_93]

Der Nachteil von CRLs ist, daß nach Ablauf des Gültigkeitszeitraums eines Zertifikats eine ggf. zur „Lebenszeit“ des Zertifikats erfolgte Sperrung anhand der aktuellen CRL nicht mehr festgestellt werden kann.

3.4 Verteilung von CRLs

Die Verteilung der CRLs erfolgt in der Regel durch Veröffentlichung in einem Verzeichnisdienst (z.B. einem X.500-Directory) durch die zuständige CA. CRLs sollten in regelmäßigen Zeitabständen publiziert werden. Der Publikationszeitraum sollte nicht zu groß gewählt werden, um die Aktualität der Zertifikatsinformationen nicht zu stark einzuschränken, aber auch nicht zu gering, um den Verteilungsaufwand zu begrenzen.

Üblicherweise wird vorgeschlagen, die Veröffentlichung einer CRL auf einen festen, regelmäßigen Termin zu legen. Dieses Vorgehen hat allerdings in großen Public Key-Infrastrukturen einen entscheidenden Nachteil: Es verursacht Spitzenlasten im Zugriff auf den Verzeichnisdienst und bei großen CRLs zudem erhöhten Bandbreitebedarf zum jeweiligen Publikationszeitpunkt.

3.5 CRL Distribution Points und Delta CRLs

Umfaßt die Rückrufliste einige tausend oder gar hunderttausend Rückrufe, wird eine CRL sehr umfangreich. Eine regelmäßige Abfrage der jeweils aktuellen CRL vom Verzeichnisdienst kann bei gleichzeitigen Zugriffen vieler Client-Komponenten sowohl die Bandbreite der Netzverbindung als auch die Leistungsfähigkeit des Verzeichnisdienstes übersteigen.

Daher sollten große CRLs in Teillisten aufgespalten werden. Diese Teillisten können nach unterschiedlichen Kriterien erstellt werden; üblich ist eine Aufteilung in Zertifikatsrückrufe eines festgelegten Seriennummern-Bereichs. Solche „Teil-CRLs“ sind damit in ihrer maximalen Länge begrenzt. Jede dieser Teil-CRLs muß einzeln von der CA signiert werden.

Der X.509v3-Standard sieht zu diesem Zweck CRL Distribution Points vor, die für die Sperrung von Zertifikaten jeweils einer Seriennummern-Gruppe zuständig sind [ITU_93]. In das X.509v3-Zertifikat eines öffentlichen Schlüssels wird dazu ein Verweis auf den jeweils zuständigen CRL Distribution Point aufgenommen.

Eine weitere Möglichkeit zur Verringerung des Umfangs von CRLs und der erforderlichen Bandbreite für die Verteilung ist die Ausstellung von CRLs für vergleichsweise lange Zeiträume (z.B. mehrere Wochen) und die Herausgabe von „Delta-CRLs“ im Falle dringlicher Rückrufgründe, die nur die Änderungen zur aktuellen CRL enthalten. Nachteil dieses Ansatzes ist, daß bei der Prüfung eines Zertifikats jedesmal online z.B. über den Verzeichnisdienst nach aktuellen Delta-CRLs gesucht werden muß.

3.6 Revocation Announcement

Im Falle einer Zertifikatsperrung, die durch eine CA veranlaßt wurde, sieht PKIX die Möglichkeit einer Informationsnachricht an den Schlüsselinhaber vor, in der dieser über den bevorstehenden oder bereits erfolgten Rückruf in Kenntnis gesetzt wird (Revocation Announcement, [AdFa_98]).

```
RevAnnContent ::= SEQUENCE {
        status              PKIStatus,
        certId              CertId,
        willBeRevokedAt     GeneralizedTime,
        badSinceDate        GeneralizedTime,
        crlDetails          Extensions  OPTIONAL
        -- zusätzliche CRL-Angaben (z.B. Nummer der CRL, Rückrufgrund etc.) }
```

Abb. 4: Aufbau eines Revocation Announcements [AdFa_98]

Mit einer ähnlichen Struktur, einem „CRL Announcement“, kann eine CA die Herausgabe einer CRL ankündigen. Ein solcher Mechanismus läßt sich gut mit Delta-CRLs kombinieren, um zu verhindern, daß bei jeder Zertifikatsprüfung aktiv nach aktuellen Delta-CRLs gesucht werden muß.

3.7 Revocation Certificates

Von Rueppel stammt der Vorschlag, statt CRLs einzelne Rückrufzertifikate auszustellen [Ruep_95]. Rückrufzertifikate sind Zertifikate, die die folgenden Einträge enthalten:

- Seriennummer des zurückzurufenden Zertifikats
- Rückrufzeitpunkt und Rückrufgrund (optional)
- Initiator des Rückrufs und vermuteter Kompromittierungszeitpunkt
- sowie Angaben zur Signatur (Algorithmus) und der das Zertifikat ausstellenden Zertifizierungsinstanz.

Rückrufzertifikate haben gegenüber CRLs die folgenden Vorteile:

- Sie können (ähnlich Delta-CRLs) unmittelbar nach Eingang eines Sperrantrags und unabhängig von einem CRL-Publikationstermin ausgestellt und im Verzeichnisdienst publiziert werden
- Benutzer müssen nicht eine komplette CRL laden und prüfen, sondern können sich auf ein einziges Zertifikat beschränken.

Sie haben allerdings auch einen wichtigen Nachteil: Rückrufzertifikate erfordern einen Online-Zugriff auf einen Verzeichnisdienst. Eine verläßliche Signaturprüfung ist damit offline nicht möglich; das jedoch erlauben CRLs in dem angegebenen Gültigkeitszeitraum.

4 Online-Gültigkeitsabfrage

Für besonders sensible Informationen kann es jedoch auch erforderlich sein, die Gültigkeit eines Schlüsselzertifikats zweifelsfrei feststellen zu können. Diesem Zweck dienen Online-Abfragedienste, über die bei einer CA oder einer dafür vorgesehenen Instanz der Status eines Zertifikats verläßlich erfragt werden kann.

4.1 Online Certificate Status Protocol

Mit der Spezifikation von OCSP (Online Certificate Status Protocol) wird im Rahmen der PKIX-Spezifikation derzeit von der IETF ein Protokoll standardisiert, das eine online-Abfrage des Zertifikats-Status erlaubt [MAMG+_98].

Das Protokoll besteht aus einem einfachen Request und einer digital signierten Response einer autorisierten Stelle. Die Anfrage kann optional ebenfalls digital signiert werden. Das Zertifikat, dessen Status abgefragt werden soll, wird dabei durch einen Hashwert des Namens des Issuers, einen Hashwert des Public Keys des Issuers und die Seriennummer des Zertifikats identifiziert (CertID, siehe Abb. 5).

```
OCSPRequest      ::=    SEQUENCE {
     tbsRequest           TBSRequest,
     optionalSignature [0]EXPLICIT Signature OPTIONAL }

TBSRequest::=    SEQUENCE {
     version [0]                 EXPLICIT Version DEFAULT v1,
     requestorName [1]           EXPLICIT GeneralName OPTIONAL,
     requestList                 SEQUENCE OF Request,
     requestExtensions [2]       EXPLICIT Extensions OPTIONAL }

Signature   ::=  SEQUENCE {
     signatureAlgorithm  AlgorithmIdentifier,
     signature           BIT STRING,
     certs [0]           EXPLICIT SEQUENCE OF Certificate OPTIONAL}

Request     ::=  SEQUENCE {
     reqCert       CertID,
     singleRequestExtensions [0]       EXPLICIT Extensions OPTIONAL }

CertID  ::=  SEQUENCE {
     hashAlgorithm       AlgorithmIdentifier,
     issuerNameHash      OCTET STRING, -- Hashwert des DN des Issuers
     issuerKeyHash       OCTET STRING, -- Hashwert des Public Key des Issuers
     serialNumber        CertificateSerialNumber }
```

Abb. 5: OCSP-Anfrageformat [MAMG+_98]

Die Antwort der OCSP-Instanz enthält neben einer Status-Meldung, in der beispielsweise die Nichtverfügbarkeit der Instanz zurückgemeldet werden kann, eine digital signierte, mit einem Ausstellungszeitpunkt und einem Gültigkeitszeitraum versehene Angabe des gesuchten Zertifikats-Status (good/revoked/unknown; siehe Abb. 6).

```
BasicOCSPResponse      ::=    SEQUENCE {
     tbsResponseData          ResponseData,
     signatureAlgorithm  AlgorithmIdentifier,
```

```
        signature     BIT STRING,
        certs [0]     EXPLICIT SEQUENCE OF Certificate OPTIONAL }

ResponseData      ::=     SEQUENCE {
        version [0]           EXPLICIT Version DEFAULT v1,
        responderID           ResponderID,
        producedAt            GeneralizedTime,
        responses             SEQUENCE OF SingleResponse,
        responseExtensions [1]    EXPLICIT Extensions OPTIONAL }

SingleResponse    ::=     SEQUENCE {
        certID          CertID,
        certStatus      CertStatus,
        thisUpdate      GeneralizedTime,
        nextUpdate [0]        EXPLICIT GeneralizedTime OPTIONAL,
        singleExtensions [1] EXPLICIT Extensions OPTIONAL }

CertStatus  ::=     CHOICE {
        good [0]              IMPLICIT NULL,
        revoked [1]           IMPLICIT RevokedInfo,
        unknown [2]           IMPLICIT UnknownInfo }

RevokedInfo       ::=     SEQUENCE {
        revocationTime        GeneralizedTime,
        revocationReason [0]      EXPLICIT CRLReason OPTIONAL }
```

Abb. 6: OCSP-Response-Format [MAMG+_98]

Im Fall einer vorliegenden Sperrung des Zertifikats werden der Sperrzeitpunkt und die Rückrufgründe (analog dem CRL-Format nach X.509v2) zurückgeliefert. Die Response kann im Feld singleExtension auch einen Hinweis auf eine CRL enthalten, in der der entsprechende Rückruf gefunden werden kann.

4.2 Anforderungen nach SigG

Das Signaturgesetz (SigG) verlangt explizit, daß Zertifikate über öffentliche Telekommunikationsverbindungen nicht nur abrufbar, sondern auch nachprüfbar sein müssen (§ 5 SigG [SigG_97]). Damit fordert das Signaturgesetz die Bereitstellung einer Online-Gültigkeitsabfrage als Dienst der CA.

Ein solcher Abfragedienst muß Anfragen nach der Gültigkeit eines Zertifikats bei Angabe des Zertifikats und eines Datums verläßlich (d.h. mit digitaler Signatur der Zertifizierungsstelle) beantworten. Das Protokoll für einen solchen Dienst wird derzeit im Rahmen der Interoperabilitäts-Spezifikation des BSI festgelegt [Berg_99]. Der aktuelle Vorschlag basiert auf OCSP, erweitert dieses Protokoll jedoch um zwei Möglichkeiten:

- die Angabe eines (zurückliegenden) Zeitpunkts, für den die Gültigkeit angegeben werden soll, sowie
- die Möglichkeit, eine Zusendung des Zertifikats zusammen mit der Response beim Request anzufordern.

5 Ansatz von Rivest

Von Ronald L. Rivest stammt ein interessanter Ansatz, der das „CRL-Paradigma“ in Frage stellt. Nach seiner Überzeugung sollte nicht demjenigen, der ein Zertifikat überprüfen möchte, die Aufgabe der CRL-Abfrage und -Prüfung aufgebürdet werden, sondern müsse umgekehrt der Schlüsselinhaber in die Pflicht genommen werden: Es sei Sache des Schlüsselinhabers, seinen Schlüssel zusammen mit einer Bestätigung einer vertrauenswürdigen dritten Instanz zu versenden, daß der Schlüssel gültig und nicht gesperrt ist.

Vorteil dieses Ansatzes ist, daß er auch die dritte bei der Prüfung der Gültigkeit von Zertifikaten zu überprüfende Bedingung für den Nutzer des Zertifikats objektiv prüfbar macht. Umgekehrt verlagert sich damit das Risiko auf die bestätigende Instanz. Für die Praxis wichtig ist dabei, daß der Aufwand für die Prüfung von Zertifikaten und deren Komplexität erheblich reduziert werden kann. Auch die für die Versendung von CRLs und ARLs erforderliche Kommunikationsbandbreite kann verringert werden.

Naturgemäß wird das Gültigkeitsintervall einer solchen Bestätigung jedoch kürzer sein als das eines herkömmlichen Zertifikats. Daher wird die Last der solche Bestätigungen ausstellenden Instanz stark ansteigen.

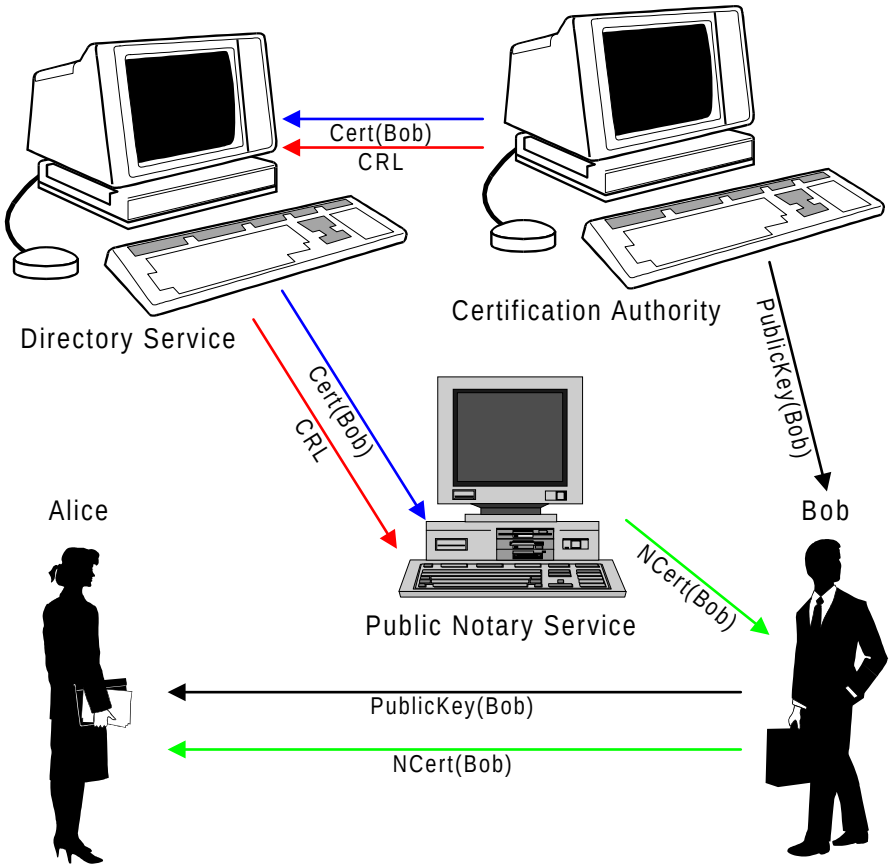

Abb. 7: Einsatz von „Notariaten“

Dieser Aufwand kann dadurch „skaliert“ werden, daß eine zwischen Schlüsselinhaber und CA angesiedelte „Notariatsinstanz“ eingeführt wird, die auf der Basis ihr bekannter Zertifikate und CRLs/ARLs, möglicherweise unterstützt durch einen Online-

Status-Anfragedienst kurzzeitig (z.B. nur wenige Stunden) gültige Bestätigungen für Schlüsselinhaber ausstellt. Die in großen Infrastrukturen aufwendige regelmäßige Verteilung von aktuellen CRLs kann damit unterbleiben.

6 Folgerungen

In der Praxis bergen Schlüsselzertifikate eine Reihe von Schwierigkeiten. Zum einen führt die Offline-Generierung zu einem Aktualitätsproblem: Zertifikate können aus unterschiedlichen Gründen (z.B. Verlust des geheimen Schlüssels des Schlüsselinhabers oder Kompromittierung des Schlüssels) vorzeitig ungültig werden.

Auch der Rückruf von Zertifikaten verursacht Probleme: Rückruflisten (CRLs) müssen verteilt, von den Kommunikationsteilnehmern geprüft und ausgewertet werden. Dies verursacht ggf. einen erheblichen zusätzlichen Bedarf an Kommunikationsbandbreite; außerdem stellen CRLs zusätzliche Anforderungen z.B. an die Verfügbarkeit der Rückruflisten im Verzeichnisdienst.

Eine Möglichkeit, Lastspitzen beim Zugriff auf CRLs zu vermeiden, ohne einen online-verfügbaren Prüfdienst (mit den damit einhergehenden Nachteilen) einzuführen, ist die folgende:

- Teil-CRLs werden für einen Gültigkeitszeitraum von bis zu einem Monat ausgestellt und im Verzeichnisdienst publiziert.
- Aktualisierte Teil-CRLs (CRL Distribution Points) werden täglich in den Verzeichnisdienst (X.500) aufgenommen und über den dort vorgesehenen Replikationsmechanismus verteilt. Eine neue Teil-CRL ist auch dann auszustellen, wenn seit der Publikation der letzten Teil-CRL keine Rückrufe erfolgt sind (die aktualisierte Teil-CRL enthält in diesem Fall dieselben Rückrufe, aber besitzt einen geänderten Gültigkeitszeitraum).

Da eine (Teil-) CRL bis zu einem Monat gültig ist, aber täglich aktualisiert wird, können zu einem Zeitpunkt mehrere (Teil-) CRLs einer Zertifizierungsstelle gültig sein. Wichtig ist allerdings, daß immer (nur) die von der zuständigen CA zuletzt ausgegebene (Teil-) CRL im Verzeichnisdienst abgerufen werden kann.

Über die Akzeptanz der jeweils vorliegenden Rückrufliste muß bei der Prüfung des Zertifikats entschieden werden. Dazu sollte in der Prüfkomponente ein Gültigkeitszeitraum für die lokal gespeicherte Teil-CRLs festgelegt werden können, der zwischen 0 („immer aktuelle CRL prüfen“) und der Gültigkeit der Teil-CRL variieren kann.

Dieses Vorgehen hat mehrere Vorteile:

- Durch die Verwendung von CRL Distribution Points werden nur diejenige Teil-CRL vom nächsten Verzeichnisdienst angefordert, in der sich ein Rückruf für das zu prüfende Zertifikat befinden könnte.
- Die Anforderung aktueller Rückruflisten erfolgt nicht durch alle Clients zugleich an einem einheitlichen Veröffentlichungstermin, sondern nur im Bedarfsfall oder

höchstens im 24-Stunden-Rhythmus.[7]

- Durch eine Verringerung des Gültigkeitszeitraums lokal gespeicherter Teil-CRLs kann zugleich nach Bedarf die Aktualität der Gültigkeitsprüfung benutzerkontrolliert vergrößert oder verringert werden.

Das Setzen auf einen Online-Abfragedienst als Ersatz für die Abfrage und Verwendung von CRLs (durch OCSP oder ein Protokoll nach Signaturgesetz) führt hingegen die Idee von Zertifikaten ad absurdum. Denn bei einer Online-Prüfmöglichkeit genügt technisch der Schlüssel selbst (oder eine eindeutige Schlüssel-ID) als Identifikator; Zertifikate als „offline-Gültigkeitsnachweis" sind damit vollständig überflüssig.

Eine sehr interessante Alternative zur Verwendung von CRLs ist der Einsatz von „Notariaten", die die Gültigkeit von Zertifikaten kurzfristig bestätigen. Dieses Konzept erfordert jedoch den Verzicht auf das heute allgemein verbreitete „CRL-Paradigma"; daher ist eine Durchsetzung dieses Konzepts derzeit leider unwahrscheinlich.

7 Literatur

AdFa_98 Adams, Carlisle; Farrell, S.: *Internet X.509 Public Key Infrastructure: Certificate Management Protocols*. <draft-ietf-pkix-ipki3cmp-09.txt>, November 1998.

AdZu_98 Adams, Carlisle; Zuccherato, Robert: *A General, Flexible Approach to Certificate Revocation*. Entrust Technologies White Paper, June 1998.

Berg_99 Berger, Andreas: *Signatur-Interoperabilitätsspezifikation: Zertifikate und Dokumentenformate*. Tagungsband des 9. GMD-SmartCard-Workshops, Darmstadt, Februar 1999, S. 15.1-15.10.

HFPS_99 Housley, R.; Ford, W.; Polk, W.; Solo, D.: *Internet X.509 Public Key Infrastructure, Certificate and CRL Profile*. Request for Comments (RFC) 2459, Januar 1999.

ITU_93 International Telecommunication Union: *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*. ITU-T Recommendation X.509 (1993 E).

Kohn_78 Kohnfelder, L. M.: *A Method for Certification*. MIT Lab. for Computer Science, Cambridge, May 1978.

MAMG+_98 Myers, Michael; Ankney, Rich; Malpani, Ambarish; Galperin, Slava; Adams, Carlisle: *Online Certificate Status Protocol – OCSP*. <draft-ietf-pkix-ocsp-07.txt>, September 1998.

Rive_98 Rivest, Ronald L.: *Can We Eliminate Certificate Revocation Lists?* Proceedings of Financial Cryptography, 1998.

Ruep_95 Rueppel, Rainer A.: *Revocation and Revocation Certificates*. Proceedings of the EDI Trusted Third Party Workshop, Barcelona (SP) 1995, S. 1-8.

[7] Dennoch werden sich Lastspitzen zu Tagesbeginn (wenn Mitarbeiter ihre E-Mails lesen) in der Praxis wahrscheinlich nicht vermeiden lassen.

SigG_97 *Gesetz zur digitalen Signatur (Signaturgesetz – SigG)*. Beschluß des Bundestages vom 13. Juni 1997 (BT-Drs. 13/7934 vom 11.06.97) und Bundesrates vom 4. Juli 1997; in Kraft seit 1. August 1997.

SigV_97 *Verordnung zur digitalen Signatur (Signaturverordnung – SigV)*. Beschluß der Bundesregierung vom 8. Oktober 1997; in Kraft seit 1. November 1997.