secorvo
security consulting

Public Key Infrastrukturen

Secorvo White Paper

Vertrauensmodelle und PKI-Komponenten

Version 1.1
Stand 21. April 2011

Petra Barzin

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100

info@secorvo.de
www.secorvo.de

Inhaltsübersicht

Abkürzungen

AD	Active Directory
APDU	Application Protocol Data Unit
API	Application Programming Interface
CA	Certification Authority
CMS	Cryptographic Message Standard / Cryptographic Message Styntax
CP	Certificate Policy, Zertifizierungsrichtlinie
CPS	Certification Practice Statement, Regelungen für den Zertifizierungsbetrieb
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
EB-CA	European Bridge CA
EG	Europäische Gemeinschaft
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISIS	Industrial Signature Interoperability Specification
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU -Telecommunication Standardization Sector
LDAP	Lightweight Directory Access Protocol
MTT	MailTrusT
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PSE	Personal Security Environment
PKI	Public Key Infrastructure
PKIX	Public-Key Infrastructure (X.509)
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest, Shamir, Adleman Kryptosystem
SigG	Signaturgesetz
TSP	Time-Stamp Protocol

URL	Uniform Resource Locator
USB	Universal Serial Bus
XML	Extensible Markup Language
ZPO	Zivilprozessordnung

Historie

Version	Datum	Änderung	Autor
1.0	01.03.11	Erstfassung	Petra Barzin
1.1	21.04.11	Korrekturen und Ergänzungen	Petra Barzin

1 Zusammenfassung

Dieses Dokument richtet sich an PKI-Einsteiger. Es beschreibt, wofür eine PKI benötigt wird, vermittelt die Grundlagen einer PKI und gibt einen Überblick über die verschiedenen PKI Komponenten und Prozesse. Aufbau und Inbetriebnahme einer PKI sind als Themen für PKI-Fortgeschrittene nicht Gegenstand dieses White Papers.

In Kapitel 2 wird zunächst in dies Problematik des Schlüsselmanagements für asymmetrische Kryptoverfahren eingeführt und der Bedarf für eine PKI motiviert.

Die Verteilung und Verwaltung von öffentlichen Schlüsseln kann über ein „Web of Trust“ dezentral organisiert oder mittels einer zentralisierten PKI realisiert werden. Die Funktionsweise beider Ansätze wird in Kapitel 3 vergleichend dargestellt.

Die öffentlichen Schlüssel werden den Schlüsselinhabern über eine Art „digitalen Ausweis“ zugeordnet. Dieser Ausweis wird als Zertifikat bezeichnet. In Kapitel 4 wird beschrieben, wie ein solches Zertifikat aussieht, welche Konzepte einer PKI zugrunde liegen und welche Komponenten für eine PKI erforderlich sind.

Kapitel 5 beschreibt die relevanten PKI Standards. Neben dem X.509-Standard gibt es zahlreiche Internetstandards (RFCs), Public Key Cryptography Standards (PKCS) und in Deutschland – wichtig im Behördenumfeld - die Common-PKI-Spezifikationen.

Die verschiedenen Möglichkeiten zur Verknüpfung von unterschiedlichen PKIs, um eine Zusammenarbeit von Teilnehmern aus unterschiedlichen Organisationen und Bereichen über die Grenzen ihrer jeweiligen PKI hinweg zu ermöglichen, sind in Kapitel 6 erläutert. Empfehlenswert ist in diesem Zusammenhang auch die Lektüre des Secorvo White Papers „Das Policy-Rahmenwerk einer PKI“ [WP15].

Wenn digital signierte Dokumente elektronisch archiviert werden sollen, ergeben sich neue zusätzliche Anforderungen an das Archivierungssystem. Ein Lösungsansatz zur Langzeit-archivierung von PKI-bezogenen Daten wird in Kapitel 7 beschrieben.

2 Einführung

Public-Key-Anwendungen wie Digitale Signaturen, Benutzerauthentifikation und Verschlüsselung erfordern die Zuordnung von Schlüsseln zu einem Schlüsselinhaber. Dieses White Paper beschreibt, wie öffentliche Schlüssel verteilt und verwaltet werden. Hierbei gibt es in der Praxis zwei konkurrierende Ansätze, die auf verschiedenen Vertrauensmodellen basieren. Diese beiden unterschiedlichen Ansätze werden im Folgenden verdeutlicht und ihre Funktionsweise dargestellt. Hierbei werden die einzelnen Komponenten und Prozesse einer Public Key Infrastruktur (PKI) beschrieben.

Asymmetrische Kryptoverfahren nutzen Schlüsselpaare, bestehend aus einem privaten und einem korrespondierenden öffentlichen Schlüssel, um Nachrichten digital zu signieren, zu verschlüsseln oder Inhaber solcher Schlüsselpaare zu authentisieren. Zur Verifikation von Digitalen Signaturen, zur Verschlüsselung und zur Prüfung der Authentifikation werden die öffentlichen Schlüssel benötigt, d. h. diese müssen für alle Kommunikationspartner sicher verteilt und verwaltet werden. Für eine skalierbare Lösung dieses Schlüsselmanagements sollte zur Verteilung der öffentlichen Schlüssel möglichst kein persönlicher Kontakt erforderlich sein.

Wenn viele Kommunikationspartner, die sich gegebenenfalls gar nicht vorab kennen, ihre Schlüssel untereinander austauschen wollen, reicht der Austausch des öffentlichen Schlüssels alleine oft nicht aus, um sicher miteinander kommunizieren zu können. Es wird eine eindeutige Zuordnung des öffentlichem Schlüssels zum jeweiligen Schlüsselinhaber

benötigt, die eine „Relying Party“ (Zertifikatsprüfer) überprüfen kann, um sich zu überzeugen, dass eine Nachricht tatsächlich von dem vermeintlichen Absender digital signiert wurde bzw. der öffentliche Schlüssel, der zur Verschlüsselung einer vertraulichen Nachricht verwendet werden soll, zweifelsfrei dem Empfänger zugeordnet werden kann. Im Fall der Authentifizierung muss sichergestellt werden, dass der Benutzer sich mit seiner echten Identität am System anmeldet. Auch dafür muss die eindeutige Zuordnung eines Schlüssels zu einem Schlüsselinhaber demzufolge nachprüfbar sein.

Neben der sicheren Verteilung der öffentlichen Schlüssel muss es zudem auch noch eine Möglichkeit geben, Rückruf-Informationen zu ungültigen Schlüsseln zu verteilen, um Schlüssel im Fall einer Kompromittierung – oder weil die Zuordnung von Schlüssel zu Inhaber aus anderen Gründen nicht mehr gegeben ist, bspw. beim Ausscheiden eines Teilnehmers aus der Firma – als ungültig kennzeichnen zu können.

Zur sicheren Verteilung und Verwaltung der öffentlichen Schlüssel gibt es in der Praxis zwei konkurrierende Ansätze, die nachfolgend näher erläutert werden:

- Das dezentrale Vertrauensmodell, das als „Web of Trust“ bezeichnet wird
- Das zentrale Vertrauensmodell basierend auf einer PKI

3 Vertrauensmodelle

Für eine sichere Kommunikation bedarf es ein gewisses Maß an Vertrauen in die Zuordnung der verwendeten Schlüssel zum jeweiligen Schlüsselinhaber. Um einem öffentlichen Schlüssel in diesem Sinne vertrauen zu können, muss die Echtheit des Schlüssels und die Zugehörigkeit zu einer Person entweder von jedem Anwender selbst nachgeprüft – was, falls überhaupt durchführbar, schon bei moderaten Anwenderzahlen zu unverhältnismäßig hohem Aufwand führt – oder aber von einer vertrauenswürdigen Stelle bestätigt werden. Nachfolgend werden zwei Modelle dargestellt, wie Schlüssel bestätigt und vertrauensvoll verteilt werden können.

3.1 Web of Trust

Das Web of Trust bietet keine zentrale technische oder organisatorische Infrastruktur, sondern die Verteilung der öffentlichen Teilnehmerschlüssel erfolgt selbstorganisiert nach einem dezentralen Vertrauensmodell. Das Vertrauen basiert auf Gegenseitigkeit, wobei das Modell auch mittelbares Vertrauen zulässt, d. h. das Vertrauen in einen Schlüssel kann an einen Dritten weitergegeben werden. Das Web of Trust wird vorwiegend für private und persönliche Kommunikation verwendet, findet aber auch im geschäftlichen Umfeld Verwendung.

Der Schlüsselaustausch zwischen den Kommunikationspartnern erfolgt über eine persönliche Weitergabe des öffentlichen Schlüssels. Zur Überprüfung des übermittelten öffentlichen Schlüssels werden i. d. R. Hash-Werte des öffentlichen Schlüssels – sogenannte Fingerprints – verwendet. Sie erlauben einen effizienteren Vergleich des abgesandten mit dem empfangenen öffentlichen Schlüssel, als wenn der volle öffentliche Schlüssel (typischerweise eine zufällig gewählte Zahl von 300 oder mehr Stellen) abgeglichen werden müsste. Bei einer elektronischen Übertragung des öffentlichen Schlüssels sollte diese Überprüfung der Hash-Werte Out-of-Band, d. h. über einen anderen Kommunikationskanal erfolgen, z. B. über das Telefon. Alle Teilnehmer bestätigen sich so gegenseitig die Echtheit ihrer Schlüssel. Dabei muss jedoch nicht jeder Schlüssel von jedem anderen Teilnehmer geprüft und bestätigt werden, sondern das Vertrauen in Schlüssel kann weitergegeben werden. Durch diese vielen und teilweise auch transitiven Vertrauensbeziehungen entsteht das Web of Trust. Mit dem Web of Trust ist somit ein direkter und schneller Schlüsselaustausch

möglich, der allerdings ein persönliches Treffen oder eine zusätzliche Kommunikation voraussetzt und nur zwischen einander bekannten Kommunikationspartnern funktioniert.

Der Rückruf eines öffentlichen Schlüssels ist nur dann zuverlässig möglich, wenn dieser noch nicht an Dritte weitergegeben wurde. Wurde der Schlüssel weitergegeben, kann nicht sichergestellt werden, dass die Rückrufinformation wirklich alle Kommunikationspartner erreicht.

Im Vertrauensmodell des Web of Trust bestätigt ein Schlüsselinhaber die Echtheit seines eigenen öffentlichen Schlüssel durch die Signatur mit seinem zugehörigen privaten Schlüssel, d. h. in der Regel sind alle Schlüssel selbstsigniert, d.h. mit dem eigenen privaten Schlüssel signiert. Es gibt aber auch die Möglichkeit, verschiedene fremde Teilnehmerschlüssel von einer vertrauenswürdigen Instanz signieren zu lassen. Über das Konzept eines solchen *Trusted Introducers* kann auch – ähnlich wie im nachfolgend beschriebenen zentralen Vertrauensmodell - eine zentrale Instanz als Bestätigungsstelle fungieren. Der Trusted Introducer prüft öffentliche Schlüssel und bestätigt diese durch seine Digitale Signatur. Typischerweise gibt es beim Einsatz in einem Unternehmen einen oder wenige solcher Trusted Introducer. Der Vorteil eines Trusted Introducers besteht darin, dass externe Kommunikationspartner sich nur noch von der Echtheit des öffentlichen Schlüssels des Trusted Introducers überzeugen müssen und dann allen öffentlichen Schlüsseln vertrauen können, die von diesem Trusted Introducer digital signiert wurden. D. h. der externe Kommunikationspartner prüft nur noch die Digitale Signatur des Trusted Introducers und muss nicht mehr die Fingerprints aller öffentlichen Schlüssel verifizieren. Die Sicherheit dieses Verfahrens beruht somit auf dem Vertrauen in den Trusted Introducer. Die Verteilung der öffentlichen Teilnehmerschlüssel kann durch sogenannte Key Server erfolgen. Allerdings ist dann auch kein systematischer Rückruf von Schlüsseln mehr möglich, da potentiell jeder die Schlüssel vom Server abrufen kann und deren Verbreitung dann nicht mehr nachvollziehbar ist.

Die Rückrufinformation eines Schlüssels wird in diesem Verfahren über ein zusätzliches Attribut an den Schlüssel angehängt und dieser dann erneut auf einem Key Server publiziert. Verfahrensbedingt gibt es aber keine Notwendigkeit für einen externen Kommunikationspartner, einen bereits lokal vorhandenen öffentlichen Schlüssel erneut vom Key Server zu holen. Somit bleibt der Sperrvermerk ggf. unbemerkt.

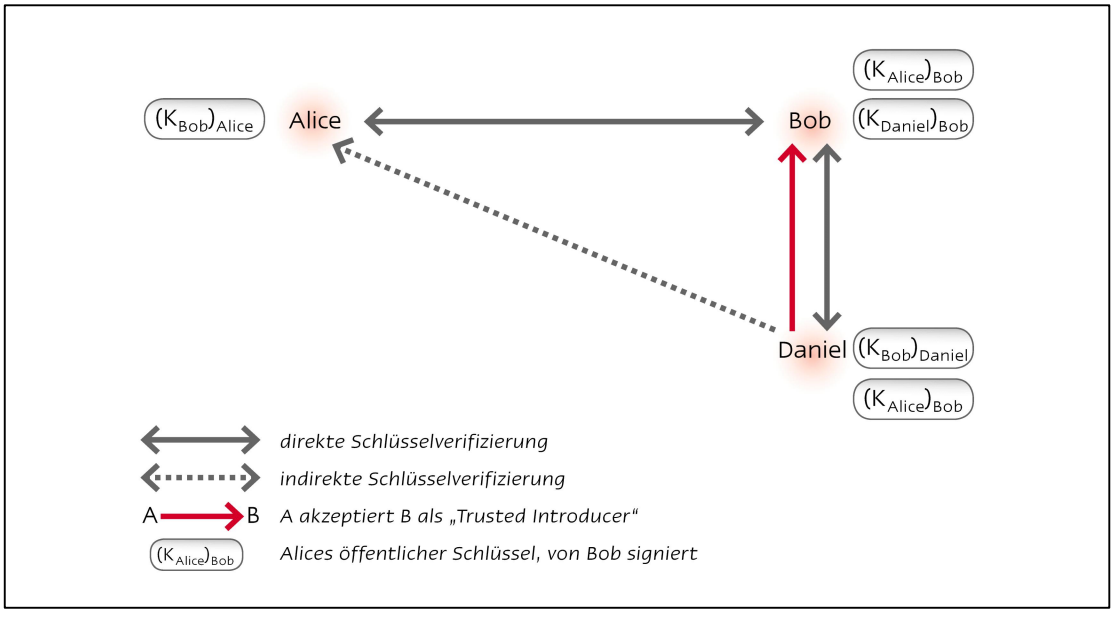

Abbildung 1: Beispiel „Web of Trust“

Das Sicherheitsniveau des Web of Trust lässt sich nicht klar einschätzen. Im Allgemeinen ist nicht reglementiert und dokumentiert, wie Schlüssel erzeugt und Identitäten sowie Fingerprints überprüft werden. Die Sperrung von öffentlichen Schlüsseln kann nicht durchgesetzt werden.

Das Beispiel in Abbildung 1 zeigt, wie das dezentrale Vertrauensmodell funktioniert. Alice und Bob sowie Daniel und Bob haben bilateral ihre öffentlichen Schlüssel ausgetauscht und vertrauen sich gegenseitig. Daniel akzeptiert Bob als Trusted Introducer und hat damit auch eine indirekte Vertrauensbeziehung zu Alice (indirekte Schlüsselverifizierung).

3.2 Zentrales Modell (PKI)

Das zentrale Vertrauensmodell basiert auf einer zentralen Infrastruktur, der Public Key Infrastruktur (PKI). Durch die PKI werden die zentralen Dienste des Schlüsselmanagements erbracht. Die Prozesse und Verantwortlichkeiten sind klar geregelt. Die Regelungen für die PKI werden in Policy-Dokumenten festgelegt.

In einer PKI werden die öffentlichen Schlüssel durch eine vertrauenswürdige Instanz – die sogenannte Zertifizierungsstelle – bestätigt. Alle Kommunikationspartner, die einen durch die betreffende PKI bestätigten Schlüssel verwenden wollen, müssen nur dieser Zertifizierungsstelle vertrauen. Ein weiterer Vorteil ist, dass nur eine einzige Überprüfung des Schlüssels pro Teilnehmer, nämlich mit der Zertifizierungsstelle, nötig ist. Die Kommunikationspartner untereinander müssen ihre öffentlichen Schlüssel nicht mehr bilateral auf sichere Weise austauschen und überprüfen.

Die öffentlichen Schlüssel können in einem sogenannten Schlüsselverzeichnis publiziert werden. Es genügt, vor der Verwendung eines aus diesem Verzeichnis abgerufen öffentlichen Schlüssels die beigefügte Bestätigung der Zertifizierungsstelle zu überprüfen.

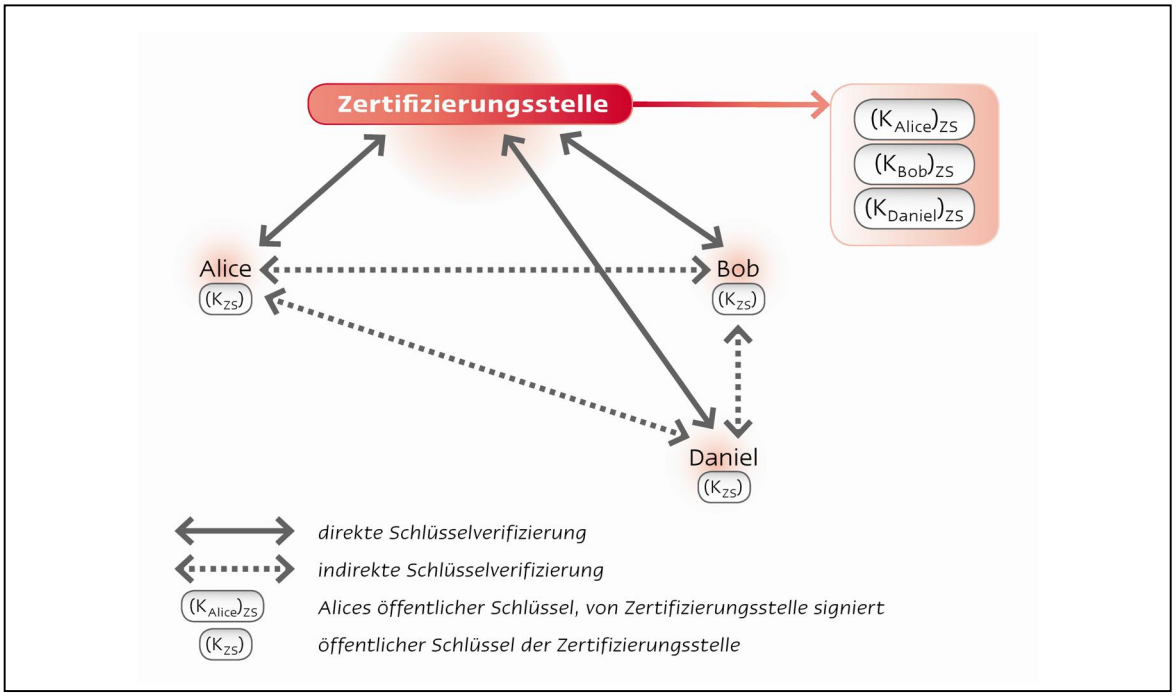

Abbildung 2: Beispiel „Zentrales Vertrauensmodell“

Das Beispiel in Abbildung 2 zeigt, wie das zentrale Vertrauensmodell funktioniert. Alice, Bob, und Daniel haben alle eine direkte Vertrauensbeziehung zu der Zertifizierungsstelle. Da alle der gleichen Zertifizierungsstelle vertrauen, haben sie auch alle untereinander eine indirekte

Vertrauensbeziehung. Die Zertifizierungsstelle veröffentlicht alle von ihr bestätigten öffentlichen Schlüssel in einem Schlüsselverzeichnis.

4 Public Key Infrastruktur

4.1 Zertifikate und CRLs

Die Bestätigung der Zuordnung zwischen Schlüssel und Schlüsselinhaber wird in einer PKI über Zertifikate ausgedrückt. Diese Zertifikate dienen als eine Art „digitaler Ausweis“. Das gebräuchliche Format für PKI-Zertifikate wurde von der ITU im Standard X.509 festgelegt [X509].

Zertifikate werden von einer Zertifizierungsstelle oder englisch *Certification Authority* (CA) ausgestellt. Sie bestätigt in einem formal aufgebauten elektronischen Dokument mit ihrer Digitalen Signatur, dass ein vorliegender öffentlicher Schlüssel dem benannten Schlüsselinhaber zugeordnet ist. Über die Digitale Signatur der CA wird die Integrität und Authentizität der Zuordnung von öffentlichem Schlüssel und Schlüsselinhaber gewährleistet. Diese Zuordnung kann nicht unbemerkt verfälscht werden, es sei denn ein Angreifer hat den privaten Schlüssel der CA kompromittiert, der zur Signaturerstellung benötigt wird.

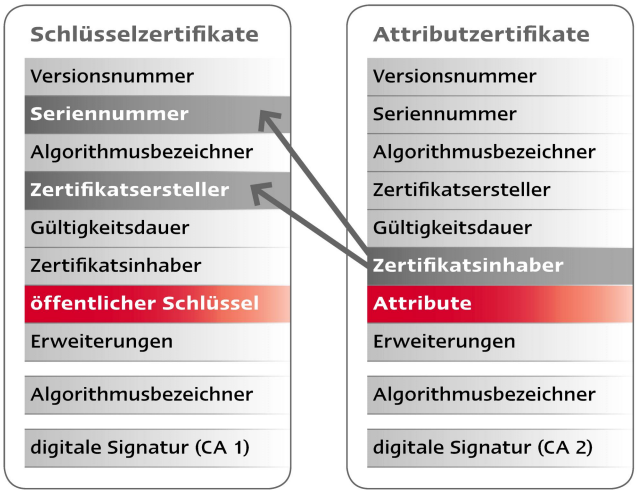

Abbildung 3: Aufbau Schlüssel- und Attributzertifikate

Zertifikate enthalten in der Regel außer dem Namen des Schlüsselinhabers, seinem öffentlichen Schlüssel, einer eindeutigen Seriennummer und einer Gültigkeitsdauer noch weitere Zusatzinformationen, z. B. Nutzungsbeschränkungen, alternative Namensformen oder Informationen für einen vereinfachten Aufbau des Zertifizierungspfades. Weitere Informationen zu Zertifikatsinhalten finden sich in [RFC5280] und [X509].

Außer diesen sogenannten Schlüsselzertifikaten gibt es noch Attributzertifikate, die zusätzliche Informationen an das Schlüsselzertifikat und damit an den Zertifikatsinhaber binden (siehe Abbildung 3). Der Zertifikatsinhaber wird hierbei über eine Referenz auf sein Schlüsselzertifikat identifiziert. Hintergrund der Attributzertifikate ist das Bestreben, nicht zu viele personenbezogene Daten in dem Schlüsselzertifikat aufzunehmen, sondern diese in ein oder mehrere Attributzertifikate auszulagern. Außerdem können die zusätzlichen Attribute im Attributzertifikat mit einer kürzeren Gültigkeitsfrist versehen werden als das Schlüsselzertifikat oder separat davon gesperrt werden. Je nach Anwendung kann der

Zertifikatsinhaber das Attributzertifikat auswählen, das die für diese Anwendung benötigten Informationen enthält.

Soll ein Zertifikat zurückgezogen werden, z. B. weil der Schlüssel kompromittiert wurde oder der Schlüsselinhaber seinen Namen gewechselt hat, so setzt die CA die Seriennummer dieses zu sperrenden Zertifikats auf ihre Sperrliste (Certificate Revocation List, CRL). Eine CRL ist eine von der CA signierte Liste mit einer begrenzten Gültigkeit, welche die Seriennummern aller durch diese CA gesperrten Zertifikate enthält (siehe Abbildung 4). Bei der Verifikation eines Zertifikats greift die „Relying Party“ auf die aktuelle CRL zurück und prüft, ob die Seriennummer des zu prüfenden Zertifikats dort enthalten ist.

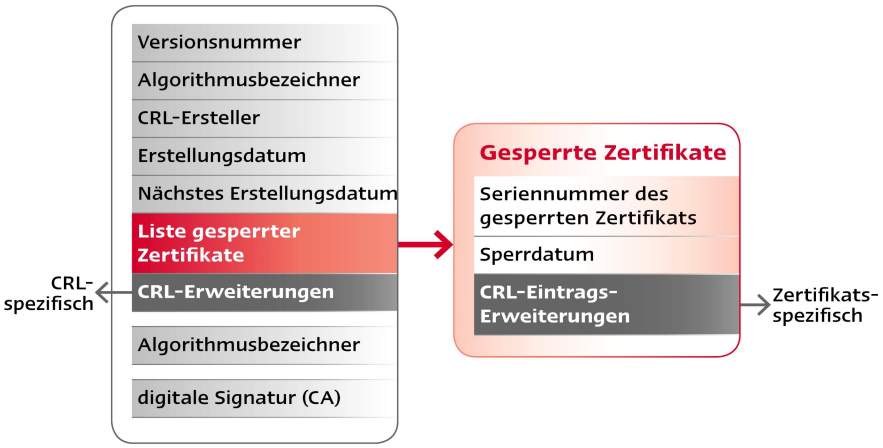

Abbildung 4: Aufbau einer CRL

Ein Nachteil von Sperrlisten ist, dass eine Sperrliste für einen definierten Zeitraum gültig ist, nämlich vom Erstellungsdatum bis zum nächsten geplanten Erstellungsdatum. Wird in diesem Zeitraum ein Zertifikat zurückgezogen, ergeben sich für die ausstellende CA zwei Alternativen: Entweder sie stellt umgehend eine neue Sperrliste aus oder sie wartet mit der Ausstellung der neuen Sperrliste bis regulär die nächste Sperrliste ausgestellt wird. Im ersten Fall gibt es zwei gültige Sperrlisten, d.h. ein Angreifer könnte z. B. die aktuelle Sperrliste im Verzeichnis durch die alte noch gültige Sperrliste ersetzen, um die Sperrung des betreffenden Zertifikats zu vertuschen. Im zweiten Fall gibt es zwar immer nur eine gültige Sperrliste, aber die Sperrinformation wird der „Relying Party“ (Zertifikatsprüfer) bis zur Veröffentlichung der nächsten Sperrliste vorenthalten. Daher ist es empfehlenswert, bei Rückruf eines Zertifikats umgehend eine neue Sperrliste auszustellen und zu veröffentlichen, so dass für eine „Relying Party“ die aktuellen Sperrinformationen sofort verfügbar sind. Allerdings gibt es in der Praxis einige Anwendungen, die sich keine aktuelle Sperrliste holen, solange die letzte lokal vorliegende Sperrliste noch nicht abgelaufen ist. Diese Restrisiken von nicht bekannten Sperrinformationen sind umso geringer, je kürzer der Ausstellungszyklus einer Sperrliste gewählt wird.

Schlüsselzertifikate, Attributzertifikate und Sperrlisten werden in dem Standard X.509 definiert [X509]. Seit der Version 3 dieses Standards gibt es die Möglichkeit, über Erweiterungen zusätzliche Informationen in einem Zertifikat, einer CRL oder CRL-Einträgen hinzuzufügen. So können in X.509v3 Zertifikaten beispielsweise:

- zusätzliche Namensformen wie eine E-Mail Adresse angegeben werden,
- zwischen Benutzer und CA Zertifikaten unterschieden werden,
- die Verwendung des öffentlichen Schlüssels eingeschränkt (bspw. auf die ausschließliche Verwendung digitalen Signatur von CRLs) oder

- mehrere URLs spezifiziert werden, über die CA-Zertifikat und CRLs heruntergeladen werden können.

4.2 Zertifizierungshierarchien

CAs stellen nicht nur Zertifikate für Endteilnehmer (wie z. B. Benutzer, Client-Computer oder Server) aus, sondern auch für untergeordnete Zertifizierungsstellen. So entstehen baumförmige Zertifizierungshierarchien mit einer Wurzelzertifizierungsstelle (Root-CA) als oberstem (Wurzel-)Knoten, mehreren zwischengeordneten Zertifizierungsstellen (Intermediate-CAs) und den Endteilnehmern als Blattknoten. Der öffentliche Schlüssel der Root-CA (der üblicherweise in Form eines selbst signierten Zertifikats der Root-CA vorliegt) dient als Sicherungsanker für die gesamte PKI und muss bei jedem Teilnehmer mit großer Sorgfalt vor Manipulation geschützt werden. Gelingt es einem Angreifer den öffentlichen Schlüssel der Root-CA bei einem Teilnehmer als „Relying Party“ auszutauschen, so kann er diesem beliebige Identitäten vorspiegeln, die er mit seiner eigenen CA zertifiziert hat. Ein auf diese Weise gefälschtes Zertifikat wird stets mit dem lokalen manipulierten Schlüssel der Root-CA erfolgreich verifiziert werden.

Die Root-CA und die operativen CAs, die Zertifikate für Endteilnehmer ausstellen, sollten immer durch eine Hierarchie getrennt sein, so dass das Zertifikat einer operativen CA bei Kompromittierung ihres privaten Schlüssels gesperrt werden kann. Ohne eine übergeordnete CA müsste in diesem Fall die Sperrliste mit dem eigenen kompromittierten privaten Schlüssel signiert werden und würde wegen des so entstehenden Henne-Ei-Problems keine sichere Aussage über den Sperrstatus der gesperrten Zertifikate erlauben.

Der geheime (private) Schlüssel der Root-CA sollte besonders gut gegen Schlüsselverlust und -kompromittierung geschützt werden, z. B. durch Verwahrung in einem Tresor oder durch Erzeugung und Speicherung auf einem Hardware Security Modul (HSM). So ist die Root-CA als Vertrauensanker der PKI gut gesichert vor Kompromittierung und Missbrauch. Die Root-CA wird nur benötigt, um ggf. weitere untergeordnete CAs zu zertifizieren und um – typischerweise jährlich – eine neue Sperrliste auszustellen. Nur das Zertifikat der Root-CA muss an die externen Kommunikationspartner verteilt werden. Bedingt durch die sichere Verwahrung, den seltenen Einsatz und die höheren Sicherheitsmaßnahmen beim Betrieb der Root-CA ist die Wahrscheinlichkeit einer Kompromittierung des privaten Root-CA Schlüssels sehr gering. Die externen Kommunikationspartner können so mehr Vertrauen und eine größere Gewissheit über die Konstanz dieses Zertifikats haben, das sie in ihre Plattformen oder Anwendungen aufnehmen und als vertrauenswürdig anerkennen müssen.

4.3 Verifikation einer Digitalen Signatur

Zur Verifikation einer Digitalen Signatur muss zunächst der Zertifizierungspfad beginnend mit dem Absender, der die Signatur erzeugt hat, bis hin zur einer für den Empfänger vertrauenswürdigen CA aufgebaut werden. Diese vertrauenswürdige CA kann die Root.CA, aber auch eine untergeordnete CA sein. Ein Zertifizierungspfad ist die Aneinanderreihung von Zertifikaten, von denen jedes mit dem jeweils übergeordneten Zertifikat verkettet ist. Diese Verkettung erfolgt über die Signatur der CA (Zertifikatsaussteller) und die Übereinstimmung des Namens der CA mit dem Zertifikatsinhaber im übergeordneten Zertifikat.

Beim Aufbau des Zertifizierungspfades müssen für jedes einzelne Zertifikat im Pfad

- die Digitale Signatur,
- seine Gültigkeit,
- die Übereinstimmung der Namen von Zertifikatsaussteller und übergeordnetem Zertifikatsinhaber sowie

- sein Sperrstatus

überprüft werden.

Nur wenn die Digitale Signatur des Absender erfolgreich verifiziert werden kann und ein gültiger Zertifizierungspfad – bestehend aus zeitlich gültigen und nicht gesperrten Zertifikaten – aufgebaut werden kann, ist die Digitale Signatur des Absenders als gültig anzuerkennen.

4.3.1 Gültigkeitsmodelle

In [X509] standardisiert, weit verbreitet und anerkannt ist das sogenannte Schalenmodell für die Verifikation von Zertifikaten. Beim Schalenmodell müssen alle Signaturen einer Zertifikatskette zum Zeitpunkt der Prüfung gültig sein. Dieser Zeitpunkt kann durch die Certificate Policy festgelegt werden (siehe Abschnitt 4.5) und beispielsweise der (tatsächliche oder angenommene) Signaturzeitpunkt, der Zeitpunkt der ersten Verifikation oder der aktuelle Zeitpunkt sein. Typischerweise werden Signaturen zu Authentifikationszwecken auf den aktuellen Zeitpunkt geprüft, während bei Dokumentsignaturen die Verifikation auf den Erstellungszeitpunkt charakteristisch ist. Jedes untergeordnete Zertifikat muss bei diesem Modell in seiner Gültigkeit innerhalb der Gültigkeit des übergeordneten Zertifikats (Schale) liegen, damit ein gültiger Zertifizierungspfad zustande kommen kann. Daher kommt der Name Schalenmodell.

Das sogenannte Kettenmodell ist aus dem deutschen Signaturgesetz abgeleitet. Das Signaturgesetz fordert, dass jede Signatur gültig ist, wenn zum Erstellungszeitpunkt das Zertifikat des Signaturerstellers gültig war. In der Regel wird jedoch jedes einzelne Zertifikat eines Zertifizierungspfades zu einem anderen Zeitpunkt signiert. Somit gibt es mehrere „verkettete“ Prüfzeitpunkte, da jedes Zertifikat zu seinem Erstellungs-, d. h. Signaturzeitpunkt überprüft werden muss.

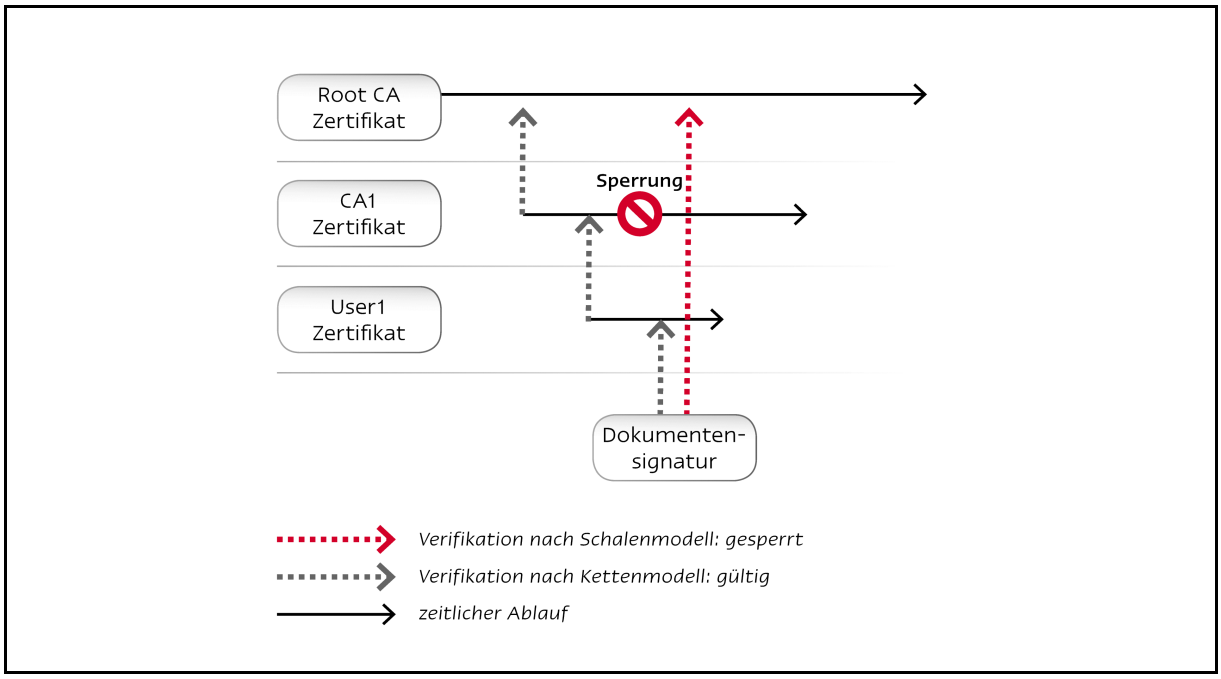

Abbildung 5: Vergleich Gültigkeitsmodelle

Bei einem gesperrten oder abgelaufenen Zertifikat kann die Verifikation einer Digitalen Signatur in Abhängigkeit vom verwendeten Gültigkeitsmodell zu unterschiedlichen Ergebnissen kommen. Dies illustriert das Beispiel in Abbildung 5: Angenommen ein CA-

Zertifikat wird während seiner Laufzeit gesperrt. Als das CA-Zertifikat noch nicht gesperrt war, wurde von dieser CA ein Benutzerzertifikat ausgestellt. Der Benutzer hat mit diesem Zertifikat ein Dokument signiert. Sein Benutzerzertifikat ist zum Zeitpunkt der Signatur des Dokuments noch nicht abgelaufen. Eine Verifikation gemäß des Schalenmodells führt zu dem Ergebnis, dass die Digitale Signatur ungültig ist, da das CA-Zertifikat zu dem einen in diesem Modell betrachteten Prüfzeitpunkt gesperrt ist. Legt man dagegen das Kettenmodell der Verifikation zu Grunde, so erhält man ein positives Verifikationsergebnis: Die Digitale Signatur ist gültig, da zu jedem Zeitpunkt einer Signaturerstellung (Dokumenten- oder Zertifikatssignatur) das zugehörige Zertifikat gültig war.

4.4 Komponenten und Prozesse einer PKI

Die einzelnen Komponenten und Kommunikationsbeziehungen innerhalb einer PKI sind in Abbildung 6 dargestellt. Zusätzlich zu den dargestellten Instanzen gehören zum Aufbau und zur Inbetriebnahme einer PKI auch die Beschreibung der organisatorischen Abläufe und die rechtlichen Regelungen für den Betrieb und die Leistungen der PKI. Im Bereich der qualifizierten Signaturen gehört zu letzteren insbesondere das Signaturgesetz (SigG) und die zugehörige Rechtverordnung.

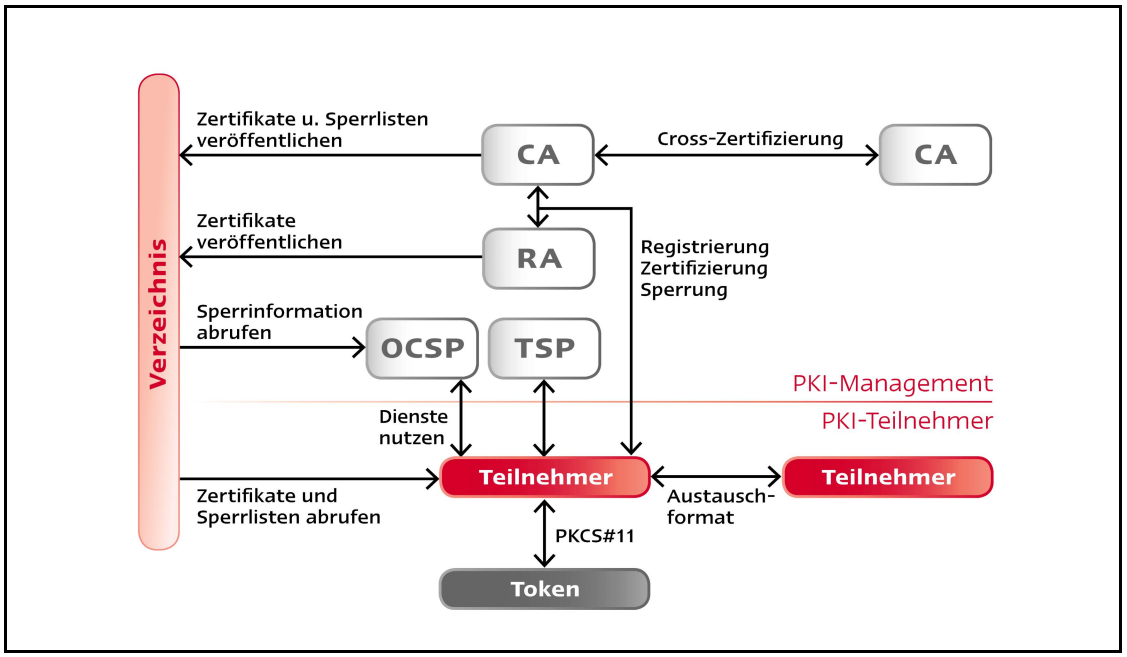

Abbildung 6: Komponenten einer PKI

Zertifizierungs- und Registrierungsstelle

Eine PKI besteht aus verschiedenen Instanzen. Zunächst gibt es die bereits dargestellten CAs, die digital signierte Gültigkeitsbestätigungen („Zertifikate“) nach eindeutigen Regeln ausstellen.

Doch bevor ein Zertifikat ausgestellt werden kann, muss der Benutzer registriert und seine Identität überprüft werden Diese Registrierung erfolgt oft losgelöst von der Ausstellung der Zertifikate durch sogenannte Registrierungsstellen (Registration Authority, RA). Die Auslagerung der RA Funktionalität bietet sich an, wenn eine Organisation über verschiedene Standorte verteilt ist, aber die CA zentral betrieben wird. An den einzelnen Standorten können die Benutzer durch lokale RAs registriert werden. Diese leiten die von ihnen

erhobenen und überprüften Registrierungsinformationen zur Zertifizierung auf sicherem Weg an die CA weiter.

Verzeichnisdienst

Die CA veröffentlicht in der Regel die ausgestellten Zertifikate und ihre CRL in einem Verzeichnisdienst. Diese Veröffentlichung erfolgt über standardisierte Verfahren (meist ein LDAP Directory). Alle PKI Teilnehmer benötigen lesenden Zugriff auf diesen Verzeichnisdienst, um Zertifikate und CRLs beziehen zu können.

Für den Verzeichnisdienst ist ein Mindestniveau an Daten-Integrität sicherzustellen, damit keine Zertifikate oder CRLs durch einen Angreifer gelöscht oder durch alte Versionen ersetzt werden können. Durch solche Manipulationen mit ungültigen Zertifikaten oder CRLs könnte der Angreifer Denial-of-Service-Situationen auslösen. Gelingt ihm das Einspielen einer alten CRL, die zeitlich noch gültig ist, könnte er sogar die Sperrung eines Zertifikats vertuschen.

CA-Zertifikate und CRLs können alternativ oder zusätzlich zur Bereitstellung in einem Directory auch auf einem Web-Server im Internet veröffentlicht werden. Wenn die entsprechenden URLs in den Benutzerzertifikaten eingetragen werden, können die Clients diese Information auch von dort automatisiert abrufen.

Online Status-Auskunftsdienst

Eine Alternative (oder Ergänzung) zur Verwendung von CRLs ist der sogenannte Online-Status-Auskunftsdienst (Online Certificate Status Protocol Responder, OCSP Responder). Dieser OCSP Responder liefert eine signierte Antwort zum Status eines angefragten Zertifikats. Dabei wird nicht das zu prüfende Zertifikat selbst an den OCSP Responder übergeben, sondern nur der Name (*Distinguished Name*) des Zertifikatsausstellers und die Seriennummer des Zertifikats. Dieses Datenpaar bildet immer eine eindeutige Referenz auf ein Zertifikat. Mögliche Antworten des OCSP Responders sind „good“, „revoked“ oder „unknown“. „Unknown“ liefert der OCSP Responder einer CA bei Anfragen zu Zertifikaten, die nicht von dieser CA ausgestellt wurden.

In der Regel basieren die Auskünfte eines OCSP Responders auf einer CRL, d. h. der OCSP Responder durchsucht die aktuelle CRL der CA nach der Seriennummer des angefragten Zertifikats und liefert „good“ zurück, wenn die Seriennummer des Zertifikats dort nicht gefunden wird, bzw. „revoked“, wenn die Seriennummer des Zertifikats in der CRL enthalten ist. Weitere Informationen finden sich bei [RFC2560].

Wie bereits in Abschnitt 4.3.1 „Gültigkeitsmodelle“ dargestellt, gibt es in Deutschland mit den signaturgesetzkonformen Zertifikaten eine Sonderform der PKI. In Bezug auf Statusinformationen zu einem signaturgesetzkonformen Zertifikat gibt es in diesem Zusammenhang weitere Anforderungen: Ein signaturgesetzkonformer OCSP Responder darf nicht auf Basis einer Negativliste (wie eine CRL) eine Statusauskunft erteilen, sondern die Auskunft muss auf einer Positivliste beruhen. Daher dürfen signaturgesetzkonforme OCSP Responder für eine Statusauskunft nicht auf CRLs zurückgreifen, sondern müssen ihre Aussage auf Basis einer Liste aller ausgestellten Zertifikate treffen. Alle ausgestellten Zertifikate werden in einem Verzeichnisdienst verwahrt. So wird die Kompromittierung einer CA verbunden mit einer Totalfälschung von Zertifikaten ausgeschlossen. Dieser Verzeichnisdienst, der alle ausgestellten Zertifikate verwaltet, muss besonders geschützt werden, so dass auch bei Kompromittierung des CA-Schlüssels die bereits ausgestellten Zertifikate ihre Gültigkeit bewahren. Im signturgesetzkonformen Umfeld würden dann alle Zertifikate, die in diesem Verzeichnisdienst enthalten sind, trotz Kompromittierung des CA Schlüssels weiterhin gültig bleiben. Um im Fall einer Kompromittierung einer CA zu erkennen, wenn neue Zertifikate mit

alten bereits vergebenen Seriennummern ausgestellt wurden, muss bei der Statusanfrage der Hashwert des angefragten Zertifikats enthalten sein. So werden gefälschte Zertifikate bei der Statusanfrage an den signaturgesetzkonformen Verzeichnisdienst als „unknown“ enttarnt.

Zeitstempeldienst

Über einen Zeitstempeldienst (Time-Stamp Protocol, TSP) können Zeitstempel eingeholt werden, um so beispielsweise die Existenz eines bestimmten Dokumentes zu einem definierten Zeitpunkt beweisen zu können oder um den Zeitpunkt der Signaturerstellung durch einen Anwender nachweisen zu können. Ein Zeitstempel ergibt sich aus der Signatur eines Zeitstempeldienstes auf den Hashwert eines Dokuments, d. h. es werden keine vertrauenswürdigen Daten übermittelt, da nur der Hashwert des Dokuments oder Datums, für das ein Zeitstempel eingeholt werden soll, an den Zeitstempeldienst gesendet wird. Weitere Informationen finden sich bei [RFC3161].

Zeitstempel werden in der Praxis z. B. bei elektronischer Einreichung von Patentanträgen, Einreichung von elektronischen Angeboten auf eine Ausschreibung oder bei der Sicherung von Datensätzen in Archivierungssystemen eingesetzt.

Personal Security Environment

Die Schlüssel und Zertifikate eines Benutzers müssen für ihn zugänglich gespeichert werden. Dies geschieht in einer sogenannten Personal Security Environment (PSE). Je nach angestrebtem Sicherheitsniveau kann ein Benutzer seine PSE in Software oder Hardware speichern.

Eine Speicherung des Schlüsselmaterials in Software ist nicht standardisiert, sondern von dem jeweiligen Software-Hersteller abhängig. Anwendungen von verschiedenen Herstellern können in der Regel nicht die gleiche Software-PSE verwenden, wobei inzwischen viele Windows-Anwendungen den Microsoft Certificate Store unterstützen. Doch auch bei einer proprietären Speicherung des Schlüsselmaterials unterstützen die meisten Produkte zumindest zum Austausch von PSEs ein standardisiertes Format. Somit können existierende Schlüssel und Zertifikate aus einer Anwendung exportiert und in eine andere Anwendung wieder importiert werden. In diesem Fall arbeitet der Anwender jedoch parallel mit zwei verschiedenen Kopien seiner PSE.

Bei der Speicherung in Hardware wie einer Smartcard oder einem USB-Token sollten die Schlüssel möglichst schon auf der Smartcard oder dem USB-Token generiert werden, so dass der private Schlüssel niemals außerhalb der Hardware vorliegt. Im Folgenden werden Smartcards und USB-Token unter dem Begriff Hardware-Token zusammengefasst. Ein Hardware-Token zeichnet sich u. a. dadurch aus, dass der private Schlüssel nicht ausgelesen werden kann. Der Zugriff auf Hardware-Token sollte über eine standardisierte Schnittstelle erfolgen, so dass eine Vielzahl unterschiedlicher Anwendungen darauf zugreifen kann. Außerdem ist durch die Standardisierung auch gewährleistet, dass ein Wechsel des Hardware-Tokens möglich ist, ohne die Implementierung der Anwendung ändern zu müssen.

In der Praxis weit verbreitet sind zwei alternative Software-Schnittstellen, über die eine Anwendung auf ein Hardware-Token zugreifen kann: Entweder verwendet sie die PKCS#11-Schnittstelle und einen entsprechenden PKCS#11-Treiber für den Zugriff auf das Hardware-Token oder sie verwendet den Microsoft-Standard der Crypto-API, der über einen Cryptographic Service Provider (CSP) auf das Hardware-Token zugreift. Neben diesen beiden Möglichkeiten kann eine Anwendung auch direkt Hardware-Token-spezifische

Kommandos (Application Protocol Data Unit, APDU) an ein Hardware-Token schicken. Diese APDU-Schnittstelle nutzt beispielsweise auch ein Smartcard Management System zur Personalisierung von Smartcards.

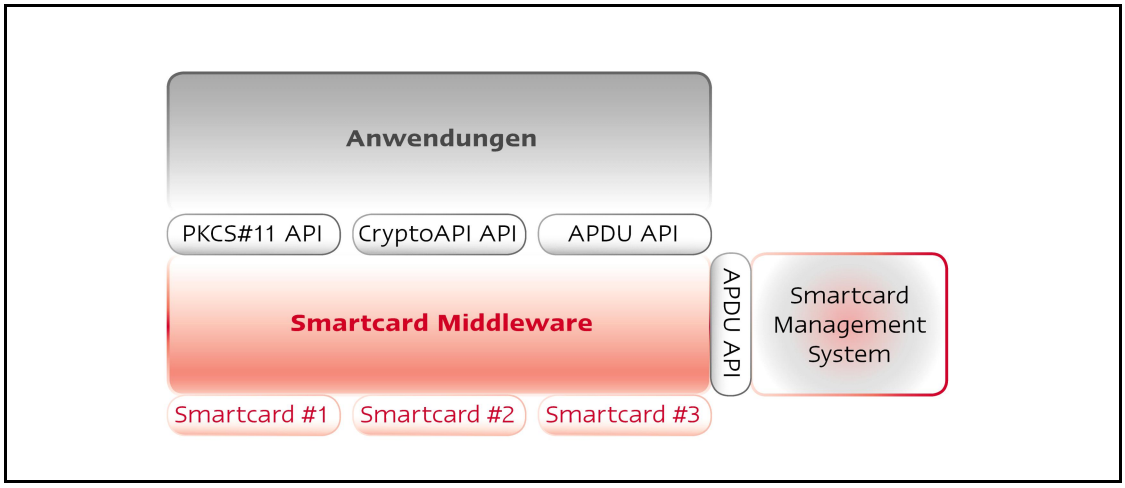

Abbildung 7: Schnittstellen zwischen Anwendung und Smartcard

Smartcard Management System

Werden Schlüssel auf Hardware-Token gespeichert, bietet es sich an, diese Token mit Hilfe eines Smartcard Management Systems zu verwalten. Diese Systeme gewinnen aktuell immer mehr an Bedeutung, wenn z. B. zusätzlich temporäre oder permanente Ersatzkarten benötigt werden oder Benutzer über sogenannte Self-Services[1] ihre Token selbst verwalten sollen.

Mit der Einführung von Hardware-Token in einem Unternehmen ist es naheliegend, die Benutzeranmeldung am Betriebssystem auch auf Hardware-Token umzustellen[2]. Speziell ein Hardware-Token in Form einer Smartcard lässt sich gut mit einem Unternehmensausweis kombinieren. So kann ein Benutzer beispielsweise mit ein und derselben Karte, die einen kontaktlosen Chip (z. B. Legic oder Mifare) und einen kontaktbehafteten Chip (für die PKI-Operationen) enthält, Zutritt zum Gebäude und Zugriff auf seine Anwendungen erhalten. Benötigt er diese Karte auch zur Bezahlung in der Kantine, so kann darüber hinaus technisch sichergestellt werden, dass mit dem Ziehen der Smartcard der Bildschirm des Benutzers während der Mittagspause gesperrt und vor unberechtigten Zugriffe geschützt ist. Die meisten auf dem Markt existierenden Smartcard Management Systeme können sowohl kontaktbehaftete als auch kontaktlose Chips personalisieren und auch Karten bedrucken. Durch diese Entwicklung im Bereich der Smartcard Management Systeme lässt sich beobachten, dass in den Unternehmen die Bereiche IT-Security und Corporate Security, die bisher völlig losgelöst voneinander koexistierten, nun verstärkt zusammenarbeiten, da sie gemeinsame Interessen und Ziele verfolgen.

Smartcard Management Systeme benötigen eine Vielzahl an Schnittstellen, um in die bestehende Infrastruktur und Prozesse einer Organisation effektiv eingebunden werden zu können. So müssen sie auf die Smartcard zugreifen, einen Kartendrucker ansteuern, ein

---

1 Self-Services (oder deutsch: Selbstbedienungstechnologien) ermöglichen einem Benutzer beispielsweise das selbständige Rücksetzen seiner PIN.

2 Windows Smartcard Logon: Statt seines Windows Passworts gibt der Benutzer die PIN seiner Smartcard oder seines USB-Tokens an. Die Authentifizierung basiert auf Zertifikaten.

Zertifikat bei einer CA beantragen und auf die Backend-Systeme zugreifen können, in denen die Benutzer verwaltet und Zutrittsberechtigungen vergeben werden.

Schlüsselerzeugung

Bei der Schlüsselerzeugung wird zwischen zentraler und dezentraler Schlüsselerzeugung unterschieden. Beide Verfahren haben Vor- und Nachteile, die im Anschluss an die Beschreibung der beiden Ansätze erläutert werden.

Bei der zentralen Schlüsselerzeugung werden die Schlüssel von einer zentralen Instanz (CA oder RA) erzeugt. Die Anwesenheit des Benutzers ist nicht erforderlich, aber möglich. Je nach Art der Prozesse erhält der Benutzer seine Schlüssel, Zertifikate und PIN auf sicherem Weg übermittelt oder direkt vor Ort ausgehändigt. Der Ablauf einer Zertifizierung mit zentraler Schlüsselerzeugung könnte in einem Beispiel, bei dem die CA gleichzeitig als RA fungiert, wie folgt aussehen:

1. Der Benutzer wird bei einer CA vorstellig.
2. Die CA stellt die Identität des Benutzers fest und erzeugt ein Schlüsselpaar (privater und öffentlicher Schlüssel).
3. Die CA erstellt ein Zertifikat für den Benutzer, das mit dem privaten Schlüssel der Zertifizierungsstelle signiert ist.
4. Der Benutzer erhält seinen privaten Schlüssel, sein Zertifikat, das seinen öffentlichen Schlüssel enthält, und das Zertifikat der CA.
5. Die CA stellt das Zertifikat des Benutzers in ein allgemein zugängliches Verzeichnis ein.

Bei der dezentralen Schlüsselerzeugung werden die Schlüssel vom Benutzer selbst erzeugt und nur der öffentliche Schlüssel zur Zertifizierung an die CA übermittelt. Der Ablauf einer Zertifizierung mit dezentraler Schlüsselerzeugung könnte beispielhaft so aussehen:

1. Der Benutzer erzeugt ein Schlüsselpaar mit öffentlichem und privatem Schlüssel.
2. Der Benutzer wird bei der CA vorstellig und übergibt seinen öffentlichen Schlüssel.
3. Die CA stellt die Identität des Benutzers fest und überzeugt sich, dass er den zu dem öffentlichen Schlüssel gehörenden privaten Schlüssel besitzt (mittels eines sogenannten „Proof of Possession“).
4. Die CA erstellt ein Zertifikat für den Benutzer, das mit dem privaten Schlüssel der CA signiert ist.
5. Der Benutzer erhält sein Zertifikat, das seinen öffentlichen Schlüssel enthält, und das Zertifikat der CA.
6. Die CA stellt das Zertifikat des Benutzers in ein allgemein zugängliches Verzeichnis ein.

Ein Vorteil der zentralen Schlüsselerzeugung ist, dass die Aufgabe der Schlüsselerzeugung aus der Verantwortung der Benutzer genommen ist und so für den Benutzer einfacher und für das Help Desk mit weniger Aufwand verbunden und damit kostengünstiger ist. Oftmals lassen sich auch die Prozesse für eine Schlüsselhinterlegung (siehe nachfolgenden Abschnitt zu Key Recovery) damit leichter umsetzen als bei einer dezentralen Schlüssel-erzeugung. Die Erzeugung eines wirklich zufälligen, nicht von Dritten reproduzierbaren Schlüsselpaars erfordert neben einem gewissen Maß an Know-How eine gute Zufallsquelle. In vielen Fällen kann man einer zentralen, spezialisierten Instanz in diesem Punkt mehr Kompetenz zubilligen als einem nicht mit der Materie vertrauten Anwender.

Bei der dezentralen Schlüsselerzeugung ist der Benutzer für die Erzeugung seiner Schlüssel selber verantwortlich, was zwar einerseits zu Problemen und Fehlern führen kann, andererseits aber auch mehr Sicherheit für den Benutzer bedeutet, wenn sein privater Schlüssel stets nur in seinem Besitz ist. So kann niemand in seinem Namen eine digitale Signatur leisten. Andererseits kann er, weil er das Verfahren kontrolliert, auch absichtlich ein „schwaches“ Schlüsselpaar erzeugen und hinterher von ihm geleistete Signaturen mit dem Argument abstreiten, der Schlüssel sei kompromittiert worden.

Schlüsseltrennung

Während man anfänglich beim Einsatz von PKIs für alle Benutzer nur ein einziges Schlüsselpaar vorgesehen hatte, ist es heute gängige Praxis, zwei oder gar drei verschiedene Schlüsselpaare für jeden Benutzer zu erzeugen, um Schlüssel nach ihrem Verwendungszweck zu trennen. Typischerweise gibt es einen Signatur-, einen Authentisierungs- und einen Verschlüsselungsschlüssel. Die Trennung der verschiedenen Schlüssel ist durch die verschiedenen Anforderungen der jeweiligen Anwendung gerechtfertigt, so kann bspw. ein Verschlüsselungsschlüssel in einem Unternehmen hinterlegt werden (vgl. den folgenden Abschnitt); der Signaturschlüssel hingegen sollte stets nur im Besitz des Anwenders verbleiben. Weitere Unterscheidungsmerkmale können die Gültigkeitsdauer des zugehörigen Zertifikats oder die ausstellende CA sein.

Key Recovery

Bei Einführung von Verschlüsselung in einem Unternehmen ist ein Key Backup und Recovery oder ein Data Recovery (siehe nachfolgenden Abschnitt zu Data Recovery) unabdingbar. Verschlüsselte Daten müssen auch bei Nicht-Verfügbarkeit des privaten Schlüssels – z. B. nach dem Ausscheiden eines Mitarbeiters – noch entschlüsselt werden können. Bei Hinterlegung des privaten Anwenderschlüssels, der zur Entschlüsselung dient, können im Bedarfsfall verschlüsselte Daten durch Schlüsselwiederherstellung wieder entschlüsselt werden. Dabei muss der Schlüsselwiederherstellungsprozess geeignet abgesichert sein, z. B. durch ein Vieraugenprinzip. Hinterlegt werden sollte nur der Entschlüsselungsschlüssel, auf keinen Fall der Signatur- oder Authentisierungsschlüssel.

Abhängig von anderen etablierten Prozessen können die Schlüssel entweder zentral bei der CA oder bei einer dritten vertrauenswürdigen Instanz oder dezentral beim Anwender hinterlegt werden. Bei einer dezentralen Hinterlegung muss organisatorisch sichergestellt werden, dass jeder Benutzer seinen privaten Entschlüsselungsschlüssel sicher aufbewahrt und dieser im Bedarfsfall berechtigten Dritten zugänglich ist.

Data Recovery

Im Gegensatz zur Schlüsselhinterlegung werden beim „Data Recovery“ die Daten für einen Dritten mit verschlüsselt, d. h. es findet keine Hinterlegung von privaten Nutzerschlüsseln statt. Für eine Data Recovery-Lösung muss im Unternehmen ein globaler Recovery Key eingeführt werden, der für alle Verschlüsselungsoperationen als zusätzlicher Empfänger[3] gehandhabt wird. Alle Daten werden nicht nur für den eigentlichen Empfänger verschlüsselt, sondern zusätzlich auch für den globalen Recovery Key.

[3] Im Falle einer verschlüsselten Speicherung von Daten entspricht der Begriff „Empfänger“ den leseberechtigten Benutzern.

Voraussetzung für eine Data Recovery Lösung ist, dass alle Verschlüsselungsanwendungen in einem Unternehmen die Verschlüsselung für einen zusätzlichen Empfänger – den globalen Recovery Key – unterstützen. Nachteil dieses Ansatzes ist, dass externe Kommunikationspartner in der Regel diesen globalen Recovery Key nicht kennen und nicht unterstützen. Folglich sind verschlüsselte Nachrichten von Externen zunächst einmal nicht über den globalen Recovery Key entschlüsselbar, sondern müssen beim ersten Entschlüsseln innerhalb des Unternehmens unter Berücksichtigung des globalen Recovery Key neu verschlüsselt werden.

Beim Data Recovery können der Benutzer und der Recovery Agent (der Inhaber des Recovery Key) beide jeweils mit ihrem privaten Schlüssel die verschlüsselte Nachricht entschlüsseln. Dabei muss der Zugriff auf den privaten globalen Recovery Key geeignet abgesichert sein, z. B. durch ein Vieraugenprinzip.

4.5 Policies für Public Key Infrastrukturen

Die Policies einer PKI bilden die Grundlage zur Vertrauensbildung bei PKI-basierten Anwendungen. Sie geben einer sogenannten *Relying Party* Aufschluss darüber, wie viel Vertrauen sie in eine PKI und in die Glaubwürdigkeit eines Zertifikats haben kann. Die Relying Party ist der Empfänger von gesicherten Informationen, die er mit Hilfe der PKI-Dienste überprüft.

In einer Certificate Policy werden von der CA die Anforderungen an die Sicherheit ihrer Infrastruktur, an die Identifikationsverfahren der Benutzer, an das Zertifikatsmanagement und die Überprüfung ihrer Abläufe sowie Haftung, Schadensersatz und Datenschutz festlegt. Durch diese öffentliche Dokumentation kann eine *Relying Party* das Sicherheitsniveau der CA und somit das Maß an Vertrauen in die ausgestellten Zertifikate einschätzen.

Nähere Informationen zu Certificate-Policy-Dokumenten finden sich im „Certificate Policy and Certification Practices Framework“ [RFC3647] und Secorvo White Paper „Das Policy-Rahmenwerk einer PKI“ [WP15].

5 Standards im Bereich PKI

Die zentralen Standards und Spezifikationen für Public Key Infrastrukturen sind:

- Der X.509 Standard
- PKIX-Standards
- PKCS-Standards

In Deutschland wurden im Rahmen der Common PKI Interoperabilitätsspezifikation viele wichtige Standards aus dem Umfeld von X.509, PKIX, PKCS und von weiteren Standardisierungsgremien zusammen gestellt und mit dem Ziel profiliert[4], dass PKI-Komponenten und PKI-Anwendungen verschiedener Hersteller auf dieser Grundlage problemlos miteinander zusammen arbeiten können.

5.1 Der X.509 Standard

Der X.509 Standard ist ein ITU-T-Standard und definiert das Format für Schlüsselzertifikate, Attributzertifikate und Sperrlisten sowie ein Verfahren zur Verifikation des Zertifizierungs-

[4] D. h. hinsichtlich der zulässigen Optionen präzisiert und eingeschränkt.

pfades. Die in den verschiedenen Ausgaben von X.509 definierten Versionen dieser standardisierten Datenformate sind in Tabelle 1 dargestellt[5].

X.509 Ausgabe	Schlüsselzertifikat	Sperrliste	Attributzertifikat
1. Ausgabe: 11/1988	Version 1	Version 1	/
2. Ausgabe: 11/1993	Version 2	Version 1	/
3. Ausgabe: 08/1997	Version 3	Version 2	Version 1
4. Ausgabe: 03/2000	Version 3	Version 2	Version 2
5. Ausgabe: 08/2005	Version 3	Version 2	Version 2

Tabelle 1: Überblick über die Ausgaben des X.509 Standards

5.2 PKIX Standards

Da der X.509 Standard spätestens ab seiner dritten Ausgabe, die oft kurz als X509v3 bezeichnet wird, eine sehr generische und komplexe Datenstruktur für Zertifikate und CRLs definiert, treten in der Praxis bei einer Vielzahl von unterschiedlichen Anwendungen und Umgebungen Interoperabilitätsprobleme auf. Um den X.509v3 Standard für eine Internet-PKI anwendbar machen, hat daher die PKIX Arbeitsgruppe der *Internet Engineering Task Force* (IETF) eine Reihe von Internet-Standards, sogenannte *Requests for Comment* (RFC), festgelegt, mit denen eine praxisgerechte und interoberabele Implementierung von PKI-Objekten, -Prozessen und -Produkten möglich werden soll.

In [RFC5280] wird ein Zertifikats- und CRL-Profil definiert. Es legt fest, welche Erweiterungen im Rahmen der Möglichkeiten von X.509 verwendet werden müssen, sollen oder nicht verwendet werden dürfen. Im Hinblick auf signaturgesetzkonforme PKIs definiert der [RFC3739] das Profil für qualifizierte Zertifikate. Dieses Profil kann durch nationale Regelungen für die Verwendung im Rechtsverkehr anerkannt werden.

Die PKIX Arbeitsgruppe hat noch viele weitere Internetstandards (RFCs) für den Bereich der Internet-PKI veröffentlicht. Nennenswert sind außer den PKIX-Profilen noch die PKIX-Protokolle, wie beispielsweise die operationalen Protokolle zur Abfrage von Zertifikaten und Statusinformationen (LDAPv3, OCSP, und die Verwendung von FTP und HTTP zum Transport von PKI Nachrichten) sowie die „Certificate Management“-Protokolle. Darüber hinaus stammen das Zeitstempeldienstprotokoll (Time Stamp Protocol [RFC3161]), das „Policy and Certification Practices Framework“ [RFC3647] und verschiedene Protokolle zur Verifikation von Zertifikaten, CRLs und Signaturen von der PKIX Arbeitsgruppe. Weitere Informationen finden sich bei [PKIX].

5.3 PKCS Standards

Die Public Key Cryptography Standards (PKCS) sind sogenannte Industriestandards, die in offenen Arbeitsgruppen von vielen Akteuren aus Industrie und Wissenschaft unter Federführung von RSA Inc. seit 1991 entwickelt wurden. Der Fokus der PKCS Standards liegt auf technischen Aspekten der PKI und Kryptographie. Die derzeit relevanten PKCS Standards sind:

5 http://www.itu.int/rec/T-REC-X.509/en

- **PKCS#1**: Der *RSA Encryption Standard* findet Verwendung in PKI-Komponenten, die den RSA-Algorithmus ausführen. Der RSA-Algorithmus wird dabei i. d. R. in einem kryptografischen Schema zusammen mit anderen Verfahren verwendet, um Sicherheitsdienste wie Verschlüsselung oder Digitale Signatur zu realisieren. Bei einer Implementierung von RSA gibt es in Details verschiedene Realisierungsvarianten, die bei ungünstiger Wahl angreifbar sind. PKCS#1 macht Vorschläge für die sichere Implementierung des RSA-Algorithmus. Der PKCS Standard #1 wurde im Februar 2003 fast wortgetreu mit nur einigen Korrekturen als IETF RFC 3447 veröffentlicht.
- **PKCS#7**: Der *Cryptographic Message Standard* (CMS) spezifiziert ein Datenaustauchformat und wird dort verwendet, wo kryptografisch behandelte (d. h. im wesentlichen verschlüsselte und/oder signierte) Objekte mit anderen ausgetauscht werden, z. B. eine E-Mail, ein Dokument oder ein Zertifikat. Die neueste Version der in PKCS#7 definierten Cryptographic Message Syntax wird durch RFC 5652 standardisiert.
- **PKCS#10**: Der *Certification Request Syntax Standard* wird verwendet, um Zertifizierungsanfragen an eine Zertifizierungsstelle zu richten.
- **PKCS#11**: Mit dem *Cryptographic Token Interface Standard* wird eine Programmierschnittstelle für Anwendungsprogrammierer spezifiziert, die Hardware-Token in ihrer Anwendungssoftware nutzen möchten.
- **PKCS#12**: Der Personal *Information Exchange Syntax Standard* definiert ein Datenformat, mit dem das gesamte Schlüssel- und Zertifikatsmaterial inklusive dem privaten Schlüssel passwortgeschützt und portabel zum Transport[6] in einer Datei gespeichert werden kann.
- **PKCS#15**: Der *Cryptographic Token Information Format Standard* wurde im Jahr 2004 von ISO/IEC 7816-15 abgelöst. Er spezifiziert die Anwendungsdatenstrukturen auf einem Hardware-Token, d. h. die Verzeichnisstruktur und die notwendigen Datenelemente. Diese Strukturen werden in der Regel beim Initialisieren auf das Hardware-Token aufgebracht und ermöglichen konformen Anwendungen ohne Abhängigkeit von einem bestimmten PKCS#11 oder CSP Treiber auf Daten wie Zertifikate, die auf dem Hardware-Token gespeichert sind, zuzugreifen.

Weitere Informationen finden sich bei [PKCS].

Die PKCS-Standards kommen in verschiedenen Produktklassen zum Einsatz. Beispielsweise verwenden die aktuellen Web-Browser die Standards PKCS#1, #7, #10, #11 und #12. Smartcards nutzen PKCS#1, #11 und teilweise auch PKCS#15. PKI-Core- und Client-Software unterstützt in der Regel PKCS#1, #7, #10, #11, #12 und ggf. auch PKCS#15. Diese breite Unterstützung von PKCS Standards zeigt deren hohe praktische Relevanz.

6 PKCS#12 wird auch als Format verwendet für den Ex- und Import von eigenem Schlüsselmaterial in und aus verschiedenen PSEs.

5.4 Common PKI Spezifikationen

Die Common PKI (vormals ISIS-MTT) Spezifikation stammt von T7[7] und TeleTrusT[8]. Sie ist historisch gewachsen aus der Industrial Signature Interoperability Specification (ISIS) und der MailTrusT (MTT) Spezifikation. Die Common PKI Spezifikation ist – ähnlich wie die PKIX Profile – ein Profil über international verbreitete und anerkannte Standards für Digitale Signaturen, Verschlüsselung und Public Key Infrastrukturen. Bei der Erstellung wurden mehr als 30 Basisstandards berücksichtigt. Dabei berücksichtigt sie auch die Anforderungen für die qualifizierte elektronische Signatur nach dem deutschen Signaturgesetz (SigG). Die aktuelle Version der Common PKI Spezifikation besteht aus den folgenden Teilen:

- Part 1: Certificate and CRL Profiles
- Part 2: PKI Management
- Part 3: Message Formats
- Part 4: Operational Protocols
- Part 5: Certificate Path Validation
- Part 6: Cryptographic Algorithms
- Part 7: Signature API
- Part 8: XML Signature and Encryption Message Formats
- Part 9: SigG-Profile

Weitere Informationen finden sich bei [ComPKI].

Zusätzlich zu der Common PKI Spezifikation stehen eine korrespondierende Testspezifikation und ein Testbed Prototyp zur Verfügung. Mit diesem können Hersteller und Prüflabore PKI Produkte auf Konformität mit der Common PKI Spezifikation testen. Wenn alle Anforderungen der Spezifikation erfüllt werden, kann über T7 e.V.[9] ein Common PKI Siegel beantragt werden. Dieses Siegel ist ein Nachweis für Interoperabilität von Common-PKI-konformen Produkten und Lösungen. In Deutschland ist diese Konformität obligatorisch im Bereich E-Government für die Sicherung der E-Mail-Kommunikation und den gesicherten Dokumentenaustausch.

6 Verknüpfung von PKIs

Wenn einzelne Organisationen sich ihre eigene interne Public Key Infrastruktur (PKI-Domäne) aufgebaut haben und nicht nur interne PKI-Anwendungen einsetzten wollen, stellt sich die Frage, wie Teilnehmer aus unterschiedlichen PKI-Domänen miteinander sicher kommunizieren können, auch wenn sie keine gemeinsame Root-CA haben. Ziel dieser

---

7 T7 e.V. ist eine Arbeitsgemeinschaft von Trustcenterbetreibern und Zertifizierungsdiensteanbietern im Bereich qualifizierter elektronischer Signaturen nach dem deutschen Signaturgesetz.

8 TeleTrusT Deutschland e.V. ist ein gemeinnütziger Verein und ein nichtkommerzielles Netzwerk mit Mitgliedern aus Industrie, Wissenschaft, Forschung und öffentlichen Institutionen. Sein Ziel sind verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik.

9 http://www.t7ev.org/common-pki/siegel-und-prueflabore.html

Überlegungen ist es, dass mehrere PKIs zusammenarbeiten und die Teilnehmer aus allen beteiligten Domänen einander vertrauen können.

6.1 Crosszertifizierung

Eine mögliche Lösung zu Verknüpfung von PKIs stellt die sogenannte Crosszertifizierung dar, bei der Zertifizierungshierarchien miteinander verknüpft werden. Dabei wird die eine Root-CA von der anderen zertifiziert und umgekehrt. Ein Crosszertifikat unterscheidet sich in seiner Form nicht von einem untergeordneten CA Zertifikat, d. h. es lässt in Struktur und Aufbau keinen Unterschied zu einem normalen Zertifikat erkennen. Crosszertifikate haben die zusätzliche Eigenschaft, dass sie einseitig oder beidseitig (als Paar von Crosszertifikaten) zwischen zwei CAs ausgestellt werden können.

Theoretisch können mit einer Crosszertifizierung nicht nur die obersten Knoten zweier PKI-Hierarchien, die Root-CAs, miteinander verbunden werden: Crosszertifikate können, wie in Abbildung 8 beispielhaft dargestellt, auch dafür genutzt werden, um Zertifizierungspfade (Zertifikatsketten) zu verkürzen. In der Praxis führen solche zusätzlichen Zertifikatspfade allerdings zu einer erhöhten Komplexität bei der Verifikation von Zertifikaten: Zunächst muss nämlich aus dem Graphen der Zertifizierungsbeziehungen, der nun kein einfacher Baum mehr ist, ein Zertifikatspfad ausgewählt werden. Crosszertifikate erhöhen die Zahl der möglichen Pfade, die nachverfolgt werden können. In jedem der möglichen Pfade können ein oder mehrere gesperrte Zertifikate auftreten, so dass u. U. dieser Zertifizierungspfad wieder verworfen und nach einem anderen gesucht werden muss. Daher werden in der Regel Crosszertifizierungen nur auf der Root-Ebene der PKI-Domänen durchgeführt.

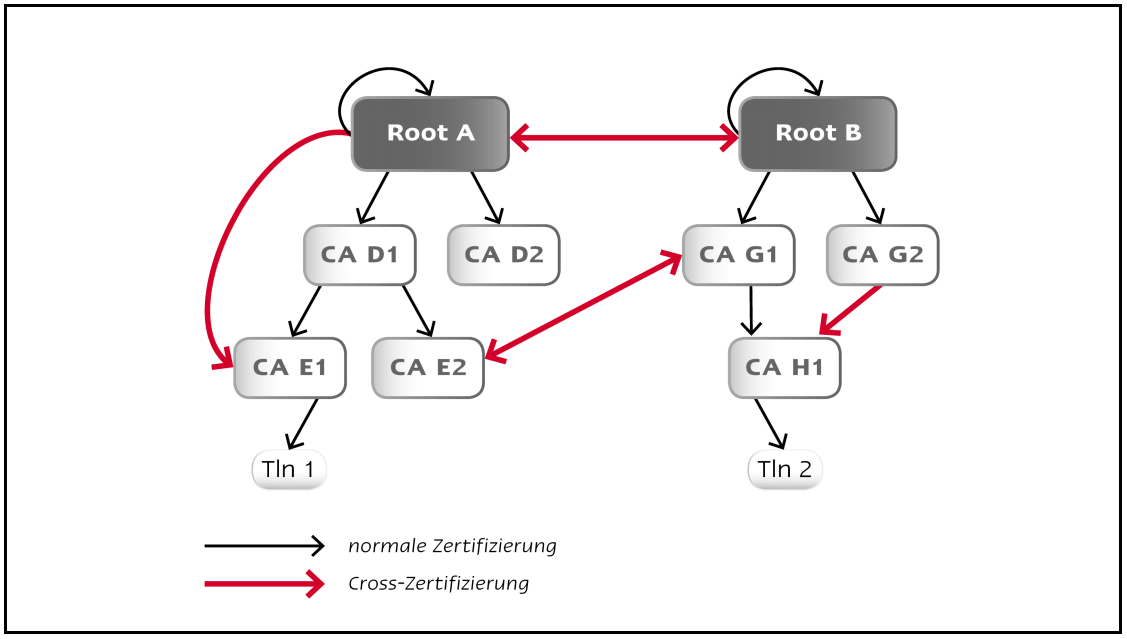

Abbildung 8: Cross-Zertifizierung

6.2 European Bridge CA

Eine Alternative zu Crosszertifikaten stellt in Europa die European Bridge CA (EB-CA) dar. Diese EB-CA stellt keine eigenen Zertifikate zur Verbindung von PKI-Inseln aus, sondern verteilt eine signierte Liste der von ihr geprüften und anerkannten Root-Zertifikate an alle ihre Mitglieder. Alle Mitglieder schließen einen Vertrag mit der EB-CA und verpflichten sich auf

die Einhaltung ihrer Mindestanforderungen, u. a. die Verfügbarkeit von Certification Policy (CP) [10] oder Certification Practice Statement (CPS) und erfolgreich absolvierte Interoperabiltitätstests. Somit entfallen für die Mitglieder die bilateralen Vertragsvereinbarungen und Prüfungen mit allen anderen Mitgliedern. Sie erhalten die Liste der vertrauenswürdigen CAs und müssen diese in ihrer Infrastruktur bzw. in ihren Anwendungen als vertrauenswürdig integrieren. Dieser Aufwand für die technische Umsetzung zur Integration der externen Root-Zertifikate muss trotz Zertifizierung durch die EB-CA geleistet werden.[11].

Die EB-CA war ursprünglich eine Initiative der Deutschen Bank und der Deutschen Telekom. Heute wird sie von TeleTrusT e.V. betrieben. Weitere Informationen finden sich bei [BRIDGE].

6.3 Verteilung von Root-Zertifikaten

Die wohl am weitesten verbreitete Art, PKI-Domänen miteinander zu verknüpfen, ist die Verteilung der Root-Zertifikate. Dazu muss das eigene Root-Zertifikat sicher an die externen Kommunikationspartner und im Gegenzug das Root-Zertifikat der externen Kommunikationspartner intern verteilt und – i. d. R. als eines von vielen – als vertrauenswürdig anerkannt werden. Etwas hochtrabend wird diese Variante der Verknüpfung von PKI-Domänen auch als *Cross Recognition* bezeichnet.

Um das eigene Root-CA-Zertifikat an alle Kommunikationspartner zu verteilen, bieten sich verschiedene Möglichkeiten:

- Aufnahme des eigenen Root-Zertifikats in gängige Browser und Betriebssysteme. Als Voraussetzung für eine solche Aufnahme ist ein WebTrust-Gütesiegel für Certification Authorities oder eine Zertifizierung nach einem vergleichbaren ETSI-Standard erforderlich. [12]
- Zertifizierung der eigenen Root:CA durch eine CA, deren Zertifikat bereits in gängige Browser und Betriebssysteme integriert ist. Diese Dienstleistung ist unter der Bezeichnung „Root Signing“ geläufig; sie wird von mehreren kommerziellen Trustcentern angeboten.
- Das Root-Zertifikat wird zum Download im Internet bereitgestellt. Die Relying Party, die das Root-Zertifikat herunterlädt, muss dessen Fingerprint über einen zweiten, unabhängigen Kanal beziehen und geeignet prüfen, um sich von der Korrektheit des Root-Zertifikats zu überzeugen.

Um ein externes Root-.Zertifikat intern zu verteilen, muss im aufwendigsten Fall eine Installation des Root-Zertifikats auf jedem einzelnen Client vorgenommen werden. Wenn möglich, sollte die Verteilung der externen Root-Zertifikate daher schon beim Ausrollen einer PKI-Anwendung erfolgen. Wenn die PKI-Anwendungen den Microsoft Certificate Store verwenden und im Unternehmen ein Active Directory (AD) im Einsatz ist, können die vertrauenswürdigen Root-Zertifikate vom Administrator über AD und Group Policy automatisch an alle Anwender verteilt werden. Falls kein anderer Mechanismus zur Verfügung steht, muss ein Anwender, sofern er die nötigten Rechte besitzt, die benötigten

---

10 Die European Bridge-CA stellt eine Certificate Policy mit Anforderungen an Bridge-CA Teilnehmer bereit: https://www.bridge-ca.org/download-directory/EBCA-Certificate-Policy.pdf

11 Im Fall der Verknüpfung von PKI-Domänen über Crosszertifikate fällt dieser Aufwand dagegen nicht an.

12 Siehe auch http://www.cabforum.org/ und http://www.webtrust.org/

externen Root-Zertifikate selbst im Internet herunterladen und in seiner PKI-Anwendung importieren.

Um den Benutzern die Handhabung zu erleichtern, sind in den Standard-Browsern schon eine Vielzahl an Root-Zertifikaten als vertrauenswürdige Sicherungsanker vorinstalliert. Diesen Root-Zertifikaten und allen weiteren von diesen Root-CAs ausgestellten CA-Zertifikaten vertrauen die Benutzer automatisch und in aller Regel unbesehen. Es findet meist keine weitere Überprüfung dieser CAs z. B. anhand ihrer Certificate Policies statt. Eine solche Prüfung kann nur manuell erfolgen und ist daher sehr aufwändig. So bleibt es bzgl. der Prüfung und Akzeptanz von Root-Zertifikaten bei dem Spagat zwischen Benutzerfreundlichkeit durch vorkonfigurierte Root-Zertifikate auf der einen Seite und hohem Sicherheitsbewusstsein mit manueller Prüfung von Certificate Policies durch den Anwender oder seine Organisation auf der anderen Seite.

7 Langzeitarchivierung

Elektronische Langzeitarchivierung bezeichnet die Aufbewahrung elektronischer Informationen für mehr als zehn Jahre. Im Kontext digital signierter Dokumente stellen sich hierbei neue zusätzliche Herausforderungen, insbesondere bei qualifizierten elektronischen Signaturen als Ersatz einer herkömmlichen Unterschrift bei Schriftformgebot: Der Sicherheitswert der Digitalen Signatur muss für den gesamten Archivierungszeitraum erhalten bleiben, um die Beweiskraft der elektronischen Signatur zu gewährleisten[13].

Die Langzeitsicherung von qualifizierten elektronischen Signaturen ist nicht gesetzlich verankert, aber immerhin als Hinweis in §6 SigG „Unterrichtungspflicht“ enthalten: „*Der Zertifizierungsdiensteanbieter [...] hat den Antragsteller darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.*“

Die Lebensdauer Digitaler Signaturen ist zum einen beschränkt durch die rasante technische Weiterentwicklung von Hard- und Software (Vernetzung, Rechenkraft), die zum Brechen des verwendeten Kryptoverfahrens zur Verfügung steht, und zum anderen durch die Fortschritte der Kryptanalyse. So gibt es verschiedene Gründe, warum eine Digitale Signatur erneuert werden muss. Diese Gründe können sein, dass:

- eine Schwachstelle in einem verwendeten Hashalgorithmus aufgedeckt wird,
- die Länge der Hashwerte nicht mehr den aktuellen Anforderungen entspricht,
- eine Schwachstelle in einem verwendeten Signaturalgorithmus aufgedeckt wird oder
- die verwendete Schlüssellänge bei der Digitalen Signatur nicht mehr den aktuellen Anforderungen entspricht.

Um den Sicherheitswert von digital signierten Dokumenten zu erhalten, kann entweder das Langzeitarchiv mit technisch-organisatorischen Maßnahmen die Unversehrtheit der archivierten Dokumente garantieren oder der Sicherheitswert der Digitalen Signatur kann über Nachsignierung bzw. Erneuerung von Signaturen erhalten werden. Dabei muss die erneute Signatur nicht zwingend von dem ursprünglich Signierenden geleistet werden, sondern digital signierte Dokumente werden typischerweise über Zeitstempel „aufgefrischt“, d. h. über die Signatur eines Zeitstempeldienstes, der damit bestätigt, dass die ursprüngliche

[13] Für qualifizierte elektronische Signaturen gilt der gesetzliche Anscheinsbeweis nach § 371a ZPO.

Signatur bereits zu einem Zeitpunkt vorgelegen hat, zu dem Algorithmen und Schlüssellängen noch den vollen Sicherheitswert besaßen.

Bei einem Langzeitarchiv wäre das regelmäßige Einholen eines Zeitstempels für den Hashwert eines jeden archivierten Dokuments sehr ineffizient. Daher sieht der in [RFC 4998] beschriebene Lösungsansatz zur Langzeitarchivierung ein baumbasiertes Verfahren vor (Hashtree). Über alle archivierten Dokumente werden in einer Baumstruktur gemeinsame Hashwerte im Archivierungssystem gebildet und ein einziger Archivzeitstempel für den Hashwert an der Wurzel des Baumes eingeholt, der alle Dokumente gemeinsam signiert. Dieser Zeitstempel wird bei Bedarf erneuert.

Abbildung 9 zeigt beispielhaft den Aufbau eines solchen Hashtrees. Die Blätter des Baumes bilden die Hashwerte der einzelnen Dokumente. Auf den höheren Ebenen wird jeweils ein Hashwert über zwei Hashwerte der darunter liegenden Ebene erstellt, d. h. pro Ebene wird die Anzahl der Hashwerte auf die Hälfte reduziert. Der Zeitstempel *t* an der Wurzel des Baumes sichert in diesem Beispiel alle archivierten Datenobjekte *d1, d2, d3* und *d4.*

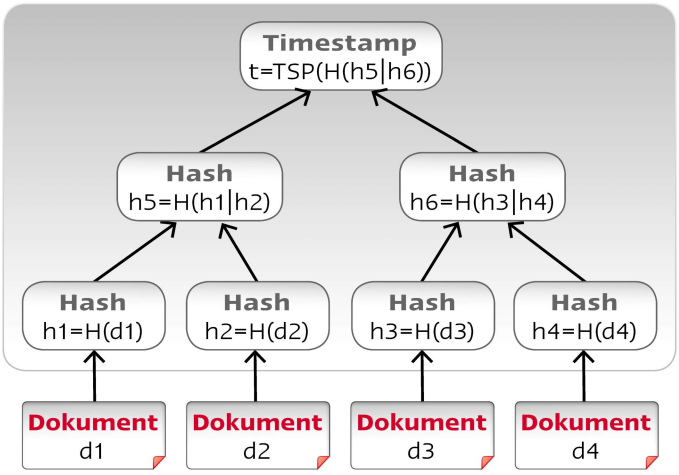

Abbildung 9: Beispiel für einen Hashtree
(H(d) bezeichnet die Berechnung eines Hashwerts über das Datum d,
TSP(h) die Erstellung eines Zeitstempels für den Wert h)

Wird ein archiviertes Dokument aus dem Archivierungssystem angefordert, so werden zusätzlich zum Originaldokument auch alle für die Zurückverfolgung des Hashtree-Weges benötigten Hashwerte vom Archivierungssystem zurückgeliefert, so dass die Überprüfung des Archivzeitstempels möglich ist. Bei einer erfolgreichen Verifikation des Zeitstempels ist der Nachweis gegeben, dass der Sicherheitswert und damit die Beweiskraft des angeforderten digital signierten Dokuments erhalten geblieben ist.

Dieser Lösungsansatz zur Langzeitarchivierung erfüllt zudem die Anforderungen des Datenschutzes zu Datensparsamkeit und Datenvermeidung, da die Löschung von einzelnen archivierten Datenobjekten möglich ist, wenn diese nicht mehr erforderlich sind. Nur die Hashwerte zu den gelöschten Datenobjekten müssen aufbewahrt werden, um jederzeit den Archivzeitstempel für den Hashwert an der Wurzel des Baumes verifizieren zu können.

8 Schlussbemerkung

Das Thema PKI bietet vielerlei Facetten. Dieses White Paper vermittelt die Grundlagen einer PKI und geht daher bei den verschiedenen Aspekten und Feinheiten einer PKI nicht in die Tiefe. Für vertiefende Informationen wird auf die im Literaturverzeichnis aufgeführten Veröffentlichungen verwiesen.

9 Literatur

[WP15] *Petra Barzin, Stefan Kelm:* „Das Policy-Rahmenwerk einer PKI“, Secorvo White Paper, März 2008

[PKCS] *RSA Laboratories,* http://www.rsasecurity.com/rsalabs/pkcs/

[PKIX] *IETF*, http://www.ietf.org/dyn/wg/charter/pkix-charter.html

[ComPKI] *T7 e.V., vormals T7 e.V. &TeleTrusT e.V:* http://www.common-pki.org/

[BRIDGE] *TeleTrusT e.V.,* http://www.bridge-ca.de

[X509] *International Telecommunication Union*: Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks, ISO/IEC 9594-8:2005 (E), ITU-T Recommendation X.509, Aug. 2005

[RFC5280] *D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk*: „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, Mai 2008

[RFC4998] *T. Gondrom, R. Brandner, U. Pordesch:* „Evidence Record Syntax (ERS)”, Aug. 2007

[RFC3739] *S. Santesson, M. Nystrom: „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”, März 2004*

[RFC3647] *S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu*:„Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework“, Nov. 2003

[RFC3161] *C. Adams, P. Cain, D. Pinkas, R. Zuccherato*: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), Aug. 2001

[RFC2560] *M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams*: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP, Juni 1999