# Public Key Infrastructures

## Eine Basistechnologie für sichere Kommunikation

Autor: Jan Grell

Herausgeber: grell-netz.de – computer services
Jan Grell
Auf dem Damm 36
53501 Grafschaft
http://www.grell-netz.de

Stand: 18. März 2002

# 0 Inhalt

# 1 Einführung in das Thema "Public Key Infrastrukturen" (PKI)

Für den Ablauf einer sicheren Kommunikation gibt es drei zentrale Sicherheitsaspekte.

So sollen nur berechtigte Personen die Nachricht lesen können (**Vertraulichkeit**).

Ebenso soll sicher gestellt sein, dass die Nachricht auch unverändert, d.h. ohne Manipulation durch Dritte, den Empfänger erreicht (**Integrität**).

Der dritte Aspekt ist die **Authentizität** einer Nachricht. Dabei wird gewährleistet, dass die Nachricht auch wirklich von dem angegebenen Absender stammt.

Diese Punkte werden durch den Einsatz eines Public-Key-Verfahrens abgedeckt.

# 2 Verschlüsselung

Grundlage einer vertraulichen Kommunikation sind Verschlüsselungsalgorithmen. Es gibt zwei Arten von Verschlüsselungsalgorithmen:

## 2.1 Symmetrische Verfahren

Hierbei wird der gleiche Schlüssel zum ver- und entschlüsseln benutzt. Es wird sofort klar, dass dadurch jeder, der den Schlüssel kennt, die Nachricht entschlüsseln kann. Demnach muss der Schlüssel geheim gehalten, und darf nur berechtigten Empfängern bekannt gemacht werden.

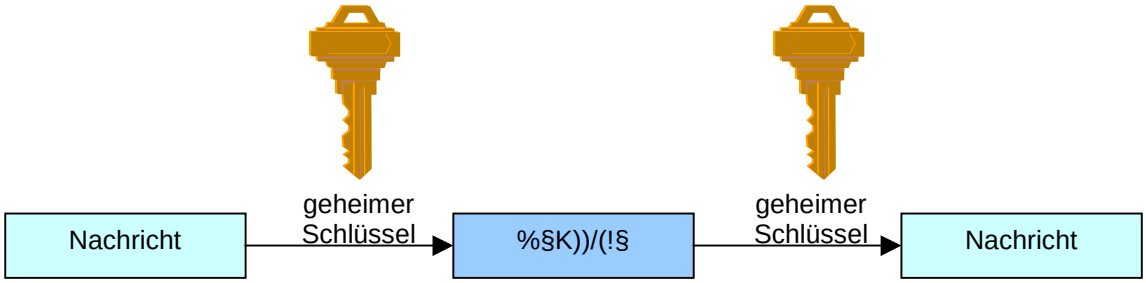


Abbildung 1: symmetrische Verschlüsselung

## 2.2 Asymmetrische Verfahren

Hier kommen zwei Schlüssel, einer zum Verschlüsseln und einer zum Entschlüsseln, zum Einsatz. Ein Schlüssel wird veröffentlicht (öffentlicher Schlüssel, public key), der andere vom Eigentümer geheim gehalten (privater Schlüssel, private key). Die verwendeten mathematischen Verfahren müssen so gewählt werden, dass man bei alleinigem Besitz des öffentlichen Schlüssels den privaten Schlüssel nicht oder nur mit erheblichem Aufwand errechnen kann. Da heute übliche Verfahren erst bei relativ langen Schlüsseln (z.B. RSA mit 1024 bit langen Schlüsseln) als sicher zu betrachten sind, erfordern sie im Vergleich zu den symmetrischen Verfahren erheblich mehr Rechenzeit.

Aus diesem Grund werden in einer PKI symmetrische und asymmetrische Verfahren kombiniert, auch Hybridverfahren genannt: Zur sicheren Übertragung des geheimen Schlüssels (für die symmetrische Verschlüsselung) wird dieser mittels asymmetrischer Verschlüsselung, mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Nur der Empfänger kann, da nur er den privaten Schlüssel besitzt, diese Nachricht entschlüsseln.

Aus Performancegründen wird die weitere Kommunikation symmetrisch mit dem zuvor sicher übertragenen Schlüssel verschlüsselt.

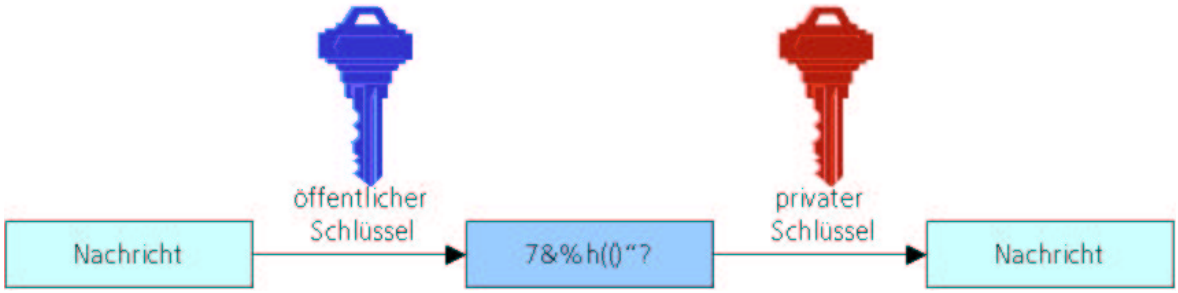


Abbildung 2: asymmetrische Verschlüsselung

## 3 Digitale Signatur

Damit der Empfänger auch sicher sein kann, dass die Nachricht nicht manipuliert wurde, wird die digitale Signatur verwendet. Dazu erstellt der Sender eine Prüfsumme mittels einer sogenannten Hashfunktion (auch als *hashen* bezeichnet). Diese Prüfsumme signiert er dann mit seinem privaten Schlüssel (beim RSA-Verfahren entspricht dies einer Verschlüsselung). Zur Feststellung der Integrität der Nachricht entschlüsselt der Empfänger die Prüfsumme mit dem öffentlichen Schlüssel des Senders und vergleicht sie mit der Prüfsumme, die er selbst aus der Nachricht erstellt hat. Bei Übereinstimmung kann der Empfänger sicher sein, die Nachricht unverändert empfangen zu haben.

Wichtig ist hierbei die Kollisionsfreiheit der Hashfunktion. Sie gewährleistet, dass unterschiedliche Dokumente auch mit an Sicherheit grenzender Wahrscheinlichkeit unterschiedliche Hashwerte erhalten.

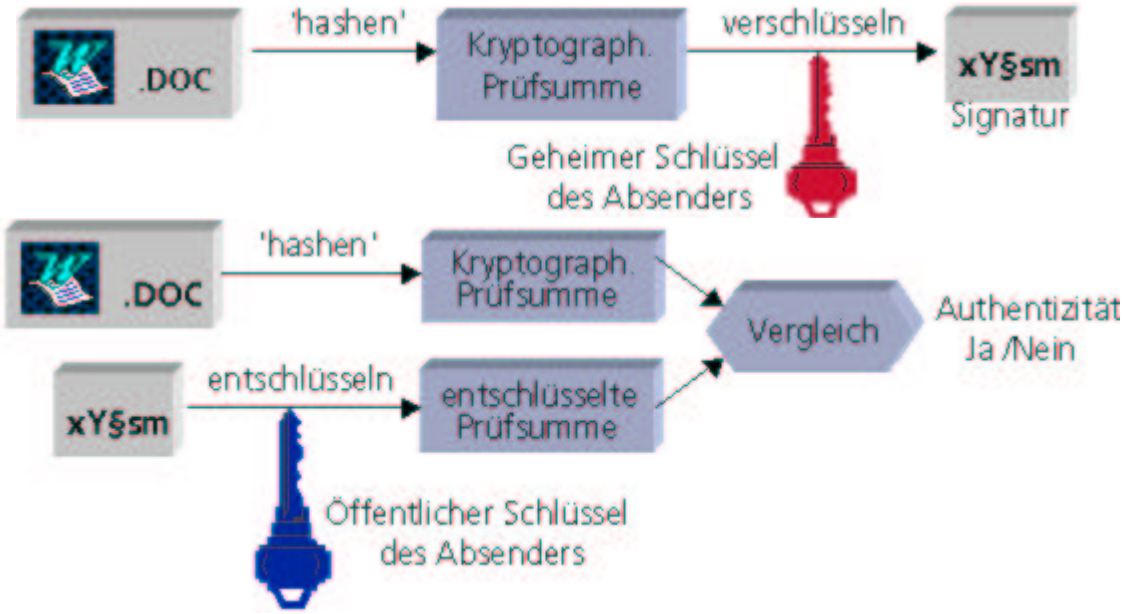


Abbildung 3: Signatur prüfen

Die Nachricht ist bei erfolgreicher Entschlüsselung der Prüfsumme mit dem öffentlichen Schlüssel des Senders auch als authentisch festgestellt, da diese Entschlüsselung nur gelingen kann, wenn die Prüfsumme auch wirklich mit dem privaten Schlüssel des Senders verschlüsselt wurde.

## 4 Digitale Zertifikate

Zur Dokumentation einer Zuordnung von Person und öffentlichem Schlüssel werden sogenannte Zertifikate eingesetzt. Diese sind nach [X509] standardisiert und enthalten neben einigen weiteren Angaben einen öffentlichen Schlüssel und den Namen des Inhabers. Diese Informationen sind von einer Zertfizierungsstelle digital signiert.

Zur Veranschaulichung könnte man ein digitales Zertifikat mit dem Personalausweis und die digitale Signatur mit der handschriftlichen Unterschrift vergleichen. Insbesondere hier verdeutlicht dies auch die Sicherheitsanforderungen an eine PKI.

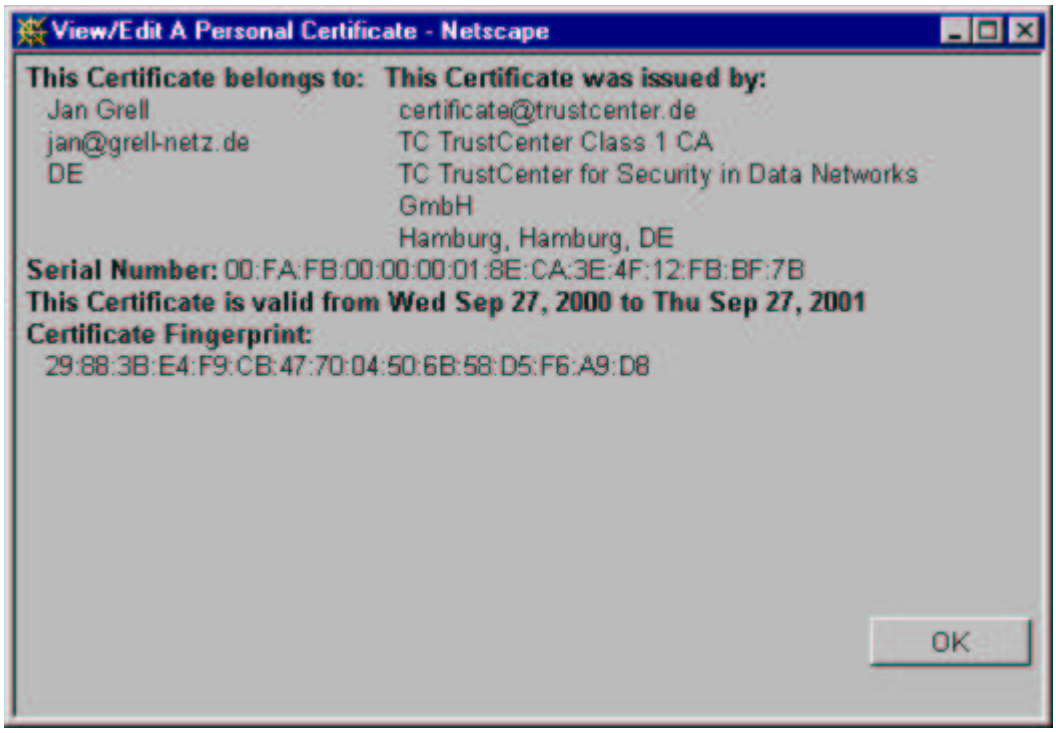


Abbildung 4: Ansicht eines Zertifikats im Netscape Communicator

Als Beispiel für die Inhalte eines digitalen Zertifikats nach X.509 Version 3 soll ein Emailzertifikat dienen (Hier die Klartext-Aufschlüsselung der Zertifikatsstruktur):

```
Certificate:
Data:
        Version: 3 (0x2)
Serial Number:
            fa:fb:00:00:00:01:8e:ca:3e:4f:12:fb:bf:7b
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for
                Security in Data Networks GmbH, OU=TC TrustCenter
                Class 1 CA/Email=certificate@trustcenter.de
        Validity
            Not Before: Sep 27 19:35:11 2000 GMT
            Not After : Sep 27 19:35:11 2001 GMT
        Subject: C=DE, CN=Jan Grell/Email=jan@grell-netz.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c4:9a:06:f4:2e:a4:44:55:2b:43:bc:72:8c:d0:
                    bf:e2:a7:16:11:bb:9e:cd:aa:29:a8:df:f8:d5:0f:
                    aa:ee:2c:fd:bb:8b:9b:79:de:d5:22:44:7a:a8:04:
                    c1:0c:ba:85:d9:0d:d1:4e:f5:69:64:db:b8:e6:31:
                    2c:4e:74:07:2a:ee:e0:fe:c9:ec:1b:fe:1a:d3:80:
                    b3:6c:15:1e:82:03:48:6e:69:88:99:6e:23:ca:b5:
                    a5:57:5f:8e:22:7c:27:26:91:e6:36:36:3c:d3:75:
                    ba:47:25:0f:0e:29:02:4b:86:80:d8:88:4c:d9:07:
                    c9:40:9d:44:6e:a6:17:e4:55
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Netscape CA Policy Url:
                http://www.trustcenter.de/guidelines
            Netscape Cert Type:
                SSL Client, S/MIME
            Netscape Revocation Url:
                https://www.trustcenter.de/cgi-bin/check-
                rev.cgi/FAFB000000018ECA3E4F12FBBF7B?
    Signature Algorithm: md5WithRSAEncryption
        7f:c2:bb:8d:ff:c3:76:c5:00:46:68:8f:29:e0:1a:0f:cc:8a:
        1d:83:b3:0d:d1:9b:20:ca:7e:68:88:16:0f:a5:35:3f:23:32:
        72:a7:8f:07:04:5d:e8:1a:f1:41:fa:c6:ba:f8:e3:e1:32:fe:
        89:52:5d:b2:74:e7:38:8a:d9:74:ed:80:d0:4a:10:33:cd:39:
        2b:b2:32:37:7b:41:0a:c3:75:2e:0d:76:0c:89:34:5c:53:8d:
        cf:2b:d7:30:ff:af:6c:d6:04:52:a6:74:ed:2c:8f:82:43:c4:
        ca:4c:51:e8:8f:0e:90:5d:0e:da:90:d6:53:a8:8b:9a:a8:ba:
        87:76
```

# 5 Komponenten einer PKI

## 5.1 Certification Authority (CA)

Zentrales Organ einer PKI ist die Certification Authority (CA). Sie nimmt Zertifizierungsanfragen entgegen, überprüft diese, stellt ihren Benutzern digitale Zertifikate aus und verwaltet Statusinformationen aller Vorgänge.

Die Abläufe in einer CA werden in einem Certification Practice Statement (CPS) und die Bedingungen für eine Zertifizierung sowie der Einsatzzweck eines Zertifikats in einer Certificate Policy dokumentiert. Eine CPS kann auch Informationen zur Haftung einer CA bezüglich der Zertifizierung oder Verpflichtungen der Benutzer (etwa Sicherheitsvorgaben) enthalten. Zu Struktur und Inhalt gibt die [RFC2527] ein Rahmenwerk vor.

## 5.2 Registration Authority (RA)

Für die Registrierung der Benutzer einer PKI sind die Registrierungsstellen, engl. Registration Authorities (RA) zuständig. Speziell, bei geographisch stark verteilten Public Key Infrastrukturen, bietet sich auch die Einrichtung mehrerer lokaler RA (LRA) an. Für den Benutzer vereinfacht sich die Situation, da für verschiedene Standorte lokale Ansprechpartner für alle administrativen Kontakte zur CA vorhanden sind.

RA sind für die korrekte Zuordnung von Benutzer und öffentlichem Schlüssel verantwortlich und überprüfen, ob der betreffende Benutzer berechtigt ist, ein Zertifikat von ihrer CA zu bekommen. Nach erfolgreicher Prüfung und Zuordnung wird der Zertifikatsantrag von der RA an die CA weitergeleitet. Dieser Antrag kann z.B. von einem RA-Officer digital signiert und an die CA zur Ausstellung eines Zertifikats weitergeleitet werden. Die RA benötigt dann auch ein Zertifikat ihrer CA.

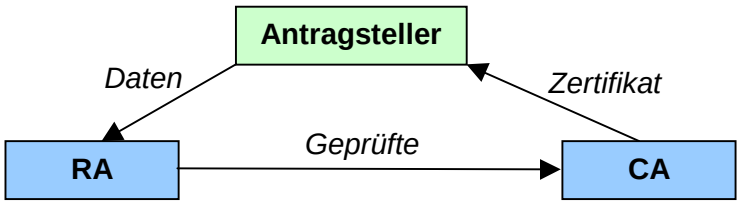


Abbildung 5: Ablauf einer Registrierung

Die Registrierungsstelle ist verantwortlich für die korrekte Identifizierung des Antragstellers. Gemäß der Signaturverordnung §3 (1) [SigV] gilt:

> *„Die Zertifizierungsstelle hat die Identifikation des Antragstellers gemäß § 5 Abs. 1 Satz 1 des Signaturgesetzes anhand des Bundespersonalausweises oder Reisepasses oder auf andere geeignete Weise vorzunehmen. Der Antrag auf ein Zertifikat muß eigenhändig unterschrieben sein. Soweit ein Antrag auf ein Zertifikat mit einer digitalen Signatur des Antragstellers versehen ist, kann die Zertifizierungsstelle von einer erneuten Identifikation und eigenhändigen Unterschrift absehen.“*

### 5.3 Verzeichnisdienst (Directory Service)

Meist direkt an die CA gekoppelt beinhaltet eine PKI einen Verzeichnisdienst zur Veröffentlichung der Zertifikate und Sperrlisten. Im Normalfall ist dies ein X.500 kompatibler Server, der das LDAP (Leightweight Directory Access Protocol) bereit stellt. Nach [X500] werden Einträge im Verzeichnisdienst in einer Baumstruktur abgelegt. Die einzelnen Knoten bezeichnen einzelne Elemente, die jeweils durch einen eindeutigen Namen ("Distinguished Name", DN) bezeichnet werden. Ein DN setzt sich aus allen Knotenbezeichnern zusammen, die zwischen der Wurzel und dem Element liegen, das er bezeichnet. Die einzelnen Bestandteile eines DN sind Informationen der Form "Attribut = Wert", wobei die Attribute im sogenannten LDAP-Schema definiert werden.

Attribute sind zum Beispiel: c=DE (Country, Land), st=Rheinland-Pfalz (Staat, Provinz, Bundesland), l=Grafschaft (Locality, Stadt, Ort), o=grell-netz.de (Organisation), ou=Webdesign (Organisational Unit, Untereinheit), cn=Jan Grell (Common Name, gewöhnlicher Name), userCertificate;binary=... (Benutzerzertifikat, Binärformat).

Ein Beispiel für einen DN wäre "cn=Jan Grell, ou=Webdesign, o=grell-netz.de, c=DE". Wenn dem Objekt weitere Informationen hinzugefügt werden, sind diese als zusätzliche Attribute definiert, aber nicht Bestandteil des DN.

### 5.4 End-Entity

Als End-Entity einer CA werden die Anwender und Systeme bezeichnet, die von ihr Zertifikate erhalten.

### 5.5 Web of Trust

Bei einem Web of Trust sprechen sich die einzelnen Benutzer ihr gegenseitiges Vertrauen aus. Dies geschieht durch digitales Signieren der öffentlichen Schlüssel, so ähnlich wie bei digitalen Zertifikaten. Ab einer gewissen Größe wird das jedoch recht unübersichtlich und für Unternehmen untragbar. Daher ist das Web of Trust eher im privaten Bereich anzutreffen und wird hier nicht näher beleuchtet. Das Verschlüsselungs- und Signierprogramm Pretty Good Privacy (PGP) basiert ursprünglich auf dieser Philosophie.

### 5.6 Zertifizierungshierarchie

Eine Zertifizierungshierarchie ist durch eine klare Strukturierung (Baumstruktur) wesentlich übersichtlicher und daher einfacher zu verwalten als das Web of Trust.

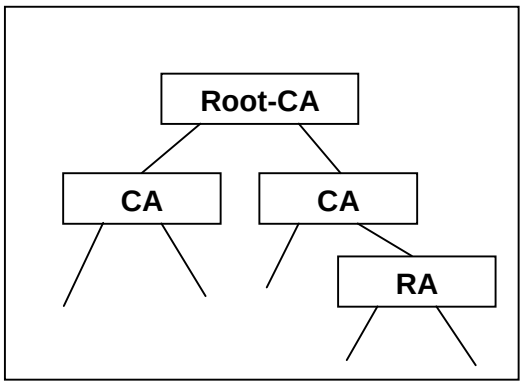


Abbildung 6: Zertifizierungshierarchie

An der Wurzel sitzt die sogenannte Root CA. Man erkennt eine Root CA an dem selbst signierten Zertifikat (self-signed root certificate). Darunter liegen in der Hierarchie weitere CA-Systeme, deren Zertifikate von der Root CA ausgestellt werden, sie werden auch als "Subordinate CA" (abgekürzt "SubCA") bezeichnet.

Der Weg, der bei der Prüfung eines Endbenutzerzertifikats bis zur Root CA zurückgelegt wird, heißt Zertifizierungspfad oder Zertifikatskette.

## 5.7 Cross-Zertifizierung

Bei einer Cross-Zertifizierung sprechen sich zwei CA ihr gegenseitiges Vertrauen aus, in dem sie sich gegenseitig je ein Zertifikat ausstellen. Beispielsweise könnten die Wurzelinstanzen zweier Unternehmen eine Cross-Zertifizierung durchführen, um den

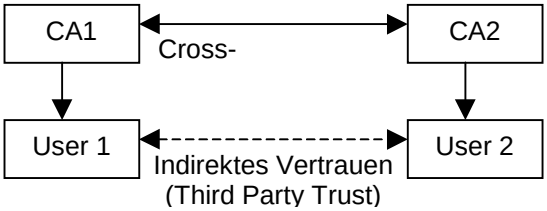


Abbildung 7: indirektes Vertrauen durch Cross-Zertifizierung

Mitarbeitern eine sichere Kommunikation untereinander zu ermöglichen. Ohne diese gegenseitige Zertifizierung müsste jeder Mitarbeiter, der mit einem Mitarbeiter der anderen Firma kommunizieren möchte, explizit sein Vertrauen gegenüber der CA dieser Firma aussprechen.

## 5.8 Schlüsselverwaltung

### 5.8.1 Schlüsselverteilung

Um in der Lage zu sein, anderen Kommunikationspartnern eine verschlüsselte Nachricht senden zu können, benötigt man von jedem Empfänger einer Nachricht dessen öffentlichen Schlüssel. Dem Sicherheitsziel der Authentizität entsprechend, muss jeder öffentliche Schlüssel von einer Certification Authority unterzeichnet worden sein, womit belegt wird, dass der vorliegende Schlüssel auch tatsächlich zu dem mutmaßlichen Empfänger gehört. Der öffentliche Schlüssel der Certification Authority muss daher zur Überprüfung dieser Signaturen jedem Mitarbeiter vorliegen. Dieser wird aus dem Zertifikat der CA entnommen, welches sicher an die Anwender zu verteilen ist. Somit ist jeder Schlüssel einem Zertifikat und damit auch einer Person eindeutig zugeordnet.

Die Emailprogramme Microsoft® Outlook® und Netscape® Messenger liefern in ihrer Grundeinstellung schon einige Zertifikate von Certification Authorities mit. Bei Netscape® sind dies unter anderem Digital Signature Trust Co. ®, Entrust®, GTE® Cybertrust®, GlobalSign®, TC TrustCenter®, ValiCert® und VeriSign®. Dieser Liste können weitere Zertifikate von Certification Authorities frei hinzugefügt werden.

### 5.8.2 Revocation

Ähnlich wie bei Kreditkarten kann es auch bei digitalen Zertifikaten vorkommen, dass sie zurückgerufen (revoked) werden müssen. Dies ist immer dann nötig wenn:

- Der private Schlüssel nicht mehr dem Eigentümer alleine bekannt (kompromittiert) ist (hier genügt bereits der Verdacht der Kompromittierung für eine Sperrung!)
- Der private Schlüssel verloren ging (Smart Card verloren oder defekt, Datei gelöscht etc.)
- Der Mitarbeiter das Unternehmen verlässt (keine Signatur im Namen der Firma mehr!)
- Angaben im Zertifikat nicht mehr korrekt sind (Name ändert sich etc.)

### 5.8.3 Revocation Checking

Damit nicht allen Benutzern einzeln mitgeteilt werden muss, dass ein Schlüssel bzw. Zertifikat zurückgerufen wurde, gibt es Listen (CRL, Certificate Revocation List), in denen sämtliche zurückgerufenen Schlüssel aufgeführt sind. Diese Listen werden bei jeder neuen Revocation aktualisiert. Für die Praxis bedeutet dies, dass der Anwender selbst für die Überprüfung der Gültigkeit eines Schlüssels verantwortlich ist. Dies gilt besonders vor einer Verschlüsselung, da mit einem kompromittierten Schlüssel keine Sicherheit mehr gewährleistet ist.

Für eine verbesserte Aktualität der Statusprüfungen definiert [RFC2560] mit dem Online Certificate Status Protocol (OCSP) ein Verfahren, bei dem die Zertifikatsprüfung gegen die Sperrliste durch einen Server erledigt wird.

### 5.8.4 Key Update / Rezertifizierung

Das Public-Key-Verfahren basiert auf der Verwendung von Schlüsselpaaren, die einen privaten und einen öffentlichen Schlüssel beinhalten. Private Schlüssel werden für das Entschlüsseln von verschlüsselten Nachrichten und für die Signaturerstellung verwendet. Mit öffentlichen Schlüsseln werden Daten verschlüsselt und Signaturen verifiziert. Aus Sicherheitsgründen sollte die Gültigkeit eines Zertifikates und dessen Schlüssel zeitlich begrenzt sein (vgl. Personalausweis). Damit ergibt sich aber der Bedarf einer Verlängerungsmöglichkeit oder der Erneuerung von Zertifikaten. Mit einer solchen

Verlängerung kann auch die Erneuerung der Schlüssel kombiniert werden. Dem Besitzer sollte das neue Zertifikat automatisch zugestellt oder eine einfache Möglichkeit für die Erneuerung seiner Schlüssel angeboten werden.

Trotz Key Update sollte sicher gestellt sein, dass alte Daten, die mit den vorherigen Schlüsseln verschlüsselt wurden, weiterhin lesbar bleiben. Dazu müssen technisch-organisatorische Maßnahmen getroffen werden, z. B. kann die PKI für jeden Benutzer eine Key-History führen.

### 5.8.5 Key Backup und Key Recovery

Ein weiterer Punkt ist die Wiedererlangung eines Schlüssels (**Key Recovery**). Es kann vorkommen, dass ein Benutzer das Passwort für den Zugriff auf den Schlüssel vergisst oder seinen Schlüssel verliert (in letzterem Fall sollte der Schlüssel zurückgerufen werden!). Für diese Situation ist es sinnvoll, die Schlüssel an einer geschützten Stelle gespeichert zu haben. Im Fall eines Unternehmens hat dies auch den zusätzlichen Vorteil, dass das Unternehmen trotzdem Zugriff auf die verschlüsselten Daten seiner Mitarbeiter hat (z.B. im Falle eines Ausscheidens).

Key Backup & Recovery ist eine Notfallmaßnahme! Auf der einen Seite gibt es ein Gefühl von Sicherheit, da die Schlüssel noch verfügbar sind, auf der anderen ist es eine Sicherheitslücke, da die Schlüssel an einer weiteren Stelle vor unbefugtem Zugriff geschützt werden müssen. Als sicherer Ort bietet sich beispielsweise die CA an.

### 5.8.6 Dual-Key Prinzip

Ein Problem beim Key Backup stellt eine eventuell unbefugte Nutzung der Schlüssel dar. So könnte beispielsweise auch mit einem unrechtmäßig erlangten Schlüsselpaar im Namen des rechtmäßigen Inhabers digital signiert werden.

Abhilfe schafft hier das sogenannte Dual-Key Prinzip, auch wenn es derzeit noch an Umsetzungen mangelt. Dabei beinhaltet das erste Paar je einen Schlüssel für das Ver- und Entschlüsseln (encryption public key und decryption private key) und das zweite je einen für Signieren und Verifizieren (signing private key und verification public key). Durch die getrennten Aufgabengebiete ergibt sich ein Vorteil für das Key Backup, da bei Bedarf nur der decryption private key gespeichert wird und nicht noch zusätzlich der signing private key. Ein

Key Backup des signing private key ist prinzipiell nicht notwendig, da bereits ausgestellte elektronische Signaturen weiterhin durch den öffentlichen Schlüssel geprüft werden können. Das deutsche Signaturgesetz verbietet ausdrücklich die Archivierung bzw. das Backup von Signaturschlüsseln.

## 6 Standards & Protokolle

Im PKI-Bereich kommen diverse Standards und Protokolle zum Einsatz, um Interoperabilität zu ermöglichen. Die nachfolgende Auflistung erhebt keinen Anspruch auf Vollständigkeit.

- **LDAP:** Leightweight Directory Access Protocol: Zugriffsprotokoll für Verzeichnisdienste nach [X500]
- **PKCS:** Public Key Cryptography Standards: Standards und Protokolle rund um PKI von RSA Security
  - **PKCS #1:** RSA Cryptography Standard [PKCS1]
  - **PKCS #7:** Cryptographic Message Syntax Standard [PKCS7]
  - **PKCS #10:** Certification Request Syntax Standard [PKCS10]
  - **PKCS #11:** Cryptographic Token Interface Standard [PKCS11]
  - **PKCS #12:** Personal Information Exchange Syntax Standard [PKCS12]
  - **PKCS #15:** Cryptographic Token Information Format Standard [PKCS15]
- **S/MIME:** Secure Multipurpose Internet Mail Extension (Kombination von PKCS#7 und X.509 in MIME): Erweiterung des MIME-Standards für sichere Email
- **SSL:** Secure Socket Layer: Verschlüsselung von Netzwerkverbindungen; definiert einen Layer, auf dem Protokolle wie z.B. http aufsetzen können
- **X.500:** Standard für Verzeichnisdienste [X500]: Definiert eine Struktur für Verzeichnisdienste und die Adressierung von Informationen
- **X.509:** Standard für digitale Zertifikate [X509]: Definiert die Struktur von digitalen Zertifikaten

## 7 Quellen

[Fegh98] Feghhi, J., Feghhi, J., Williams, P.: Digital Certificates - Applied Internet Security, Addison-Wesley, September 1998

[OSPKI] OpenCA Team: Open Source PKI Book Version 2.4.7, http://ospkibook.sourceforge.net/, 23. Juli 2000

[PKCS1] RSA Laboratories: PKCS #1 v2.0: RSA Cryptography Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html, 01. Oktober 1998

[PKCS7] RSA Laboratories: PKCS #7 v1.5: Cryptographic Message Syntax Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html, 01. November 1993

[PKCS10] RSA Laboratories: PKCS #10 v1.7: Certification Request Syntax Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-10/index.html, 26. Mai 2000

[PKCS11] RSA Laboratories: PKCS #11 v2.1: Cryptographic Token Interface Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html, Dezember 1999

[PKCS12] RSA Laboratories: PKCS #12 v1.0: Personal Information Exchange Syntax Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/index.html, 24. Juni 1999

[PKCS15] RSA Laboratories: PKCS #15 v1.1: Cryptographic Token Information Format Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-15/index.html, 06. Juni 2000

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C.: X.509 Internet Public Key Online Certificate Status Protocol - OCSP, http://www.ietf.org/rfc/rfc2560.txt, Juni 1999

[SigG] Regierung der Bundesrepublik Deutschland: Gesetz zur digitalen Signatur (Signaturgesetz - SigG), http://www.regtp.de/imperia/md/content/gesetze/22.pdf, 22. Juli 1997

[SigV] Regierung der Bundesrepublik Deutschland: Verordnung zur digitalen Signatur (Signaturverordnung - SigV), http://www.regtp.de/imperia/md/content/gesetze/23.pdf, 1. November 1997

[X500] ITU-T: Recommendation X.500: Information Technology - Open Systems Interconnection - The Directory: Overview of Concepts, Models and Series, November 1993

[X509] ITU-T: Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, November 1993