Zertifikate - Grundlagen

Zuvor eine Warnung und gleichzeitig eine Ermutigung:
Das Thema ***Zertifikate*** ist kein Alltagsthema und vom Inhalt her etwas kompliziert bzw. nicht sofort einzusehen. Deshalb sollte man sich bei der Lektüre Zeit lassen. Wir sind allerdings sicher, dass Sie danach vom Mehrwert der digitalen Zertifikate überzeugt sind. 

Im diesem Beitrag wird auf die digitalen Zertifikate **vom Typ** X509 **eingegangen, die im Rahmen der Public Key Infrastructure des Deutschen Forschungsnetzes(DFN) von der** Zertifizierungsstelle der Universität Freiburg **(Uni FR CA) herausgegeben werden. Der Artikel soll Hintergrundinformationen zum Thema „Zertifikate“ liefern, die im Wiki-Beitrag** WWW - Sichere Seiten **stichwortartig angesprochen werden. Ausführliche allgemeinere Informationen zu diesem Thema finden Sie auch im Wikipedia-Artikel** http://de.wikipedia.org/wiki/Digitales_Zertifikat **bzw. den Artikeln zu damit zusammen hängenden Themen wie z.B. „Digitale Signatur“ oder „Asymmetrisches Kryptosystem“.**

Einleitung

Man kann sich ein Zertifikat als Personalausweis in digitaler Form vorstellen: Beim Personalausweis garantiert die vertrauenswürdige Stelle „Meldeamt“, dass die Unterschrift, die sich auf dem Ausweis befindet, auch tatsächlich zu der Person gehört, deren Stammdaten und Passbild sich auf dem Ausweis befinden. Beim Zertifikat wird von diversen Zertifizierungsstellen, darunter auch der Uni FR CA eine entsprechende Sicherheit gegeben. Man unterscheidet mehrere Qualitätsstufen (einfach, fortgeschritten, qualifiziert), je nach Aufwand bei der Ausstellung des Zertifikates bzw. der Signatur.

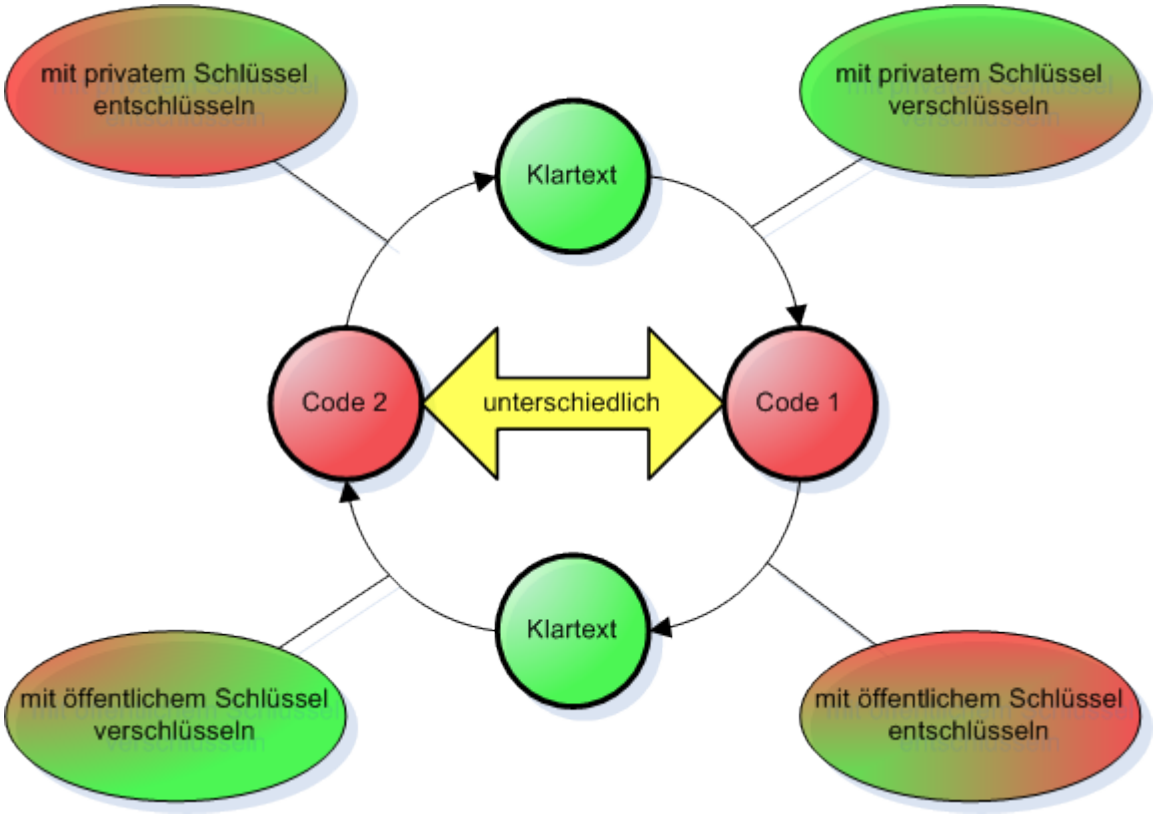
Ein Zertifikat enthält den Namen des Inhabers bzw. die Internetadresse eines Servers, seinen öffentlichen Schlüssel, eine Seriennummer, eine Gültigkeitsdauer und den Namen der Zertifizierungsstelle. Diese Daten sind in der Regel mit dem privaten Schlüssel der Zertifizierungsstelle verschlüsselt und können somit mit dem öffentlichen Schlüssel der Zertifizierungsstelle überprüft werden.

Mit Hilfe eines persönlichen Zertifikates, das in der Regel auch mit einer persönlichen Mailadresse verknüpft ist, kann die Inhaberin / der Inhaber Daten (Nachrichten, Formulare usw.) mit einer „digitalen Unterschrift“ versehen, die gewährleistet, dass diese Daten in der Originalversion vorliegen und genau der Person zugeordnet werden können, die Inhaberin des Zertifikates ist. Voraussetzung ist natürlich, dass der private Schlüssel nicht in die falschen Hände geraten ist.

Das Public Key - Verfahren

Beim Public Key - Verfahren (z.B. **RSA**) wird zunächst mit Hilfe einer passenden Rechenvorschrift ein Schlüsselpaar berechnet, das aus einem geheimen (privaten) und einem öffentlichen Schlüssel besteht. Daten, die mit dem privaten Schlüssel verschlüsselt werden, können nur mit dem öffentlichen Schlüssel wieder entschlüsselt werden - und umgekehrt. Deshalb nennt man eine solche

Methode auch „asymmetrische Verschlüsselung“.



Der besondere Vorteil dieses Verfahrens ist, dass die beiden Parteien keinen gemeinsamen geheimen Schlüssel kennen müssen. Bei der symmetrischen Verschlüsselung hat man dagegen immer das aufwändige Problem, den geheimen Schlüssel, der zum Ver- und Entschlüsseln verwendet wird, sicher zu allen Kommunikationspartnern zu übertragen.

Ein Nachteil ist allerdings, dass diese Art der Verschlüsselung sehr rechen- und damit zeitaufwändig ist und somit die verschlüsselte Kommunikation „ausbremst“. Deshalb wird in der Regel zwischen zwei Kommunikationspartnern mit Hilfe des Public Key - Verfahrens ein geheimer gemeinsamer Schlüssel (session key) für die schnellere symmetrische Verschlüsselung (z.B. nach **DES**) ausgehandelt, der dann für die Datenübertragung maximal für die Dauer der aktuellen Sitzung verwendet wird.

In der Praxis: Sobald Sie mit dem Webbrowser Ihrer Wahl (Firefox, IE) einen Zertifikatsantrag starten (z.B. auf den Antragsseiten der Uni FR CA), wird im Browser eventuell unbemerkt dieses Schlüsselpaar erzeugt. Der private Schlüssel verbleibt grundsätzlich im Zertifikatsspeicher dieses Browsers. Deshalb ist es erforderlich, dass Sie das von der Zertifizierungsstelle gelieferte Zertifikat auch wieder mit demselben Browser laden, denn dazu wird der private Schlüssel benötigt.

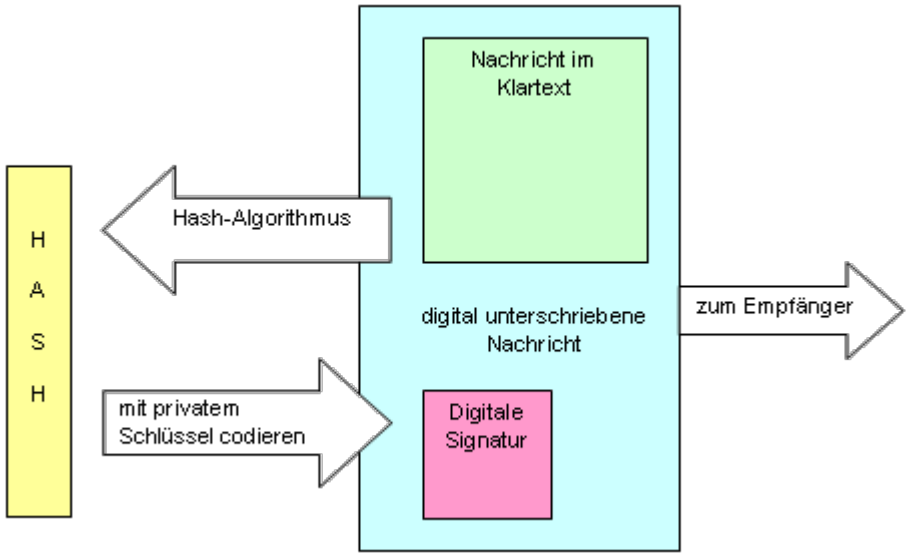
Die digitale Signatur

Für die digitale Signatur wird zunächst mit Hilfe einer speziellen Rechenvorschrift (z.B. **MD5** oder **SHA**) aus der zu übermittelnden Nachricht eine Zahl (bzw. eine Zeichenkette) berechnet. Diese Zahl wird als **Hash** bezeichnet. Dabei soll das Rechenverfahren gewährleisten, dass zwei verschiedene Datensätze nie zu demselben Hashwert führen.

Der Hashwert ist somit eine Art eindeutiger Fingerabdruck oder „Quersumme“ aus einem Datensatz und kann in Kenntnis des Rechenverfahrens von jedem Empfänger des Datensatzes wiederholt werden. Auf diese Weise wird die Integrität des Originaldatensatzes nachgewiesen.

Voraussetzung dazu ist allerdings, dass der Hashwert vom Absender sicher zum Empfänger gelangt, damit dieser darauf vertrauen kann, dass er seinen selbst berechneten Hashwert auch tatsächlich mit dem vom Sender gelieferten Original vergleicht.

Hier kommt nun das Public Key - Verfahren zum tragen: Der Sender einer Nachricht erzeugt einen Hashwert seiner zu sendenden Daten, verschlüsselt ihn mit seinem privaten Schlüssel und fügt die so erzeugte Signatur der Nachricht bei. Der Empfänger, der im Besitz des öffentlichen Schlüssels des Absenders ist, entschlüsselt die Signatur im Anhang und vergleicht das Ergebnis (= Original-Hash) mit seiner eigenen Hash-Berechnung (natürlich ohne die angehängte Signatur!). Bei Gleichheit der Hashwerte kann der Empfänger sicher sein, dass die Nachricht unterwegs nicht verfälscht wurde - vorausgesetzt, der geheime Schlüssel des Senders ist nicht in falsche Hände geraten.



In der Praxis: Die beschriebene Vorgehensweise ist Teil der Methode zum digitalen Unterschreiben von Mails. Wenn Sie eine Mail digital unterschreiben, wird dieser Vorgang der Hash-Erzeugung automatisch und von Ihnen unbemerkt auf den Mail-Text und die eventuell vorhandenen Anhänge angewandt. Auf diese Weise wird dem Empfänger die Sicherheit gegeben, dass der Mail-Inhalt unterwegs nicht manipuliert wurde.
Einige Mailclients verweigern übrigens das **Abtrennen** der Anhänge von digital signierten Mails, offenbar um die Aussagen über Herkunft und Unversehrtheit beibehalten zu können.

Das digitale Zertifikat

Beim digitalen Zertifikat handelt es sich um einen Satz von Daten, die den Eigentümer dieser Daten und üblicherweise weitere Eigenschaften eines öffentlichen Schlüssels beglaubigen.

Bestandteile eines Zertifikates sind unter anderem

- Der Aussteller des Zertifikates (die Zertifizierungsstelle, Certificate Authority (CA))
- Die Gültigkeitsdauer des Zertifikates
- Der öffentliche Schlüssel
- Angaben zum Eigentümer des öffentlichen Schlüssels
- Die digitale Signatur des Zertifikates, die von der Zertifizierungsstelle mit Hilfe des eigenen geheimen Schlüssels über alle übrigen Daten des Zertifikates gebildet wird.
  Sie dient der Überprüfung der Echtheit des Zertifikates.
- Erweiterungen, z.B. Angaben zum Geltungsbereich, zum Verwendungszweck oder zu den **Zertifikats-Sperrlisten**.

Zum speichern von Zertifikaten werden verschiedene Formate benutzt. Hier einige Beispiele:

- DER ist ein binäres Format mit den typischen Dateinamenserweiterungen .der oder .crt
- PEM ist ein Base64-codiertes Format mit der Erweiterung .pem, das man sich mit einem beliebigen Texteditor ansehen kann.
  Zum lesen muss allerdings wie auch bei den binären Formaten ein passendes Programm (z.B. **keytool** oder **openSSL**) benutzt werden.
- PKCS#12 ist ein binäres Format, das Zertifikate ohne oder mit privatem Schlüssel enthalten kann.
  Falls ein privater Schlüssel enthalten ist, werden die Dateien über ein Passwort geschützt.
  Diese Dateien mit der Namenserweiterung .p12 oder .pfx werden z.B. zum Sichern oder Übertragen von Zertifikaten und geheimen Schlüsseln verwendet, wie es in **User-Zertifikat beantragen** für die Übertragung eines Benutzerzertifikates aus Mozilla Firefox nach Mozilla Thunderbird beschrieben ist.

Muster eines PEM-Formates:

```
-----BEGIN CERTIFICATE-----
MIIDnzCCAoegAwIBAgIBJjANBgkqhkiG9w0BAQUFADBxMQswCQYDVQQGEwJERTEc
MBoGA1UEChMTRGV1dHNjaGUgVGVsZWtvbSBBRzEfMB0GA1UECxMWVC1UZWxlU2Vj
...
6iFhkOQxIY40sfcvNUqFENrnijchvllj4PKFiDFT1FQUhXB59C4Gdyd1Lx+4ivn+
xbrYNuSD7Odlt79jWvNGr4GUN9RBjNYj1h7P9WgbRGOiWrqnNVmh5XAFmw4jV5mU
Cm26OWMohpLzGITY+9HPBVZkVw==
-----END CERTIFICATE-----
```

Die Darstellung im Klartext mit dem bei der Java-Entwicklungsumgebung mitgelieferten Programm keytool.exe sieht dann z.B. so aus:

```
Eigner: CN=Deutsche Telekom Root CA 2, OU=T-TeleSec Trust Center, O=Deutsche
Telekom AG, C=DE
Aussteller: CN=Deutsche Telekom Root CA 2, OU=T-TeleSec Trust Center,
O=Deutsche Telekom AG, C=DE
```

```
Seriennummer: 26
Gültig von: Fri Jul 09 14:11:00 CEST 1999 bis: Wed Jul 10 01:59:00 CEST 2019
Digitaler Fingerabdruck des Zertifikats:
     MD5:  74:01:4A:91:B1:08:C4:58:CE:47:CD:F0:DD:11:53:08
     SHA1: 85:A4:08:C0:9C:19:3E:5D:51:58:7D:CD:D6:13:30:FD:8C:DE:37:BF
     Unterschrift-Algorithmusname: SHA1withRSA
     Version: 3

Erweiterungen:

#1: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#2: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 31 C3 79 1B BA F5 53 D7   17 E0 89 7A 2D 17 6C 0A  1.y...S....z-.l.
0010: B3 2B 9D 33                                        .+.3
]
]

#3: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:5
]
```

Ein Zertifikat erstellen

Mit den oben schon erwähnten Werkzeugen (keytool oder openSSL) kann die gesamte Prozedur zum Herstellen eines Zertifikates durchgeführt werden.

- **Schritt 1:** Grundsätzlich beginnt die Herstellung eines Zertifikates mit der Erzeugung eines Schlüsselpaares. Man speichert dieses in einer Datei ab, die als Schlüsselspeicher (keystore) bezeichnet wird. Da jeder Eintrag in einem Schlüsselspeicher mit einem Namen (alias) versehen wird, kann man sich bei nachfolgenden Operationen (z.B Vergabe eines Passwortes) auf den gewünschten Eintrag beziehen. Wenn ein Schlüsselspeicher mehrere Schlüsselpaare enthält, spricht man sinnigerweise auch oft von einem Schlüsselbund (key ring)  .

Vor dem nächsten Schritt muss man sich entscheiden, ob ein selbst-signiertes (self-signed) Zertifikat hergestellt werden soll, oder ob man sich sein Zertifikat von einer Zertifizierungsstelle beglaubigen lassen will.

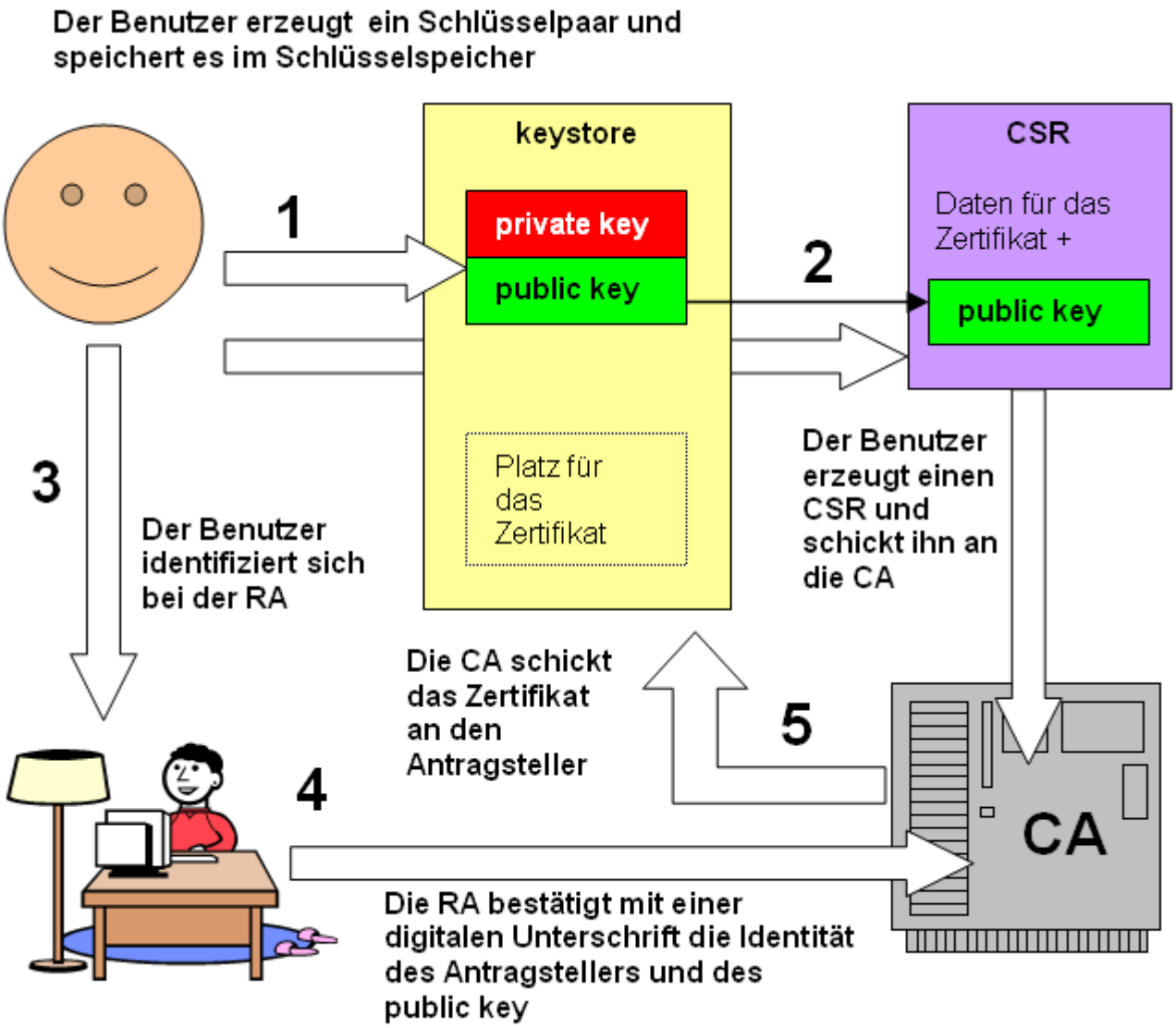
Selbst-signierte Zertifikate stellen keine Mechanismen zur automatischen Überprüfung der

Vertrauenswürdigkeit zur Verfügung. Sie werden meist zu Testzwecken installiert und in der Produktionsphase von fremd-signierten Zertifikaten abgelöst. Auf jeden Fall bieten Sie einen schnellen und unbürokratischen Weg zu einer verschlüsselten Kommunikation.

Wir wollen uns aber in diesem Artikel auf die Zertifkate konzentrieren, die von der Uni FR CA ausgestellt werden.
Deshalb sieht die weitere Prozedur wie folgt aus:

- In **Schritt 2** erzeugt man einen Zertifikatsantrag (certificate signing request, CSR), der neben dem öffentlichen Schlüssel die Daten aufnimmt, die ins Zertifikat übernommen werden sollen. Der CSR wird als separate PEM-Datei üblicherweise mit der Dateiendung .csr abgespeichert und an die Zertifizierungsstelle geschickt. Bei der Beantragung eines persönlichen Zertifikates wird der CSR vom Browser implizit durchgeführt.
- **Schritt 3:** Die vorgelagerte Registrierungsstelle (registration authority, hier die Uni FR RA) identifiziert den Antragsteller/die Antragstellerin, indem diese/r persönlich dort erscheint und sich mit einem amtlichen Dokument ausweist.
- **Schritt 4:** Nach erfolgter Identifizierung unterschreibt die RA den Zertifikatsantrag digital und löst damit die Herstellung des Zertifikates aus.
- **Schritt 5:** Die CA erzeugt das gewünschte Zertifikat und schickt es dem Antragsteller an die im CSR genannte Mailadresse zu.

Zur Illustration:



Ein Zertifikat überprüfen

Wie kann nun der Empfänger eines digitalen Zertifikates die Vertrauenswürdigkeit überprüfen?

Wie weiter oben schon erwähnt wurde, enthält das Zertifikat eine digitale Signatur des Ausstellers, in diesem Fall der Uni FR CA. Sie wird gebildet aus Zertifikatsdaten mit Hilfe des geheimen Schlüssels der Uni FR CA.

Hat man nun das Zertifikat der Uni FR CA zur Verfügung, besitzt man auch den öffentlichen Schlüssel dieser Instanz und kann die Signatur des empfangenen Zertifikates überprüfen. Man weiß damit, ob das Zertifikat tatsächlich von der Uni FR CA ausgestellt wurde. Kann man deshalb dem Zertifikat vertrauen? Die Antwort ist: Genau dann, wenn man der Uni FR CA vertraut.

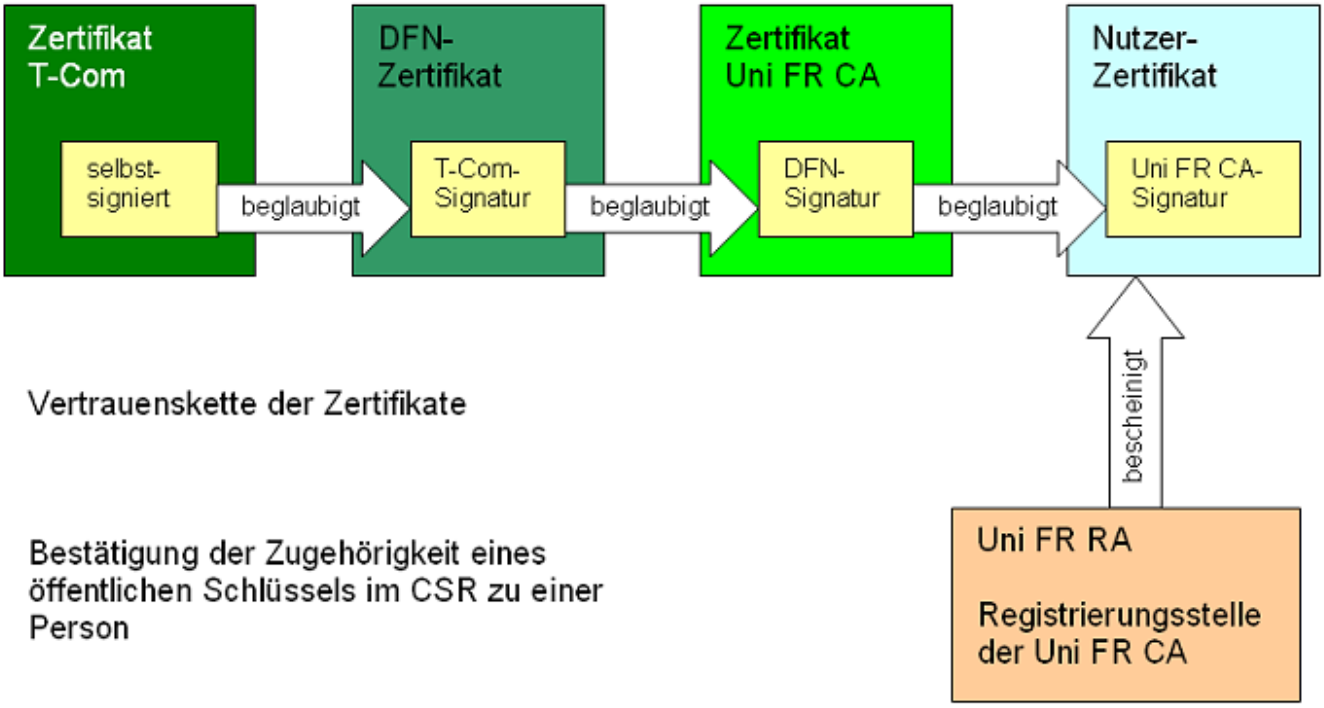
Das dürfte den Mitgliedern der Uni Freiburg sicher nicht schwer fallen  In der vorliegenden Public Key Infrastructure des DFN ist dies jedoch nicht nötig, denn es existiert eine „Vertrauenskette“ über den DFN-Verein bis hoch zur Deutschen Telekom:

Das Zertifikat der Uni FR CA wurde ja ausgestellt von der Global CA des DFN und enthält somit eine digitale Signatur dieser Instanz. Also lässt sich die Vertrauenswürdigkeit des Uni FR CA - Zertifikates auf die oben beschriebene Weise auf die des DFN-Zertifikates zurückführen.

Letzteres wurde aber ausgestellt von der Zertifizierungsstelle der Deutschen Telekom, die dem Zertifikat ihre digitale Signatur mitgegeben hat. Also lässt sich die Vertrauenswürdigkeit des DFN-Zertifikates auf die des Telekom-Zertifikates zurückführen.

Hier endet nun die „Vertrauenskette“ beim Wurzel-Zertifikat (root certificate) und man muss endlich seine Entscheidung treffen, ob man dieser Instanz vertraut und damit automatisch allen von deren Zertifikat abgeleiteten Zertifikaten.

Im folgenden Bild soll das veranschaulicht werden:



In der Praxis: Die Überprüfung der Vertrauenskette wird z.B. von Ihrem Mailprogramm oder dem PDF-Reader vollautomatisch durchgeführt. Sie erhalten dann auch eine positive Aussage über die Korrektheit der Unterschrift, wenn das entsprechende Programm in seinem Speicher für vertrauenswürdige Wurzelzertifikate das Wurzelzertifikat der Vertrauenskette vorfindet.

Man beachte: Wenn der Server nicht die gesamte Vertrauenskette ausliefert bzw. ein Zwischenzertifikat beim Client fehlt, wird dieser mit einer Fehlermeldung reagieren und anmerken, dass er dem Zertifikat nicht vertraut. Hier hilf nur die genaue Analyse des empfangenen Zertifikates und des Zertifikatspeichers im Client.

Viele Wurzelzertifikate werden bereits mit den Installationspaketen der Clients verteilt, weil die Herausgeber der Wurzelzertifikate den Herstellern der Clients gegenüber ihre Vertrauenswürdigkeit bewiesen haben. In diesem Fall müssen die Benutzer nicht einmal mehr dem Wurzelzertifikat gegenüber manuell ihr Vertrauen aussprechen bzw. werden vom Client nicht mehr danach gefragt. An der Notwendigkeit für die Server,

die Zwischenzertifikate zu liefern, ändert sich damit jedoch nichts.

Die Qualität von Zertifikaten

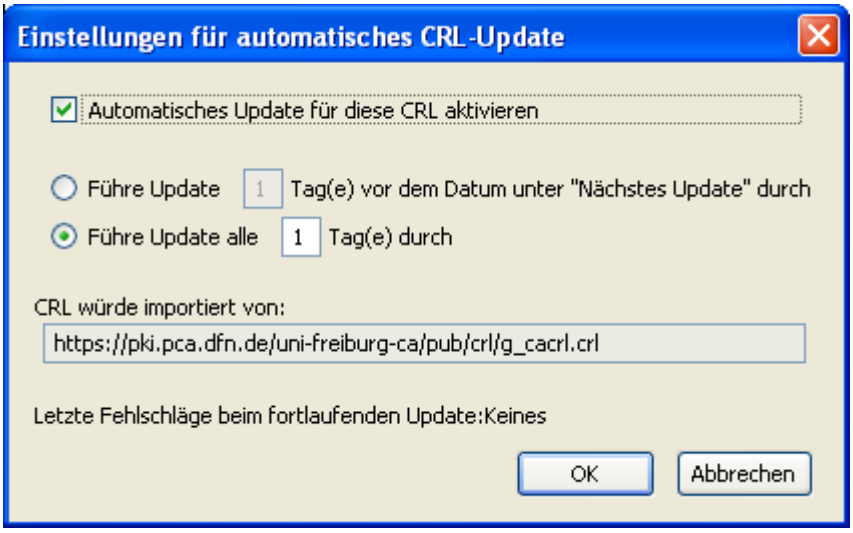
Zertifikate werden in unterschiedlichen Qualitätsstufen ausgegeben. Das wurde bereits in der **Einleitung** erwähnt.

Zur Qualität trägt z.B. bei:

1. wie aufwändig die Zuordnung eines Zertifikates und seines öffentlichen Schlüssels zu seinem Eigentümer (=Antragsteller) kontolliert wird.
   Gelegentlich werden kostenfreie(!) Zertifikate herausgegeben, die diese Kontrolle nicht durchführen.
   Die Uni FR CA betreibt eine Registrierungsstelle, bei der sich die Antragsteller persönlich ausweisen müssen, bevor derzen Zertifikatsantrag freigegeben werden kann.
   Dazu schreibt der DFN:
   „In der DFN-PKI werden fortgeschrittene Zertifikate ausgestellt, da für persönliche Zertifikate alle gesetzlichen Anforderungen an fortgeschrittene elektronische Signaturen erfüllt sind. Darüber hinaus muss sich jeder Antragsteller mit einem amtlichen Ausweispapier mit Lichtbild persönlich identifizieren. Damit wird bei der Zuverlässigkeit der Identifikation zum Erhalt eines persönlichen Zertifikats in der DFN-PKI ein vergleichbares Sicherheitsniveau erreicht wie bei der Identifikation zum Erhalt eines Zertifikats zur Ausstellung von qualifizierten elektronischen Signaturen (Vgl. § 5 Abs. 1 S. 1 SigG).“
   Gleichwohl dürfen sich diese Zertifikate nicht „qualifiziert“ nennen, da bei der Ausstellung keine Behörde wie z.B. die Bundesnetzagentur beteiligt ist.

2. ob und wie schnell ein ungültig gewordenes Zertifikat gesperrt werden kann und wie rasch diese Information an die Nutzer gelangt.
   Zertifikate, deren geheimer Schlüssel verloren wurde oder in die falschen Hände geraten ist sollten vorzeitig gesperrt werden können. Die Sperrung wird üblicherweise in Sperrlisten (certificate revocation list, **CRL**) veröffentlich, die regelmäßig gelesen bzw. importiert werden müssen oder über ein spezielles Verfahren (z.B. **OCSP**) online abgefragt werden können.
   Die Uni FR CA testet zur Zeit OCSP-fähige Zertifikate.

Zu 2:



Web- oder Mailclients sollten den Download von CRLs ermöglichen. Im nebenstehenden Bild sehen Sie das Konfigurationsfenster von Mozilla Firefox, in dem ein täglicher Download eingestellt ist. Damit wird zumindest zugesichert, dass eine veröffentlichte Sperrliste spätestens nach einem Tag beim Browser angekommen ist. Das sagt natürlich nichts darüber aus, wie schnell der Inhaber des Zertifikates mit einer Sperrung reagiert hat.

Ein betrübliches Bild liefert beim Firefox wie auch beim Thunderbird die in den Sperrlisteneinträgen genannten Aktualisierungszeiten, denen man hoffentlich nicht glauben muss ☹ Da wird nämlich meist von monatlichen Intervallen, z.T. weit in der Vergangenheit, erzählt. Bei einer manuellen Aktualisierung widerspricht sich das Programm anschließend selbst.

Sicherheit - Artikelübersicht, Zertifikate - Artikelübersicht