Public Key Infrastruktur

Stand: 11 Mai 2007

Ausgegeben von:

Rechenzentrum Hochschule Harz

Sandra Thielert

Hochschule Harz
Friedrichstr. 57 – 59
38855 Wernigerode
03943 / 659 – 0

Inhalt

Abkürzungen

ARL	Authority Revocation List
CA	Certificate Authority
CRL	Certificate Revocation List
DFN	Deutsches Forschungsnetz
DN	Distinguished Name
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
PCA	Policy Certificate Authority
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority

1 Einleitung

Vorraussetzung für einen effizienten Sicherheitsdienst innerhalb einer Organisation ist eine vertrauenswürdige Infrastruktur. Diese Infrastruktur, genannt PKI (Public Key Infrastruktur), leistet Dienste zur Erzeugung, Verteilung und Sperrung von Schlüsseln bzw. Zertifikaten. In einer solchen Infrastruktur werden Richtlinien und Regeln für die Handhabung der Schlüssel, für den Ablauf der Zertifikatserstellung und Identitätsprüfung aufgestellt. Weiterhin werden die gültigen und gesperrten Zertifikate veröffentlicht.

Eine PKI dient als End-zu-End-Sicherheit z.B. bei der Kommunikation über E-Mail und auch für eine unternehmensweite Sicherheit. Hierbei sollten Aspekte der Wirtschaftlichkeit in Bezug auf Aufwand, Kosten und Managebarkeit beachtet werden [Achter].

Eine PKI- Anbieter muss sich bei der Aufstellung seiner Regeln und Richtlinien an bestimmte Gesetzlichkeiten, wie z.B. das Signaturgesetz halten, um eine Rechtsverbindlichkeit zu erlangen.

Das Konzept der asymmetrischen Verschlüsselung ist die Basis einer PKI. Bei diesem Algorithmus wird mit einem Öffentlichen Schlüssel, Public Key und einem Privaten Schlüssel, Private Key gearbeitet, die in einem mathematischen Zusammenhang stehen.

2 Aufbau einer PKI

Das zentrale Ziel einer PKI ist das Management und die Sicherung der Zertifikate und Schlüssel innerhalb ihres eigenen vertrauenswürdigen Netzwerkes. Aus diesem Grund wird in diesem Abschnitt der Aufbau einer PKI in einer Organisation beschrieben werden.

2.1 Instanzen und ihre Aufgaben

Eine PKI Architektur verfügt über mehrere Instanzen, die ihre eigenen Aufgaben und ihre Pflichten im Netzwerk haben. In den nachfolgenden Abschnitten werden die einzelnen Instanzen kurz erläutert.

2.1.1 Endteilnehmer

Ein Endteilnehmer ist ein Inhaber von einem oder auch mehreren Schlüsselpaaren, mit einem Zertifikat, welches die Identität des Endteilnehmer bestätigt. Endteilnehmer sind also Endanwender in einer PKI, hierbei wird nochmals unterschieden in Endteilnehmer als natürliche Personen, Server und Objekte, wie z.B. Rooter sowie in die Endteilnehmer-Komponenten. Endteilnehmer-Komponenten können untergeordnete CA’s oder RA’s sein, die wiederum Endteilnehmer zertifizieren.

2.1.2 Authorities

RA (Registration Authority)

Eine RA (Registration Authority), auch als ORA (Organizational Registration Authority) bezeichnet, ist für die Identitätsprüfung verantwortlich, hierbei wird jeder Endteilnehmer identifiziert und registriert. Die Identifizierung erfolgt, anhand eines Ausweises und persönlicher Vorstellung. Eine weitere Aufgabe die der RA übertragen werden kann ist die Generierung von Schlüsseln, dabei muss beachtet

werden das der generierte private Schlüssel nach der Übergabe an den Endteilnehmer gelöscht wird [TeleTrust].

CA (Certificate Authority)

Die CA, oft auch als Zertifizierungsstelle bezeichnet, ist die oberste Instanz einer Public Key Infrastruktur. Sie ist verantwortlich für das Management und die sichere Verwahrung der Daten, Zertifikate und Schlüssel. Diese Instanz legt die Richtlinien und die Regeln zur Zertifizierung und zu Verhaltenweisen innerhalb des Netzwerkes fest. Diese Richtlinien sind für alle Teilnehmer bindend, die sich zertifizieren lassen wollen. Mit Hilfe dieser Bestimmungen von Richtlinien, die öffentlich bekannt gemacht werden, kann eine CA ihr vertrauenswürdiges Netzwerk aufbauen.

Die CA ist weiterhin auch für die Verwaltung der Verzeichnisdienste verantwortlich, die nachfolgend erläutert werden. In der nachfolgenden Tabelle sind einige Zertifizierungsstellen aufgelistet.

Nicht kommerzielle CA's	
DFN-PCA[1]	www.cert.de
GMD Trustfactory[2]	www.secude.com/GMD-TrustFactory/
IN-CA[3]	www.in-ca.individual.de
Heise CA[4]	www.heise.de/ct/pgpCA/
Kommerzielle CA's	
Trustcenter[5]	www.trustcenter.de
CCI[6]	www.cci.de
IKS[7]	www.iks-jena.de
D-Trust[8]	
TÜV-Informationstechnik (TÜV-IT)	
DATEV[9]	
Bundesnotarkammer	
DE-CODA[10]	

Tabelle 1: Auflistung von Zertifizierungsstellen [Camphausen]

[1] Die DFN-PCA stellt Zertifikate für Zertifizierungsstellen in Rechenzentren der Hochschulen aus.
[2] Eine CA der Secude GmbH, aufgebaut im Rahmen des ICE-TEL-Projektes.
[3] Individual Network e.V.
[4] PGP CA der Computerzeitschrift c't.
[5] Trustcenter for Security in Data Networks GmbH, Hamburg.
[6] Competence Center Informatik GmbH, Meppen.
[7] IKS GmbH, Jena.
[8] Joint-Venture der Debis IT Security Services GmbH und der Bundesdruckerei GmbH, Berlin.
[9] Datenverarbeitung und Dienstleistung für den steuerberatenden Beruf eG, Nürnberg.
[10] Gesellschaft zur elektronischen Zertifizierung von Dokumenten mbH, Tochter des Deutschen Industrie- und Handelstages (DIHT), Bonn.

Bei kleineren Infrastrukturen wird die CA und die RA zusammengefasst zu einer Instanz. Dann übernimmt die CA die Aufgaben der RA.

2.2 Modelle für den Aufbau einer Infrastruktur

Ein Vertrauensnetz kann in verschiedener Weise aufgebaut werden. Nachfolgend sind drei Modelle aufgezeigt.

Hierarchisches Trustmodell (Zertifizierungshierachie)

Innerhalb diesen Modells gelten eindeutige Vertrauensbeziehungen, sogenannte Trustpfade. Die oberste Instanz (Zertifizierungsinstanz) ist die PCA (Policy Certificate Authority), wie in der Abbildung 1 abgebildet. Sie legt im Modell eindeutige Richtlinien fest, die in der gesamten Organisation ihre Gültigkeit haben. Jedem Endteilnehmer wird eine CA zugeteilt. Zertifikate werden nur von der höheren Instanz an untere Instanzen zertifiziert.

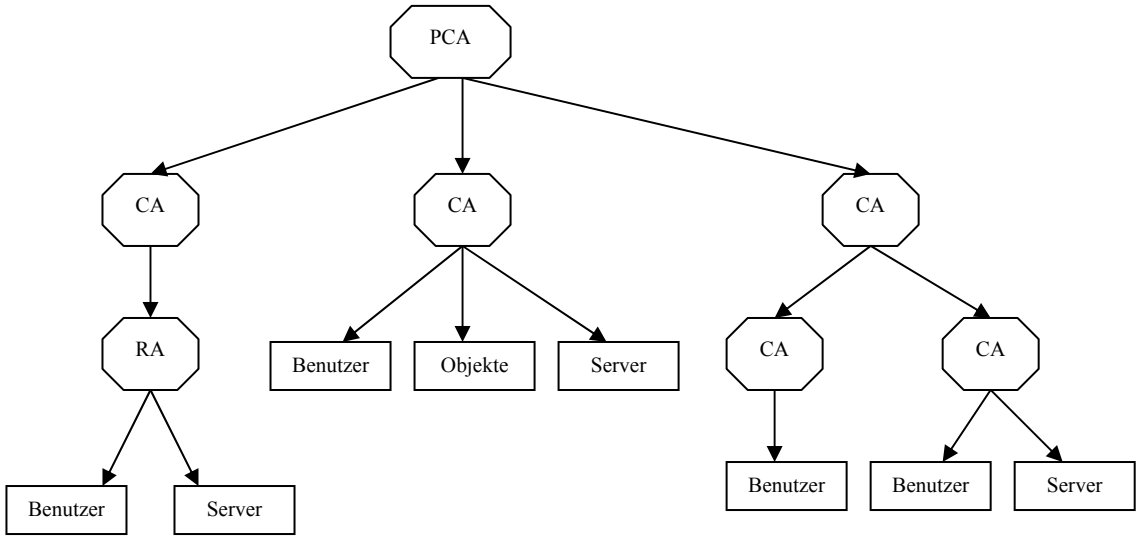

Abbildung 1: Hierarchisches Modell

Zertifizierungsnetze

Zertifizierungsnetze (Abbildung 2) ermöglichen eine Cross-Zertifizierung der Teilnehmer, d.h. die einzelnen Teilnehmer können sich gegenseitig zertifizieren, so können zwei verschiedene PKI – Systeme miteinander kommunizieren. Nachteil dieses Modells ist, dass keine einheitlichen Richtlinien an die Vertrauenswürdigkeit der einzelnen CA's durchgesetzt werden können.

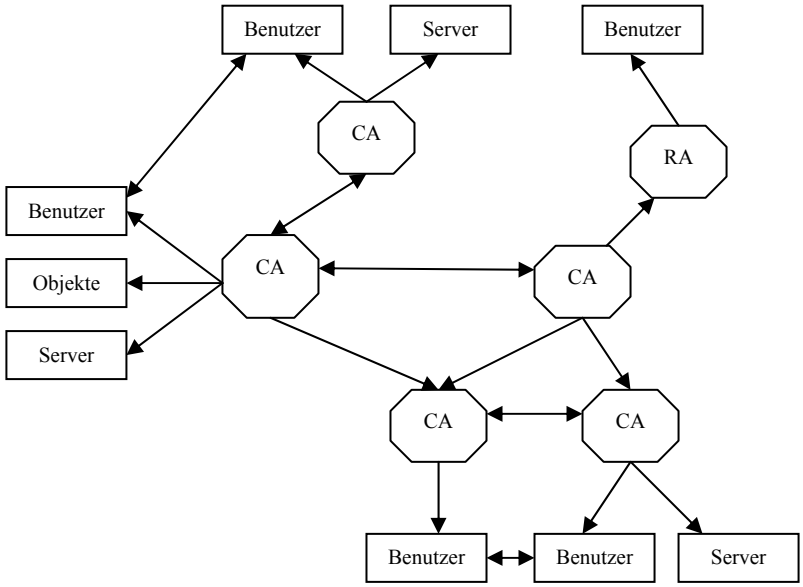

Abbildung 2: Zertifizierungsnetz

Hybride Ansätze

Dieses Modell (Abbildung 3) ist eine Mischform aus den beiden vorhergegangenen Modellen. Es erlaubt die gegenseitige Zertifizierung der CA's. Die übergeordnete Instanz, die Policy Management Authority (PMA), definiert die Richtlinien, die in der gesamten Organisation ihre Gültigkeit haben.

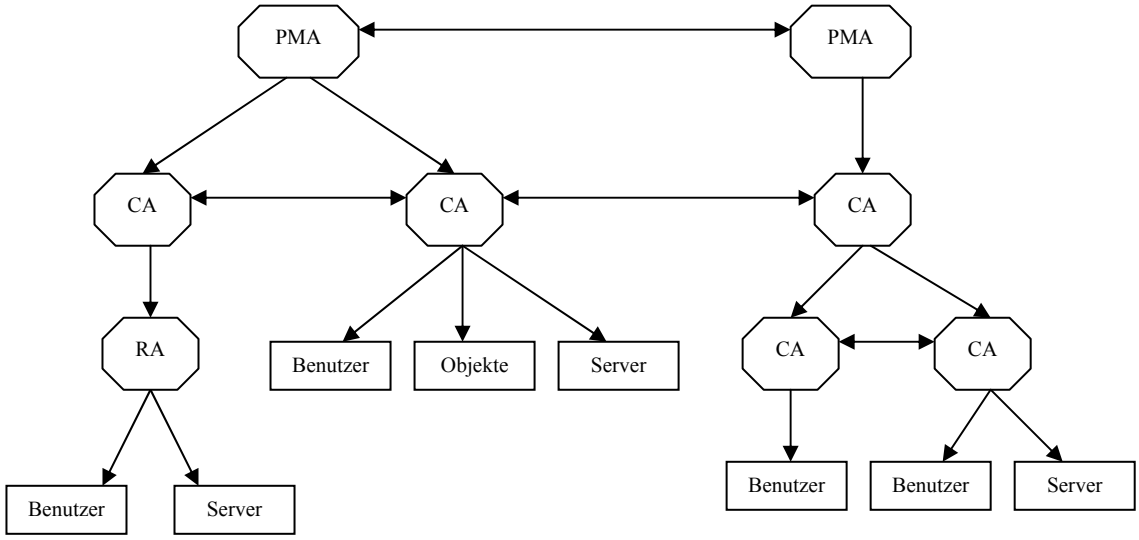

Abbildung 3: Hybrider Ansatz

2.3 Zertifikate

Zertifizierungsstellen sollen die Echtheit einer Person, Institution, Rechner oder wiederum einer untergeordneten Zertifizierungsinstanz bestätigen. Dies erfolgt hier über Zertifikate in denen beglaubigt wird das der Öffentliche Schlüssel und diese Person oder Einrichtung zusammengehören. Die Zertifizierungsstellen veröffentlichen den Öffentlichen Schlüssel, so dass jeder sich mit diesem Schlüssel von der Echtheit der Zertifizierungsstellen überzeugen kann. Hierbei ist die Glaubwürdigkeit der Zertifizierungsstelle, eine der wichtigsten Vorraussetzungen für das Management der Schlüssel- und Zertifikatsverwaltung.

Nach der Beantragung von Zertifikaten können diese in bestimmte Klassen eingeteilt werden. Die nachfolgende Liste zeigt und erläutert die 5 verschiedenen Klassen der Zertifikatseinteilung.

Class 0 Ausgabe erfolgt nur für Testzwecke, ohne eine Überprüfung der Identität. Zertifikate dieser Kategorie sind zeitlich begrenzt.

Class 1 Die Ausstellung erfolgt nur an Privatpersonen mit Angabe der E-Mail-Adresse.

Class 2 Zertifikate für private und auch geschäftliche Nutzung
Firmen → Der Handelsregistereintrag wird überprüft
Privatkunde→ Ausweisung erfolgt über den Personalausweis

Class 3 Zertifikate für Unternehmen und Privatkunden mit zusätzlichen Überprüfungen, findet Einsatz beim Online-Banking und bei E-Commerce

Class 4 die Ausstellung erfolgt nur an Privatpersonen mit höchster Authentisierung durch Identitätsfeststellung.

2.3.1 **Detailinformationen zu Zertifikaten**

Zertifikate sind ein wichtiger Bestandteil bei der Authentisierung in einer Public Key Infrastruktur. Sie enthalten Informationen zum Schlüssel im Zusammenhang mit der Identität des Schlüsselinhabers. Zertifikate werden in zwei verschiedenen Formaten ausgegeben, zum Einen im X.509v3 Format und zum Anderen im PGP (Pretty Good Privacy) Format.

X.509v3 Format

Das X.509v3 Format wurde von der IETF (Internet Engineering Task Force) erarbeitet und 1997 von der ITU (International Telecommunication Union), einem Dachverband der Telefongesellschaften verschiedener Länder, standardisiert. Dieses Format basiert auf dem X.500 Format, welches den Verzeichnisdienst beschreibt. Im X.509 Format sind alle nötigen Vorraussetzungen, wie Datenformate und Protokolle definiert und die Zertifikatserweiterungen erhöhen die Flexibilität gegenüber den vorhergehenden Versionen. In der nachfolgenden Tabelle sind alle Felder aufgezeigt die in einem Zertifikat vorhanden sein müssen.

Feld	**Bedeutung**
Administrative Informationen	
Version	Identifizierung der Version
Serial Number	Seriennummer des Zertifikates
Signature	Verwendeter Algorithmus für die Signatur
Informationen zur Ausgabestelle	
Issuer	Identifizierung der Certificate Authority, die das Zertifikat ausgegeben hat
Issuer UniqueID	ID für die Widerverwendbarkeit
Validity	Gültigkeitsdauer Angabe Anfangsdatum und Enddatum
Informationen zum Eigentümer	
Subject Name	Name des Eigentümers
Subject Public KeyInfo	Öffentlicher Schlüssel verwendeter Algorithmus für Schlüsselerstellung
Subject UniqueID	ID für die Widerverwendbarkeit
Zusätzliche Informationen	
Extensions	Individuelle Attribute z. B. Certificate Policies – Konditionen CRL Distribution Points – Adresse der Widerrufsliste Angaben zum Eigentümer (Emailadressen, alternative Namen, Qualifikationen) Nutzungsbeschränkungen
Signatur der CA	

Tabelle 2: Zertifikatsinformationen nach dem X.509v3 Standard

Für die Erstellung von Zertifikaten diesen Formats werden verschiedene Softwarelösungen angeboten. Es soll hier nur auf die OpenSource Software OpenSSL verwiesen werden.

Die Identifikation der Personen erfolgt über einen Distinguished Name (DN), nach dem X.509 Format, siehe Tabelle 3.

DN Feld	**Abkürzung**	**Bedeutung**
Country	C	ISO Ländercode
State	ST	Staat, Provinz, Gegend
Locality	L	Stadt, Sitz der Organisation
Organization	O	Firma oder Organisation
Organizational Unit	Ou	Abteilung
Common Name	CN	Name der Person Hostname des Servers

Tabelle 3: Identifizierung einer Person nach [Kredel]

PGP Format

PGP ist eine international anerkannte Möglichkeit für die Verschlüsselung von Informationen. Dieses Format wird vorrangig für die E-Mailverschlüsslung eingesetzt. Für die Generierung der Schlüssel und Verschlüsselung der Dokumente kann das gleichnamige Programm, entwickelt von Philip Zimmermann, verwendet werden. Freeware-Fassungen können von der Internetseite http://www.pgpi.com geladen werden.

Der Public Key Server verwaltet alle öffentlichen Schlüssel die ausgegeben wurden.

2.3.2 Verzeichnisdienste

Veröffentlichung der Zertifikate und der öffentlichen Schlüssel

Ein öffentlicher Schlüssel und das zugehörige Zertifikat, welches die Identität des Schlüsselinhabers bestätigt, muss an einer geeigneten Stelle veröffentlicht werden, so das jeder die Möglichkeit hat mittels dem öffentlichen Schlüssel dem Schlüsselinhaber eine verschlüsselte Nachricht zuzusenden.

CRL (Certificate Revocation List)

Die CRL ist eine Sperrliste, in der alle Teilnehmerzertifikate[11] gelistet werden die gesperrt wurden vor Ablauf ihrer Gültigkeitsdauer: Die Liste gibt Auskunft über den Grund und den Zeitpunkt der Sperrung. Für die Prüfung der Echtheit einer solchen Sperrliste wird diese von der zuständigen CA signiert, dabei darf der Signierschlüssel nicht mit dem Schlüssel der Zertifizierungsstelle übereinstimmen.

ARL (Authority Revocation List)

Eine ARL ist eine Sperrliste in der alle gesperrten Zertifikate von CA's aufgelistet werden. Für die Prüfung der Echtheit kann hier ebenfalls die Signatur genommen werden.

[11] Im Sinne diesen Skriptes natürliche Personen und Server

2.3.3 Ungültigkeit bzw. Sperrung von Zertifikaten

Ein Zertifikat kann als gesperrt erklärt werden, wenn

- die gemachten Angaben bei der Identifizierung und Registrierung nicht den Tatsachen entsprechen,
- der privaten Schlüssels verloren oder beschädigt wurde,
- die im Zertifikat ausgewiesenen Informationen sich verändert haben,
- der Teilnehmer sein Zertifikat nicht mehr benutzt,
- das Zertifikat durch ein anderes ersetzt wird, während die Gültigkeitsdauer noch nicht abgelaufen ist, z.B. bei Verlängerungszertifikaten.

Eine Sperrung eines Zertifikats erfolgt meist auf Antrag (Revocation Request) eines Teilnehmers selbst. Nach Beantragung muss die CA den Teilnehmer authentifizieren, um eine ungerechtfertigte Sperrung zu vermeiden. Im Sperrantrag müssen alle Informationen enthalten sein die auch in der Sperrliste erscheinen werden, siehe Quelltext 1.

```
Revocation Request
certDetails                          -- Seriennummer des Zertifikats
                                     -- Name der ausstellenden CA
revocationReason      OPTIONAL       -- Angabe des Rückrufgrundes
badSinceDate          OPTIONAL       -- Ungültigkeitszeitpunkt
crlEntryDetails       OPTIONAL       -- gewünschte zusätzliche Angaben für Sperreintrag
```

Quelltext 1: Datenstruktur eines Sperrantrages (Revocation Request), Beispiel [TeleTrust2]

Sobald die Zertifikate ihre Gültigkeit verloren haben werden sie von der CRL oder ARL verwaltet. Hier werden die Zertifikate aufgenommen mittels ihrer Seriennummer und dem Sperrungsgrund. Für die Prüfung des Aktualität sollte immer ein Zeitstempel und eine Angabe, wann die nächste Aktualisierung erfolgt, vorhanden sein. Nach Beendigung der Lebensdauer werden die Zertifikate von den Listen gelöscht. Das verwendete Format für die Sperrlisten ist das X.509. Dieses Format bestimmt die enthaltenen Angaben bei der Erstellung der Speerlisten.

3 Zertifizierung

In diesem Abschnitt soll der gesamte Ablauf und die Vorraussetzungen einer Zertifizierung eines Teilnehmers dargestellt werden. Zu Beachten ist dabei das jede CA ihre eigenen Zertifizierungsvorschriften veröffentlicht. Zur Verdeutlichung der allgemeinen Vorgehensweise wurde dazu die nachfolgende Liste mit den Vorraussetzungen und die Abbildung 4 für den Ablauf einer Zertifizierung erstellt.

Vorraussetzungen für eine Zertifizierung:

1. Erzeugung eines Schlüsselpaares vom Teilnehmer,
2. Erzeugung einer Zertifikatsanfrage mit öffentlichem Schlüssel (Certification Request). Diese Anfrage muss alle Informationen enthalten die für eine Ausstellung eines Zertifikates gebraucht werden.,
3. Teilnahmeerklärung ausfüllen, hiermit erklärt sich der Teilnehmer bereit die Richtlinien zur Arbeitsweise der CA anzuerkennen,
4. Registrierung und Identifizierung des Teilnehmers, direkt bei der CA bzw. bei einer RA und Übergabe der Unterlagen an die CA. Die Identifizierung erfolgt mittels einem gültigen Ausweises.

Nach erfolgreicher Prüfung und Vollständigkeit der Unterlagen erhält der Teilnehmer von der CA eine Zertifizierungsantwort (CertRepMessage), mit dem Zertifikat des Teilnehmers und der Zertifikate der CA. Weiterhin wird das Zertifikat an den dafür vorgesehenen Stellen veröffentlicht.

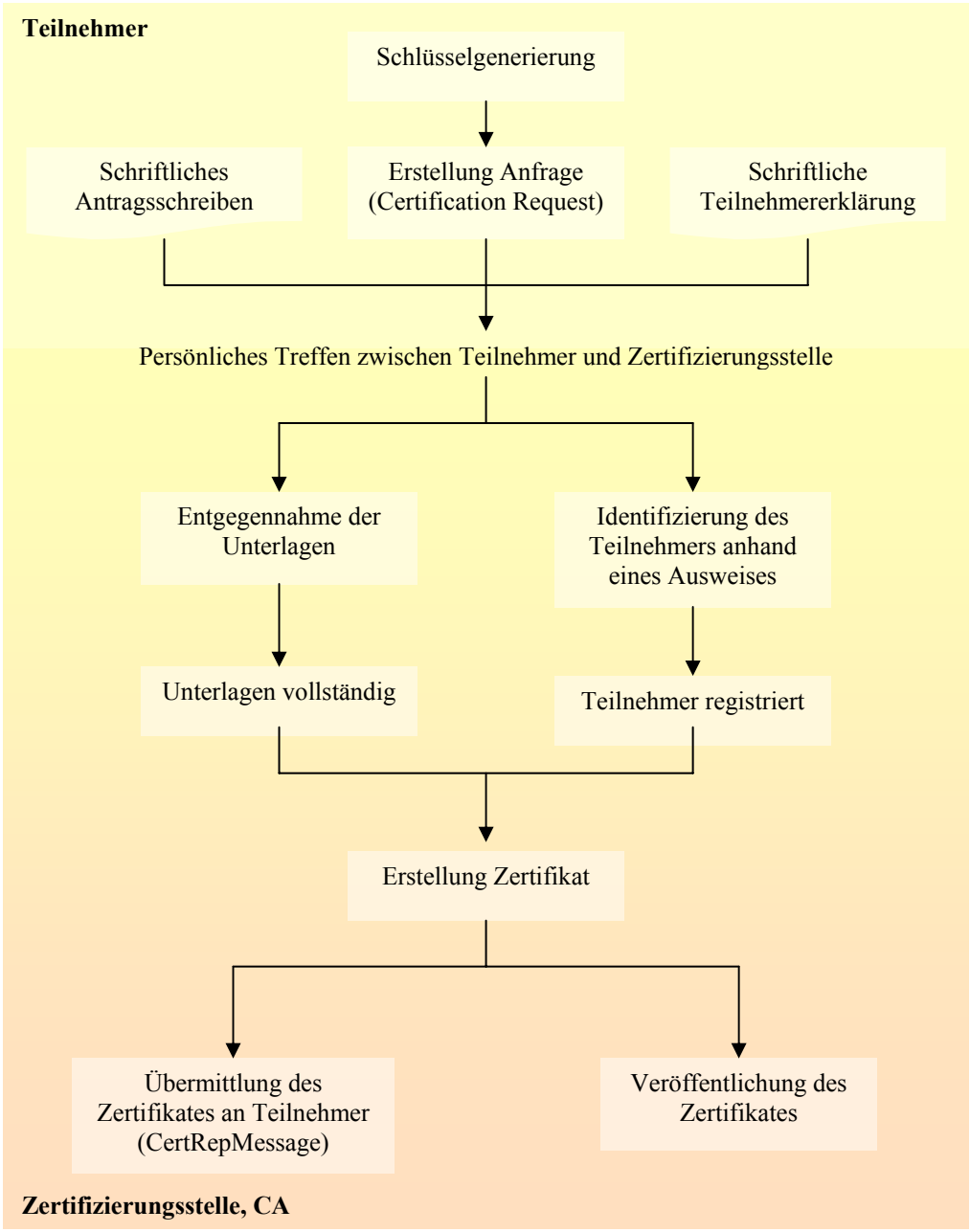

Abbildung 4: Ablauf der Zertifizierung eines Teilnehmers

Literatur

[Kredel] Kredel, Heinz: http over SSL (HTTPS); .

[TeleTrust] TeleTrust: MailTrust Version 2 Gesamtkonzeption, Aufbau und Komponenten einer PKI. 16.03.99.

[TeleTrust2] TeleTrust: MailTrust Version 2 PKI-Management. 16.03.99.

[Camphausen] Camphausen, Ingmar; ...: Aufbau und Betrieb einer Zertifizierungsinstanz.

[Achter] Achter, Sven; PKI – Public Key Infrastructure.