

Public-Key- Infrastrukturen



Anforderungen für sichere Kommunikation über das Internet

Die größte Stärke des Internets ist auch seine größte Schwäche. Das Internet ist offen, global und unreguliert, fantastisch aber auch verräterisch. Besonders für Unternehmen, Öffentliche Verwaltungen und private Nutzer. Kommunikation im Internet findet in der Regel ungeschützt statt, Kommunikationsteilnehmer können „beobachtet“ werden.

Teilnehmer an elektronischen Transaktionen und an einer vertrauenswürdigen elektronischen Kommunikation müssen eindeutig identifizierbar sein. Die Übertragung von Daten über das Internet kann von Unberechtigten abgefangen, die Nachricht selber aber auch verändert weitergeleitet werden. Auch können Verträge abgeschlossen werden, bei denen eine Partei im Nachhinein bestreitet, vertraglich festgelegte Verpflichtungen übernommen zu haben.

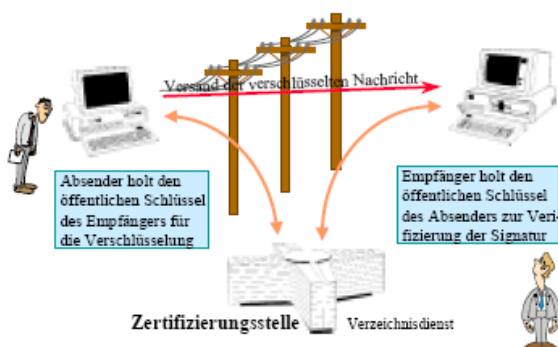
Daher sind die vier Hauptanforderungen für einen sicheren Gebrauch des Internets

- **Glaubwürdigkeit (Authentizität):** Wie kann ich sicher sein, wer am anderen Ende ist?
- **Unversehrtheit (Integrität):** Wie kann ich eine Veränderung meiner Daten feststellen?
- **Vertraulichkeit:** Wie kann ich meine Daten gegen nicht autorisiertes Abfangen oder Mitlesen schützen?
- **Nachweisbarkeit:** Wie kann ich sicherstellen, dass Transaktionen oder Verträge nicht im Nachhinein geleugnet werden?

Die Lösung

Kryptographie ermöglicht zwei Partnern, über beliebige Kommunikationsnetze miteinander Daten geschützt auszutauschen, ohne dass ein Dritter fähig wäre, Nachrichten mitzulesen oder unbemerkt zu verändern. Neben der vertraulichen Datenübertragung bietet die Kryptografie auch Mechanismen zur Authentifizierung d.h. zur eindeutigen Identifikation von Kommunikationspartnern.

Public-Key-Kryptografie wird von Fachleuten als derzeit beste Methode für die sichere Kommunikation per Internet angesehen. Sie stellt ein kryptografisches System dar, in dem für jeden Teilnehmer ein einzigartiges Schlüsselpaar verwendet wird und zwar mit einem öffentlichen und einem korrespondierenden (geheimen) privaten Schlüssel.



Verschlüsselung ist ein Verfahren, um digitale Daten in ein Format zu verwandeln, das nicht ohne Kenntnis des richtigen Schlüssels gelesen werden kann. Bei der Public-Key-Kryptografie verschlüsselt man die Daten mit dem öffentlichen Schlüssel des Empfängers. Nur dieser kann die Daten mit Hilfe des nur ihm bekannten zugehörigen privaten Schlüssels wieder entschlüsseln.

Die **elektronische Signatur** entspricht einem Siegel oder einer eigenhändigen Unterschrift.

Die **digitalen Signatur** ist ein asymmetrisches kryptografisches Verfahren, das ein digitales Schlüsselpaar verwendet, das aus einem privaten (geheimen) Schlüssel (auch Signierschlüssel, Private Key) und einem öffentlichen (nicht geheimen) Schlüssel (auch Signaturprüfschlüssel, Public Key) besteht. Mit dem privaten Schlüssel und den eigentlichen digitalen Daten wird eine digitale Signatur berechnet, die an die digitalen Daten angehängt wird. Mit dem zugehörigen öffentlichen Schlüssel kann die Unversehrtheit der Daten und der Eigentümer des Schlüssels festgestellt werden.

Der öffentliche Schlüssel ist jedermann zugänglich – beispielsweise über einen Verzeichnisdienst, während der korrespondierende private Schlüssel nur dem Inhaber verfügbar sein darf. Erhält man eine signierte oder sendet man eine verschlüsselte Nachricht, muss man den öffentlichen Schlüssel und seine Bindung an den Kommunikationspartner überprüfen können. Dazu dienen digitale Zertifikate.

Zertifikat als elektronischer Ausweis

Ein digitales Zertifikat bindet den öffentlichen Schlüssel einer Person, Firma, Anwendung oder eines Geräts an die entsprechende Identität.

Diese Bindung erreicht man durch eine digitale Signatur des Herausgebers des Zertifikats. Mit dem Zertifikat kann sich jeder Teilnehmer gegenüber seinen Kommunikationspartnern ausweisen.



Aspekte des Vertrauens

Wo bekomme ich ein digitales Zertifikat?

Zertifikate werden von Zertifizierungsstellen (Certification Authority – CA) als vertrauenswürdiger Instanz (Trusted Third Party – TTP) ausgestellt. Die CA verifiziert die Identität und Angaben eines Antragstellers und den Besitz der zugehörigen Schlüssel und verleiht dem Inhalt des Zertifikates damit Vertrauenswürdigkeit.

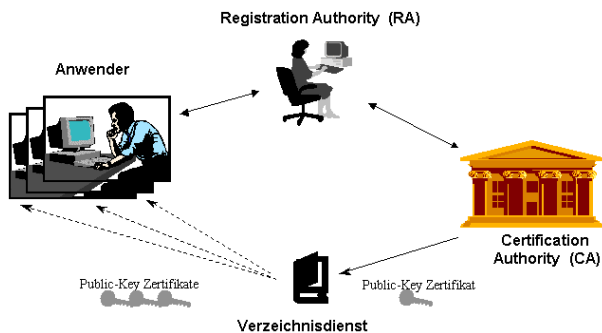
Die Verwaltung der Zertifikate durch eine CA wird in einer organisatorisch-technischen Umgebung, einer Public-Key-Infrastruktur (PKI), durchgeführt. Eine PKI besteht aus Technologie, Standards und definierten Sicherheitsanforderungen (Policy). Die Policy definiert u.a. Haftung, Gewährleistung, Organisation, Standards einzusetzende Technologie und deren Handhabung.

Eine PKI stellt Dienstleistungen wie Schlüssel-Management (Schlüsselerstellung, Aktualisierung, Wiedergewinnung, ...), Zertifikat-Management (Erzeugung, Bereitstellung, Erneuerung, Sperrung, ...) oder Zeitstempeldienste zur Verfügung.

Zu einer PKI gehören folgende Komponenten:

- Die **Zertifizierungsstelle (Certification Authority – CA)** erstellt die digitalen Zertifikate für den Nutzer und verwaltet sie.
- Die **Registrierungsstelle (Registration Authority – RA)** verifiziert die Identität und Angaben des Antragstellers. Sie organisiert die Zertifikatsausgabe im Namen der CA.
- Der **Verzeichnisdienst** stellt eine öffentliche Datenbank zur Verfügung, in der Zertifikate geführt werden. Gesperrte Zertifikate werden über eine Sperrliste (Certificate Revocation List – CRL) gekennzeichnet. Eine Alternative zur CRL ist das „Online

Certificate Status Protocol“ (OCSP), mit dem der Status eines Zertifikates online überprüft werden kann.



- Der **Zeitstempeldienst** bestätigt die Vorlage von digitalen Daten zu einem bestimmten Zeitpunkt. Dies ist von besonderer Bedeutung bei Verträgen und Urkunden.

Aufbau und Betrieb einer PKI

Jede Organisation oder jedes Unternehmen, das seinen internen und/oder externen Datenaustausch sicher gestalten möchte und sich entscheidet, mit Zertifikaten zu arbeiten, kann seine eigene PKI aufbauen und einsetzen. Dabei kann die Firma/Organisation den organisatorischen und technischen Betrieb der PKI selbst übernehmen oder Dienste eines externen Dienstleisters (Certification Service Provider – CSP) nutzen.

Zur Kommunikation mit anderen PKI bieten sich folgende Möglichkeiten:

- Eine **gemeinsame Wurzelinstanz (Root)** stellt sicher, dass Teilnehmer der nachgeordneten CA's direkt miteinander sicher kommunizieren können (hierarchisches Modell).
- Über **Cross-Zertifizierung** können zunächst unabhängig aufgebaute PKI nachträglich durch gegenseitige Anerkennung miteinander verbunden werden.
- Die gegenseitige Anerkennung unterschiedlicher PKI kann über eine **Bridge-CA** vereinfacht werden. Dabei entfällt die individuelle Vereinbarung der Cross-Zertifizierung der Partner untereinander. Sie wird durch Vereinbarungen der einzelnen PKI mit der Bridge-CA ersetzt.

Bei allen Alternativen ist grundsätzlich auf die Verträglichkeit der Policies der so verbundenen PKI zu achten.

TeleTrusT betreibt seit März 2001 eine herstellerunabhängige, gemeinnützige Bridge-CA mit dem Ziel, vor allem im Bereich E-Mail organisationsübergreifend sicher und vertrauenswürdig zu kommunizieren. Teilnehmer der European Bridge-CA kommen sowohl aus dem privaten Sektor als auch aus Einrichtungen der öffentlichen Verwaltung.

Aufbewahrung des privaten Schlüssels

Um Missbrauch zu verhindern, darf die Nutzung des privaten Schlüssels nur dem Besitzer und nur nach seiner Authentifizierung, z.B. nach Eingabe des Passwortes oder nach biometrischer Identifikation, möglich sein. Es gibt verschiedene Methoden, den privaten Schlüssel zu schützen, z.B.:

- Verschlüsselte Ablage auf Datenträgern: Der private Schlüssel wird auf einer Diskette oder Festplatte des eigenen Computers/PDA verschlüsselt aufbewahrt.
- Auslesesichere Komponenten, wie zum Beispiel Kryptohardware, Smartcards, USB-Token, SIM-Karten (mobile Telefonie): Um ein hohes Niveau des Schutzes sicherzustellen, wird der private Schlüssel in einer solchen Komponente erstellt, aufbewahrt und benutzt. Der private Schlüssel verlässt niemals das sichere Gerät.

Anwendungen

Eine PKI kann u.a. in folgenden Bereichen hilfreich unterstützen:

- sichere Internet-Verbindungen (z.B. SSL/TLS, HTTPS)
- sichere E-Mail (z.B. S/MIME)
- sicherer Zahlungsverkehr (z.B. SET, EDIFACT)
- Unterschreiben von elektronischen Formularen
- Elektronische Signatur äquivalent zur eigenhändigen Unterschrift
- Bankanwendungen (z.B. HBCI / online Brokerage)
- Urheberrecht / digitale Wasserzeichen
- sicherer Daten-Transfer
- Virtual Private Networks (z.B. IPSec)
- Mobile Commerce (M-Commerce).

TeleTrusT

TeleTrusT wurde 1989 gegründet, um die Vertrauenswürdigkeit von Informations- und Kommunikationstechnik in einer offenen Systemumgebung zu fördern.

Der gemeinnützige Verein hat sich durch seine Satzung zur Aufgabe gemacht,

- die Akzeptanz der digitalen Signatur als Instrument zur Rechtssicherheit einer elektronischen Transaktion zu erreichen;
- die Forschung zur Sicherheit des elektronischen Datenaustausches (EDI) und die Anwendung ihrer Ergebnisse sowie die Entwicklung von Standards für dieses Gebiet zu unterstützen;
- mit Institutionen in anderen Ländern zusammenzuarbeiten, um Ziele und Standards innerhalb der Europäischen Union und global zu harmonisieren.

TeleTrusT unterstützt die Berücksichtigung der Vertrauenswürdigkeit in bestehenden oder geplanten IT-Anwendungen in öffentlichen Einrichtungen, in Verbänden und in Unternehmen.

Kontakte

TeleTrusT Deutschland e.V.

Chausseestraße 17
D-10115 Berlin
Tel.: +49-30 / 4005 4310
Fax: +49-30 / 4005 4311
E-Mail: info@teletrust.de
URL: <http://www.teletrust.de>



European Bridge-CA

E-Mail: info@eb-ca.de
URL: <http://www.bridge-ca.de>

