martin schönbeck
Beratungen GmbH

Sichere Kommunikation

Ein Vortrag von Martin Schönbeck

martin schönbeck Beratungen GmbH

Eckpunkte sicherer Kommunikation

- Unversehrtheit (Integrität)
- Vertraulichkeit
- Urheberfeststellung (Authentizität)
- Berechtigung (Authorisierung)

Unversehrtheit

- Schreibbeschränkung
- Lesen ohne Beschränkung möglich

  Erreichbar durch eine „Prüfsumme“
  - Prüfsumme muß separat kommuniziert werden
  - Oder ebenfalls unveränderbar sein
    - Asymmetrische Verschlüsselung

Vertraulichkeit

- Lesebeschränkung
- Schreiben keine Einschränkung nötig

  Erreichbar durch Verschlüsselung
  - Symmetrische Verschlüsselung

    problematische Schlüsselverteilung
  - Asymmetrische Verschlüsselung

    langsam

Urheberfeststellung

- Fest einer Person zugeordnetes Merkmal
  - Zertifikat

Berechtigungsprüfung

- Kenntnis eines Geheimnisses
  - Benutzerkennung / Passwort
  - Privater Schlüssel eines Zertifikats

Praxis

- Websites
  - Verschlüsselung und Signatur mit Zertifikat
  - Benutzerkennung + Passwort oder Zertifikat
- E-Mail
  - Eigenes Zertifikat zur Signatur
  - Fremdes Zertifikat zum Verschlüsseln
- Austausch über Datenträger
  - Wie E-Mail
  - Separat ausgetauschter Schlüssel

Zertifikate

Bestehend aus

- Öffentlichem Schlüssel
- Daten des Benutzers (Name, E-Mail-Adresse)
- Signatur mittels eines weiteren Zertifikats

  Dies Zertifikat gehört typischerweise einer CA (Certification Authority) und ist selbstsigniert.
- Zugehöriger privater Schlüssel ist nicht Teil des Zertifikats

Anwendung von Zertifikaten

- Signieren

  Von den Daten, die signiert werden sollen, wird eine Prüfsumme errechnet.

  Diese Prüfsumme muß so berechnet werden, daß es nicht (mit vertretbarem Aufwand) möglich ist, Daten mit einer vorher feststehenden Prüfsumme zu bilden.

  Verschlüsselung der Prüfsumme mit dem privaten Schlüssel.

  Entschlüsselung mit öffentlichen Schlüssel des Zertifikats.

Anwendung von Zertifikaten

- Verschlüsseln

  Daten werden mit zufällig erzeugtem Einmalschlüssel verschlüsselt.

  Dieser Schlüssel wird mit dem öffentlichen Schlüssel (aus dem Zertifikat) des Empfängers verschlüsselt.

  Zusätzlich mit eigenem öffentlichen Schlüssel.

  Empfänger und man selbst kann den Einmalschlüssel entschlüsseln und damit die Daten.

Typen von Zertifikaten

- Qualifizierte Zertifikate (X.509)
  - Privater Schlüssel technisch geschützt
  - CA muß zugelassen sein
- Fortgeschrittene Zertifikate (X.509)
  - Privater Schlüssel durch Passphrase geschützt
  - CA prinzipiell frei (Beweiskraft)
- Zertifikatsnetze (PGP)
  - Keine CA, andere Teilnehmer signieren
  - Vertrauen in den jeweils Signierenden nötig

Zertifikate nutzen

- Qualifizierte Zertifikate
  - Hardware erforderlich
  - PIN-Eingabe regelmäßig
  - Kosten
- Fortgeschrittene Zertifikate
  - Freigabe bei Start des E-Mail Programms (z.B.)
  - Teilweise kostenfrei zu bekommen (Cacert, Thawte)

Zeitstempel

- Signaturen sind zeitlich begrenzt
- Zeitstempel sichern, daß das Dokument (ggf. mit Signatur) zum gestempelten Zeitpunkt so existiert hat.
- Eine Dokument mit ablaufender Signatur muß also vor dem Ablaufzeitpunkt gestempelt werden.