Programmiertechnik II

X.509: Eine Einführung

X.509

- ITU-T-Standard: Information Technology – Open Systems Interconnection – The Directory: Public Key and attribute certificate frameworks
  - Teil des OSI Directory Service (X.500)
  - parallel veröffentlicht als ISO/IEC/ITU 9594-8
- Public Key Infrastructure (PKI)
- Definition eines Formats für Zertifikate
  - aktuelle Version: v3 (Unterstützung für Erweiterungen)
- Anwendung im Internet: PKIX
  - RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Public Key Cryptographie

- Asymmetrisches Verschlüsselungsverfahren:
  - öffentlicher und privater Schlüssel (Schlüsselpaar)
  - privater Schlüssel lässt sich theoretisch aus öffentlichem ermitteln, praktisch nicht
- Zwei Operationen: Verschlüsseln und Entschlüsseln
  - Verschlüsseln mit öffentlichem Schlüssel, Entschlüsseln mit privatem
    - Schutz von Nachrichten vor Abhören: nur Besitzer des privaten Schlüssels kann die Nachricht entschlüsseln
  - Verschlüsseln mit privatem Schlüssel, Entschlüsseln mit öffentlichem
    - Schutz von Nachrichten gegen Fälschungen: nur Besitzer des privaten Schlüssels konnte die Nachricht formulieren
    - Unterschreiben (Signieren)

Zertifikate

- elektronische Ausweise: Zertifikat beweist, dass der Besitzer eine bestimmte Identität hat
- Certificate Authority (CA): Aussteller von Zertifikaten
  - CA besitzt eigenen privaten Schlüssel, veröffentlicht passenden öffentlichen Schlüssel
  - Antragsteller generiert sich ein Schlüsselpaar
  - CA generiert Zertifikat: Identität und öffentlicher Schlüssel werden von CA unterschrieben (mit privatem Schlüssel der CA)
- Überprüfung von Unterschriften unter Dokumenten:
  - Autor des Dokuments signiert mit seinem privaten Schlüssel
  - Empfänger des Dokuments überprüft, ob die Unterschrift zum öffentlichen Schlüssel des Autors (enthalten im Zertifikat) passt
  - Empfänger überprüft außerdem, ob das Zertifikat echt ist
    - Test, ob Unterschrift im Zertifikat tatsächlich von CA stammt, anhand des CA-Zertifikats

Vertrauen in CAs

- Jede CA führt Identitätsüberprüfung bei Zertifikatsausstellung
  - durch persönliches Erscheinen des Antragstellers, evtl. mit Ausweis
  - durch Kommunikation mit Antragsteller über Telefon oder Email
  - durch Vorlage eines zuvor erteilten Passworts

  ⇒ Vertrauen in CA sollte von CA Policy abhängen
- CA-Hierarchie: CA-Zertifikat selbst ist wieder von CA ausgestellt
  - Root CA: Zertifikat hat sich die CA selbst ausgestellt

Daten im Zertifikat

- Name des Zertifikatsbesitzers (Subject)
  - X.500 Distinguished Name (Country, State, City, Organization, Common Name, ...)
  - eventuell alternative Namen (Email, DNS-Name)
- Name des Ausstellers
- Beginn und Ende der Gültigkeit
  - üblich: 1 Jahr (CA-Zertifikate länger)
- öffentlicher Schlüssel des Besitzers
- Zertifikatsverwendungszwecke (Signieren, Verschlüsseln)
  - erweiterte Zwecke: Webserver, Webclient, Email, ...
- beliebige weitere Erweiterungen
- alle Daten sind von CA unterschrieben

Zertifikatsverwendung: HTTP+SSL

- Webserver besitzt ein Schlüsselpaar und Zertifikat
  - Common Name ist DNS-Name des Rechners
- Webserver sendet Zertifikat an Klient
  - unterschreibt Nachricht mit privatem Serverschlüssel
- Klient überprüft Server-Zertifikat
  - CA-Zertifikat muss vorliegen und vertrauenswürdig sein
  - empfangene Nachricht muss sich mit öffentlichem Schlüssel verifizieren lassen
- Klient verwendet dann öffentlichen Schlüssel, um Schlüssel für symmetrische Verschlüsselung sicher zu übertragen
- weitere Kommunikation über symmetrische Verschlüsselung

Zertifikatsverwendung: Klientenauthentifizierung

- Server sendet Serverzertifikat sowie Liste von akzeptierten CAs
- Klient sendet eigenes Zertifikat
  - Nachricht unterschrieben mit privatem Schlüssel des Klienten
- Server überprüft Echtheit des Zertifikats und Echtheit der Unterschrift
- Server entscheidet dann aufgrund der Identität des Klienten, ob der Zugriff erlaubt wird (Autorisierung)

Zertifikatsverwendung: Email

- Email-Signierung: Absender sendet sein Zertifikat, unterschreibt Nachricht mit privatem Schlüssel
  - Empfänger verifiziert erst Zertifikat, dann Unterschrift
- Email-Verschlüsselung: Absender benötigt vorab Zertifikat des Empfängers
  - Windows: Zertifikat aus Active Directory erhältlich
  - sonst: Empfänger muss zunächst unterschriebene Nachricht senden
  - Absender verschlüsselt Nachricht mit öffentlichem Schlüssel des Empfängers

Weitere Aspekte

- Kryptographie: Welche Algorithmen kommen zum Einsatz?
- Weitere Verwendungszwecke:
  - andere Protokolle (SMTP, IMAP, LDAP, ...)
  - Code signing
- Zertifikatsspeicherung: Wie wird der private Schlüssel geschützt
  - Windows, OSX: Schlüsselbund ist mit Nutzerpasswort geschützt
  - Mozilla/Firefox: Schlüsselbund ist mit separatem Masterpasswort geschützt
  - PKCS12: Zertifikatsaustausch, privater Schlüssel ist in Datei mit Passwort geschützt