Verschlüsselt Mailen

PC-Treff-BB

Peter Rudolph

Inhalt

- **Verschlüsseln - Konzept**
- **Vertrauen**
- **S/MIME und OpenPGP**

Schlüssel

- **symmetrische Schlüssel**
  - gleicher Schlüssel für Ver- und Entschlüsselung
- **asymmetrische Schlüssel**
  - zwei zueinander gehörende Schlüssel
  - was mit dem einen verschlüsselt wurde kann nur mit dem anderen entschlüsselt werden
  - privater Schlüssel wird sorgfältig verwahrt
  - öffentlicher Schlüssel wird verteilt

Verschlüsseln und Signieren

- **Verschlüsseln**
  - Mit öffentlichem Schlüssel des Empfängers
  - Nur Empfänger kann entschlüsseln (mit seinem privaten Schlüssel)
- **Signieren**
  - Signatur (Anhang): Die komplette Mail mit dem privaten Schlüssel des Senders verschlüsselt
  - Signatur prüfen: Signatur entschlüsseln mit öffentlichem Schlüssel des Senders, dann vergleichen

Vertrauen

- **Woran erkenne ich, dass ein öffentlicher Schlüssel keine Fälschung ist?**
- **Certificate Authorities (CA)**
  - Zentrale Instanzen
  - Mailprogramm enthält öffentliche Schlüssel der CAs
  - Echtheit eines Schlüssels erkennt man daran, dass er von einer CA signiert ist.
- **Web of Trust**
  - Jeder kann Schlüssel von anderen signieren
  - Echtheit eines Schlüssel erkennt man daran, dass man von mindestens einer der Signaturen auf dem Schlüssel weiß, dass sie echt ist.
- **NSA-Skandal**
  - Keinem SW-Hersteller aus USA kann vertraut werden!

Wichtig

- **Vertrauen in öffentliche Schlüssel**
  - Sicherstellen, das öffentlicher Schlüssel keine Fälschung ist
  - Öffentlicher Schlüssel am besten persönlich übergeben
- **Privaten Schlüssel sicher verwahren**
  - Digitale Signatur ist juristisch mit einer Unterschrift vergleichbar
  - In fremden Hände ist er wie eine Blankounterschrift auf unendlich vielen Blättern!
  - Schlüsseldatei nie aus der Hand geben!
  - Sehr sicheres Kennwort für Schlüssel verwenden!
- **Mails bleiben im Postfach verschlüsselt**
  - Auch alte private Schlüssel nicht wegwerfen

S/MIME

- **Öffentliche Schlüssel werden von "Certificate Authorities" (CA) signiert**
- **Öffentlicher Schlüssel wird bei jeder signierten Mail mitgeschickt**
- **Vorteile**
  - Einfaches Verfahren zum Austausch öffentlicher Schlüssel
  - In den meisten PC-Mail-Programmen integriert
- **Nachteile**
  - Vertrauen in CA nicht immer gegeben, insbesondere seit NSA-Skandal
  - Schlüssel werden über Browser-Tool der CA erzeugt

OpenPGP (PGP, GnuPG)

- **Web of Trust: Öffentliche Schlüssel werden von anderen OpenPGP-Nutzern signiert**
- **Öffentlicher Schlüssel wird auf Schlüssel-Server hochgeladen und/oder manuell weitergegeben**
- **Vorteile**
  - Vertrauen basiert auf persönlichem Vertrauen
  - Für NSA schwer zu unterwandern
- **Nachteile**
  - Vertrauen muss mühsam aufgebaut werden
  - Öffentliche Schlüssel müssen manuell beschafft werden (vom Server runterladen oder als Datei weitergeben)

PC-Mailprogramme

- **Outlook (Windows)**
  - S/MIME eingebaut
  - OpenPGP über Add-On
  - Outlook und Sicherheit ist ein Widerspruch
    - kommt von Microsoft (aus USA)
    - "wagenweit offene" Tore für Viren und Trojaner
    - Also besser ein anderes Mailprogramm verwenden!
- **Thunderbird (Windows, Mac und Linux)**
  - S/MIME eingebaut
  - GnuPGP über AddOn "EnigMail"
  - OpenSource

Mobilgeräte

- **Android**
  - K9 Mail
    - eines der beliebtesten Mail-Programme für Android
    - Zusatz-App "APG" für OpenPGP
    - kostenlos
  - R2Mail2
    - einfaches Mail-Programm
    - integriert OpenPGP und S/MIME
    - Hersteller aus Österreich
    - Lizenz kostet 4,80 EUR
- **Apple (iOS)**
  - S/MIME mit Standard-Mail-App
  - OpenPGP mit alternative Mail-Apps