Vertrauen im Internet

Julian Fagir

22.11.2013

Gliederung

1. X.509
2. PGP
3. Kommandozeilentools
4. Sonstiges

X.509 allgemein

- 3. Juli 1988 als ITU-T X.509, aktuell: RFC5280
- Ursprünglich komplexere Struktur (Internet Policy Registration Authority, IPRA, dann Policy Certification Authoritcy, PCA, dann CA)
- zentrale Certificate Authorities beglaubigen andere Zertifikate (Trusted Third Party)
- Zertifikate werden über die Zertifikatskette verifiziert
- Baumstruktur, ggf. mit mehreren Wurzeln

X.509 Anwendungen

- SSL
- StartTLS
- S/MIME
- Sonstige Zertifizierungen
- z.B.: https, imaps, smtp, xmpp, ...

X.509 Gängige Probleme

- Sicherheit der CAs
- Einflussnahme von Staaten
- Implementierungsprobleme
- merkwürdige Praktiken bei Aufnahme von Root-CAs
- Reizüberflutung - Wegklicken
- je nach Implementierung Keine Meldung bei Nicht-Verwendung (Web)
- Vertrauen (für Firmen intaktes Modell)

PGP allgemein

- Pretty Good Privacy (PGP) von Phil Zimmermann 1991
- *Export* nach Europa
- meist verwendet in Form von GnuPG (GPG)
- Netzwerkstruktur (Web Of Trust) bzw. strukturlos
- Vertrauen wird an andere Personen in gewissem Maße weiterdelegiert, Vertrauen insgesamt wird mathematisch berechnet

PGP Anwendungen

- Mail
- Jabber
- jegliche schriftliche (!) Kommunikation

PGP Gängige Probleme

- Privatsphäre durch Web Of Trust gefährdet?
- Komplizierte Benutzung (Vertrauensmodelle?)
- Vertrauen basiert meist auf staatlicher Infrastruktur - was ist Vertrauen?
- Sehr spezielle Benutzung

Anderes

- DNSSec
- OAuth, OpenID
- OTR

Benutzung der Kommandozeilentools

- Meist sehr mächtige Kryptotoolkits
- Dateiverschlüsselung
- Serverabfrage
- Schlüsselabfrage
- Schlüssel- und Zertifikatsgenerierung
- Validierung