Signaturen verwenden

Ein Bürgernetz-Vortrag für Privatleute und Gewerbetreibende

Heimstetten im Juni 2003

www.hi-response.com
rzwarg@hi-response.com

Telefon:
(089) 9077 5043
Fax:
(069) 1330 6224 472
Anrufbeantworter:
(069) 1330 6224 472

Anforderungen: sichere eMail

- Vertraulichkeit durch Verschlüsselung
- Integrität und Authentizität durch Signatur
- garantierte Identität durch Zertifizierung

Verschlüsselung (techn.Sicherheit)

- **Schlüssellänge**
  (Übergang von 64 Bit auf 128 Bit erhöht die Sicherheit um den Faktor 2^{64}, also 18 Trillionen !)
- **Kodierungsverfahren**
- **Schlüsselverteilung**

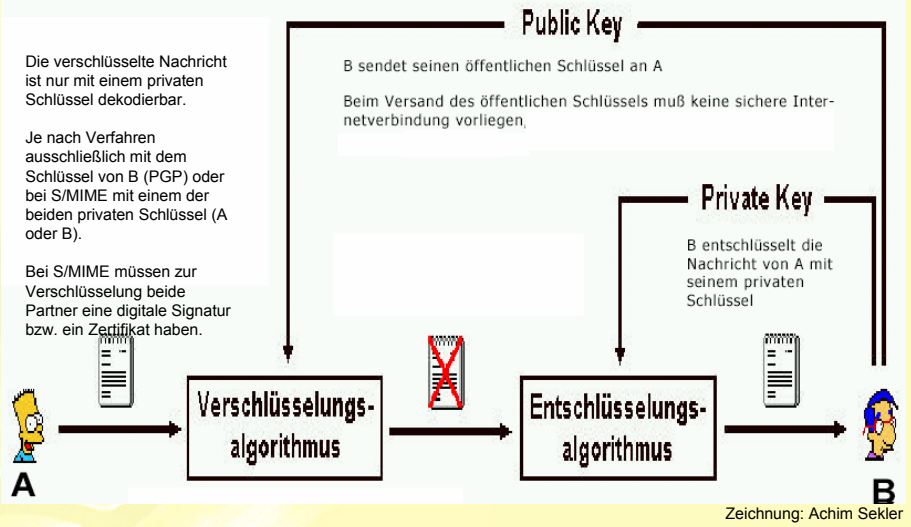
Verschlüsselung (Anforderungen)

- **Sichere kryptographische Verfahren**
- **Einmalige Signaturschlüsselpaare**
- **Bindung der geheimen, privaten Signatur-schlüssel an die rechtmäßigen Nutzer**
- **Zuverlässige Nachprüfung der Gültigkeit von Zertifikaten**
- **Widerrufbarkeit der Signaturen**

Zertifizierungsdiensteanbieter

- Signaturschlüssel erzeugen
- Qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar zu halten
- bescheinigen, dass bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben (Namenszertifikate)
- qualifizierte Zertifikate nachprüfbar und abrufbar halten

Ablauf der Verschlüsselung



Zeichnung: Achim Sekler

Links

http://www.exchange2000faq.de/Konzepte/smimepgp.htm

(in diesem informativen 4-seitigen Dokument sind viele Links aufgeführt, so dass ich hier gar keine weiteren aufführe. Bis auf...)

http://www.thawte.com (...wegen des Zertifikats)

Reinhard Schmitt empfiehlt noch das Buch

„Geheime Botschaften“ von Simon Singh