



your key to information security

Problemfelder der elektronischen Signatur

David Ochel, david@atsec.com

atsec information security GmbH, Köln



Agenda

- Problemstellung elektronische Unterschrift, Lösungsansatz: Zertifikate
- technische Sicherheit von Signaturen & Zertifikaten
- Problemfelder in Organisation und Infrastruktur
- Signatur-Gesetzgebung & Co
- Zusammenfassung



Elektronische Unterschrift (Signatur)

- Public Key-Kryptographie: digitale Schlüsselpaare



Public Key:
Signaturprüf Schlüssel




Private Key:
Signatur Schlüssel

Wer hat den Vertrag unterschrieben?

Auftrag

Lieferung von
10 Schaufelradbaggern

elektronische
Unterschrift:
Hans Muster

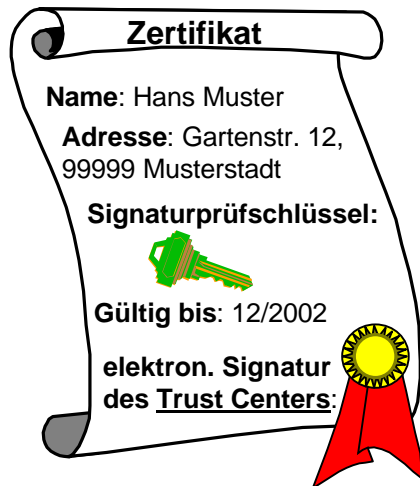


- Auftraggeber
 - ist dem Auftragnehmer unbekannt
 - leistet elektronische Signatur mit seinem Signaturschlüssel
- Auftragnehmer
 - kann nicht feststellen, welche Identität hinter der Signatur steht

=> Verbindlichkeit ??

Zertifikate zum Identitätsnachweis

© 2001 atsec information security GmbH



Der Aussteller

(Zertifizierungsinstanz)

- signiert das Zertifikat mit seinem Signaturschlüssel
- steht damit für die Richtigkeit der **Zuordnung Name ↔ Signaturprüf-schlüssel** des Zertifikat-Inhabers ein
- ist vertrauenswürdig (Trust Center)

@sec
the information security provider

5

Zertifikate sind „sicher“ !

© 2001 atsec information security GmbH

- Public Key-Kryptographie:
 - mathematische Problemstellungen
 - erforschte Algorithmen
 - nur mit hohem Rechenaufwand brechbar
- Schlüsselmaterial:
 - Qualitätsparameter: Zufallszahlen, Einmaligkeit, ...
- Einsatzumgebung:
 - Trust Center im Hochsicherheits-Trakt
 - Schlüsselmaterial auf Smartcards

@sec
the information security provider

6

Sicherheit ist relativ !!

- Public Key-Kryptographie
 - mathematische Probleme können gelöst werden
 - Rechenleistung nimmt zu
 - Implementierung muss korrekt erfolgen
- Schlüsselmaterial
 - Qualität bei der Erzeugung muss gewährleistet sein
- Einsatzumgebung
 - Benutzer-Anwendungen laufen auf ungeschütztem PC

Problemfelder in Organisation & Infrastruktur I

- Abbildung von Organisations-Strukturen
 - klassische Zertifizierungs-Infrastrukturen sind hierarchisch
- Zertifikat-Rückruf
 - Verwaltung von Sperrlisten (CRLs)
 - CA-Zertifikat-Rückruf
- Skalierbarkeit
 - z. B. Nutzung in mobilen Netzen

Problemfelder in Organisation & Infrastruktur II

© 2001 atsec information security GmbH

- Anwendungen
 - Existenz und Verbreitung
 - Integration
- Interoperabilität
 - Zertifikat-Formate
 - Algorithmen
 - Produkte
- Faktor Mensch, z. B.
 - Registrierung
 - Bestätigung der Signatur



9

Signatur-Gesetzgebung

© 2001 atsec information security GmbH

- Signaturgesetz und –verordnung (1997 / Mai 2001)
 - Umsetzung der EU-Richtlinie zur elektronischen Signatur
 - qualifizierte Zertifikate & qualifizierte elektronische Signaturen
- Formanpassungsgesetz (Juli 2001)
 - BGB: elektronische Form = Alternative zur Schriftform
 - ZPO: Anscheinsbeweis für Willenserklärungen in elektronischer Form („Sicherheitsvermutung“)



10

Verbindlichkeit von Signaturen

- Verbindlichkeit beliebiger Zertifikate
 - in der Privatwirtschaft unabhängig vom SigG
 - Verbindlichkeit qualifizierter Zertifikate
 - Kompromittierung von Signaturschlüsseln schwierig zu belegen
 - Beweislastumkehr durch Anscheinsbeweis hat potentiell schwerwiegende Folgen für Zertifikat-Inhaber
-
- Datenschutz
 - gesicherte Identität & zentralisierte Datensammlungen

Zusammenfassung

Zertifikate bzw. Zertifizierungs-Infrastrukturen

- sind keine „eierlegende Wollmilchsau“
- haben Nachholbedarf, z. B.
 - Sicherheit von Anwendungs-Umgebungen
 - Integration von Anwendungen
- sind begrenzt in ihren Einsatzmöglichkeiten
 - Abbildung von Hierarchien
 - fehlende Anwendungen & Inter-Operabilität
 - Skalierbarkeit
- benötigen einen „passenden Rahmen“
 - rechtlich, organisatorisch, technisch, geschäftlich, ...