

Zertifikate und digitale Signaturen rechtliche Standortbestimmung

Mirko Thomas Oberholzer, lic. iur. HSG, M.B.L.-HSG,
Rechtsanwalt, Telekurs-Gruppe
Rechtskonsulent der Swiskey AG

28. März 2001

FGSec PKI

Die nächsten 45 Minuten

- Allgemeine Bemerkungen
 - Aspekte der Informationssicherheit
- Rechtliche Aspekte der digitalen Signatur
 - PKI-Mechanismen und ihre rechtliche Bedeutung
 - Elektronisches Dokument und Schriftform
 - Digitale Signatur und eigenhändige Unterschrift
 - Elektronisches Dokument als Beweismittel
- Internationale Aspekte
- Und die Schweiz?
- Beispiel Mehrwertsteuer
- Anforderungen an PKI

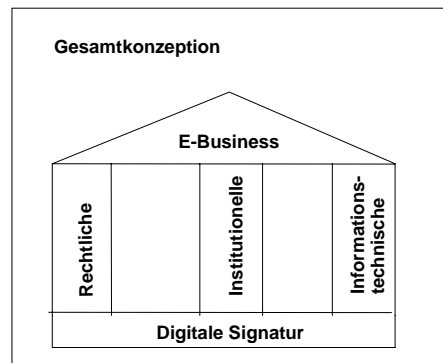


28. März 2001

2

FGSec PKI

Allgemeine Bemerkungen



28. März 2001

3

FGSec PKI

Aspekte der Informationssicherheit I

- Formale Ziele
 - Rechtmässigkeit
 - Wirtschaftlichkeit
 - soziale Akzeptanz

- Grundbedrohungen
 - Verlust der Vertraulichkeit
 - Verlust der Integrität
 - Verlust der Verfügbarkeit
 - Verlust der Authentizität
 - Verlust der Verbindlichkeit



28. März 2001

4

FGSec PKI

Aspekte der Informationssicherheit II

- Mechanismen
 - Verschlüsselung und Entschlüsselung
 - Symmetrische und asymmetrische Verschlüsselungsverfahren
 - Digitale Signatur
 - Authentizitätsprüfung
 - Zugriffskontrolle

28. März 2001

5

FGSec PKI

Rechtliche Aspekte der digitalen Signatur

28. März 2001

6

FGSec PKI

PKI-Mechanismen und ihre rechtliche Bedeutung

- Authentifikation
- Digitale Signatur
- Verschlüsselung
- „Notariatsdienste“
- Time Stamping

28. März 2001

7

FGSec PKI

Elektronisches Dokument und Schriftform

- Formvorschriften
- Zweck und Funktion gesetzlicher Formvorschriften
- Urkundenbegriff
- Forderungen für elektronische Dokumente
- Handlungsbedarf



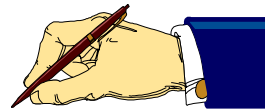
28. März 2001

8

FGSec PKI

Digitale Signatur und eigenhändige Unterschrift

- Allgemeines
- Zweck und Funktion der Unterschrift
- Folgerungen für die digitale Signatur
- Handlungsbedarf



28. März 2001

9

FGSec PKI

Die digitale Signatur stellt sicher

- Authentizität der Teilnehmer im elektronischen Umfeld
- Integrität der elektronisch verschickten Dokumente
- Nichtabstreitbarkeit des Ursprungs



Digitale Signatur =
elektronisches Siegel

(Ein digital signiertes Dokument bleibt
lesbar; es ist nicht verschlüsselt!)

28. März 2001

10

FGSec PKI

Der klassischen Unterschrift überlegen

- Fälschungssicher
- Signierte Inhalte nicht veränderbar
- Direkte digitale Weiterverarbeitung - kein Medienbruch
- 24h/Tag online überprüfbar
- In der elektronischen Welt schon bald nicht mehr wegzudenken

28. März 2001

11

FGSec PKI

Elektronische Dokumente als Beweismittel

- Allgemeines
- Eigenhändig unterzeichnete Urkunden
- Elektronische Dokumente mit und ohne digitale Signatur
- Folgerungen für elektronische Dokumente
- Beweisverfahren
 - Augenschein
 - kein Urkundenbeweis
 - Sachverständiger

28. März 2001

12

FGSec PKI

Beweis in einem Prozess

- Kryptographisches Verfahren
- Technische Komponenten und Verfahren bei der Schlüsselherstellung
- Technische Komponenten und Verfahren bei der Überprüfung der Signatur
- Anwenderprogramm und Dokumentenstruktur
- Architektur der Verfahren muss sicher sein vor Fälschung, Verfälschung und nicht gewollter Abgabe einer Willenserklärung
- Überprüfung der Signatur ergibt kein unzutreffendes Ergebnis



Bedarf an Regeln in Bezug auf

- Gültigkeit elektronisch ausgetauschter Willenserklärungen
- Anforderungen an die Formvorschriften im Vertragsrecht
- Berücksichtigung von berechtigten Konsumenten-schutzinteressen
- Anerkennung der digitalen Signatur bzw. Gleichbehandlung wie die eigenhändige Unterschrift
- Anerkennung der elektronischen Urkunde bzw. deren Gleichbehandlung wie eine Papierurkunde; insbesondere deren beweisrechtliche Gleichbehandlung

Internationale Harmonisierungsbestrebungen

28. März 2001

15

FGSec PKI

Bedarf an harmonisierten Regeln in Bezug auf

- Gültigkeit elektronisch ausgetauschter Willenserklärungen
- Anforderungen an Formvorschriften im Vertragsrecht
- Berücksichtigung von berechtigten Konsumentenschutzinteressen
- Anerkennung der digitalen Signatur bzw. deren Gleichbehandlung wie die handschriftliche Unterschrift
- Anerkennung der elektronischen Urkunde bzw. deren Gleichbehandlung wie eine Papierurkunde; insbesondere deren beweisrechtliche Gleichbehandlung
- Liberalisierung des Handels mit kryptologischen Technologien

28. März 2001

16

FGSec PKI

EUROPÄISCHE UNION

26. Mai 1994 1994	„Bangemann-Report“ Programm der Kommission: „Europas Weg in die Informations- gesellschaft: ein Aktionsplan“	
16. April 1997:	Europäische Initiative für den elek- tronischen Geschäftsverkehr	
8. Oktober 1997:	Mitteilung der Kommission: „Sicherheit und Vertrauen in der elektronischen Kommunikation – ein europäischer Rahmen für digitale Signaturen und Verschlüsselungen	
13. März 1998:	Entwurf Direktive über gemeinsame Rahmen bedingungen für elektronische Signaturen	
30. November 1999:	Verabschiedung der Richtlinie	
28. März 2001	17	FGSec PKI

International

- UNCITRAL: Modellgesetz für den elektronischen Handel
1996
- OECD: Aktivitäten im Bereich Kryptographiepolitik
- WTO: Studie hinsichtlich elektronischer Handel
und seiner Rolle
- Infos auf: www.mbc.com
(Mc Bride Baker & Coles)

Und die Schweiz?

28. März 2001

19

FGSec PKI

Verordnung über Dienste der elektronischen Zertifizierung (ZertDV, 12.4.2000)

- Seit 1. Mai 2000 in Kraft
- Regelungsbereich
- Gesetzliche Grundlage
- Ausführungsvorschriften in Vernehmlassung

28. März 2001

20

FGSec PKI

Signaturgesetz I

- Entwurf „Bundesgesetz über die elektronische Signatur (BGES)“ in Vernehmlassung
- Regelungsbereich
- Konsumentenschutz
- Register- und Zwangsvollstreckungsrecht

28. März 2001

21

FGSec PKI

Signaturgesetz II

- EU-kompatibel?
- technisch neutral?
- Haftungsordnung
- weitere offene Fragen
- Fazit

28. März 2001

22

FGSec PKI

Beispiel Mehrwertsteuer

- Gesetz und Verordnung per 1.1.2001 in Kraft
- Papierlose Übermittlung und Aufbewahrung von Daten und Informationen
- Verlangt wird:
 - Nachweis des Ursprunges
 - Nachweis der Integrität
 - Nichtabstreitbarkeit von Versand und Empfang
- Ausführungsbestimmungen

28. März 2001

23

FGSec PKI

Anforderungen an PKI

- CH: heute Verordnung
- EU: Richtlinie und national Gesetze
- Generelle Anforderungen

28. März 2001

24

FGSec PKI

Danke

28. März 2001

25

FGSec PKI