

Signaturgesetz, quo vadis ?

9. DFN-CERT Workshop
„Sicherheit in vernetzten Systemen“
26./27. Februar 2002

Stefan Kelm
kelm@secorvo.de



Inhaltsübersicht

- ◆ Einleitung
- ◆ Historie
- ◆ Der aktuelle Stand...
 - der EU-Richtlinie
 - des Signaturgesetzes
- ◆ Anwendungen
 - Pilotprojekte
 - Elektronische Abrechnung
- ◆ Ausblick in die Zukunft



Historie

- ◆ Europäische Signaturrechtlinie am 19.01.2000 in Kraft getreten
- ◆ Novelliertes Signaturgesetz ist am 22.05.2001 in Kraft getreten und löst das seit 01.08.1997 gültige SigG ab
 - neue Signaturverordnung ist am 21.11.2001 in Kraft getreten
- ◆ „Geeignete Algorithmen“ vom 24.01.2002 (BSI)
 - jährliches Review
- ◆ Formvorschriftenanpassungsgesetz
 - Neuer § 126a BGB - Elektronische Form (18.07.2001)
- ◆ Kabinettsbeschluss vom 16.01.2002
 - *Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung*

© Secorvo



Aktuelle Regelungen

- ◆ Aktuelle Regelungen zur elektronischen Signatur:

	Privatrecht	öffentlicher Bereich
Rahmenbedingungen	SigRL SigG, SigV	SigRL SigG, SigV
Rechtsfolgen	SigRL Formgesetz	SigRL Erprobungsgesetz

© Secorvo



EU-Signaturformate

- ◆ **(Einfache) Elektronische Signaturen**
 - Beigefügte oder verknüpfte Daten zur Authentifizierung
- ◆ **Fortgeschrittene elektronische Signaturen**
 - Signierer wird durch die Signatur identifiziert
 - Ausschließliche Zuordnung zum Signierer
 - Signaturbildung mit Mitteln, die der Signierer unter seiner alleinigen Kontrolle halten kann
 - Verknüpfung mit Daten, so daß nachträgliche Veränderungen erkannt werden können
- ◆ **„Qualifizierte“ elektronische Signaturen**
 - Basierend auf qualifiziertem Zertifikat (Anhänge I und II)
 - Verwendung einer sicheren (HW-basierten) Signaturerstellungseinheit (Anhang III)

© Secorvo



Standardisierung

- ◆ **European Electronic Signature Standardization Initiative (EESSI)**
- ◆ **ETSI SEC ESI**
 - Elektronische Signaturformate
 - Qualifizierte Signaturprofile
 - Richtlinien für Zertifizierungsdienstleistungsanbieter (CSP)
 - Zeitstempelprofile
- ◆ **CEN/ISSS E-SIGN**
 - Sicherheitsanforderungen für vertrauenswürdige Systeme
 - Sicherheitsprofile für sichere Signaturerstellungseinheiten
 - Anforderungen für Signaturerstellung und -überprüfung
- ◆ **„Algorithms and Parameters“**
- **Können zur „Norm“ erklärt werden**

© Secorvo



Umsetzung innerhalb der EU

- ◆ **Teilweise rechtliche Umsetzung erfolgt**
 - Deutschland, Italien
 - Portugal, Österreich, Spanien
 - Frankreich, Dänemark, UK, Irland, Luxemburg, Schweden, Belgien
- ◆ **Gesetzgebung in Vorbereitung**
 - Griechenland, Niederlande, Finnland
- ◆ **Harmonisierung, Anerkennung von Zertifikaten ?**
- ◆ **„Artikel-9-Ausschuss“**
 - Verhältnis zur EU-Kommission ?
- ◆ **Operierende ZDA**
 - **D: 16, A: 1, UK: 1, DK: 1**
 - ⇒ <http://www.pki-page.info/>

© Secorvo



Überblick zum Signaturgesetz

- ◆ **Novellierung**
 - Neues Gesetz seit 22.05.2001 in Kraft
 - Löst altes Signaturgesetz ab
 - Übergangsregelungen
- ◆ **Ziele der Novellierung**
 - Umsetzung der EU-Signaturrechtlinie
 - Berücksichtigung der Erkenntnisse der Evaluierung des SigG
 - Berücksichtigung der Bedürfnisse „freier Berufe“

© Secorvo



Umsetzung der EU-Richtlinie

- ◆ **Keine Genehmigungspflicht (§ 4 Abs. 1 SigG)**
 - aber Anzeigepflicht
- ◆ **Optional Verfahren zur **freiwilligen Akkreditierung****
 - Gütezeichen als Nachweis der „*umfassend geprüften Sicherheit*“ (§ 15 Abs. 1 SigG)
 - Bestandsschutz für Anbieter nach altem SigG („*gelten als akkreditiert*“) (§ 25 Abs. 1 SigG)
- ◆ **Zusätzliche Anforderungen an den öffentlichen Bereich möglich (§ 1 Abs. 3 SigG)**
- ◆ **Abweichende Haftungsregelung**
- ◆ **SigG/SigV-Regelungen teilweise abweichend bzw. weiterführend**

© Secorvo



„Elektronische Form“

- ◆ **Formvorschriftenanpassungsgesetz**
- ◆ **Option zur gesetzlichen Schriftform (§ 126 BGB)**
 - Von der Option kann immer dann Gebrauch gemacht werden, falls nicht per Gesetz ausgeschlossen
- ◆ **Voraussetzungen (§ 126a BGB)**
 - Aussteller muß der Erklärung seinen Namen hinzufügen
 - Dokument muß mit einer qualifizierten elektronischen Signatur versehen werden

© Secorvo



Änderungen der ZPO

- ◆ Einreichung elektronischer Dokumente bei Gericht (§ 130a ZPO)
- ◆ Anschein der Echtheit von Willenserklärungen in elektronischer Form (§ 292a ZPO)
 - Nur für qualifizierte elektronische Signaturen
 - **Beweiserleichterung zugunsten des Empfängers**
 - Entsprechend Beweis des ersten Anscheins
 - Nur durch Tatsachen zu erschüttern, die es ernsthaft als möglich erscheinen lassen, daß die Erklärung nicht willentlich abgegeben wurde

© Secorvo



Signaturniveaus nach SigG

Form	Qualität	Rechtliche Wirkung
Stufe 0: „Einfache“ elektronische Signatur	Nicht definiert	Ohne Schriftformerfordernisse verwendbar; als Beweismittel vor Gericht zugelassen; weitere Rechtsfolgen unklar
Stufe 1: „Fortgeschrittene“ elektronische Signatur	Mindestanforderungen an: <ul style="list-style-type: none"> ● Zertifikate ● Integrität und Authentizität 	
Stufe 2: Stufe 1 + „Qualifizierte“ elektronische Signatur	<ul style="list-style-type: none"> ● Geprüfte Produkte ● Sichere Signaturerstellungseinheiten ● Sichere Schlüsselerzeugung 	Gleichstellung mit der <u>handschriftlichen Unterschrift</u> (Schriftformerfordernisse)
Stufe 3: Stufe 2 + „Anbieterakkreditierung“	<ul style="list-style-type: none"> ● Stufe 2 + Evaluierung und Bestätigung der CA vor Aufnahme des Zertifizierungsbetriebs 	

© Secorvo



Einsatz qualifizierter Signaturen

◆ Vorteile

- Anscheinsbeweis
- Haftung
- Sicherheit
- Nachprüfbarkeit

◆ Nachteile

- Inflexibilität
- Kosten
- Fehlende Akzeptanz
- Lösungsauswahl
- Heutige Lösungen
- Grenzüberschreitende Anerkennung
- Auslagerung
- Rechtlicher Rahmen

© Secorvo



Inhalt

- ◆ Einleitung
- ◆ Historie
- ◆ Der aktuelle Stand...
 - der EU-Richtlinie
 - des Signaturgesetzes
- ◆ Anwendungen
 - Pilotprojekte
 - Elektronische Abrechnung
- ◆ Ausblick in die Zukunft

© Secorvo



Media@Komm

- ◆ **Förderprojekt des Bundes (BMWi)**
 - Esslingen, Bremen und Nürnberg als Sieger
- ◆ **Smartcards für die Bürger**
 - „Elektronisches Rathaus“ / „virtueller Marktplatz“
 - Verlagerung von über 100 Geschäftsprozessen in das Internet
 - Digitale Signatur, Bezahlungsfunktion, evtl. weitere Anwendungen
 - z.B. Meldewesen, Registerauskünfte, Mahnanträge, Einreichung von Bauanträgen, Anwohnerparkausweise
 - Zertifizierung durch kommerzielle Zertifizierungsstellen
 - Wenn möglich SigG-konform
- ◆ **Hat Potential zur PKI-Massenanwendung**
 - Derzeitige Anwendungen noch nicht überzeugend
 - „...ungenügende Verbreitung und fehlende Kompatibilität...“

© Secorvo



Projekt SPHINX

- ◆ **Digital signierte und vertrauliche Kommunikation von Bundesministerien und Bundesbehörden mit anderen Einrichtungen und Privatpersonen**
 - z.B. IVBB
 - Offene PKI nach **MailTrust v2**
- ◆ **Software und Hardware von verschiedenen Herstellern, die MailTrust-interoperabel sind**
- ◆ **Teilnehmer aus ca. 50 Organisationen aus Bund, Ländern, Kommunen, Forschung und Wirtschaft**
 - ca. 30.000 Teilnehmer
- ◆ **Gleitender Übergang in den Wirkbetrieb („PKI-1-Verwaltung“)**
 - 20. Februar 2001

© Secorvo



Exkurs: Identrus

◆ *Globaler* Zusammenschluss von Kreditinstituten

- ABN Amro, Barclays, Bank of America, Bankers Trust, Chase, Citibank, CIBC, Deutsche Bank, HypoVereinsbank, Sanwa
- Stand heute: 51 Kreditinstitute (Ziel: 300)
- Gründung: 21.10.1998 (ehemals: GTO)

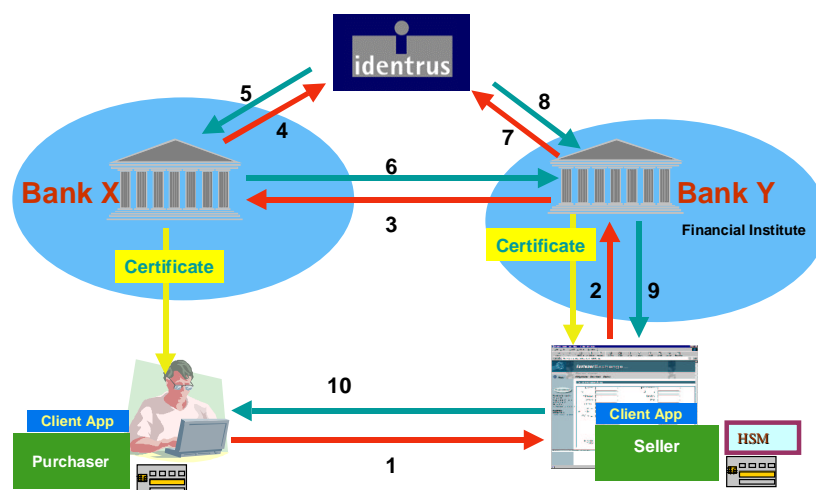
◆ Ziel

- Aufbau einer PKI für „Business-to-Business“ (B2B)
- Anwendungen werden unterstützt von
 - Baltimore, Chrysalis ITS, Computer Associates, CyberTrust (Baltimore), Datakey Inc, Entrust, Gemplus, iD2 Technologies (Smarttrust), ID Certify, Litronic Inc., Microsoft (*Win2K*), nCipher, Oberthur Card Systems, Rainbow Technologies, Schlumberger, SECUDE, Setec, SPYRUS, TC TrustCenter, ValiCert, VeriSign, ...
- Unterstützung aller verbreiteten Standards

© Secorvo



Identrus: Prozesse



© Secorvo

Quelle: Identrus



Beispiel-Anwendung

- ◆ **Elektronische Abrechnung**
 - Seit 01.01.2002 ist die elektronische Abrechnung für „umsatzsteuerliche Zwecke“ (Vorsteuerabzug) zugelassen
- ◆ **Änderung im Rahmen des Steuersenkungsgesetzes**
 - Änderung des Umsatzsteuergesetzes (StÄndG 2001)
 - Änderung der Abgabenordnung
- ◆ **Voraussetzung: *qualifizierte Signatur mit Anbieterakkreditierung* muss Bestandteil der Rechnung sein**
- ◆ **GDPdU:**
 - „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“
 - regelt Anforderungen zur Prüfung elektronischer Unterlagen im Rahmen von Außenprüfungen der Finanzbehörden

© Secorvo



E-Abrechnung

- ◆ **Rechtliche Probleme I**
 - Es findet sich keine Regelung die festlegt, wer die Form (elektr. oder Papier) bestimmen darf: „Macht des Stärkeren“?
 - Anerkennung internationaler Rechnungen fraglich
 - Hohe Anforderung an die elektr. Rechnung nicht nachvollziehbar (qual. Signatur mit Anbieterakkreditierung)
 - Papierrechnung braucht nicht einmal eine Unterschrift
 - bisher keine eindeutige Identifizierung z.B. R-Nr verlangt
 - Rechnung kleiner 200 DM müssen nicht einmal den Empfänger enthalten
 - Argument, elektr. Daten sind leichter zu fälschen ist diskussionswürdig
 - Rechnungen auf Papier können leicht kopiert oder selbst generiert werden

© Secorvo



E-Abrechnung

◆ Rechtliche Probleme II

- GDPdU verlangt die Prüfung der Signaturberechtigung und die Dokumentation des Ergebnisses
 - Wie dies auszusehen hat, ist unklar
 - Bisher gibt es keine gesetzl. Grundlagen, die eine Signaturberechtigung zur Rechnungsstellung regeln
- Lieferant kann die Rechnungserzeugung an „Dritte“ übertragen
 - Durchaus auch an den Rechnungsempfänger
 - Wie hier Transparenz und Prüfbarkeit gewährleistet werden sollen, ist unklar
- Forderung, dass elektr. Rechnung auf einem nicht mehr änderbaren Medium gespeichert werden muss, erscheint überflüssig
 - Veränderung kann durch Integritätsschutz festgestellt werden
 - Wenn kryptographische Algorithmen gebrochen sind, können die elektr. Rechnung samt Speicherung ausgetauscht werden
- Forderung, dass das **Zertifikat des Empfängers** gespeichert werden muss ist nicht nachvollziehbar, da der Empfänger eigentlich kein Zertifikat braucht

© Secorvo



E-Abrechnung

◆ Praktische Probleme der GDPdU

- die Finanzbehörde hat das Recht, „*die mit Hilfe eines Datenverarbeitungssystems erstellte Buchführung des Steuerpflichtigen durch Datenzugriff zu prüfen*“
- Auf welche Daten genau der Prüfer zugreifen darf, ist nicht spezifiziert („*alle steuerrelevanten Daten*“)
- Prüfer kann sich die Daten auch auf maschinell lesbaren Datenträger aushändigen lassen
 - Wie diese dann ausgewertet werden sollen, ist noch unklar
 - Wie, wann, durch wen und durch wen kontrolliert diese Daten wieder gelöscht werden, ist unklar
- Es werden sehr hohe Anforderungen an die Archivierung der Daten gestellt
 - Fraglich, ob es Anbieter gibt, die diese Anforderungen erfüllen können

© Secorvo



Die Realität

- ◆ **Wer wird SigG-Signaturen nutzen (können) ?**
 - Angehörige bestimmter Berufskammern (als ZDA)
 - Rechtsanwälte, Steuerberater, Wirtschaftsprüfer, Notare, etc.
 - Verwendung von Attribut-Zertifikaten
 - Aufbau elektronischer **Berufsregister**
 - Unternehmen für E-Rechnungen (Vorsteuerabzug)
 - Abwarten
 - ggf. Privatanwender für die Behördenkommunikation („G2C“)
 - Wann, wie teuer ?
 - neuer §3a VwVerfG: öffentliches Recht, z.B. E-Vergabe
- ◆ **Wer wird SigG-Signaturen *nicht* nutzen ?**
 - Homebanking-Anwender (HBCI)
 - E-Commerce-Anwender
 - Unternehmen im „B2B“-Umfeld

© Secorvo



Erfahrungen, Ausblick

- ◆ **Wirklich umfangreiche und aussagefähige SigG-Erfahrungen fehlen noch immer**
 - Viele Pilotprojekte bereits etabliert
 - Zusammenarbeit einzelner Lösungen ?
- ◆ **Einige Probleme tauchen immer wieder auf**
 - Interoperabilität, Sperrmanagement, Directory/Naming
 - Darstellungskomponente, Gültigkeitsmodell, Trojaner
 - Langzeitarchivierung
- ◆ **Rechtliche Rahmenbedingungen wurden erarbeitet**
 - Standardisierung, z.B. ISIS-MTT ?
- ◆ **PKI-Projekte mit großem Potential sind vorhanden**
 - Media@Komm, SPHINX, Identrus, (BundOnline 2005)

© Secorvo



Konsequenz

**„Es ist anwendungsbezogen zu entscheiden, ob
qualifizierte elektronische Signaturen mit Anbieter-
Akkreditierung erforderlich sind.“**

(Quelle: Kabinettsbeschluss)

© Secorvo



Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455
E-Mail info@secorvo.de
<http://www.secorvo.de>