

# Das Deutsche Signaturgesetz und Auswirkungen auf die Wirtschaft

12.01.2010

Wenzl Sarah

# Gliederung

## 1a) Definition Signaturgesetz

- Ziele und Aufgaben
- Was regelt das Signaturgesetz nicht

## 1b) Elektronische & Digitale Signatur

- Unterschiede

## 1c) Signaturverordnung

## 1d) Sicherungsinfrastruktur

## 1e) Signaturarten

# Gliederung

## 2.) Definition Zertifikatdiensteanbieter (ZDA)

- Anforderungen & Voraussetzungen
- Aufgaben & Dienstleistungen
- Haftung

## 3.) Änderungen seit Einführung

## 4.) Probleme

- auf nationaler Ebene
- auf internationaler Ebene

## 5.) Fazit

## Def. Signaturgesetz

### 1a) Signaturgesetz (SigG)

- Wort Signatur stammt vom lateinischen Begriff *Signum* und bedeutet Zeichen
- Gesetz über Rahmenbedingungen für elektronische Signaturen, kurz SigG oder SigG2001
- Novelliert wurde SigG zuletzt am 16. Mai 2001, löste damit Signaturgesetz vom 22. Juli 1997 ab
- Erste Gesetzesänderung am 4. Januar 2005 (SigÄndG)
- Signaturverordnung vom 16. November 2001 (SigV)

# Def. Signaturgesetz

## Ziele / Aufgaben:

- Erhöhte Rechtssicherheit für E-Commerce und das E-Government
- SigG und SigV legen Anforderungen fest
- Zertifizierungsdienste
- Nachträgliche Beweisbarkeit einer tatsächlichen und endgültigen Willenserklärung
- Technikneutralität soll gewährleistet werden
- Gleichstellung zwischen Papiersignatur und einer elektronischen Signatur
- Grenzüberschreitende Regelungen, EU- Richtlinie

## Def. Signaturgesetz

### Was regelt das SigG nicht?

- SigG regelt ausschließlich Erbringung von Zertifizierungsdienste!!
- Signaturgesetz definiert nur unter welchen Voraussetzungen eine digitale Signatur als qualifizierte elektronische Signatur anerkannt wird.
- Rechtswirkung sind nicht im SigG definiert  
Regelungen werden im BGB sowie im Verwaltungsverfahrensgesetz getroffen
- "Digitale Identität" nicht in allen Anwendungsfällen geregelt.  
Nur Regelungen von digitalen Zertifikaten für natürliche Personen, Zertifikate

## 1b) Elektronische und digitale Signatur

Lt. §2 Abs. 1 SigG: *„Im Sinne dieses Gesetzes sind „elektronische Signaturen“ Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.“*

- Unter einer elektronischen Signatur versteht man mit elektronischen Information verknüpfte Daten, mit denen man den Unterzeichner bzw. Signaturersteller identifizieren und die Integrität der signierten elektronischen Informationen prüfen kann
- In der Regel elektronische Dokumente
- Technisch gesehen gleicher Zweck wie eigenhändige Unterschrift auf Papierdokument
- früher digitale Signatur!

## Unterschied digitaler und elektronischer Signaturen

- Digitale Signatur bezeichnet eine Klasse von kryptografischen Verfahren.
- Elektronische Signatur ist ein rein rechtlicher Begriff.
- Ziel Elektronische Signatur nicht an eine bestimmte Technologie zu koppeln
- Definition der elektronischen Signatur umfasst neben der digitalen Signatur auch andere, nicht auf kryptographischen Methoden basierende Verfahren

## 1c) Signaturverordnung SigV (SigV 2001)

- Verordnung zur elektronischen Signatur ergänzt das SigG um Einzelregelungen bzgl. der Verfahren und Abläufe der Zertifizierungsstellen:
  - Ergänzungen zu Anforderungen an den ZDA bzgl. des Ablaufs der Zertifizierung, einzusetzender Komponenten für Signaturerstellung
- SigV trat am 22. November 2001 in Kraft
- löste Signaturverordnung vom 22. Oktober 1997 ab

# Sicherungsinfrastruktur

## 1d) Sicherungsinfrastruktur

- Nach dem SigG 2 Instanzen: Wurzelinstanz und Teilnehmerschnittstelle
- Wurzelinstanz -> Regulierungsbehörde für Telekommunikation und Post (RegTP)
- Teilnehmerschnittstellen -> Zertifizierungsdienstleister (ZDA)
- Kontrolle des ZDAs obliegt der nationalen Behörde (Regulierungsbehörde (RegTP) = Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn (BNetzA) § 13 SigG)
- RegTP unterliegt Weisungsbefugnis des Bundeswirtschaftsministers
- Wurzelinstanz kann gegenüber ZDA Maßnahmen zur Einhaltung des SigGs oder der SigV treffen

### 1e) “Einfache elektronische Signatur” § 2 Abs. 1 SigG

-Laut § 2 Abs. 1 SigG sind elektronische Signaturen *„Daten in elektronischer Form, die anderen elektronische Daten beigefügt oder logisch mit ihnen verknüpft sind“*

- Diese dienen lediglich der „Authentifizierung“, d.h. der Identifizierung des Urhebers der Daten

- An die elektronische Signatur werden keine weiteren Sicherheitsanforderungen gestellt. Diese unterliegen ebenfalls keiner spezifischen Rechtsfolge im SigG

**Beispiel:** gescannte Unterschrift, Iris- Gesichtserkennung, Daumenabdrücke

-> nur Authentifikation

## “Fortgeschrittene elektronische Signaturen“ § 2 Abs. 2 SigG

- neben der “einfachen elektronischen Signatur“ vier wesentliche Funktionsmerkmale:
  - *Sie sind ausschließlich dem Signaturschlüssel-Inhaber zuzuordnen*
  - *Sie ermöglichen die Identifizierung des Signaturschlüssel-Inhabers*
  - *Sie werden mit Mitteln erzeugt, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann*
  - *nachträgliche Veränderung der Daten kann erkannt werden (§ 2 Nr. 2 SigG)*

Bei „fortgeschrittenen elektronischen Signaturen“ spielen sowohl die Authentizität als auch die Integrität, Nachweis der Vollständigkeit und Sicherung einer unveränderten Datentransformation, eine große Rolle

**Beispiel:** Pretty Good Privacy (PGP) -> E-Mail Verkehr absichern, Nachrichten verschlüsseln oder Bezahlen im Internet sicher machen

## “Qualifizierte elektronische Signatur” § 2 Nr. 3 SigG

- „fortgeschrittene elektronische Signaturen“, die sich das Prädikat der „Qualifizierung“ durch zwei Merkmale verdienen:
  - *Sie müssen auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen*
  - *Sie müssen mit einer sicheren Signaturstellungseinheit erzeugt werden (§ 2 Nr. 3 SigG)*
- Aufgabe Bescheinigung der Identität einer elektronisch signierten Person (Authentizität)
- Reihe von Anforderungen an ZDA
- verwendung einer „sicheren Signaturstellungseinheit“ (SSEE), sog. *“Trust-Center”*  
(*SW bzw. HW zur Erzeugung, Speicherung von Signaturschlüssel*)
- beschränkte Haftung der ZDA -> keiner freiwilligen Überprüfung durch die RegTP unterzogen

# Signaturarten

## Qualifizierte elektronische Signatur mit Anbieter-Akkreditierung

- „akkreditierte Signatur“
- Anbieter qualifizierter Zertifikate müssen sich einer freiwilligen Prüfung von der Regulierungsbehörde (Root CA) unterziehen
- Hierbei wird die Einhaltung des Signaturgesetzes, die notwendigen Sicherheitsmaßnahmen sowie die Seriosität abgefragt und in regelmäßigen Abständen durch unabhängige Dritte kontrolliert und bestätigt.
- Freiwillige Akkredierung → Steigerung des Sicherheitsniveaus. Höherer Beweiswert als Signaturen ohne Akkreditierungen



High Security  
Signaturgesetz

regtp Z 0 0 0 3

## 2a.) Zertifizierungsdiensteanbieter (ZDA)

- ZDA stellt Grundlage für digitales Signieren und für Nachrichtenverschlüsselung dar
- Gewährleistet Integrität und Vertraulichkeit von elektronischen Daten
- Beispiel für Anbieter: DATEV eG, TC TrustCenter AG, Deutsche Post Com GmbH
- der ZDA erhält zur Erstellung einer qualifizierten elektronischen Signatur alle nötigen Komponenten (Schlüsselgeneratoren, Funktionsbibliotheken, Zeitstempeldienstkomponenten)

## Anforderungen & Voraussetzungen für ZDAs

### Formelle Voraussetzung:

- “genehmigungsfrei”
- keine Kontrollerlaubnis, stattdessen „geeignetes System zur Überwachung der in ihrem Hoheitsgebiet niedergelassenen Zertifizierungsdienstanbieter, die öffentlich qualifizierte Zertifikate ausstellen“ (Art. 3 Abs. 3 EU-RL)
- Anzeigepflicht (§ 4 Abs. 3 SigG) und behördlichen Überwachung durch die RegTP

### Materielle Anforderungen:

- Betreiberpflichten (§ 4 Abs. 2 SigG), Orientierung an EU-RL
- Zertifizierungsdienst nur wenn ZDA:
  - Zuverlässig ist,
  - erforderliche Fachkenntnisse für den Betrieb,
  - eine Deckungsvorsorge nach § 12 SigG
  - weitere Voraussetzungen des SigG und der SigV, erfüllt.

## Inhalt qualifizierter Zertifikate

*„Der Inhalt qualifizierter Zertifikate (§ 7 SigG) richtet sich nach ihrer Funktion, die Identität eines Signaturschlüssel-Inhabers zu bestätigen. Die Angaben müssen aus diesem Grund eindeutig sein.“ (§ 14 Abs. 1 SigV)*

## Betreiberpflichten (§ 5 SigG)

- Identifizierung des Antragstellers,
- Gewährleistung von technischen Vorkehrungen,
- die persönliche Übergabe des Signaturschlüssels und der Identifikationsdaten an Inhaber,
- Sperrung qualifizierter Zertifikate auf Verlangen

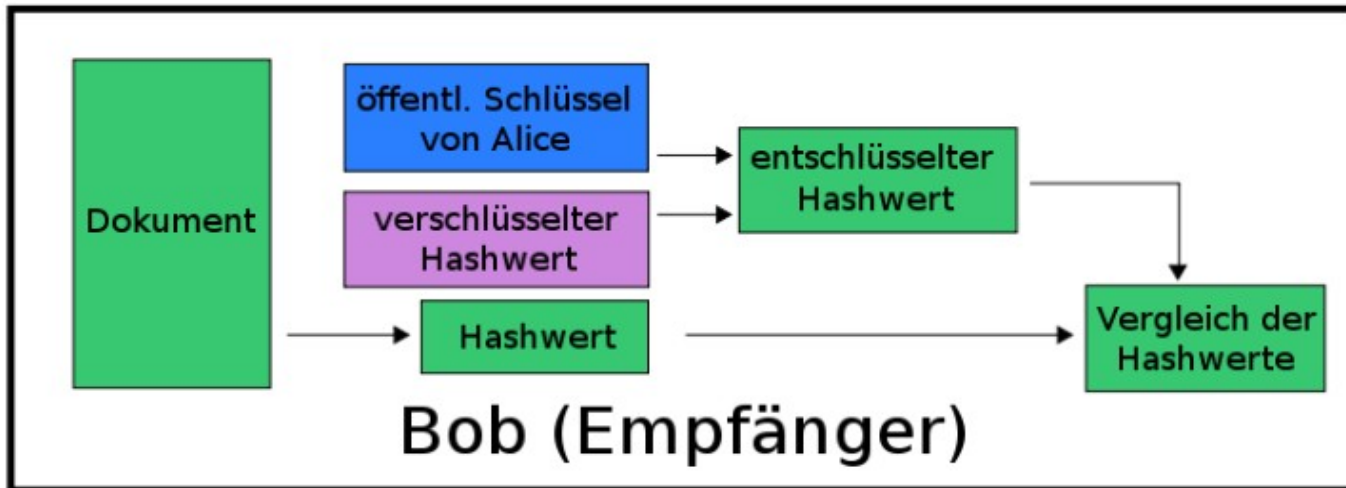
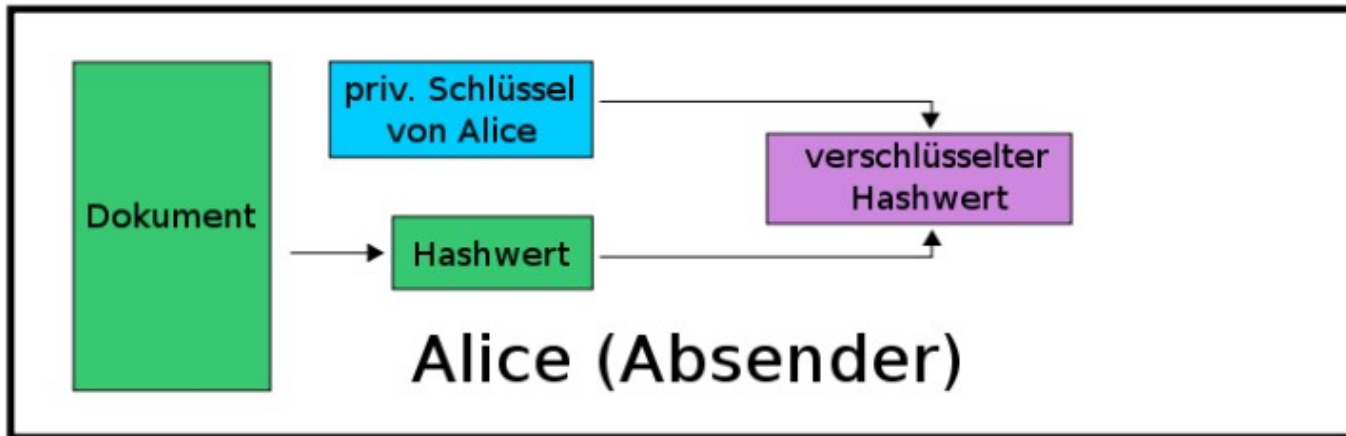
## Bereitstellung von Produkten für qualifizierte elektronische Signaturen - (§ 5 Abs. 5 SigG)

- sichere Signaturerstellungseinheiten, sonstige technische Komponenten für Zertifizierungsdienste

## Aufgaben und Dienstleistungen

- im deutschen SigG festgeschriebenen Aufgaben → von der Regulierungsbehörde für Telekommunikation und Post (Reg TP), wahrgenommen
- Schlüsselgenerierung / Key Generation
- Schlüsselzertifizierung / Certification Authority
- Personalisierung / Personalisation Service
- Identifizierung und Registrierung / Registration Authority
- Verzeichnisdienst / Directory Service
- Zeitstempeldienst / Time Stamping Service

# ZDA - Aufgaben



## ZDA - Aufgaben

- Teilnehmerdaten müssen von zuständiger Stelle registriert und identifiziert werden, um ein Zertifikat beantragen zu können

(Untransparente Prozesse innerhalb ZDA, vom Teilnehmer nicht wahrgenommen)

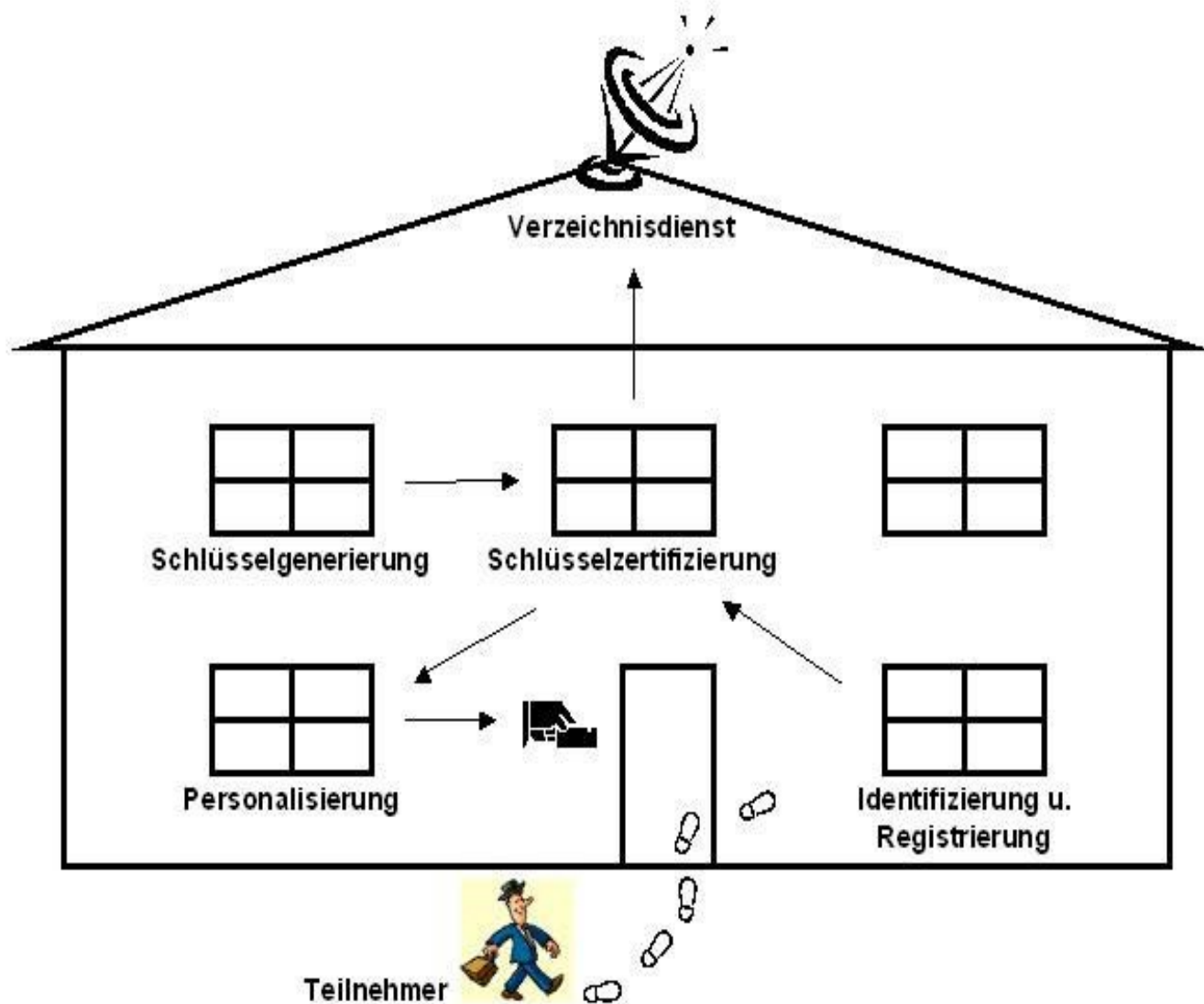
- beantragtes Zertifikat wird anhand der Teilnehmer- und Schlüsseldaten von der Schlüsselzertifizierungsabteilung erstellt

→ Personalisierungsdienst und an Verzeichnisdienst übermittelt

## ZDA - Aufgaben

- Personalisierungsdienst überträgt die für den Teilnehmer relevante Daten auf ein Sicherheitsmedium PSE (personal security environment)  
  
→ wird Teilnehmer übergeben (enthält Schlüssel, Zertifikat)
- Im Verzeichnisdienst werden Zertifikate über ein öffentliches Verzeichnis abrufbar gehalten, wenn der Teilnehmer einer solchen Veröffentlichung nicht widerspricht
- ständige Überprüfbarkeit ob Zertifikat gesperrt ist oder nicht!

# ZDA - Aufgaben



# ZDA - Haftung

## Haftung der Zertifizierungsdienstanbieter

Haftung des ZDA gegenüber Person, die auf ein Zertifikat vertraut

### - Haftungs begründende Voraussetzungen:

Nach § 11 Abs.1 Satz 1 SigG hat ein ZDA einem Dritten den Schaden zu ersetzen, den dieser dadurch erleidet, dass er :

- auf die Angaben in einem qualifiziertem Zertifikat,
- einem qualifizierten Zeitstempel
- oder zu einer Auskunft über die Zuordnung eines Signaturschlüssels zu einer bestimmten Person nach § 5 Abs. 1 Satz 2 SigG vertraut hat.
- Sein Vertrauen ist jedoch nur geschützt, soweit es aus dem Inhalt des Zertifikates gerechtfertigt ist

## - Haftungsausschluss

Ausgeschlossen ist die Ersatzpflicht:

- falls dem Dritten Fehlerhaftigkeit der Information im entsprechenden qualifizierten Zertifikat bekannt ist bzw. bekannt sein müsste, § 11 Abs.1 Satz 2 SigG
- Bei Mitverschulden des Dritten kann sich nach § 254 BGB eine Minderung des Schadensersatzes ergeben
- Hat der Zertifizierungsdiensteanbieter nicht schuldhaft gehandelt, tritt nach § 11 Abs. 2 SigG die Ersatzpflicht nicht ein (Beweislastumkehr)

## - Haftung für Dritte Nach § 4 Abs. 5 SigG

- bestimmte Aufgabenübertragung an Dritte
- In diesem Fall haftet der ZDA für den von ihm beauftragten Dritten wie für sein eigenes Handeln (§ 11 Abs. 4 Satz1 SigG)

# Gesetzesänderungen

## - Deckungsvorsorge - § 12 SigG

- zur Abdeckung möglicher Schäden geeignete Deckungsvorsorge treffen
- Die Mindestsumme durch ein haftungsauslösendes Ereignis entstehenden Schaden beträgt jeweils 250.000 €
- Den Nachweis einer ausreichenden Deckungsvorsorge hat der ZDA im Zusammenhang mit seiner Anzeigepflicht bei Betriebsaufnahme nach § 4 Abs. 3 Satz 2 SigG zu erbringen

## 3.) Änderungen seit Einführung

- Digitale statt Elektronische Signatur
- Mit dem 2001 in Kraft getretene novellierte SigG traten zwei wichtige Übergangsvorschriften in Kraft (§ 25 SigG ):
  - alle genehmigten Zertifizierungsstellen gelten als akkreditierte ZDA
  - alle bereits ausgestellten Zertifikate == qualifizierten Zertifikaten
- Abschaffung der Genehmigungspflicht von 1997

# Gesetzesänderungen

- Möglichkeit der freiwilligen Akkreditierung

"Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen erhalten" (vgl. § 15 Abs. 1 SigG)

- materielle Regelungen, Anforderungen des SigG an die Haftung eines ZDA
- Bußgeldvorschriften gemäß § 21 SigG
- Zeitstempel (nachsignieren) Ende 2007
- Ab 2008 Verwendung neuer Schlüssellängen

## 4.) Probleme

### Probleme auf nationaler Ebene:

- Grundsätzlich gilt: elektronische Signatur == eigenhändigen Unterschrift
- Problem: Nachweis eines elektronisch abgeschlossenen Rechtsgeschäftes vor Gericht
- Beweiswert richtet sich dann danach, inwieweit das Gericht von der Echtheit und Unverfälschtheit der Daten überzeugt werden kann
- Signaturen, die nicht auf einem qualifizierten Zertifikat beruhen, können ebenfalls als Beweismittel vor Gericht eingesetzt werden können
- Die konkreten Rechtsfolgen einer solchen „einfachen“ oder fortgeschrittenen elektronischen Signatur (im Unterschied zur qualifizierten elektronischen Signatur) werden jedoch nicht weiter geregelt und liegen somit bei einem Streitfall im Ermessen des Gerichtes (Objekte des Augenscheins).

## 4.) Probleme

- Fälschung der Signatur kann nur zuverlässig ausgeschlossen werden, wenn geeignete Software zur Erstellung und zur Prüfung der Signatur verwendet wird

- kaum feststellbar, ob diese Voraussetzung tatsächlich erfüllt ist!

- Abhilfe: SigG § 17 Anforderungen an Produkte für qualifizierte elektronische Signaturen

- Oftmals Fokus auf rein mathematisch-technische Aspekte

- Faktor Mensch bleibt oftmals außer Betracht

- Was tun bei verlorenen Signaturkarten oder vergessenen Geheimzahlen? (siehe eGK)

- Abhilfe: seit 2002 ELENA-Verfahren (früher JobCard)

# Probleme

- Konkurrenz durch vertrauenswürdige Digitalisierung der eigenhändigen Unterschrift
  - Institutionen z.B. Kreditinstitute
  - Prozessen wie der Kontoeröffnung
  - eigenhändige Unterschriften digital erfassen
  - biometrischen Daten als Zertifikatsersatz in die elektronischen Anträge einzubetten
  
- Ziel E-Commerce voranzutreiben
  - Kunden können Geschäfte im Internet abwickeln
  - Personal einsparen
  - Offen ist derzeit die Frage, wann über das Internet verschickte Dokumente eine elektronische Unterschrift brauchen und wann nicht.
  - Dies wird in einem eigenen Gesetz geregelt. (BGB bzw. Verwaltungsverfahrensgesetz)

# Probleme

## Probleme auf internationaler Ebene:

### - Begrenzte europäische Harmonisierung:

→ rechtliche Relevanz einer handgeschriebenen Unterschrift variiert unter den Staaten erheblich!

→ Benutzer muss die Regeln des Mitgliedsstaates zur handgeschriebenen Unterschrift kennen bzgl. einer qualifizierten elektronischen Signatur!

→ *Beispiel:* in Großbritannien stellt handgeschriebene Unterschrift nur ein Indiz dar dessen Beweiswert von Fall zu Fall zu entscheiden ist

→ Unterschiede ob qualifizierte Zertifikate und fortgeschrittene elektronische Signaturen nur natürlichen Personen oder auch Organisationen zugeordnet sein können.  
Mitgliedsstaaten regeln dies unter sich

# Probleme

- Trotz technischer Gegebenheiten und umsetzbarer Möglichkeiten besteht mangelnder Gebrauch elektronischer Signaturen

--> Grund sind evtl. die sehr kostenintensiven und noch benutzerunfreundlichen Lösungen

--> Die Unterstützung marktgängiger Systeme ist ebenfalls nicht zufrieden stellend (Betriebssysteme, Browser, E-Mail-Client)

## Probleme in folgenden Bereichen:

- **Darstellungskomponente:**

- sichere Darstellung der zu signierenden Daten ist bis dato noch nicht gelungen

- anstatt Papierdokumente werden Bitfolgen (elektronische Dokumente) unterschrieben, dessen Präsentation für Benutzer nicht immer eindeutig ist

--> Grund hierfür ist, dass Text- oder Grafikprogramme auf unterschiedliche Bibliotheken oder Zeichensätze zugreifen, um das Dokument vor dem Signieren darzustellen.

# Probleme

- **Schutz zu signierender Daten:**

Bevor Daten elektronisch signiert werden können, müssen sie vom PC zur SmartCard transportiert werden --> Schutz vor Manipulation

Hierfür sind Sicherheitsmechanismen notwendig, die wiederum die Flexibilität der Systemumgebung einschränken. Schlimmsten Falls kann eine bestimmte Chipkarte nur mit einer bestimmten Software eingesetzt werden

- **Viren und Trojaner:**

Beispiel: falsches Dokument signiert oder vor dem Signieren verändert

- **Gültigkeitsbegrenzung:**

- immer neuere, verbesserte Methoden der Kryptoanalyse & leistungsfähigere Rechner
- Angriffe auf Verschlüsselungsverfahren z.B. RSA im Vormarsch
- Zertifikat i.d.R. Nicht länger als 3 Jahre gültig!

## Fazit

- Bei erster Betrachtung hat dieses Gesetz nur Auswirkungen auf Rechtsgeschäfte, die einer eigenhändigen Unterschrift bedürfen
- Praxis zur *Digitalen Signatur* wird von Urteilen der Gerichte geprägt sein
- keine offensichtlich beschleunigende Auswirkungen auf die Umsetzung des E-Commerce
- Es braucht mindestens Jahre, bis traditionelle Verfahren durch neue abgelöst werden
- finanziell und technisch hohe Anforderungen
- Nach wie vor sind Geschäfte mit hoher Bedeutung nicht elektronisch signierbar, z.B. Grundstücksgeschäfte und Bürgschaften

## Fazit

- Internationale Sachverhalte, verlangen nach einer länderübergreifenden Lösung
- Signaturgesetze enthalten deshalb Bestimmungen zur Anerkennung von ausländischen Zertifizierungsdiensteanbietern
- Als einziger Masstab → internationale Vorgaben
- Insofern müssen die nationalen Gesetze, was die technische Umsetzung angeht, möglichst harmonisiert werden.