Informationstag 'Elektronische Signatur'

Gemeinsame Veranstaltung von TeleTrusT und VOI

Berlin, 24.09.2010

Dr. Gisela Quiring-Kock
Der Hessische Datenschutzbeauftragte

„Elektronische Signatur – Risiken und Nebenwirkungen aus der Sicht der Bürgerin“

Gliederung

- Einführung (Begriffe, Grundlagen)
- 6 Thesen zur elektronischen Signatur
- Beispiele
  - neuer Personalausweis (PA)
  - Bundesmelderegistergesetz-Entwurf 2008
  - De-Mail Gesetz-Entwurf 2010

Fortgeschrittene elektronische Signatur (FES) § 2 Nr. 2 SigG

a) ausschließlich Signaturschlüssel-Inhaber zugeordnet

b) ermöglicht Identifizierung des Signaturschlüssel-Inhabers

c) mit Mitteln erzeugt, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann

d) mit Daten so verknüpft, dass nachträgliche Veränderung der Daten erkannt werden kann

Qualifizierte elektronische Signatur (QES) § 2 Nr. 3 SigG

- Fortgeschrittene Signatur
- Zum Zeitpunkt der Erzeugung gültiges qualifziertes Zertifikat
- Mit sicherer Signaturerstellungs-einheit erzeugt

(Empfehlung: qualifizierter Zeitstempel nach der Signatur)

Elektronische Form

- Elektronische Form (§ 126a BGB):
  Erklärung und Name und QES
  ersetzt schriftliche Form

- Elektronische Form (§ 3a Abs. 2 VwVfG):
  Elektronisches Dokument und QES (nicht mit Pseudonym) kann Schriftform ersetzen

- Rechtsfolgen QES s. Vortrag Dr. Lapp

Begriffe (Quelle: BSI: E-Government-Handbuch)

- Identifikation bzw. Identifizierung (engl. identification):
  Feststellung der Identität einer Person anhand eines eindeutigen Unterscheidungsmerkmals (im Rahmen der **Registrierung**)

- Authentisierung (engl. authentication):
  Vorlage eines Nachweises eines Kommunikationspartners, in dem bestätigt wird, dass er tatsächlich derjenige ist, der er vorgibt zu sein (im **Fachverfahren**)

- Authentifizierung (engl. authentication):
  Prüfung einer Authentisierung, d.h. die Überprüfung, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein

Authentisierung mit Authentisierungsschlüsseln

- Authentisierungsdaten inhaltlich und rechtlich unwichtig
- Keine weiteren Rechtsfolgen ...
  - Unwichtig, ob Dokument existiert, das den gerade authentisierten (Hash-)Wert besitzt
  - Keine Zurechnung eines nicht sichtbaren/ erkennbaren Dokumentes
  - Keine ungewollte Willenserklärung

Authentisierung und Signatur

nutzen das gleiche technische Verfahren:

Hashwertbildung und Verschlüsselung,

aber:

- Signatur ⇔
  Aussage über Dokument oder Nachricht
- Authentisierung ⇔
  Aussage über Person
  oder Systemkomponente

Standards (RFC 5280, COMMON PKI) 1

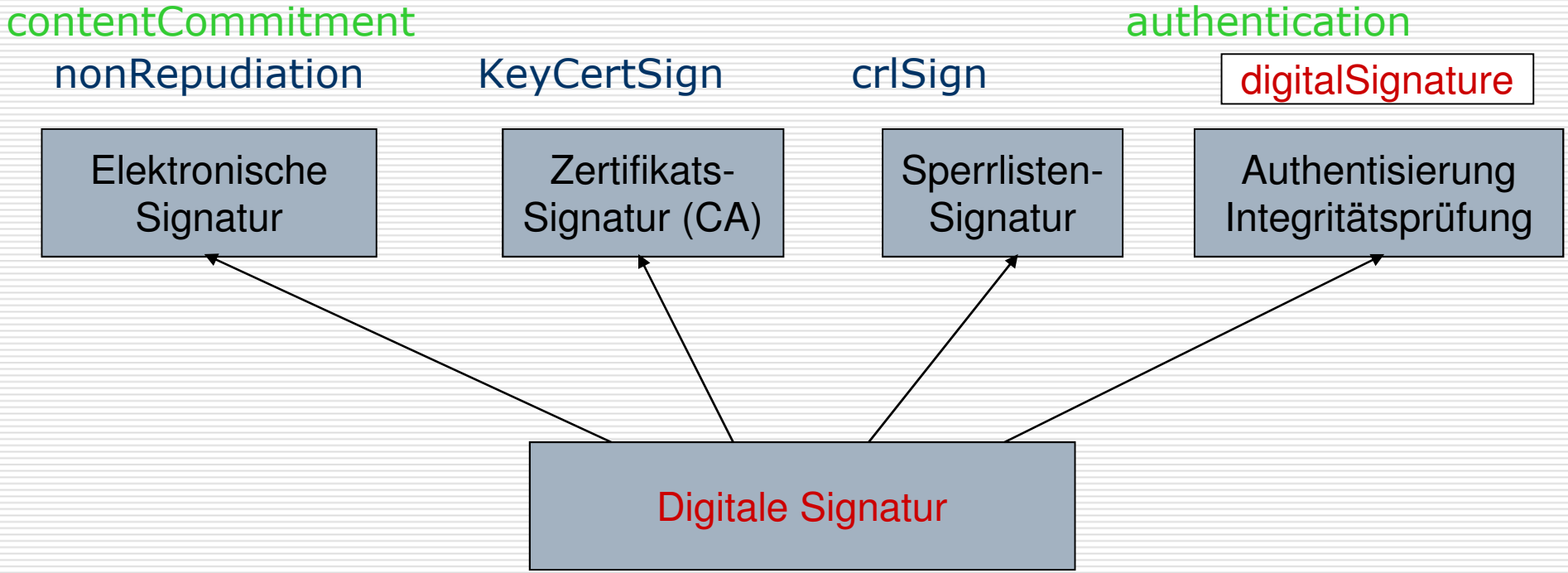
Digitale Signatur (Definition):

- Sicherungsmechanismus für elektronische Daten,
- bei dem aus der Information mittels eines geheimen Schlüssels [und Kryptografischer Verfahren] ein Wert erzeugt wird,
- der mit Hilfe eines zugehörigen öffentlichen Schlüssels verifiziert werden kann

(BSI: Das E-Government-Glossar, [...] QU)

Standards (RFC 5280, COMMON PKI) 2

Key Usage Feld im Zertifikat (Anwendung)



Technische Ebene

Gliederung

- Einführung (Begriffe, Grundlagen)
- 6 Thesen zur elektronischen Signatur
- Beispiele
  - neuer Personalausweis (PA)
  - Bundesmelderegistergesetz-Entwurf 2008
  - De-Mail Gesetz-Entwurf 2010

T1: Transparenz der Verfahren

- Bürgerin will wissen, was sie tut bzw. bekommt
- Zutreffende Bezeichnungen verwenden
  - in Standards, Policies, Anwendungen
- Zutreffende Funktion nutzen
  - Signatur ⇔
    Aussage über Dokument, Willenserklärung
  - Authentisierung ⇔ Aussage über Person
  - Verschlüsselung ⇔ Geheimhaltung
- Keine „Mogelpackung“
  - Bundesmelderegister-Entwurf 2008
  - ELSTER

T2: Dokumentsignatur sinnvoll gestalten

- Dokumentsignatur gilt ab Signaturerstellung unbefristet

  wie bei manueller Unterschrift

  - ✓ QES nach SigG (Kettenmodell) mit Übersignatur (§ 17 SigV)
  - ✓ FES Entwurf neue V-PKI (Hybridverfahren)
  - ☹ QES nach RL 1999/93/EG Anhang IV (Schalenmodell)
  - ☹ FES max. bis Ablauf Zertifikat (Schalenm.)

T3: Transparenz und Sicherheit der Funktionen

- Zutreffende Signaturprüfung
  - abhängig von Art der Signatur bzw. Prüfmodell
  - in Policy bzw. Zertifikat festlegen
  - Prüfsoftware muss alle Varianten korrekt prüfen
- Funktionstrennung im Zertifikat
  (Key Usage, Extended Key Usage)
  - ✓ QES
  - ☹ Kein Standard fordert sie [„MUSS“]
    (COMMON PKI, X.509, RFC 5280), nur Empf.
  - damit Nutzbarkeit der Authentisierungsfunktion erhalten

Risiken Funktionsvermischung

- Keine „Warnfunktion“ mehr wie bei ausschließlicher Verwendung von Signaturschlüsseln zum Signieren (QES)
- Falsche Behauptung möglich, Bürger habe el. Dokument signiert (Beweislast? Rechtsfolgen?)
- Gezielter Missbrauch von Authentisierungsverfahren möglich (SSO, Challenge Response etc.)
- ...

T4: Selbstdatenschutz ermöglichen

- Infrastruktur für Ende zu Ende Sicherheit für E-Mail Adressen
- Nutzung QES im eGovernment (C2G) nicht einschränken
- Sichere, vertrauliche (!) und beschlagnahmefeste Aufbewahrung elektronischer Dokumente
- Technik muss sicher und einfach handhabbar sein

T5: Kosten für Infrastruktur fair verteilen

- Prinzip: Wer den Nutzen hat, zahlt
- QES-Infrastruktur für Bürgerinnen fördern
- Beispiel QES in Österreich:
  - QES für Bankkarten, eGK oder Mobiltelefon
  - QES auf eGK oder Handy-Signatur für Bürger kostenlos, Kosten übernimmt Bund
  - QES auf Bankkarte kostet 15,60 Euro / Jahr, freischalten einmalig 12 Euro
  - ca. 60 % der Bankkunden können QES für Internet-Banking verwenden
  - anfangs Zuschuss für Leser

T6: Siegel oder Paraphe statt FES?

Elektronisches Siegel, elektronische Paraphe

- eigener Key Usage = Seal bzw. Paraphe
- gewährleisten als „technische Signatur“
  - Authentizität (Quelle, Data-Origin-Authentication) und Integrität (Unverfälschtheit)
  - von beliebigen Daten (Software, E-Mails etc.)
- Paraphe nur für natürliche Personen sinnvoll
- Siegel für Maschinen und jur. Personen möglich

T6: Siegel oder Paraphe statt FES?

Siegel und Paraphe

- keine elektronische Signatur,
- kein Unterschrifts-Ersatz
- keine Willenserklärung
- keine Aussage über eine Person (Entity-Authentisierung)
- technische Qualität und Einsatz muss ggf. festgelegt werden

Gliederung

- Einführung (Begriffe, Grundlagen)
- 6 Thesen zur elektronischen Signatur
- Beispiele
  - neuer Personalausweis (PA)
  - Bundesmelderegistergesetz-Entwurf 2008
  - De-Mail Gesetz-Entwurf 2010

Neuer Personalausweis (PA) 1

- Neu: Biometrische Charakteristika
  - Digitales Gesichtsbild
  - Freiwillig: Fingerabdrücke
- Neue Funktionen (freiwillig)
  - QES
    (optional, kontaktlos!, kostenpflichtig)
  - elektronischer Identitätsnachweis (eID)

Neuer Personalausweis (PA) 2

Technik für PA:

- „Ausweis App“ (SW) kostenlos
- Chipkartenleser (BSI TR-03119)
  - Basis-Leser (generisch, für PA)
  - Standard-Leser (mind.: PIN-Pad, kontaktlose Karten)
  - Komfort-Leser (PIN-Pad, Display, kontaktlose und kontaktbehaftete Karten (eGK), QES für PA)

Neuer Personalausweis (PA) 3

QES

Infrastrukturkomponenten für eCards
Förderung durch Bundes-CIO:

- verbilligte oder kostenlose Abgabe von IT-Sicherheitskits
  - B-Leser
  - S- oder C-Leser, der auch eGK unterstützt
- Nicht gefordert: QES auf nPA!
- Bedeutung für Nutzung QES?

Neuer Personalausweis (PA) 4

eID

- ausgeklügeltes Verfahren
- kein Authentisierungsverfahren!
  - für online-Registrierung, Altersnachweis ...
- Ausweis (Besitz) und PIN
  - => PA / eDA darf weder hinterlegt noch kopiert werden (§ Abs. 1 PAuswG)
  - keine Überprüfung, ob richtige Person „da“ z.B. mit Biometrie
- eID Funktion muss nach CC zertifiziert werden

Bundesmelderegistergesetz-Entwurf (April 2008) 1

§ 10 (Selbstauskunft übers Internet):

- alle gespeicherten Daten
- [regelmäßige] Übermittlungen
- unabhängig von Auskunftssperren

=> sehr interessant für Angreifer!

Lösung Gesetz-E:

- Verfahren frei geschaltet für alle Bürger
- Fortgeschrittene Signatur (FES)
  „für Urheberschaft des Antrags“

[wie wird geprüft, ob Signatur fortgeschritten?]

Bundesmelderegistergesetz-Entwurf (April 2008) 2

Lösung HDSB:

- Opt-In Lösung
- Vor.: Nachweis, dass Bürger „sicheren Identitätsnachweis“ hat (PA?)
- Bürger kann festlegen, dass seine Selbstauskunft nur mit zusätzlichem, QES signiertem Antrag erfolgt (Sicherheit, Nachweis bei Missbrauch)
- Strafvorschrift für Missbrauch

DE-Mail Gesetz-Entwurf (Juli 2010)

Ziele:

- sichere „De-Mail“ mit Postfach- und Versanddienst
- nachweisbare elektronische Kommunikation (Versand und Empfang)
- Zugangsbestätigung ohne Mitwirkung des Empfängers!

Anm.:

- De-Safe: DA hat Zugriff auf Klartext
- De-Ident: überflüssig, eID (PA) besser
- De-Mail kann keine FES oder QES ersetzen!

DE-Mail Gesetz-Entwurf (Juli 2010)

Fragen/Forderungen:

- Selbstdatenschutz der Bürgerinnen gewährleisten (auch für E-Mail)
- Warum Adresse unter Pseudonym nur als zweite Adresse?
- Warum auch „unsichere" Anmeldung?
- Voraussetzung für Zugangseröffnung (§3a VwVfG) und „förmliche Zustellung" =?

Was können Sie tun?

- Bei Produkten, Ausschreibungen, Pflichtenheften etc.
  auf Transport- und Anwendungs-Ebene
  die Forderungen umsetzen
- Unternehmenseigenen PKI-Einsatz
  kritisch prüfen
- Einfluss auf die Standards nehmen
- Perspektive wechseln: an Bürgerinnen denken
- Ihre Einflussmöglichkeiten kreativ nutzen

Literatur

- Entschließungen der DSB-Konferenz
  - *Datenschutz beim vorgesehenen Bürgerportal unzureichend* vom 16. 4.2009
  - *Elektronische Steuererklärung sicher und datenschutzgerecht gestalten* vom Nov.2008
  - *Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren* vom 11.10.2006
- Tätigkeitsberichte des HDSB
  - 38. TB, Ziff.7.3, 7.4 und 7.5
  - 36. TB, Ziff.8.1
  - 35. TB, Ziff.4.4
- Artikel in *Datenschutz und Datensicherheit* (DuD)
  - 7/2009 S. 391-395, S. 396-398
  - 3/2010 S. 332-333
  - 5/2010 S. 178-181

Vielen Dank für Ihre Aufmerksamkeit !

Noch Fragen ?
Kommentare?

Der Hessische Datenschutzbeauftragte
Dr. Gisela Quiring-Kock
Gustav-Stresemann-Ring 1
65189 Wiesbaden
Tel. 0611 / 14 08 - 150
email: g.quiring-kock@datenschutz.hessen.de
www.datenschutz.hessen.de