Authentizität mittels Biometrie im elektronischen Rechtsverkehr

Beweissicherheit & Persönlichkeitsschutz

11. Deutscher EDV-Gerichtstag 2002
25.-27.09.2002, Saarbrücken
Arbeitskreis Biometrie

Astrid Albrecht (Volljuristin), Referentin beim BSI

Bundesamt für Sicherheit
in der Informationstechnik

Gliederung

§ 1 Technische Grundlagen, insbesondere Sicherheitsanforderungen an biometrischer Systeme

§ 2 Authentizität im elektronischen Rechtsverkehr mittels Biometrie

§ 3 Datenschutz beim Einsatz biometrischer Verfahren

§ 4 Persönlichkeitsschutz der Arbeitnehmer im Betrieb

§ 5 Fazit & Ausblick

Technische Grundlagen

1. Herkömmliche Prinzipien der Authentizitätsprüfung

- Besitzelemente: Token wie Karten
- Geheimnisse: Passwörter, PINs

2. Biometrie: körperliche Merkmale und Verhaltensweisen

Biometrie ist die Wissenschaft von der Zählung und (Körper-)messung an Lebewesen

- **Ziel**: Trennung eines Originals von einer Fälschung (berechtigt / unberechtigt)

- **Generelle Funktionsweise** (Schlüsselelemente)
  - Personalisierung oder Registrierung des Nutzers im System (Enrolment)
  - Erstellung von Datensätzen (Templates)
  - Vergleich der aktuell präsentierten Daten mit den zuvor abgespeicherten Daten (Matching)
  - Besonderheit: Toleranzschwelle (Falschakzeptanz=FAR / Falschzurückweisung=FRR)

- **Betriebsarten**: Verifikation oder Identifikation

Marktgängige biometrische Verfahren

- Dynamische Unterschriftenerkennung
- Fingerabdruck
- Gesichtserkennung
- Handgeometrie
- Augenerkennung (Iris / Retina)
- Sprechererkennung
- Tastendruckdynamik
- Multimodale Systeme

- ? DNA-Analyse ?

Sicherheitsanforderungen

Schutz der Referenzdaten & der Vergleichsmechanismen:

1. Diese müssen tatsächlich von den Merkmalen der Person stammen, der sie zugeordnet sind.
2. Ihre Integrität, d.h. ihre Unverfälschtheit, beim Einlernen, aber auch anschließend muss stets gewährleistet sein.
3. Die Eingabedaten, die die Sensoren aus den biometrischen Merkmalen gewinnen, dürfen nicht abgehört und wiedereingespielt, aber auch nicht mit oder ohne Mitwirkung des Nutzers einfach reproduziert werden können.

- ***Erkennungsleistung*** (Toleranzschwelle=Wahrscheinlichkeiten)

- ***Überwindungssicherheit***

  Angriffsmöglichkeiten: - Erfassung des biometrischen Merkmals
  - Sensor

Sicherheitsinfrastrukturen

I. Evaluierungskriterien

• Ziele von IT-Sicherheitskriterien:

1. Richtschnur für die Entwicklung sicherer, vertrauenswürdiger Systeme
2. Objektive Bewertung dieser Systeme durch eine neutrale und kompetente Instanz, im Gegensatz zu bloßen Herstellererklärungen
3. Auswahl eines geeigneten IT-Sicherheitsproduktes durch Anwender

• Beispiele:

- BSI: Technische Evaluierungskriterien zur Bewertung und Klassifizierung biometrischer Systeme, Entwurf Version 0.6 (14.9.2000)
- BWG: Best Practices in Testing and Reporting Performance of Biometric Devices, Version 1.0 (12.1.2000)

II. Zertifizierung

• Bestätigung der Einhaltung von Evaluierungskriterien durch unabhängige Stellen

• z.B. Common Criteria: Gemeinsame Kriterien für die Prüfung und Bewertung der

Datensicherheit durch Biometrie & PET

P(rivacy) E(nhancing) T(echnology) = Philosophie der Datenvermeidung & der Datensparsamkeit

- Datensparsamkeit
- Datenvermeidung: Zerstörung der Rohdaten so bald wie möglich
- Sicherung der Daten: Verschlüsselung
- Kein Personenbezug: Anonymisierung
- Beschränkte Zugriffsmöglichkeiten: Verzicht auf zentrale Datenbanken
- Möglichst umfassende Kontrolle der Nutzer über seine biometrischen Daten
- Nutzung von Mechanismen wie Evaluierung und Zertifizierung, um ein garantiertes Maß an Vertrauen zu schaffen

Authentizität mittels Biometrie

- Bedeutung der eigenhändigen Unterschrift im herkömmlichen Rechtsverkehr
- § 126a BGB
- § 292a ZPO
- Beweiswert eines Einsatzes biometrischer Verfahren?

Eigenhändige Unterschrift

- **Schriftform, § 126 BGB**

Funktionen: Identitätsfunktion, Abschlussfunktion, Warnfunktion, Beweisfunktion, Zugangsfunktion, Signalfunktion

Ziel: Rechts- / Beweissicherheit, Vertrauenswürdigkeit

- **Bereits anerkannter Verzicht auf die Unterschrift**

- Massenrechtsverkehr
- elektronischer Zugang zu Gericht § 130a I 1 ZPO
- Gerichtsverkehr: bestimmende Schriftsätze, § 130 Nr.6 ZPO

Elektronische Form gemäß § 126a BGB

- **Grundlage: Qualifizierte elektronische Signaturen**

§ 2 Nr. 3 SigG: Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und zur Authentifizierung dienen (= elektronische Signaturen), und die auf einem (...) Zertifikat beruhen sowie mit einer sicheren Signaturerstellungseinheit erzeugt werden

- **Funktionsäquivalenz?**

Können die rechtlich bestimmten sozialen Funktionen der eigenhändigen Unterschrift durch die Technik der qualifizierten elektronischen Form prinzipiell abgebildet werden?

- **Abbildung der Warnfunktion?**

§ 17 II 1 SigG: vorheriges eindeutiges Anzeigen der zu signierenden Daten; reicht hier die Verwendung einer PIN aus?

Sicherungsinfrastruktur bei qualifizierter elektronischer Signatur

- **Zuordnung des Signaturschlüssels zu einer bestimmten Person**

- ausschließliche Zuordnung zum Signaturschlüssel-Inhaber, § 2 Nr. 2 a) SigG
- § 5 I 1 SigG: zuverlässige Identifizierung durch Zertifizierungsdiensteanbieter

- **Verlässlicher Schutz des Signaturschlüssels**

- sichere Signaturerstellungseinheit muss gegen unberechtigte Nutzung des Signaturschlüssels schützen
- § 15 I 1 SigV: nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale
- Schwachstelle: Schnittstelle Mensch-Maschine bei Verwendung der PIN
- bessere Bindung an die Person durch Biometrie?

Gesetzlicher Anscheinsbeweis, § 292a ZPO

§ 292a ZPO: Empfänger eines in elektronischer Form signierten Dokuments kann den Anschein der Echtheit der Willenserklärung nur durch Tatsachen erschüttern, die ernstliche Zweifel daran begründen, dass die Erklärung nicht mit dem Willen des Signaturschlüssel-Inhabers abgegeben wurde

Ziel der Regelung:

Beweiserleichterung für den Empfänger eines in elektronischer Form gemäß § 126a BGB signierten elektronischen Dokuments

- **Erschütterung der prima-facie-Vermutung durch „ernstliche Zweifel“?**
  - typischer Geschehensablauf? Lebenserfahrung?
  - Herkömmlicher Anscheinsbeweis: Beispiel EC-Karten-Missbrauch

Datenschutz beim Einsatz biometrischer Verfahren (1)

- **Schutzziel § 1 I BDSG:**

Der Einzelne soll durch den Umgang mit seinen personenbezogenen Daten nicht in seinem Persönlichkeitsrecht beeinträchtigt werden.

- ***Recht auf informationelle Selbstbestimmung***

- **Personenbezug** biometrischer Daten gemäß § 3 I BDSG?

„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person“

  - Rohdaten
  - Templates: *Ort der Datenspeicherung* entscheidend:
    - zentral, dezentral, Selbstauthentifizierung, spezifische Ansätze

Datenschutz beim Einsatz biometrischer Verfahren (2)

Diskriminierung

- Failure to Enrol
- Falschzurückweisung
- Falschakzeptanz: Gewährleistung der Korrektheit der Daten?
- unberechtigte Technikgläubigkeit

Zweckentfremdungsrisiko

- Verselbständigung von Daten in elektronischer Verarbeitung beinhaltet das Risiko der dysfunktionalen Verwendung
- abnehmende Transparenz und Verlust der Kontrolle
- lebenslange Bindung des Merkmals an den Betroffenen

Datenschutz beim Einsatz biometrischer Verfahren (3)

- **Unbemerkte Erhebung & Überwachungsrisiko**
  - § 4 II BDSG: Datenerhebung grds. beim Betroffenen selbst
  - Unterschiede der biometrischen Verfahren im Aktivitäts- und Kooperationsniveau
  - Videoüberwachung mit Gesichtserkennung
- **Biometrische Daten als besondere Datenkategorien?**
  - Sensible Daten, § 3 IX BDSG
- **Verhältnismäßigkeit**
  - Abwägung der widerstreitenden Interessen

Persönlichkeitsschutz der Arbeitnehmer beim betrieblichen Einsatz

- **Persönlichkeitsschutz durch § 75 II BetrVG**
  - Abwägung der widerstreitenden Interesse: kann bei objektiver Würdigung ein zwingendes betriebliches Interesse am Einsatz eines biometrischen Systems begründet werden?
  - Verbot der heimlichen Überwachung
  - keine Kündigung aufgrund automatisierter Einzelentscheidung, § 6a I BDSG

- **Mitbestimmung bei technischen Einrichtungen zur Überwachung, § 87 I Nr.6 BetrVG**
  - objektive Eignung zur Überwachung genügt
  - der Einsatz eines biometrischen Systems ist hier in aller Regel erfasst

Fazit & Ausblick

- **Biometrische Verfahren können die Authentizität im elektronischen Rechtsverkehr unter bestimmten Voraussetzungen erhöhen**
  - relevantes Anwendungsfeld: (qualifizierte) elektronische Signaturen
- **Beweiswert hängt von nachgewiesener Sicherheit ab**
  - unabhängige Evaluierung & Zeritifzierung notwendig
- **Relevanz biometrischer Verfahren in der Gesellschaft und damit im (elektronischen) Rechtsverkehr wird ansteigen**
  - u.a. Terrorismusbekämpfung: Pass- und Personalausweise, Visa
  - aber auch: Convenience-Anwendungen
- **Persönlichkeitsrechte der Nutzer müssen gewahrt werden**
  - Datenschutz durch Rahmenbedingungen & techn. Umsetzungen

Vielen Dank für Ihre Aufmerksamkeit !

Kontakt:

Astrid.Albrecht@bsi.bund.de