Datenschutz im Umgang mit digitalen Identitäten

Thilo Weichert, Leiter des ULD
Landesbeauftragter für Datenschutz Schleswig-Holstein

15. Ministerialkongress 2010
Innovation und Wandel – Gestalten ohne Finanzen?
Berlin, 09.09.2010

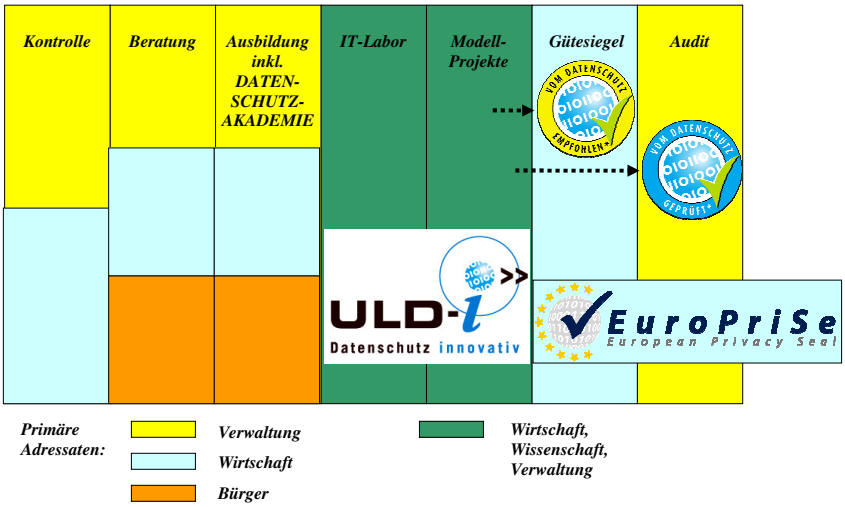
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Datenschutz
- Neuer Personalausweis
- De-Mail
- Elektronische Signatur
- Weitere elektronische Verwaltungsverfahren

ULD www.datenschutzzentrum.de

Unabhängiges Landeszentrum für Datenschutz



ULD www.datenschutzzentrum.de

ULD-Aktivitäten zum ID-Management

- 1999-2002 BioTrust
- Seit 2001 Anonymisierungsdient AN.ON
- 2002 EU-Workshop „Digitale Identität"
- 2003 Studie „Identity Management Systems (IMS) – Identification and Comparison Study"
- 2004-2008 PRIME „Privacy and Identity Management for Europe" (19 Partner)
- 2004-2008 FIDIS „Future of Identity in the Information Society" (23 Partner)
- 2007 Studie „Verkettung digitaler Identitäten"
- 2008-2011 PrimeLife
- Ab 2010 ABC4Trust (Attribute Based Credentials)

Datenschutz I

- Grundrecht auf informationelle Selbstbestimmung (1983)
- Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (2008)

- Bestimmungsrecht, wer was wann bei welchen Gelegenheit
- Zweckbindung
- Verbot von umfassenden Persönlichkeitsprofilen/Personenkennzeichen (lebenslang, bereichsübergreifend)
- Transparenz
- Verbot der Rundumüberwachung
- Informationstechnische Privatsphäre
- Datenvermeidung/Datensparsamkeit
- Technisch-organisatorische Datensicherheit

Datenschutz II

Eric Schmidt (Google): "I don't believe society understands what happens when everything is available, knowable and recorded by everyone all the time." He predicts, apparently seriously, that every young person one day will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends' social media sites (Wall Street Journal).

Zunehmende digitale Verfügbarkeit individueller Lebensäußerungen

Lebenslange Verkettungsmöglichkeit über unterschiedliche Identifikatoren (Name, Geburt, Wohnung, Geolokalisierung, Steuer-ID, Verwaltungs-Nrn.)

Neuer Personalausweis (nPA)

- Funktionen
  - Abruf biometrischer Daten
  - qualifizierte elektronische Signatur
  - elektronischer Identitätsnachweis
- Datensicherheit
  - Sperrmerkmale
  - Zugangsnummer
  - Festlegung von Verarbeitungszwecken
  - PIN
  - Datenübermittlungen zwischen Behörden
  - Datenübermittlungen an Diensteanbieter und Berechtigungsvergabe
  - Erforderlichkeitsprüfung bei Berechtigungsvergabe

nPA-Biometrie

Biometrische Merkmale nur für berechtigte Behörden

- Keine Speicherung der Unterschrift (wg. hohem Missbrauchsrisiko)
- Freiwillige Speicherung der Fingerabdrücke (anders ePass)
- Abruf von Lichtbild (und Fingerabdrücken) nur durch berechtigte Behörden

nPA – Qualifizierte Signatur

Bestätigt (nur) Identität des Absenders sowie Herkunft und Integrität des Textes

Keine Sicherung der Vertraulichkeit (keine Verschlüsselung)

- nPA als Signaturkarte sowie zur Erstellung einer sicheren Signatur
- Kartenlesegerät (ab 60 Euro)
- Zertifikat für Signatur (ca. 40 Euro pro Jahr)

NPA – Elektronischer Identitätsnachweis

- Elektronischer Nachweis der Identität ab 16 Jahren gegenüber öffentlichen und nicht-öffentlichen Stellen
- Missbrauch = OWi § 32 I Nr. 5 PAuswG
- Verschlüsselung in allgemein zugänglichen Netzen
- Datensatz: Sperrmerkmal, Gültigkeit, Namen, Vornamen, Dr., Geburtstag, Geburtsort, Anschrift, Dokumentenart, dienste- und kartenspezifische Kennzeichen, D für BRD, über/unter Alter, Wohnortabgleich, Ordens-/Künstlername

nPA – Datensicherheit I

- Sperrmerkmale (BVA führt Liste mit allgem. Sperrmerkm., diensteanbieterspezifische Sperrmerkmale bei Zertifizierungsdiensteanbieter)
- Zugangsnummer (sechsstellig, nicht als Geheimnummer, zum Abruf von Daten aus Speichermedien, Bedienung Rücksetzähler)
- Nutzung für berechtigte Behörden (Identität des Ausweisinhabers, Echtheit des Dokuments), Nutzen der Biometriemerkmale für Polizei, Zoll, Steuerfahndung, Perso-Pass- u. Meldebehörden (Auslesen, Erheben, Abgleichen)

nPA – Datensicherheit II

- PIN (Änderung der PIN über Bürgerclient, Dokumentation der Nutzung/Protokollierung: welche Stelle, wann, was)
- Datenübermittlung zw. Behörden u. durch Bürger (telefon. Sperrantrag mit Sperrkennwort, Komm. zw. Personal-ausweisbehörden, Übermittlung nach Sperrantrag bei Sperrnotruf, Übermittlung von örtl. an ausstellende Beh.)
- Datenübermittlung an Diensteanbieter (gegenseitige Identifizierung, Nutzerzentrierung, Beschränkung auf erforderliche Daten durch vorlaufende Prüfung durch BVA)

Berechtigungsvergabe an Diensteanbieter

- Keine geschäftsmäßige Datenübermittlung (§ 29 BDSG)
- Erfüllung der Anforderungen an Datensicherheit und DS
- Nur erforderliche Daten für rechtmäßigen Einsatzzweck (kein bloßes Auslesen od. Bereitstellen für Dritte)

  - Problem: Zweckfestlegung

  zu weit>zu viel Daten; zu eng>zu viele Zertifikate/Kosten

  Zweck muss sich auf ein konkretes Verfahren beziehen

  - Problem: Erforderlichkeit bzgl. Zweck incl. evtl. nötiger Rechtsverfolgung

  Einrichtung v. Kundenkonto genügt nicht, evtl. pseudonym

Erforderlichkeit

Informationsabruf – keine Daten, anonyme Nutzung möglich

Nutzung spezifischer Dienste – Merkmalsnachweis z.B. zu Alter oder Wohnort genügt (z.B. Jugendschutz, Kommunale Dienstleistung, Kureinrichtung)

Kontoführung mit Nutzerkommunikation – nicht verkettbare Zuordnung per Pseudonym (auch Prepaid-Dienstenutzung)

Personenbezogene Dienstleistung – Identifikation (kreditorisches Risiko bei Austauschverträgen, Datenschutz-Selbstauskunft, Anträge und Bescheide öffentliche Verwaltung), evtl. Verzicht auf Wohnadresse

De-Mail - allgemein

Ausgangslage: Signaturen gegen keine Auskunft über Ein- und Ausgang, Zeitstempel von Drittinstanz genügt nicht für Zugangsbest., E-Mail weit verbreitet, Signaturen nicht

Ziel: Einfache sichere elektronische Erreichbarkeit mit Zugangsbestätigung

- sichere Absenderidentität (gegen Spam und Phishing)
- digitaler Zugangsnachweis (gem. ZPO, VwVfG)
- sichere Authentisierung (mit Token z.B. nPA od. mobileTAN; Passwort genügt bei Einschreiben nicht, 2 Merkmale)
- elektronisches Postfach

Funktionalitäten: Postfachdienst – Versanddienst, elektronisches Einschreiben – Dokumentensafe – Authentisierungsdienst – evtl. Zusatzdienste der Wettbewerber – Identitätsbestätigung gegenüber Dritten

De-Mail - Akkreditierung

Akkreditierung von Dienstleistern auf Antrag

- IT-Grundschutz/ISO27001/spezifische Anforderungen
- Datenschutzanforderungen
- Zuverlässigkeit und Fachkunde
- Funktionalität

Zweistufiges Verfahren: BSI-zertifizierte Prüfstelle erstellt Gutachten, Prüfung durch BSI (Technik) und BfDI (Datenschutz)

De-Mail – Risiken u. Kritik

Ende-zu-Ende-Verschlüsselung nicht vorgesehen

Freie Beweiswürdigung der Gerichte bei nicht signierter Mitteilung

Auskunftsanspruch zur Aufdeckung von Pseudonymen nicht eindeutig geklärt

Erhebung Staatsangehörigkeit bei Kontoeröffnung

Löschpflicht für Verkehrsdaten und Kontrolle (u.a. Versand- und Eingangsbestätigung)

Elektronische Signatur

Signaturgesetz (SigG) von 1997, Reform 2001

Zweck: Ersatz der Schriftform im Rechtsverkehr

Arten:

- Einfache elektronische Signatur
- Fortgeschrittene elektronische Signatur (eindeutige Identifikation des Schlüsselinhabers)
- Qualifizierte elektronische Signatur (qualifisiertes Zertiifikat, erzeugt mit Signaturerstellungseinheit), ersetzt Unterschrift (§ 126a BGB)

Elektronische Verwaltungsverfahren

Elektronischer Reisepass (ePass)

Elektronische Steuererklärung (ELSTER)

Elektronische Gesundheitskarte (eGK) mit Telematik-Infrastruktur für medizinische Kommunikation, Abrechnung

Elektronischer Leistungsnachweis (ELENA) in Sozialverfahren

Datenschutz im Umgang mit digitalen Identitäten

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Independent Center for Privacy Protection Schleswig-Holstein (ICPP)
Holstenstr. 98, D- 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de