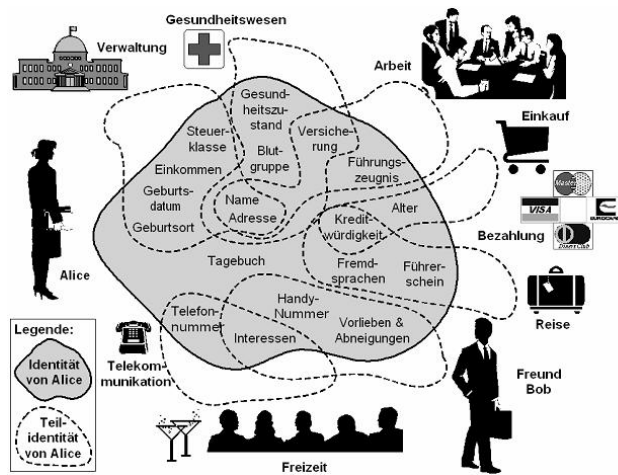


Identitätsmanagement bei den Gesundheitsdaten

BITKOM-Forum
„Digitale Identitäten – Basis einer vernetzten Welt“
5. Oktober 2006

gematik GmbH
Friedrichstraße 136
10117 Berlin

Web-ID-Profile allgemein



Darstellung von WebID-Profilen für verschiedene Anwendungen
Quelle: Marit Hansen, ULD Schleswig-Holstein, Web Identitäten BITKOM Oktober 2005

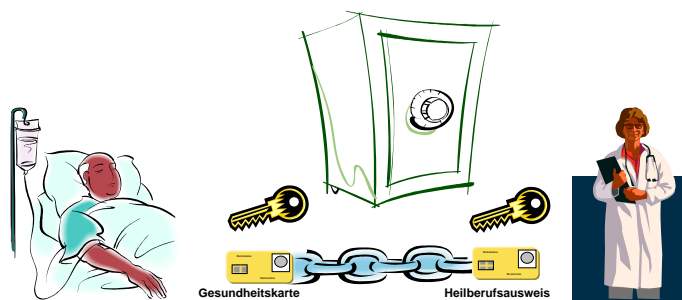
Gesundheitsdaten gehören laut BDSG (§ 3 Abs. 9) zu den besonderen Arten personenbezogener Daten

Ihre Nutzung unterliegt damit besonders strengen Vorgaben bzgl. Datenschutz und Datensicherheit

Diese Vorgaben lassen sich in der Telematik-Infrastruktur durch mehrere Maßnahmen erfüllen:

- Vor der Speicherung von medizinischen Daten muss die Einwilligung des Betroffenen vorliegen
- Vor dem Zugriff auf medizinischen Daten müssen die Identitäten der Beteiligten (z.B. Heilberufler-Versicherter) zweifelsfrei festgestellt werden
- Schützenswerte Daten werden verschlüsselt abgelegt

Beide Schlüssel und die Geheimzahl müssen präsentiert werden



Identitätsfeststellung bei den Heilberuflern

- der Heilberufsausweis (HBA) enthält eine qualifizierte elektronische Signatur, die eine hochwertige Identitätsprüfung voraussetzt
- der HBA enthält ein Attributszertifikat, in dem die Eigenschaft z.B. „Arzt“ von der zuständigen Kammer bestätigt wird
- der HBA enthält ein CV-Zertifikat mit einer Profilkennung, durch die profilbezogene Zugriffsrechte gesteuert werden

Identitätsfeststellung bei den Versicherten

- Vertragsabschluss mit Identifizierung durch Mitarbeiter der Versicherung
- Aktualisierung der Daten bei Umzug/Heirat/Vertragsänderung etc.
- Interesse des Versicherten, aktuelle Daten zu liefern

Identitätsmanagement durch die Versicherung

- Es steht ein umfangreicher Datensatz zur Verfügung:
- Persönliche Daten
- Adressdaten
- Vertragsdaten
- Einkommensbezogene Daten (bei gesetzlicher KV)

Der HBA enthält:

- X.509-Authentisierungszertifikat (allgemein nutzbar)
- X.509-Verschlüsselungszertifikat (allgemein nutzbar)
- X.509-QES-Zertifikat (allgemein nutzbar)
- X.509-Attributszertifikat

- CV-Zertifikat mit Profilkennung Heilberuf (nur im Gesundheitswesen nutzbar)

Die eGK enthält bei der Ausgabe:

allgemein nutzbar

- Versicherten-Stammdaten
- X.509-Authentisierungszertifikat
- X.509-Verschlüsselungszertifikat
- Optional: X.509-QES-Zertifikat

nur im Gesundheitswesen nutzbar

- X.509-Authentisierungszertifikat für Nachrichten
- X.509-Verschlüsselungszertifikat für eRezepte
- CV-Zertifikat mit Profilkennung eGK (nur im Gesundheitswesen nutzbar)

Die eGK enthält bei der Ausgabe (optisch):

2.2 Persönliche Daten des Versicherten

- 2.2.1 Datenfeld: Vorname des Versicherten
- 2.2.2 Datenfeld: Familienname des Versicherten
- 2.2.3 Datenfeld: Titel des Versicherten
- 2.2.4 Datenfeld: Namenszusatz
- 2.2.5 Datenfeld: Vorsatzwort
- Kartenherausgeber (Versicherungsname und IK)
- den unveränderlichen Teil der KVNR
- Bild des/der Versicherten

Die eGK enthält bei der Ausgabe (im eGK-Datensatz):

2.2 Persönliche Daten des Versicherten, u.a.

- 2.2.1 Datenfeld: Vorname des Versicherten
- 2.2.2 Datenfeld: Familienname des Versicherten
- 2.2.3 Datenfeld: Titel des Versicherten
- 2.2.4 Datenfeld: Namenszusatz
- 2.2.5 Datenfeld: Vorsatzwort
- Kartenherausgeber (Versicherungsname und IK)
- den unveränderlichen Teil der KVNR
- weitere Daten (Adressdaten, Geburtsdatum, etc.)

Die eGK enthält bei der Ausgabe (im X.509-Zertifikat):

2.2 Persönliche Daten des Versicherten

- 2.2.1 Datenfeld: Vorname des Versicherten
 - 2.2.2 Datenfeld: Familienname des Versicherten
 - 2.2.3 Datenfeld: Titel des Versicherten
 - 2.2.4 Datenfeld: Namenszusatz
 - 2.2.5 Datenfeld: Vorsatzwort
- Diese Felder bilden den „Common Name“ des Versicherten im Zertifikat
- den unveränderlichen Teil der KV-Nummer (10-stellig)
 - das Institutionskennzeichen (9-stellig)

Typen von Web-IDs

Nutzungsformen – Verwendungszweck (Auswahl)	Typ			
	Allgemeine WebIDs		Rechtssichere WebIDs	
	Anonyme WebID	Offene-/Pseudonyme WebID	Anonyme WebID	Offene-/Pseudonyme WebID
1. Rechtsgeschäfte (national – international z. B. Kaufvertrag, Notarielle Dokumente etc.)				X
2. Verbindliche Transaktionen zwischen Wirtschaft und Wirtschaft, z. B. Einkauf eines Unternehmens				X
3. Verbindliche Transaktion zwischen Wirtschaft und Nutzer, z. B. Einkauf im Internet		X		X
4. Unverbindliche Transaktion zwischen Wirtschaft und Nutzer, z. B. Werbung, kostenlose Informationsmöglichkeiten	X	X		
5. Verbindliche Transaktionen zwischen öffentliche Verwaltung und Wirtschaft z. B. Ausstellung einer Baugenehmigung				X
6. Transaktion zwischen öffentliche Verwaltung und Bürger, z. B. Ausstellung eines Führerscheins		X		X
7. Verbindliche Transaktionen zwischen Nutzer und Nutzer, z. B. Ebay		X		X
8. Unverbindliche Transaktion zwischen Nutzer und Nutzer, z. B. Nutzung von Chatrooms, Newsgroups	X	X		
9. Verbindliche Transaktionen zwischen öffentliche Verwaltung und Nutzer, z. B. E-Voting ²			X	
10. Verbindliche Transaktionen im Gesundheitswesen		X		X

Quelle: Web Identitäten BITKOM Oktober 2005

Nutzbarkeit von eGK/HBA

Nutzungsformen – Verwendungszweck (Auswahl)	Typ			
	Allgemeine WebIDs		Rechtssichere WebIDs	
	Anonyme WebID	Offene-/Pseudonyme WebID	Anonyme WebID	Offene-/Pseudonyme WebID
1. Rechtsgeschäfte (national – international z. B. Kaufvertrag, Notarielle Dokumente etc.)				X
2. Verbindliche Transaktionen zwischen Wirtschaft und Wirtschaft, z. B. Einkauf eines Unternehmens				X
3. Verbindliche Transaktion zwischen Wirtschaft und Nutzer, z. B. Einkauf im Internet		X		X
4. Unverbindliche Transaktion zwischen Wirtschaft und Nutzer, z. B. Werbung, kostenlose Informationsmöglichkeiten	X	X		
5. Verbindliche Transaktionen zwischen öffentliche Verwaltung und Wirtschaft z. B. Ausstellung einer Baugenehmigung				X
6. Transaktion zwischen öffentliche Verwaltung und Bürger, z. B. Ausstellung eines Führerscheins		X		X
7. Verbindliche Transaktionen zwischen Nutzer und Nutzer, z. B. Ebay		X		X
8. Unverbindliche Transaktion zwischen Nutzer und Nutzer, z. B. Nutzung von Chatrooms, Newsgroups	X	X		
9. Verbindliche Transaktionen zwischen öffentliche Verwaltung und Nutzer, z. B. E-Voting ²			X	
10. Verbindliche Transaktionen im Gesundheitswesen		X		X

= ENC und AUT

= QES

Quelle: Web Identitäten BITKOM Oktober 2005

Art der Speichermedien für Web-IDs

Speichermedium	Nutzungs-dauer	Mobilität	Sicherheits-level	Bequemlichkeit
Papier	Mittel	Mittel	Niedrig	Hoch
Unverschlüsselt auf Festplatte	Hoch	Niedrig	Niedrig	Mittel
Verschlüsselt auf Festplatte	Hoch	Niedrig	Mittel	Mittel
Mobiles, nicht geschütztes Speichermedium	Hoch	Hoch	Niedrig	Hoch
Mobiles, geschütztes Speichermedium z. B. USB-Token, Chipkarten	Hoch	Hoch	Hoch	Hoch

Quelle: Web Identitäten BITKOM Oktober 2005

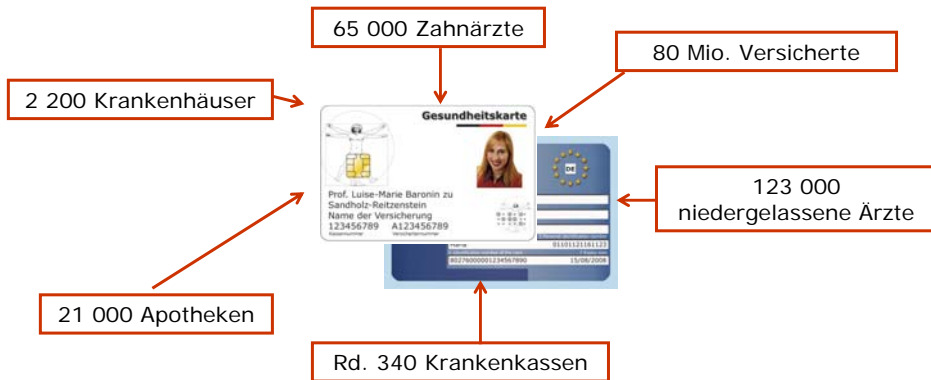
Speichermedium für eGK/HBA

Speichermedium	Nutzungs-dauer	Mobilität	Sicherheits-level	Bequemlichkeit
Papier	Mittel	Mittel	Niedrig	Hoch
Unverschlüsselt auf Festplatte	Hoch	Niedrig	Niedrig	Mittel
Verschlüsselt auf Festplatte	Hoch	Niedrig	Mittel	Mittel
Mobiles, nicht geschütztes Speichermedium	Hoch	Hoch	Niedrig	Hoch
Mobiles, geschütztes Speichermedium z. B. USB-Token, Chipkarten	Hoch	Hoch	Hoch	Hoch

Quelle: Web Identitäten BITKOM Oktober 2005

 = eGK/HBA

Mengenabschätzung Chipkarten im Gesundheitswesen



Quelle: Bundesministerium für Gesundheit

05.10.2006

Copyright by gematik mbH

19

Planungsmatrix wird durch Release-Planung abgelöst

	Release 0 (offline, VSD) = MKT+	FA 1 (online, VSD)	FA 2 (online VSD)	FA 3 (+VODD)	FA 4 (+VODD, ..)	
Teststufe 1 (Labortest)	A	B	C	D		Laborphase
Teststufe 2 (dez. Anwendertest)	E	F	G	H		Anwenderphase
Teststufe 3 (10.000er)	I	J	K	L		Feldphase
Teststufe 4 (100.000er)	M	M	M	N		Massentest
	Release 1 (offline, eRezept, Notfalldaten)	Release 2 (online, VSD, eRezept)			Release 3 (weitere Anwendungen, weitere Anwender, eKiosk)	

05.10.2006

20

Die elektronische Gesundheitskarte kommt

Ich danke
für Ihr Interesse