

Bund-Länder-Kommission:

eID: Der neue Personalausweis – Das ganze ist mehr als die Summe seiner Teile (SAFE)

Referenten:

Martin Schallbruch, Ministerialdirektor, IT-Direktor und IT-Beauftragter im Bundesministerium des Inneren (BMI)

Jürgen Ehrmann, Ministerialrat, Vorsitzender der BLK-AG IT-Standards in der Justiz, Justizministerium Baden-Württemberg

Daniela Freiheit, Koordinatorin BLK-AG IT-Standards in der Justiz, feine IT-Strategien für die Justiz

Protokoll:

Die Idee hinter SAFE ist, dass er das eID Management als Dienst für beliebig viele Anwendungen darstellen soll. Der Nutzer muss sich hierbei nur einmal registrieren und wird überall akzeptiert. Für die Anwendungen bietet sich der Vorteil, dass keine eigene Benutzerverwaltung notwendig ist.

Die Technik bleibt hierbei hinter einer Schnittstelle, damit jeder frei auf diese Schnittstelle zugreifen kann und keine weiteren Vorgaben notwendig sind. Die Technik soll vollständig hinter der Schnittstelle ablaufen und somit vollständig Bestandteil der hinteren Verwaltung sein. Durch ein Web of Trust wird der Zugriff entsprechend ermöglicht. Zum Beispiel greift ein Notar auf TD-Notare zu, welches wiederum auf TD-Deutsche-Justiz zugreift.

Nach diesem Modell soll einmal die Bundesnotarkammer die Strukturen für alle Notare anlegen, während die Justiz ihren Bereich anlegt (z.B. Gerichtsvollzieher)

SAFE nutzt hierbei den internationalen Webservice-Sack („WS-*)Standard und SAFE-Token sind nach dem SAML (Security Assertion Markup Language) beschrieben.

Der neue Personalausweis bietet hierfür gute Voraussetzungen, da er diverse Funktionen besitzt. Nach Freigabe durch den Ausweisinhaber können diese auf dem Chip gespeicherten Daten übermittelt werden:

- Familienname und Vorname
- ggf. Ordens bzw. Künstlername, Doktorgrad
- Geburtsdatum und – Ort
- Anschrift und Postleitzahl
- Dienste- und kartenspezifisches Kennzeichen
- Angabe ob ein bestimmtes Alter über oder unterschritten wird (zur Altersverifikation)
- Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht (zur Wohnortverifikation)

→ Biometrische Daten werden hierbei nicht übermittelt, da sie lediglich für hoheitliche Aufgaben verarbeitet werden.

Bei jeder Nutzung der Online-Ausweisfunktion wird geprüft, ob der Personalausweis noch gültig ist und nicht gesperrt wurde. Er ist also vor Missbrauch geschützt, da er im Verlust- oder Diebstahlsfall einfach gesperrt werden kann.

Seit 2010 wurden 23 Millionen Ausweise ausgegeben, wovon bei 7 Millionen der Identitätsnachweis aktiviert wurde (jeder Bürger kann selbst bestimmen, ob er diese Funktionen nutzen möchte).

Für die Funktionalität gibt es verschiedene Voraussetzungen.

Der Bürger benötigt neben seinem Ausweis einen Kartenleser, eine Software auf seinem Gerät und einen PIN.

Der Dienstanbieter benötigt eine Berechtigung/Zertifikat zur Nutzung. Diese wird bei dem Bundesverwaltungsamt beantragt, welches auch überprüft, ob die Nutzung einem datenschutzgerechtem Zweck entspricht. Bei positiver Prüfung erhält der Anbieter ein Zertifikat. Dies dient dazu Missbrauch zu verhindern und gegebenenfalls nachverfolgen zu können. Darüber hinaus wird vom Dienstanbieter ein Dienstleister mit eID-Server benötigt.

Praktisch kann das Verfahren wie folgt ablaufen:

Der Nutzer ruft die Rentenversicherung auf, die Website meldet, dass eine Verifizierung notwendig ist, der eID-Server teilt mit, welche Authentifizierung notwendig ist und der Anwender bestätigt per PIN die Datenabfrage. Anschließend erfolgt über einen verschlüsselten Kanal der Datenaustausch.

Dieses Verfahren bietet viele Vorteile:

- Hohe Datensicherheit
- Gegenseitige Authentisierung
- Verschlüsselte Übermittlung
- Hohe Datenqualität
- Auf Basis des hoheitlichen Ausweisdokumentes
- Medienbruchfreiheit
- Automatische Übernahme der Daten in Fachverfahren
- Vollständig elektronische Bearbeitung
- Effizientes und nutzerfreundliches E-Government
- Entlastung der Beschäftigten
- Reduktion der Kosten

eID-Funktionen bietet auch im Bereich der eJustice viele Chancen. Es kann Rechtssicherheit bei der elektronischen Kommunikation zwischen Gerichten, Verwaltungsbehörden, Rechtsanwälten, Notaren, Bürgern und Unternehmen gewährleistet werden.

Bisher gibt es über 100 Möglichkeiten zur Nutzung, insbesondere im öffentlichen Bereich und bei Versicherungen im privaten Bereich.

Durch diese Methode soll künftig auch Identitätsdiebstahl verhindert und eingedämmt werden, da Benutzername und Passwort in der bestehenden Form hinfällig werden.

Ziele des Projekts:

1. Ermittlung der Handlungsfelder mit großen Mehrwerten
2. Unterstützung attraktiver Anwendungen mit hohem Nachnutzungspotential = Leuchttürme
3. Bereitstellung von Fachwissen und Initiierung des Erfahrungsaustauschs

e-Justice Communication via Online Data Exchange e-CODEX

Ist grenzüberschreitender Datenaustausch einfach? Bisher findet er innerhalb Europas primär in Papierform statt, obwohl es bereits viele gute technische Systeme und Fachverfahren in den einzelnen Mitgliedsstaaten gibt. Es gibt jedoch keinen grenzüberschreitenden Datenaustausch, hier ist lediglich der analoge Weg über Ausdrücke und Post möglich.

E-CODEX ist am 01.12.2010 gestartet und soll voraussichtlich am 28.02.2015 enden. Es finden aber Gespräche mit der europäischen Kommission statt, ob es verlängert werden soll.

Es beteiligen sich 24 Staaten und 30 Organisationen, mit einem maximalen Budget von 24 Millionen Euro. Pilotbeginn war im Juli 2013.

Protokoll: Marc Großjean