Annika Selzer, Ulrich Waldmann

eID in Deutschland und den USA

Hintergrund
Neue Technologien wie etwa die Möglichkeit zur elektronischen Identifikation bergen Risiken für den Schutz der personenbezogenen Daten[1]. Deshalb sind diese Technologien im Hinblick auf mögliche Gefahren für Datenschutz- und Datensicherheit vorbeugend zu überprüfen.

eID in Deutschland
Der neue Personalausweis (nPA), welcher einen RFID-Chip enthält, der über ein kontaktloses Lesegerät ausgelesen werden kann, erfüllt neben der Funktion als hoheitliches Ausweisdokument auch die Funktion des elektronischen Identitätsnachweises für die Identifizierung im Internet. Für den Abruf der Daten für den elektronischen Identitätsnachweis muss der Empfänger eine Berechtigung durch ein elektronisches Zertifikat nachweisen. Es wird von einer behördlich betriebenen Vergabestelle verliehen. Die Möglichkeit, ein solches Berechtigungszertifikat zu erhalten, ist durch das PAuswG an strenge Voraussetzungen gebunden, um dem Bürger einen hohen Schutz seiner Daten zu gewährleisten und um zu verhindern, dass ein Datenempfänger eine umfangreiche Datensammlung erstellt oder unseriöse Anbieter mit eID-Daten handeln. Zudem erfolgt die Übermittlung personenbezogener Daten im Zuge des elektronischen Identitätsnachweises an einen Datenempfänger ausschließlich nach Einwilligung des betroffenen Bürgers, die durch die Eingabe der zum Ausweis gehörenden geheimen eID-PIN erteilt wird.

Neben datenschutzfreundlichen Funktionen des Ausweises sowie der pseudonymen Nutzung wird der elektronische Identitätsnachweis durch modernde Verschlüsselungstechnologien und ein pseudonymes Sperrsystem gegen Missbrauch geschützt. Ansätze, wie die eID-Kommunikation auch auf Smartphones mit kontaktlosen Kartenlesern geschützt werden kann, zeigt der Beitrag Hornung/Horsch/Hühnlein zur mobilen Authentisierung in diesem Heft.

eID in den USA
In den USA gibt es kein einheitliches Ausweisdokument, das dem bundesweit geltenden deutschen Personalausweis entspricht. Jedoch wurde in den USA ein Identifikations-Standard für Staatsbedienstete und staatlich beauftragte Unternehmer entwickelt. Die Grundlage hierfür ist die „Homeland Security Presidential Directive-12" aus dem Jahr 2004. Eineinhalb Jahre nach der HSPD-12 veröffentlichte die US-amerikanische Bundesbehörde NIST im Jahre 2006 den für Behörden verbindlichen Identifikations-Standard FIPS-201 für Personal Identity Verification (PIV) Cards. Die Karten sind sowohl Sichtausweise für die physische Zutrittskontrolle als auch Dual-Interface Chipkarten mit X.509-Zertifikaten für den Login der Mitarbeiter in die behördlichen IT-Systeme. Die PIV Card stellt über das kontaktlose wie über das kontaktbehaftete Interface frei auslesbar eine signierte Personenkennziffer (Cardholder Unique Identifier, CHUID) zur Verfügung. Mit der CHUID können der Karteninhaber und die Chipkarte eindeutig identifiziert werden. Für die lokale biometrische Authentisierung über das kontaktbehaftete Interface sind 2 Fingerabdrücke und optional ein Gesichtsbild in der Karte gespeichert, während das PKI-basierte Verfahren der Online-Authentisierung des Karteninhabers dient.

Die US-amerikanischen eID-Infrastrukturen sind aus Sicht der Anwendung und des Datenschutzes nicht mit denen in Deutschland vergleichbar. So werden bei der Registrierung für die PIV Card alle 10 Fingerabdrücke des Antragstellers aufgenommen und mit der Datenbank des FBI abgeglichen. Die auf der PIV Card gespeicherten persönlichen Daten werden in zentralen und dezentralen Datenbanken der Behörden gespeichert. Eine pseudonyme Nutzung von PIV Cards ist nicht vorgesehen. Die drei Authentisierungsniveaus mittels CHUID, mittels PIN-geschützter biometrischer Verifikation und mittels PIN-geschützter überwachter biometrische Verifikation bzw. PKI-basierter Authentisierung beruhen ausschließlich auf Prüfungen des Karteninhabers – die abfragenden Systeme authentisieren sich nicht gegenüber der PIV Card.

2006 startete industriegetrieben die Initiative zur Entwicklung einer generischen interoperablen Kartenplattform für Identifizierungs-, Authentisierungs- und Signatur-Services (IAS). Die Spezifikation des Generic Identity Command Set (GICS) ist inzwischen weit fortgeschritten und wird als ANSI-Standard veröffentlicht. GICS bietet Abwärtskompatibilität zu PIV Cards, beschränkt sich aber auf Kartenkommandos ohne weitere Systemschnittstellen zu definieren, welche bereits im Middleware-Standard ISO 24727 spezifiziert sind. Die Interoperabilität von GICS und ISO 24727 ermöglicht herstellerübergreifendes Kartenmanagement und unabhängige Entwicklung von Anwendungen. GICS unterstützt die verschlüsselte Kommunikation mit dem kontaktlosen Chip, verschiedene Authentisierungslevels und die Integration neuer Privacy-Protokolle, welche sich den in Europa entwickelten Konzepten annähern. Nicht zuletzt propagiert auch die US-Strategie eine Bandbreite verschiedener Authentisierungsmechanismen – von anonymer und pseudonymer Nutzung der Credentials bis hin zu umfassenden Identitätsprüfungen.

Ausblick
Während in Deutschland die eID-Funktion des nPA und ihre Anwendung gesetzlich geregelt sind und die benötigte Sicherheitsinfrastruktur von der öffentlichen Hand betrieben wird, sieht die US-Strategie für vertrauenswürdige Identitäten im Cyberspace eher die Privatwirtschaft und die Konsumenten in der Verantwortung. Die bestehende Infrastruktur der PIV Cards für die US-Staatsbediensteten ist wenig datenschutzfreundlich und derzeit nicht interoperabel. Auf Initiative der US-Industrie entsteht jedoch mit der GICS-Spezifikation eine interoperable technische Basis für eine einheitliche Kartenentwicklung, die zudem datenschutzfreundliche eID-Mechanismen vorsieht. Es bleibt abzuwarten, ob die US-Regierung auf dieser Grundlage eine neue eID-Strategie für Bürgerkarten oder Personalausweise entwickelt.

1 Selzer, A., Waldmann, U.: Der Schutz personenbezogener Daten von Bürgern in Europa und den USA in: Tagungsband 22. Smartcard Workshop, Fraunhofer Verlag, 2012.