Sichere Identitätsnachweise

Neue technische Entwicklungen und Trends im Identitätsbereich wurden im Mai 2016 auf der Konferenz „Secure Identification“ in Riga vorgestellt.

Das Identitätsmanagement ist eine Kernaufgabe der öffentlichen Verwaltung, was die Erfassung, Verwaltung, Prüfung und Bereitstellung personenbezogener Daten und damit auch die Ausstellung von Identitätsnachweisen betrifft. Wesentlich ist die eindeutige Zuordenbarkeit verschiedener, behördlich geprüfter, personenbezogener Daten zu einer Identität (Personenkern), um die eindeutige Identifikation einer Person zu ermöglichen.

Als personenbezogene Daten werden in diesem Zusammenhang beispielsweise Name, Geburtsdatum, Geburtsort oder Nationalität und teilweise auch biometrische Merkmale wie Fingerabdrücke oder Gesichtsbild verstanden.

Der amtliche Nachweis der eigenen Identität muss höchsten Sicherheitsstandards entsprechen. Die technologischen Mittel, die Sicherheit von Identitätsdokumenten und Nachweisen auch zukünftig zu gewährleisten, müssen daher laufend weiterentwickelt werden.

Identitätsdokumente der neuesten Generation mit integrierten Chips kommen auch in elektronischen Identifikationsprozessen vermehrt zum Einsatz.

Diesen Trends und Innovationen im Identitätsbereich widmete sich die Konferenz „Secure Identification“ am 18. und 19. Mai 2016 in Riga. Bei der internationalen Konferenz waren mehr als 200 Teilnehmer aus unterschiedlichen Ländern sowie an die 30 Unternehmen aus dem Umfeld des Identitätsmanagements vertreten.

„Laissez Passer“-Reisedokument für EU-Bedienstete: Außen- und Innenseite des Einbands, Personaldatenseite, UV-Sicherheitsmerkmal auf der Personaldatenseite.

Sichere Identitätsdokumente. Für Reisepässe gibt es Sicherheitsstandards, wie die der Europäischen Union und der Internationalen Zivilluftfahrtsgesellschaft *International Civil Aviation Organization (ICAO)*.

Beispielsweise ist der österreichische Reisepass mit einem kontaktlosen Chip ausgestattet, in dem jene Daten gespeichert sind (bis auf die Unterschrift und die Größe des Passbesitzers), die im Pass auch in gedruckter Form enthalten sind. Zusätzlich werden im Chip zwei Fingerabdrücke und das Gesichtsbild gespeichert. Somit kann eine eindeutige Zuordnung zwischen dem Passbesitzer und dem Pass hergestellt werden. Der Zugriff auf die Daten im Chip ist durch ein digitales Zertifikat geschützt, das nur von der Republik Österreich ausgestellt werden kann. Ein integrierter digitaler Kopier- und Schreibschutz erhöht zusätzlich die Fälschungssicherheit. Auch was Verschlüsselungstechnologie, Speicherkapazitäten, Zugriffsschutz oder kontaktlose Lesegeschwindigkeit betrifft, müssen die Chips auf den Identitätsnachweisen auf dem höchsten Sicherheitsstandard sein. Ausschlaggebend für die Fälschungssicherheit ist nicht nur der Chip im Identitätsdokument; auch das Dokument muss den Sicherheitsanforderungen entsprechen.

Reisedokument für EU-Bedienstete. Im Rahmen der „Secure Identification“ wurde das neue Reisedokument für EU-Bedienstete, „Laissez-passer“, vorgestellt. Das Dokument ist für Reisen in alle Mitgliedstaaten der Europäischen Union gültig sowie für Drittländer, mit denen Abkommen zur Anerkennung abgeschlossen wurden.

Dieses Reisedokument bietet durch zahlreiche Sicherheitsmerkmale, wie etwa einzigartige Druckmuster und -techniken, sowie durch moderne Chiptechnologie ein Höchstmaß an Fälschungssicherheit. Beispielsweise können spezielle Druckfarben mit mikroskopischen Pigmenten, je nach Betrachtungswinkel oder Lichteinfall, wesentliche Farbverschiebungen verursachen. Durch Stichtiefdruck kann ein erhabenes, fühlbares Abbild (ein fühlbares Merkmal) erstellt werden, was auch für die Herstellung des Kippeffekts genutzt wird.

Weitere Sicherheitstechniken beim *Laissez-passer* sind unter anderem Wasserzeichen, UV-Merkmal (Ultraviolettlicht), IR-Licht (Infrarot-Absorption) und Hologramm (kinetische Effekte, metallischer Effekt).

Ebenso enthalten staatliche Ausweise der neuesten Generation in Form von ID-Cards (Plastikkarten in der Größe einer Kreditkarte) verschiedene optische und elektronische Sicherheitsmerkmale und sind nach höchsten Sicherheitsstandards zertifiziert.

Beispielsweise hat Irland im Oktober 2015 als Reisedokument eine Passkarte (ID-Card) eingeführt, die in 30 europäischen Ländern gültig ist. Die Passkarte enthält mehr als 28 innovative Sicherheits-Features und erfüllt den internationalen Standard ICAO. Damit eine Passkarte ausgestellt werden

FOTOS: RAT DER EUROPÄISCHEN KOMMISSION/PRADO

kann, muss der Antragsteller im Besitz eines gültigen Reisepasses sein.

Printed-Code. Ein weiteres neues Sicherheitsfeature, das auf ID-Cards aufgedruckt werden kann, ist der „Printed Code“ (in Form eines 2D-Codes). Der mittels eines speziellen Algorithmus generierte Code kann Textzeichen (Name, Adresse u. a.) und biometrische Daten wie Gesichtsbild und Fingerabdrücke enthalten. Der Code kann etwa mit einem Smartphone unter Anwendung einer entsprechenden Applikation ausgelesen werden. Zur Abfrage ist weder ein Online-Zugang noch eine Datenbank erforderlich, da diese Daten im aufgedruckten Code enthalten sind. Somit kann mittels des Codes die Echtheit des Dokuments einfach überprüft werden, indem die gleichen Daten, wie sie auch am Ausweis stehen, am Smartphone angezeigt werden. Diese Kontrolle beschränkt sich aber auf den Vergleich der ausgelesen Daten am Smartphone mit denen des Ausweises.

Ausstellung von Dokumenten. Diese Beispiele zeigen, dass die Sicherheitsanforderungen bei physischen Identitätsdokumenten laufend optimiert werden, um Fälschungen weitestgehend zu verhindern. Ein weiterer Aspekt im Identitätsmanagement ist der Ausstellungprozess von Identitätsdokumenten und Ausweisen. Die Erstausstellung von Identitätsdokumenten und die damit verbundene Identitätsüberprüfung sind wesentlich, da die Echtheit von Ausgangsdokumenten wie beispielsweise Geburtsurkunden oft schwer zu überprüfen ist.

Bei der Konferenz in Riga wurde darüber diskutiert, ob der Staat für die Ausstellung von Identitätsdokumenten zuständig sein soll oder

Fingerscan: Biometrische Identifikationssysteme ermöglichen eine rasche Identitätsfeststellung.

ob diese Aufgabe an Privatunternehmen delegiert werden kann und ob eine Standardisierung von Ausgangsdokumenten auf europäischer Ebene angedacht werden sollte. Gesicherte Identifizierungen werden nur durch zentrale Register ermöglicht, die allen betroffenen Behörden zugänglich sind.

Beispielsweise hat Österreich zentral geführte Personenregister wie das zentrale Melderegister, das Identitätsdokumentenregister und das Personenstandsregister.

Bei Identitätsüberprüfungen kann von der jeweiligen Behörde auf die Identitätsdaten zugegriffen werden, was bei Ausstellungen von Dokumenten einen wesentlichen Sicherheitsaspekt darstellt. Hier gibt es unter den europäischen Ländern noch beträchtliche Unterschiede, da es oft nur dezentral geführte Datenbanken gibt und somit kein übergreifender Zugriff der Behörden auf die Identitätsdaten möglich ist.

Manche Länder verarbeiten und speichern für Identitätsfeststellungen zusätzliche Daten zu einer Person. In Schweden wird zur eindeutigen Zuordnung einer Person zu ihrer Identität schon bei der Geburt bei den ersten Blutuntersuchungen ein geringer Teil des erlangten biologischen Materials im jeweiligen Krankenhaus asserviert, um hier bei Zweifeln jederzeit die biologische Abstammung und Identifizierung eruieren zu können. Diese Aufbewahrung beinhaltet nicht die sofortige Auswertung eines DNA-Profils, sondern nur eine dauerhafte Asservierung, die im Bedarfsfall auch für andere Zwecke genutzt werden darf (z. B. zur Identifizierung von Opfern nach Naturkatastrophen).

Vor allem im Asylwesen ist eine eindeutige Identitätsfeststellung oft nur schwer möglich. Eine große Anzahl der Asylantragsteller kann oder will seine Identität nicht durch staatliche Dokumente aus dem Heimatland nachweisen. Durch die Asylantragsstellung wird so meist eine „neue“ Identität geschaffen.

Die eindeutige Zuordnung der Person zum Identitätsdokument ist ein wichtiger Baustein bei der Verhinderung von Identitätsmissbrauch. Ein Identitätsdiebstahl unter missbräuchlicher Nutzung von Personaldaten einer existierenden Person kann für das Opfer unangenehme und schwerwiegende Folgen haben.

Ein sicheres Identitätsmanagement trägt dazu bei, Kriminalität, Terrorismus sowie Asylmissbrauch besser vorzubeugen und zu bekämpfen. Grundtenor bei der Konferenz war, dass ein Identitätsmissbrauch durch gefälschte Dokumente nur durch Erreichen einer möglichst umfangreichen Nutzung und Verknüpfung von biometrischen Daten in Form von Fingerabdrücken und Lichtbildern mit den Personaldaten verhindert werden kann.

Elektronische Prozesse. Der Trend geht in Richtung Nutzung der Identitätsdokumente zur Identitätsüberprüfung auch in elektronischen Prozessen. Das erleichtert den Reiseverkehr und vereinfacht Kontrollen beim Grenzübertritt (automatisierte Identitätsüberprüfung).

Einfachstes Beispiel ist die Überprüfung der maschinenlesbaren Zone (MRZ – gemäß den Bestimmungen der ICAO-Richtlinie) bzw. das Auslesen der Daten vom Chip (Gesichtsbild, Fingerabdrücke u. a.) bei der Kontrolle von Reisedokumenten bei der Ein- bzw. Ausreise. Dabei wird auch kontrolliert, ob der Chip im Reisepass rechtmäßig ausgestellt wurde. In naher Zukunft könnte die Verifikation der Fingerabdrücke mit den im Reisepass gespeicherten Daten erfolgen. Zum Beispiel benötigen seit 1. April 2016 alle, die unter dem Visumfreiheitsprogramm (für 90 Tage oder weniger) in die USA reisen, einen biometrischen Reisepass (mit Chip).

Auch der „Printed Code“ auf ID-Cards kann bei elektronischen Prozessen Verwendung finden, da dieser auf Papierdokumente gedruckt werden kann und diese Dokumente in unterschiedlichen Verfahren somit eindeutig der jeweiligen Person zuordenbar sind.

Identitätsfeststellung. Auf der „Secure Identification“ stellten die unterschiedlichen Anbieter auch aktuelle technische Lösungen zur Identitätsfeststellung vor. Systeme die das automati-

FOTO: WWW.SECUREIDENTIFICATION.LV

sierte Auslesen von Reisepässen, deren Authentizitätsprüfungen oder eine genaue Untersuchung von Sicherheitsfeatures am Dokument ermöglichen und zusätzlich ein Referenzsystem für die detaillierte Beschreibung von unterschiedlichen Identitätsdokumenten wie Pässe oder Personalausweise verschiedener Länder beinhalten. Durch Systeme zur biometrischen Identifikation von Fingerabdrücken, Iris-Scan, Gesichtserkennung, Spracherkennung oder Handvenenscanner sind rasche Abwicklungen bei Identitätsfeststellungen möglich und können in die jeweiligen Prozesse integriert werden.

Es wurden auch innovative Lösungen in Teilbereichen des Airport-Managements vorgestellt, die 2015 auch schon bei einigen Flughäfen umgesetzt wurden, wodurch der Passagier ohne Vorweisen von Dokumenten und Interaktion mit Behörden oder Flughafenpersonal den Flughafen passieren kann. Die Zugangskontrolle ist somit ein rein elektronischer Prozess. Der Passagier braucht nur seine Boardingkarte beim Terminal einzuscannen, seine Identität wird über biometrische Daten wie der Gesichtserkennung automatisch überprüft.

„Secure Identification“: Bei der internationalen Konferenz waren mehr als 200 Teilnehmer aus unterschiedlichen Ländern sowie an die 30 Unternehmen vertreten.

Elektronische Identitäten. Traditionelle Ausweise werden nach wie vor in zahlreichen europäischen Ländern ausgegeben. In den meisten Ländern gibt es Konzepte oder Projekte, die staatliche Verantwortung im Bereich physischer Identitäten auch um elektronische Identitäten (E-ID) zu ergänzen. Durch das Vordringen der Digitalisierung in allen Lebensbereichen und die sich daraus ergebende Notwendigkeit einer eindeutigen, einheitlichen elektronischen Identifikationsmöglichkeit für Benutzer werden in den jeweiligen Ländern neue sichere Identitätsmanagementlösungen notwendig.

Grundsätzlich versteht man unter einer E-ID die elektronische Transaktion zur sicheren und eindeutigen Identifizierung und Authentifizierung von Personen gegenüber Geschäftspartnern oder anderen Personen (z. B. über das Internet). Dies erfolgt in der Informationstechnologie durch digitale Datensätze, die über Verknüpfung von Identitätsmerkmalen (Attribute) wie beispielsweise durch Name, Geschlecht, Augenfarbe, Körpergröße, Geburtsdatum oder Wohnadresse erreicht werden. Die Selbstbestimmung des Bürgers über die mögliche Weitergabe seiner ID-Daten (Attribute) in elektronischen Prozessen und die Transparenz hinsichtlich der Datennutzung muss gewährleistet sein. Das bedeutet auch, dass Rechtssicherheit und Schutz der Privatsphäre durch staatlich garantierte elektronische Identitäten gegeben ist. Auch auf europäischer Ebene wird die Weiterentwicklung der elektronischen Identitäten forciert.

Elektronische Identität: App ersetzt physische Ausweise.

Die eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen stellt die Einbindung der unterschiedlichen E-ID-Bemühungen der unterschiedlichen EU-Staaten in den EU-Binnenmarkt sicher. Diese enthält Bestimmungen betreffend die elektronische Identifizierung, signaturrechtliche Bestimmungen wurde mit 1. Juli 2016 wirksam.

Ausweise am Smartphone. Auf der „Secure Identification“ in Riga wurden mehrere Projekte vorgestellt, die im Bereich der elektronischen Identitäten Entwicklungspotenziale veranschaulichen. Mit *MIA (My Identity App)* wurde ein System eines österreichischen Unternehmens für ein integriertes Identitätsmanagement in der digitalen Welt vorgestellt.

MIA integriert verschiedene Ausweisdokumente in einer App am Smartphone. Der Ausweis (beispielsweise Führerschein oder Personalausweis) kann am Smartphone angezeigt werden. Die physischen Ausweise brauchen künftig nicht mehr mitgeführt zu werden; die gesetzliche Grundlage dazu fehlt aber noch. Am Smartphone sind keine persönlichen Daten gespeichert. Die Daten werden bei den jeweiligen zentralen Datenbanken in Echtzeit abgefragt. Dadurch lässt sich die Echtheit immer zweifelsfrei feststellen. Der Zugang zur Nutzung der Identitäts-App ist auch durch biometrische Identifikation möglich.

MIA verwendet den neuen Standard der internationalen *FIDO*-Allianz *(Fast IDentity Online)* gegen unsichere Passwörter *(FIDO* ermög-

FOTO: MIA, WWW.SECUREIDENTIFICATION.LV

Der österreichische Reisepass ist mit einem kontaktlosen Chip ausgestattet.

licht eine Mehrfaktorauthentifizierung zur Identifikation wie Fingerabdruck oder USB-Token). Derzeit gibt es noch kein Umsetzungsprojekt.

E-Residency. Estland geht einen Schritt weiter. Im Dezember 2014 initiierte die estnische Regierung das *E-Residency*-Programm. Es bietet für jeden Bürger weltweit (unabhängig der Nationalität) eine amtliche, grenzüberschreitende elektronische Identität (E-ID) und die Möglichkeit, online eine Firma zu betreiben (standortunabhängiges Online-Geschäft).

Mit der Registrierung der estnischen *E-Residency* ist weder eine Staatsbürgerschaft, eine Aufenthaltserlaubnis noch ein Recht auf Einreise nach Estland oder in die EU verbunden. Es geht hier rein um die Nutzung der E-ID im digitalen Raum mit einer estnischen elektronischen Identität. Der Antrag zu *E-Residency* kann online über *e-resident.gov.ee* getätigt werden.

Zur Ausstellung der ID-Card ist jedoch einmalig ein persönlicher Kontakt in einer Auslandsvertretung (Botschaft, Konsulat) in 35 Ländern weltweit oder bei Servicestellen der Polizei und des Grenzschutzamtes in Estland notwendig. Dies dient zur eindeutigen Identitätsfeststellung des Antragstellers. Die ID-Karte enthält kein Foto, jedoch einen Chip mit zwei Sicherheitszertifikaten. Eines wird für die Authentifizierung und das zweite für die digitale Signatur verwendet.

Die ID-Karte ermöglicht jedem *E-Recidency*-Teilnehmer eine sichere digitale Authentifizierung und das rechtsgültige digitale Signieren von Dokumenten. Um die ID-Karte nutzen zu können, wird ein entsprechender E-Card-Reader benötigt, der über USB mit dem Computer verbunden ist.

E-Residency wurde gestartet, um Estland „größer" zu machen. Durch die digitale Wirtschaft und der großen Anzahl an Kunden sollen Innovationen gefördert und Investitionen angezogen werden.

Das Ziel von Estland ist bis zum Jahr 2020 rund zehn Millionen *E-Residents* zu haben. Bis Mai 2016 haben sich bereits über 10.200 Menschen aus 129 Ländern weltweit bei E-Residency registriert. Über 500 E-Residency-Teilnehmer haben ein Online-Unternehmen gegründet. Die *E-Residency*-Plattform wird laufend weiterentwickelt, um den neuen Anforderungen gerecht zu werden und um weitere Services im digitalen Wirtschaftsraum zu ermöglichen.

Manfred Stopfer

Foto: OESD