Virtuelle Behördengänge in der Schweiz und in Deutschland – Unterschiede zwischen SuisseID und deutschem Personalausweis

Rolf Günter, Dirk Arendt, Thomas Koch

Ein Grossteil der Internetnutzenden kommuniziert heute online mit Behörden. Bürgerinnen und Bürger können sich über Politikfelder informieren, amtliche Formulare herunterladen oder online Termine vereinbaren. Der virtuelle Behördengang mit einer kompletten elektronischen Verfahrensabwicklung zwischen Bürgern und der öffentlichen Verwaltung wird aber immer noch kaum genutzt. Grund dafür ist, dass nur wenige Bürger einen wirklich eindeutigen Identitätsnachweis in der Onlinewelt erbringen können. Viele Bürger und Behörden trauen den eID-Möglichkeiten nicht. Dabei gibt es sowohl in der Schweiz als auch in Deutschland eID-Tokens, die sicher und von Behörden und Unternehmen anerkannt sind. In Deutschland ist das der neue Personalausweis, in der Schweiz die SuisseID.

Rolf Günter
Head Business Development
PDF Tools AG
rolf.guenter@pdf-tools.com

Dirk Arendt
Vice President Business Development
& Corporate Communications
OpenLimit SignCubes AG
dirk.arendt@openlimit.com

Thomas Koch
Manager Corporate Communications
OpenLimit SignCubes GmbH
thomas.koch@openlimit.com

In Deutschland verleiht seit dem 1. November 2010 der neue Personalausweis den Bürgerinnen und Bürgern die Möglichkeit, ihre Identität elektronisch nachzuweisen. Der nur noch scheckkartengrosse Ausweis hat einen Security Controller, auf dem alle aussen aufgedruckten Daten (Name, Alter, Wohnort usw.) digital abgelegt werden können. Die neue Karte eignet sich damit auch im Internet als sicheres Ausweisdokument. Voraussetzung ist, dass der Bürger die vom Bundesministerium des Innern bereitgestellte ID-Management-Software-AusweisApp auf seinem PC oder Mac installiert und ein zertifiziertes Kartenlesegerät angeschlossen hat.

Neuer Personalausweis hat sehr hohes Sicherheitsniveau

Der neue Ausweis genügt den höchsten Datenschutzansprüchen. Das bestätigten zuletzt Studien des Hasso-Plattner-Instituts in Potsdam und der Ruhr-Universität Bochum. Der Ausweis wird dem Grundrecht auf informationelle Selbstbestimmung gerecht, wonach jede Bürgerin, jeder Bürger selbst entscheidet, wer in welcher Situation Daten über ihre beziehungsweise seine Person erhält. Durch die neuartige Sicherheitsinfrastruktur und die konsequente Einbeziehung von Datenschützern in allen Projektphasen werden einerseits Datendiebstähle um ein Vielfaches erschwert und andererseits die Qualität der erhobenen Daten deutlich erhöht.

AusweisApp als Gateway für sicheren Datenaustausch

Die AusweisApp ist die Anwendungssoftware für den neuen Personalausweis. Die Software ermöglicht es dem Inhaber des Ausweisdokuments, sich vom heimischen Computer aus über das Internet auszuweisen. Das Bundesministerium des Innern (BMI) stellt die AusweisApp allen Bürgerinnen und Bürgern kostenlos zur Verfügung. Deutschland verfolgt mit der eID einen Middleware-Ansatz. Die AusweisApp als eID-Client sorgt im Zusammenspiel mit dem eID-Server dafür, dass die auf dem Ausweis gespeicherten, persönlichen Daten sicher und verschlüsselt übertragen werden. Dabei baut das EAC(Extended Access Control)-Protokoll einen kryptografisch gesicherten Tunnel vom neuen Personalausweis bis zum eID-Server auf. Sowohl die AusweisApp als auch der eID-Server verwenden für die Kommunikation Protokolle, die in der technischen Richtlinie des deutschen Bundesamtes für Sicherheit in der Informationstechnik TR-03112 (eCard-API-Framework) beschrieben sind.

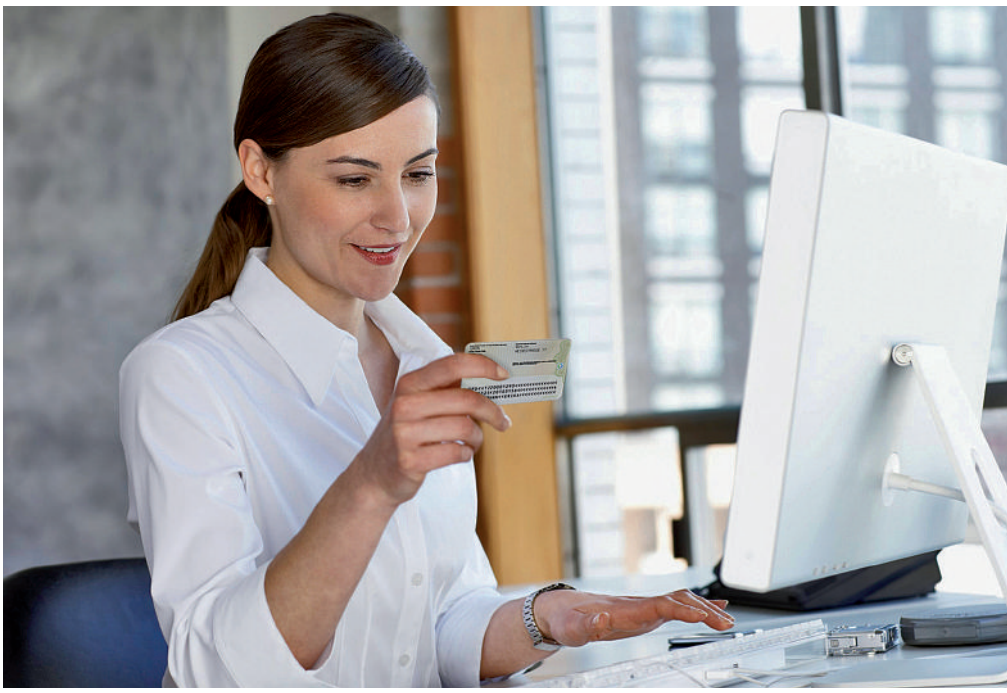
Die Kernfunktion der AusweisApp ist die Onlineauthentisierung mit dem neuen Personalausweis. Weiterhin zeigt die AusweisApp Informationen über den Dienstanbieter an, der Daten vom Ausweis auslesen möchte. Über das Programm kann ausserdem die PIN des Personalausweises geändert werden. Die AusweisApp läuft auf den gängigsten Betriebssystemen und Browsern.

Der eID-Server schafft digitales Vertrauen

Der eID-Server ist das Bindeglied zwischen AusweisApp und Website, also zwischen dem Bürger und dem Anbieter eines Onlinedienstes. Er ist die vertrauensstiftende Instanz in einem Identifizierungsprozess mit dem neuen Personalausweis über das Internet. Der eID-Server überprüft, ob der Dienstanbieter Daten vom Personalausweis abfragen darf und ob der Ausweis echt ist oder als gestohlen gemeldet wurde. Um die persönlichen Daten bei der Übermittlung vertraulich zu behandeln, verschlüsselt und signiert der eID-Server die Daten. Der eID-Server wird als logisch eigenständiger Server realisiert, sodass er von mehreren Webanwendungen genutzt werden kann. Er ist mandantenfähig und kann als Service weitervermietet werden.

Wenn eine Behörde einen bestimmten Verwaltungsakt mit elektronischer Identifizierung über den neuen Personalausweis anbieten will, sind drei Schritte notwendig. Erstens benötigt sie die Berechtigung zum Zugriff auf Datenfelder vom Personalausweis. Dafür reicht sie

beim Bundesverwaltungsamt (BVA) einen Antrag ein, in dem sie erklärt, welche Datenfelder sie zu welchem Zweck auslesen will. Mit der Berechtigungsurkunde vom BVA lässt sich die Behörde in einem zweiten Schritt von einem Zertifikatsanbieter bzw. Trust-Center ein sogenanntes Berechtigungszertifikat ausstellen. Für den technischen Umgang mit diesen Zertifikaten ist der eID-Server zuständig. Die Behörde muss einen eID-Server in ihren Onlinedienst einbinden – das ist der dritte Schritt. Dazu mietet sie sich bei einem Serviceprovider einen eID-Service, oder sie betreibt den eID-Server selber. Wer einen eID-Server betreiben will, muss die technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik einhalten. Dazu gehört neben dem Betrieb des Servers an einem gesicherten Standort auch der Einsatz eines hardwarebasierten Sicherheitsmoduls, das jeglichen, auch physischen, Zugriff von aussen verhindert. Entscheidet sich die Behörde dazu, einen eigenen eID-Server in ihrem Rechenzentrum aufzubauen, kann sie den eID-Service an andere kommunale oder städtische Einrichtungen weitervermieten.



SuisseID setzt auf zertifikatsbasierte Lösung

Die SuisseID wurde im Mai 2010 lanciert. Sie ist der erste standardisierte elektronische Identitätsnachweis der Schweiz, mit dem sowohl eine rechtsgültige elektronische Signatur wie auch eine Authentifizierung möglich sind. Im Gegensatz zum neuen deutschen Personalausweis wird die SuisseID nicht als Teil einer hoheitlichen Identitätskarte, sondern als zertifikatsbasierte Chipkarte oder USB-Stick ausgegeben. Auf dem Trägermedium befinden sich ein qualifiziertes Signaturzertifikat (SuisseID QC) konform zum Schweizer Bundesgesetz über die elektronische Signatur ZertES und ein standardisiertes Authentisierungszertifikat (SuisseID IAC). Im ZertES sind die technischen und organisatorischen Rahmenbedingungen von rechtsverbindlichen elektronischen Unterschriften geregelt.

Jede Schweizer Bürgerin und jeder Schweizer Bürger hat die Möglichkeit, ein oder mehrere SuisseID-Tokens zu beantragen. Die Ausgabe erfolgt nicht vom Staat, sondern von privatwirtschaftlichen Akteuren. Während in Deutschland in zehn Jahren jeder Deutsche eine eID besitzt, da der Personalausweis obligatorisch ist, hängt die Verbreitung der eID in der Schweiz stärker von den Use Cases ab. Durch die unterschiedlich geregelte Verbreitung beantragen Bürger die SuisseID nur, wenn sie einen konkreten Nutzen von den Anwendungen, beispielsweise auf einer Unternehmenswebsite oder einem Behördenportal, haben. Durch den privatwirtschaftlichen Ansatz ist die SuisseID aber dynamischer als der deutsche eID-Ansatz.

Unterschiedliche Datenschutzansätze in Deutschland und der Schweiz

Das Authentifizierungszertifikat, mit dem die SuisseID arbeitet, enthält aus datenschutzrechtlichen Gründen so wenig personenbezogene Attribute wie nötig. Die Integration und Nutzung der Identifikationsnummer ist freiwillig. Die Entwickler der schweizerischen eID-Variante haben die SuisseID-Nummer eingeführt, damit Onlinedienste die Nutzerinnen und Nutzer unabhängig von der Lebensdauer des Zertifikates und eineindeutig wiedererkennen können. Die SuisseID-Nummer besteht aus einer 16-stelligen Nummer, die bei der Ausgabe einer spezifischen Person zugeordnet wird. Der Inhaber des SuisseID-Tokens kann sich mit der Nummer bei allen Onlinediensten authentifizieren, die eine nummernbasierte Anmeldung unterstützen. Dies kommt einem hardwarebasierten Log-in gleich, das Name und Passwort ersetzt. Um eine Profilierung und ein Tracking von Nutzern auf der Basis der SuisseID-Nummer zu vermeiden, ist es in der Schweiz möglich und angeraten, dass eine Person mehrere SuisseID-Zertifikate mit unterschiedlichen SuisseID-Nummern beantragt und auch nutzt.

Deutschland hat hier einen anderen Ansatz gewählt. Die Konzepte «Datensparsamkeit» und «dezentrale Datenhaltung» waren für die Entwicklung des neuen elektronischen Personalausweises handlungsleitend. Angesichts der enormen Zahl von personenbezogenen Daten, die in der elektronischen Geschäftswelt im Umlauf sind (z.B. rund 21 Millionen Bankkundendaten), kommt der Datensparsamkeit eine hohe Bedeutung zu. Die Datensparsamkeit ist ein Herzstück des Datenschutzes und soll das Grundrecht der informationellen Selbstbestimmung gewährleisten. Datensparsamkeit meint, dass zweckgebunden nur die nötigsten personenbezogenen Daten gesammelt werden. Bei einer Personalausweisabfrage kann ein Dienstanbieter künftig so nur jene personenbezogenen Daten anfordern, die für den jeweiligen Dienst unbedingt erforderlich sind. Speichern darf er diese punktgenauen Daten nur nach vorheriger Zustimmung durch die Bürgerin oder den Bürger.

Dem gegenüber steht das Prinzip der Vorratsdatenspeicherung. Diese zielte in

Deutschland ursprünglich auf die Verpflichtung der Anbieter von Telekommunikationsdiensten ab, sämtliche elektronische Kommunikationsvorgänge zu speichern, ohne dass ein Anfangsverdacht oder eine konkrete Gefahr für die beteiligten Kommunikationspartner bestand. Das Gesetz zur Vorratsdatenspeicherung sah vor, vorsorglich die Verbindungsdaten aller Personen für einen Zeitraum von sechs Monaten zu speichern. Telefondaten wurden seit Anfang 2008 gespeichert, die Internetnutzung seit 2009. Die Vorratsdatenspeicherung steht somit im Widerspruch zur informationellen Selbstbestimmung. Der Personalausweis hat nichts mit Vorratsdatenspeicherung zu tun, da die persönlichen Daten hier dezentral auf dem Chip der Karte gespeichert werden.

Ein Tracking der Spuren, die ein Nutzer mit seinem Personalausweis im Netz hinterlässt, wird in Deutschland dadurch vermieden, dass pro Dienstanbieter eine spezifische Kennnummer errechnet wird. Jeder Ausweis hat eine bestimmte Nummernkombination, genau wie jeder Anbieter einer Onlinedienstleistung auch eine bestimmte Kennnummer hat. Diese beiden Zahlenkombinationen werden zu einem eineindeutigen Schlüssel verrechnet. Dadurch ist es möglich, den Nutzer bei der Anmeldung auf einer Website ohne die Übermittlung von zusätzlichen Daten nur anhand der Ausweiskarte eindeutig wiederzuerkennen. Nicht möglich ist aber, Daten von verschiedenen Onlineapplikationen zusammenzuführen und von einem Bürger oder einer Bürgerin ein Nutzerprofil zu erstellen. Der Bürger hat den Vorteil, dass er dafür nicht mehrere ID-Tokens beantragen muss, sondern sich quasi «anonym» mit einer Karte im Internet bewegt.

Identity-Provider stellen zusätzliche persönliche Attribute zur Verfügung

Da die Schweizer Lösung mit Minimalattributen auf dem Trägermedium arbeitet, sind Identity-Provider integraler Bestandteil des Konzepts als auch der eID-Infrastruktur der SuisseID. Wenn der Inhaber einer SuisseID einen bestimmten Onlinedienst in Anspruch nehmen will, der zusätzliche, personenbezogene Attribute wie das Alter oder den Wohnort nachfragt, können diese Daten unter Einbezug eines SuisseID-Identity-Providers an den Dienstanbieter übermittelt werden. Dafür muss der SuisseID-Inhaber diese Attribute vorher bei einem Identity-Provider ablegen. Dazu muss er persönlich, also physisch, bei einem der schweizerischen Identity-Provider vorstellig werden. Der ID-Provider validiert die Daten und übernimmt die Verantwortung für ihre Gültigkeit. Jetzt kann er sie bei einer elektronischen Anfrage dem SuisseID-Inhaber zur Verfügung stellen. Die Übermittlung der zusätzlichen Daten erfolgt nur nach der expliziten Zustimmung durch die Bürgerin oder den Bürger.

Das Identity-Provider-Modell hat den Vorteil, dass Personalattribute theoretisch in unbegrenztem Umfang einer Person zugeordnet werden können. Attribute wie die Berufsbezeichnung, Firmenzugehörigkeit, Zeichnungsberechtigung könnten von Providern wie Kammern, Verbänden oder Behörden zur Verfügung gestellt werden. Auf diesem Wege kann eine Person je nach Anwendungsfall zweckgebunden vertrauenswürdige Attribute elektronisch übermitteln. Der Schlüssel zu den zusätzlichen Attributen ist immer das ID-Token SuisseID oder der Personalausweis.

In Deutschland sind Identity-Provider nicht von vornherein vorgesehen. Auf dem kontaktlos auslesbaren RFID-Chip im deutschen Personalausweis befinden sich alle Datenfelder, die auch aussen auf der Karte aufgedruckt sind. Dienstanbieter können beim BVA eine Berechtigung für den Zugriff auf die Daten des Personalausweises einholen. Diese Auslesebeberechtigung müssen sie dem Ausweisinhaber jedes Mal vor dem Zugriff präsentieren (gegenseitige Authentifizierung). Sie können diejenigen Datenfelder abfragen, die zur Zweckerfüllung ihres Onlinedienstes erforderlich sind. Andere Datenfelder können nicht ausgelesen werden. Der Inhaber des Ausweises kann also je nach Anwendungsfall per Mausklick einzeln Attribute am Bildschirm an- und abwählen. Vor der Übermittlung gibt er die Daten noch per Eingabe der PIN frei. Da auf der Ausweiskarte keine Verschlüsselungszertifikate abgelegt sind, gibt es bereits erste Anbieter, die dieses zusätzliche «Attribut» in Verbindung mit dem Personalausweis anbieten wollen.

Auch im Gesundheitsbereich könnten mithilfe von Identity-Providern viele Anwendungsfälle jetzt schon realisiert werden, ohne dass auf die Ausgabe einer elektronischen Gesundheitskarte gewartet werden muss. Wenn Ärztekammern vertrauenswürdig zusätzliche Attribute zur Verfügung stellen und der Patient mit seiner eID gewissen Prozessen zustimmt, steht E-Health-Anwendungen wie dem elektronischen Rezept, der Patientenakte oder telemedizinischen Angeboten eigentlich nichts mehr im Wege.

Erfolgsfaktoren beider Projekte

Kritiker werfen den Verantwortlichen für die SuisseID und für den neuen deutschen Personalausweis vor, die Bürgerinnen und

Bürger zu wenig über die Vorteile, Anwendungsbereiche und Risiken zu informieren. Viele Bürger fühlen sich deshalb – das zeigen qualitative Umfragen nach dem Start beider eID-Projekte – nicht richtig angesprochen. Die fehlende Kommunikation könnte zum Hemmschuh werden. Bei einem Übergewicht an negativer Presse ist gar ein Scheitern möglich. Als einer der wesentlichen Erfolgsfaktoren wird es zukünftig darauf ankommen, schnellstmöglich Vertrauen bei den Nutzern zu schaffen. Die potenziellen Anwenderinnen und Anwender müssen verstehen, warum sie die eID einsetzen sollen. Die Vorteile müssen klar kommuniziert werden. Daher ist eine umfassende Informationskampagne zwingend erforderlich! Noch reden nur die Experten in kleinen und geschlossenen Arbeitsgruppen über diese Themen. Da es alle angeht, müssen alle Bürgerinnen und Bürger den Ansatz und die Notwendigkeit der Themen verstehen. Hier gilt es zu überzeugen, Verständnis, Transparenz und Glaubwürdigkeit zu schaffen, plakative Lösungen aufzuzeigen und durch glaubhafte Kommunikation Vertrauen in diese neuen Instrumente zu gewinnen.

Weiterhin ist es als sehr wichtig zu erachten, dass alle zukünftigen Gesetzesvorhaben, die die Abwicklung elektronischer Prozesse betreffen und eine Authentifizierung notwendig machen, sich einer Prüfung bezüglich der eID-Konformität unterziehen. Darüber hinaus sollten bestehende Gesetze und Verordnungen dahin gehend überprüft werden, ob die Verfahrensabwicklung auch per eID über das Internet möglich ist. Besonders in kommunalen Massenverfahren wäre dies umsetzbar, so zum Beispiel im Meldewesen, Strassenverkehrswesen, Führerscheinwesen, Katasterwesen, Steuerwesen und Bauwesen. Eine sichere elektronische Identifizierung kann sowohl in Verfahren zwischen Bürgern und Verwaltung als auch zwischen Wirtschaft und Verwaltung und ausserdem in verwaltungsinternen ressortübergreifenden Verfahren die Prozessketten erheblich vereinfachen und deren Kosten reduzieren. Kommunen werden von den neuen Möglichkeiten der elektronischen Identifizierung profitieren. Der Wegfall langer Wege zu und Wartezeiten in den Ämtern erhöht die Effizienz kommunaler Dienstleistungen. Die Verwaltung lebt komfortable und schlanke Prozesse und zeigt sich offen gegenüber dem Einsatz neuer Technologien, was sich speziell bei den jüngeren und internetaffineren Bürgerinnen und Bürgern positiv auf das Image der Behörden auswirkt. Die elektronische Identifizierung legt einen Grundstein für Formen der E-Partizipation und E-Collaboration. Bei der Planung einer Umgehungsstrasse könnten zukünftig beispielsweise mehrere gesellschaftliche Gruppen online eingebunden werden, die gemeinsam und transparent die Entscheidung über die Streckenführung vorbereiten. Noch fehlt es an klaren Konzepten, wie Bürgerinnen und Bürger mit Web-2.0-Anwendungen und sicheren Identifizierungsformen in die Arbeitsabläufe der kommunalen Verwaltung eingebunden und wie auch die Mitarbeitenden in den Verwaltungen mitgenommen und aktiv beteiligt werden können. Laut einer aktuellen Studie des E-Government-Netzwerkes Amt24 und der Universität Potsdam nutzen bereits heute 63% der Verwaltungsangestellten in Berlin und Brandenburg Web-2.0-Anwendungen.

SuisseID und Personalausweis als nationale Insellösungen?

Neben der Schweiz und Deutschland haben mehrere europäische Länder eigene eID-Infrastrukturen aufgebaut. Da Europa immer weiter zusammenwächst und es in der digitalen Welt im Grunde genommen keine Nationalgrenzen gibt, kommt der Interoperabilität der einzelnen nationalen Lösungen eine grosse Bedeutung zu. Zwischen Deutschland und der Schweiz herrscht traditionell ein reger Austausch an Arbeitskräften, Waren, Dienstleistungen, Kapital usw. So sollte frühzeitig darüber nachgedacht werden, ob SuisseID und Personalausweis auch gemeinsam funktionieren können. Aus Sicht des Bürgers müsste dies bedeuten, dass er sich unabhängig davon, ob er eine SuisseID oder einen deutschen Personalausweis besitzt, bei gewissen Internetanwendungen, beispielsweise in einem Onlineshop eines deutschen Händlers, mit seinem eID-Token authentifizieren kann. Dazu sollten jetzt Pilotprojekte gefunden und aufgesetzt werden, die eine bilaterale Integration der Ansätze zum Ziel haben.

Darüber hinaus wäre es sehr zu begrüssen, wenn die SuisseID Teil oder Partner des EU-Projektes STORK (Secure Identity Across Borders Linked) werden könnte. STORK hat zum Ziel, im Rahmen des IKT-Förderprogramms der Europäischen Union eine EU-weite Plattform für die Interoperabilität von elektronischen Identitäten einzuführen. EU-Bürgerinnen und -Bürger sollen ihre nationalen eIDs für E-Government-Dienste in mehreren europäischen Ländern nutzen können. Nationale Insellösungen werden auf Dauer keinen Erfolg haben. Deshalb kommt es darauf an, international einheitliche Richtlinien für eID herauszubilden.