BUNDESDRUCKEREI

eID-SERVICE POCKETGUIDE 2011

Der neue Personalausweis
Meine wichtigste Karte.

INHALT

KAPITEL 1
IDENTITÄTSMANAGEMENT IM 21. JAHRHUNDERT

Damit hatte sie nicht gerechnet. Ein simpler Trick hatte ausgereicht: Über eine fiktive Mailadresse, zusammengesetzt aus dem Namen und dem Geburtsdatum des Opfers, hatten die Betrüger monatelang kostspielige Bestellungen bei Versandhändlern aufgegeben.

Zahlreiche Mahnschreiben landeten im Briefkasten der um ihre Identität Betrogenen, einer Journalistin der Wochenzeitung „Die Zeit". Es kostete sie Wochen, mithilfe eines spezialisierten Anwalts den Irrtum bei Auskunfteien und Behörden aufzuklären. „Kafka hätte es nicht besser beschreiben können", so die Autorin in ihrem Artikel über den Identitätsdiebstahl.[1] Ihr Geburtsdatum und ihre Berufsbezeichnung wie früher in sozialen Netzwerken preiszugeben, kommt heute nicht mehr für sie in Frage.

Das Beispiel zeigt, dass auch in Deutschland niemand gefeit ist vor den neuen Formen des Betrugs, die mit dem Internet Einzug in den Alltag gehalten haben. Über elf Millionen US-Amerikaner werden jährlich Opfer ähnlicher Delikte. Die US-Handelsbehörde schätzt, dass so pro Jahr allein in den Vereinigten Staaten Schäden in Höhe von 52 Milliarden Dollar entstehen. Auch in Deutschland versuchen Kriminelle immer häufiger, fremde Identitäten im Netz zu kapern.

Bislang lassen sich die Bundesbürger dadurch die Freude an der Online-Welt nicht verderben: 72 Prozent der erwachsenen Deutschen nutzen das Internet, 42 Prozent kaufen online ein. Laut der Gesellschaft für Konsumforschung lag der bundesdeutsche Umsatz im eCommerce 2009 bei 15,5 Milliarden Euro, so hoch wie noch nie. Gut 70 Prozent der Bürger machen sich allerdings zunehmend Sorgen bei Transaktionen im Netz – sie fürchten, dass auch ihre Identität missbraucht werden könnte.[2]

IDENTITÄTSDIEBSTAHL – WAS IST DAS?

Der Begriff des Identitätsdiebstahls wird in der Fachliteratur unterschiedlich definiert. Meist bezeichnet man damit das „unbefugte Sichverschaffen einer Identität": Ein Täter bringt die Identität einer Person in seinen Besitz, also eine Anzahl an Daten, durch die das Opfer in einem bestimmten Zusammenhang eindeutig bezeichnet wird. Dafür nutzen Betrüger zum Beispiel die Kombination aus Name und Kreditkartendaten, Name und Anschrift oder auch Name und Geburtsdatum.[3] Dem Diebstahl folgt häufig der Missbrauch sich mit der Absicht einen finanziellen Vorteil zu verschaffen oder den Ruf des Opfers zu schädigen. Ungefähr ein Drittel aller Identitätsdiebstähle verüben Betrüger auch heute noch in der realen, physischen Welt, indem sie etwa die Daten eines gestohlenen Personalausweises für eigene Bestellungen missbrauchen. In bereits zwei Dritteln der Fälle besorgen sie sich die Daten für ihre kriminellen Attacken allerdings im Internet – häufig begünstigt durch einen allzu freigiebigen Umgang der Bürger mit ihren Daten. Die Polizei schätzt, dass Opfer von Online-Identitätsdiebstahl im Durchschnitt etwa 400 Arbeitsstunden investieren müssen, um entstandene Schäden zu beseitigen und weiteren Missbrauch zu verhindern.[4]

UNSICHERHEITEN FÜR NUTZER UND ANBIETER

Unabhängig davon, ob der Bürger in der Filiale oder via Internet ein Bankkonto eröffnen will: Er muss sich, wie im Geldwäschegesetz und in der Abgabenverordnung vorgeschrieben, eindeutig identifizieren. Entweder legt er seinen Ausweis beim Kreditinstitut vor oder er nutzt das Postident-Verfahren. Wer im Webshop bestellt, gibt seine Identität preis, wer eine Reise bucht, eine Online-Überweisung tätigt oder ein eGovernment-Angebot abruft, ebenso. Aber auch andere Diensteanbieter, zum Beispiel soziale Netzwerke und Foren, fordern ihre Kunden dazu auf, persönliche Daten und damit ihre Identität im Internet zu offenbaren. Nicht immer sind all diese Daten wirklich nötig für eine Transaktion.

Besonders großen Wert auf Datenschutz, Datensicherheit und zuverlässige Systeme legen die Menschen bei Online-Transaktionen mit staatlichen Stellen. Nur ein Drittel der Anwender bescheinigt behördlichen Angeboten heute allerdings, dass sie gute oder sehr gute Arbeit beim Datenschutz leisten. Viele bemängeln Medienbrüche bei zahlreichen eGovernment-Angeboten: Einen Antrag zwar online herunterladen und ausfüllen zu können, ihn dann aber doch zur Post bringen zu müssen, empfinden die meisten Menschen als lästig. Um sich im Netz vor Betrügern zu schützen, braucht der Anwender heute zudem eine Vielzahl von Benutzernamen, wechselnden Passwörtern und PINs. Reisebuchungen und vor allem das Online-Banking werden so zu aufwändigen Prozessen, bei denen Identitäten und Berechtigungen auf hochkomplexe Weise nachgeprüft werden. Wer rechtsgültige Verträge einfach von zu Hause aus abschließen will, braucht elektronische Signaturkarten und die entsprechende Hard- und Software. Wie anspruchsvoll die Materie ist, belegt allein der Umfang des Signaturgesetzes (SigG), das den rechtlichen Rahmen für elektronische Signaturen absteckt. Vielen Menschen sind solche Verfahren allerdings zu aufwändig. Leicht verlieren sie im Datendschungel den Überblick und machen es Online-Betrügern aus Bequemlichkeit leicht, indem sie als Passwort abwechselnd die Namen von Verwandten oder andere leicht zu erratende Passwörter verwenden.

Umgekehrt fehlen beim eCommerce auch den Anbietern Sicherheiten, zumal die Anschaffung eigener Systeme zur zuverlässigen Identitätsprüfung meist sehr kostspielig ist. Darüber hinaus ist es mit einem sehr hohen Aufwand verbunden, die Systeme zu integrieren. Kein Webshopbetreiber weiß hundertprozentig, ob der junge Mann, der gerade einen Film für Erwachsene bei ihm geordert hat, tatsächlich volljährig ist. Anbieter sind zwar laut Jugendmedienschutz-Staatsvertrag verpflichtet, das Alter ihrer Kunden nachzuprüfen. Ob die eingesandte Personalausweiskopie überhaupt demjenigen gehört, der bestellt hat, lässt sich aber nicht zweifelsfrei verifizieren.

IDENTITÄT ALS GRUNDLAGE

Was ist Identität? Was macht sie aus, was macht einen Menschen unverwechselbar? Solche Fragen, früher allenfalls unter Philosophen diskutiert, werden vor diesem Hintergrund im Internet-Zeitalter brandaktuell. Laut Definition ist Identität die Kombination derjenigen Merkmale, anhand derer sich ein Individuum von anderen unterscheiden lässt. Identität ist nicht zu verwechseln mit den Rollen eines Menschen im Alltag – als Mitarbeiter, Richter oder Arzt etwa, als Vater oder als User mit einem selbst gewählten Fantasienamen im Netz.

Anders als flexible Rollen bildet Identität die Grundlage für Individualität. Sie ist die Basis dafür, dass Bürger Rechte wahrnehmen und Pflichten erfüllen können, im beruflichen wie im privaten Leben. Man benötigt sie, um Steuernummern, Gesundheits- und Sozialleistungen zu beantragen, um in andere Länder zu reisen oder um in internationalen Unternehmen zu arbeiten. Je mobiler der Mensch, je globaler die Wirtschaftsprozesse, desto dringender braucht der Einzelne Sicherheitsmechanismen zum Schutz seiner Identität.

Um eine Identität zu prüfen, sprich eine Person zu authentifizieren, stehen verschiedene Möglichkeiten zur Verfügung: Entweder die Person weist sich über ihr Wissen aus, etwa indem sie einen Code, ein Passwort oder eine Geheimzahl angibt. Oder sie authentisiert sich über den Besitz eines Gegenstands, zum Beispiel eine Karte, die ihr allerdings nur temporär und willkürlich zugewiesen ist. Die dritte Möglichkeit ist die Authentifizierung durch biometrische Daten – körperliche Merkmale, die man weder weitergeben noch vergessen oder verlieren kann.

VOM AUSWEIS ZUR ID-CARD

Herkömmliche Ausweisdokumente stoßen heute an ihre Grenzen: Im Netz ist es unmöglich, eine Identität über die physische Vorlage des Dokuments zu überprüfen. Es reicht nicht aus, eine Ausweiskopie anzufordern oder schlicht darauf zu vertrauen, dass die Security Features traditioneller Identitätsdokumente fälschungssicher sind. Ob jemand derjenige ist, als der er sich ausgibt, muss in einem globalen, mobilen und virtuellen Umfeld auf andere Art verifiziert werden.

Technologien, die ohne physische Prüfung sichere Identitäten gewährleisten, werden damit zu Schlüsseltechnologien für die moderne Gesellschaft. Umso mehr, als das Internet sich weiterentwickelt und neue Trends auftauchen: Cloud Computing etwa ermöglicht es Nutzern, über das Internet auf externe Speicherplätze zuzugreifen – was nur dann gefahrlos ist, wenn Unbefugte sich nicht mit falschen

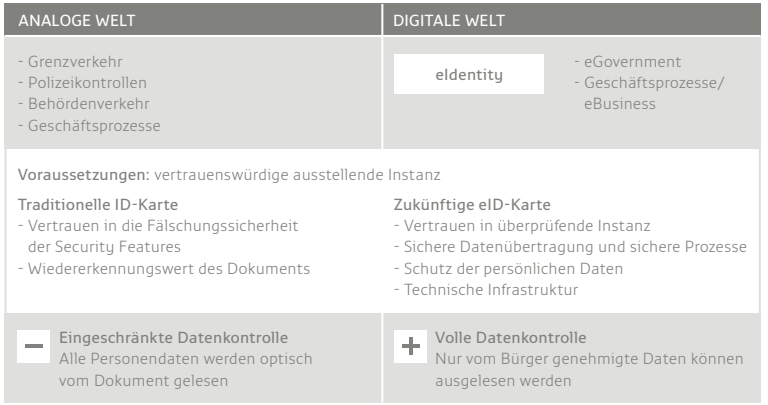
Identitäten Zugang dazu verschaffen können. Für noch mehr Vernetzung und damit einen noch größeren Bedarf an sicheren Identitäten sorgt außerdem der Siegeszug moderner Smartphones. Bereits heute nutzen elf Prozent der Deutschen ein solches Gerät. Im Jahr 2012, so schätzt man, werden mehr als 22 Prozent[5] mithilfe ihres Smartphones weltweit Informationen abrufen.

Rasant verändert sich auf diese Weise auch der Lebensstil der Nutzer: Stets vernetzt zu sein, gilt als Normalzustand. Fast 70 Prozent der Menschen geben an, dass sie täglich im Internet aktiv sind und so gut wie nie ihr Mobiltelefon ausstellen.[6] Umso wichtiger ist es, das Bewusstsein der Bürger für einen sparsamen Umgang mit persönlichen Informationen zu fördern. Herr seiner Daten bleiben und nicht mehr preisgeben als nötig – das ist oberstes Gebot, zumal eine vollständige Daten- und Netzwerksicherheit im World Wide Web niemals gegeben sein wird. Die Mehrheit der Nutzer ist sich dessen bewusst – aber gleichzeitig zunehmend überfordert damit, sich selbst angemessen vor Attacken von Online-Betrügern zu schützen. Nur 37 Prozent verwenden zum Beispiel schwer zu knackende Passwörter und ändern sie regelmäßig.[7]

DEUTSCHLAND ALS VORREITER

Politik, Wissenschaft und Unternehmen der Hochsicherheitsbranche müssen sich dieser Herausforderung gemeinsam stellen und den Bürgern Lösungen fürs Identitätsmanagement anbieten, die leicht zu handhaben sind. 20 Prozent der Weltbevölkerung sind bereits im Netz, was das enorme Marktpotenzial für sichere elektronische Identitäten verdeutlicht. Das weitere Wachstum im eCommerce hängt ebenso wie die Entwicklung des eGovernments entscheidend davon ab, wie gut es gelingt, Identitäten im Internet möglichst einfach und sicher zu verifizieren. Bereits in den vergangenen Jahren hat sich der Weltmarkt für ID-Systeme dynamisch entwickelt. Das Marktforschungsinstitut Pira International prognostiziert, dass der Umsatz mit solchen Karten von 1,4 Milliarden Euro im Jahr 2009 auf rund 3,1 Milliarden Euro im Jahr 2014 steigen wird. Das bedeutet ein jährliches Wachstum von etwa 17 Prozent. Allein in Europa sind in den vergangenen Jahren zahlreiche unterschiedliche Lösungen auf den Markt gekommen. Die derzeit zehn unterschiedlichen ID-Konzepte will die Europäische Agentur für Netz- und Informationssicherheit (ENISA) langfristig im Rahmen einer multinationalen eCard-Strategie harmonisieren.

ABBILDUNG 1: SICHERE ELEKTRONISCHE IDENTITÄT



Deutschland gehört im internationalen Vergleich zu den Vorreitern bei der Entwicklung von ID-Systemen und -Karten. Mit dem 2006 beschlossenen Programm eGovernment 2.0 hat die Bundesregierung schon frühzeitig die Weichen gestellt: Seit dem 1. November 2010 können die Bürger der Bundesrepublik Deutschland mit dem neuen Personalausweis eines der weltweit modernsten Ausweisdokumente nutzen. Wie sich der rechtliche Rahmen für seinen Einsatz gestaltet, ist im Personalausweisgesetz (PAuswG) festgelegt. Die neue ID-Karte dient nicht nur als Sichtausweis. Vielmehr wird sie mit ihrer Online-Ausweisfunktion und der Qualifizierten Elektronischen Signatur (QES) zu einer komplett neuen Qualität von Kommunikations- und Transaktionssicherheit im Internet beitragen. Die Bürger können sich ohne großen Aufwand vor Identitätsdiebstahl schützen.

Einzigartig macht den Ausweis, dass er in ein komplexes und hoch sicheres System eingebunden ist. Zentrale Komponente dieses Systems ist, abgesehen von dem Ausweis selbst, der so genannten AusweisApp, den Berechtigungszertifikaten und Sicherheitsprotokollen, vor allem der eID-Service. Er ermöglicht es Unternehmen oder Behörden, die über entsprechende Berechtigungszertifikate verfügen, die auf dem Chip des Personalausweises gespeicherten Daten auszulesen. In Deutschland dürfen gemäß den im internationalen Vergleich sehr strengen Datenschutzbestimmungen nur Unternehmen, die hohe Auflagen erfüllen, einen eID-Service anbieten. Mit ihrem akkreditierten Trustcenter D-TRUST stellt die

Bundesdruckerei einen leistungsfähigen Service bereit, der viel Erfahrung im Management elektronischer Identitäten besitzt. Statt große Summen in den Aufbau eigener Infrastrukturen investieren zu müssen, können Anbieter ihn nutzen, um ihren Kunden den Weg zu mehr Sicherheit im World Wide Web zu eröffnen.

KAPITEL___2
DER NEUE PERSONAL-AUSWEIS – FAKTEN UND FEATURES

Die Einführung des neuen Personalausweises am 1. November 2010 erregte im Vorfeld große Aufmerksamkeit. Fachleute hatten schon früh darauf aufmerksam gemacht, dass die neue ID-Karte sich als zentrales Instrument für sicheres Identitätsmanagement im Internet anbietet.

Im Juni 2010 gewann das Bundesministerium des Innern (BMI) auf der „European Identity Conference 2010" den „European Identity Award" für das neue ID-Dokument: Damit honorierte die Analystengruppe Kuppinger Cole das „innovative und technisch durchdachte Konzept, das auch Datenschutzbelangen in hervorragender Weise Rechnung trägt". Viele innovationsfreudige Bürger waren neugierig und haben gleich in den ersten Novembertagen das Identitätsdokument im Scheckkartenformat beantragt.

Die Anforderungen an den neuen Personalausweis hat das BMI festgelegt. Für die Produktion und die technische Infrastruktur, in die der Ausweis eingebettet ist, zeichnet die Bundesdruckerei verantwortlich. Sie produziert die Dokumente und stattet auch die

rund 5.500 Pass- und Personalausweisbehörden mit Hard- und Softwarekomponenten aus (zum Beispiel mit Änderungsterminals und Fingerabdruckscannern).

NEUE ANWENDUNGEN

Den neuen Ausweis kann der Bürger für alle Zwecke verwenden, für die er auch seinen Vorgänger einsetzen konnte – dabei ist er noch deutlich vielseitiger. Mit der Online-Ausweisfunktion und der Qualifizierten Elektronischen Signatur (QES) stehen zwei Anwendungen zur Verfügung, die Transaktionen im Netz komfortabler und sicherer machen. Ob und wann der Bürger diese Funktionen verwendet, entscheidet er selbst. Zum ersten Mal gibt es mit dem neuen Personalausweis ein sehr stark verbreitetes standardisiertes Identitätsdokument, mit dem sich der Bürger im Internet zu erkennen geben kann. Zugleich erleichtert es der neue Ausweis dem Nutzer, jederzeit die Kontrolle über die eigenen Daten zu behalten.

Als handliches Dokument im Format einer Scheckkarte ist die neue ID-Karte nach wie vor als so genannter Sichtausweis verwendbar, den man zum Beispiel bei Polizeikontrollen vorzeigt. Das Format ID1 entspricht dem vieler normierter Chipkarten und ist angeglichen an die Größe des europäischen Kartenführerscheins. Dank der Abmessung 86,50 mm x 53,98 mm passt der kompakte neue Ausweis bequem in jede Geldbörse.

Auf der Rückseite ist ein eigens für den Ausweis entwickeltes Logo zu sehen. Die zwei sich ergänzenden Halbkreise stehen dafür, dass die Bürger das Dokument sowohl im realen als auch im virtuellen Umfeld einsetzen können. Gleichzeitig lassen sich die Kreise als Symbol für die Authentisierung deuten, die bei Online-Transaktionen für beide Beteiligten Pflicht ist: Sowohl der Ausweisinhaber als auch der Diensteanbieter oder die Behörde müssen sich eindeutig zu erkennen geben, damit eine Online-Transaktion abgewickelt werden kann.

Wie der alte Personalausweis zählt auch die neue ID-Karte aufgrund ihrer optischen, taktilen und holografischen Merkmale und der verwendeten Sicherheitsprotokolle zu den sichersten Dokumenten der Welt. Feine, ineinander verschlungene Muster, die so genannten Guillochen, sowie Mikroschriften, spezielle Farbeffekte und fühlbare Oberflächenstrukturen machen den Ausweis fälschungssicher.

HERZSTÜCK SICHERHEITS-CHIP

Mit der sechsstelligen Zugangsnummer auf der Vorderseite sowie einem Datenfeld für Postleitzahl und Künstler- bzw. Ordensnamen auf der Rückseite enthält der Ausweis außerdem mehr Informationen als das Vorgängermodell. Herzstück ist der kontaktlose integrierte Sicherheits-Chip mit einer Speicherkapazität von über 100 kB, der tief im Inneren des Dokuments zwischen mehreren Kunststoffschichten liegt. Er ist inklusive Gehäuse nicht einmal 10 mm² groß. Versucht jemand, den Chip zu manipulieren, wird die elektronische Ausweisfunktion unbrauchbar. Das ID-Dokument kann dann nur noch als Sichtausweis dienen.

Auf dem Chip sind alle auf dem Ausweis aufgedruckten Informationen zusätzlich digital hinterlegt:

> Alle auf der Vorderseite des Dokuments verzeichneten Informationen
> Daten der aufgedruckten maschinenlesbaren Zone auf der Rückseite
> Ein digitalisiertes biometrisches Passbild

ABBILDUNG 2: DER NEUE PERSONALAUSWEIS

Damit übertrifft das Sicherheitsdesign des Ausweises unter anderem die Empfehlungen der Internationalen Zivil-Luftfahrtorganisation der Vereinten Nationen (International Civil Aviation Organization, ICAO). Sie rät ausdrücklich dazu, biometrische Daten in ID-Dokumente aufzunehmen, weil diese die eindeutige Identifizierung eines Menschen ermöglichen. Für das Porträtfoto gelten deshalb nun die international standardisierten Passbildvorgaben. Das bis 2010 noch erlaubte Halbprofil ist wie beim ePass nicht mehr zulässig, weil hier die Proportionen weniger gut überprüft werden können.

Auf Wunsch können auf dem Chip zusätzlich die Daten zweier Fingerabdrücke gespeichert werden, um eine noch stärkere Bindung zwischen Pass und Inhaber zu knüpfen. Sie können und dürfen ausschließlich von staatlich autorisierten Instanzen ausgelesen werden. Wer rechtsgültige Verträge im Internet abschließen will, muss für die Qualifizierte Elektronische Signatur außerdem die Informationen so genannter Signaturzertifikate auf der Karte speichern lassen.

AUTHENTISIERUNG IM INTERNET

Die Online-Ausweisfunktion erlaubt es, sich über persönliche Daten wie Name, Adresse und Geburtsdatum im Internet zu erkennen zu geben, ohne dafür mühsam Online-Formulare per Tastatur auszufüllen. Die Nutzung der Funktion ist freiwillig: Bürger über 16 Jahre können sie unkompliziert bei ihrer Meldebehörde an- und ausschalten lassen. Ist sie aktiviert, liest man die Daten per Lesegerät bequem am heimischen PC aus. Welche Information jemand jeweils preisgeben möchte, entscheidet er bei jeder Transaktion per Freigabe durch eine PIN neu.

NUR NACH ZUSTIMMUNG ÜBERMITTELTE DATEN

Diese Informationen muss man ausdrücklich freigeben, damit Diensteanbieter sie auslesen können:

> Familienname, Vorname
> Doktorgrad
> Tag und Ort der Geburt
> Anschrift
> Ordens- oder Künstlername
> Dokumentenart
> Dienste- und kartenspezifische Kennzeichen (Pseudonymfunktion)
> Abkürzung „D" für Bundesrepublik Deutschland (Nationalität)
> Angabe, ob der Inhaber des Ausweises ein bestimmtes Alter über- oder unterschreitet (Altersverifikation)
> Angabe, ob der Inhaber des Ausweises in einem vom Diensteanbieter abgefragten Ort, Regierungsbezirk oder Bundesland gemeldet ist (Wohnortverifikation)

Nur die Angabe, ob ein Personalausweis gesperrt ist, wird standardmäßig an Diensteanbieter im Netz übermittelt. Diese Grundprinzipien helfen dem Bürger dabei, sparsam mit seinen Daten umzugehen und nur die zusätzlichen Informationen anzugeben, die im jeweiligen Fall tatsächlich nötig sind.

Dank der mehrfach verschlüsselten und gesicherten Übertragungswege ermöglicht die Online-Ausweisfunktion damit ein neues Maß an Sicherheit und Freiheit im Internet. Anwender müssen sich nicht mehr Dutzende von Benutzernamen und Passwörtern merken, um sich bei den verschiedenen Diensten zu identifizieren. Wer im Netz nicht von anderen erkannt werden möchte, kann für die Anmeldung in Chatrooms und sozialen Netzwerken die Pseudonymfunktion des neuen Ausweises verwenden. Selbst bei Bestellungen, die erst ab einem bestimmten Lebensalter erlaubt sind, muss das genaue Geburtsdatum nicht angegeben werden: Die AusweisApp übermittelt nur ein schlichtes Ja oder Nein auf die Abfrage, ob jemand den Alterskriterien entspricht oder nicht.

Um die Online-Ausweisfunktion nutzen zu können, wird eine spezielle Treibersoftware, die so genannte AusweisApp, benötigt. Erst wenn sie und ein zugelassener Kartenleser auf dem Rechner installiert sind, kann man mit dem Ausweis kommunizieren. Zudem muss auch der Geschäftspartner im Internet die Identifikation mit dem elektronischen Identitätsnachweis ausdrücklich anbieten und sich zunächst selbst als berechtigter Online-Partner zu erkennen geben. Solche Berechtigungen erhalten nur Unternehmen, die bereit sind, präzise Angaben über ihr Angebot, ihren Geschäftssitz, ihre Datenschutzregelungen und den Grund für die möglichen Datenabfragen zu machen. Sie dürfen allerdings nur auf zuvor exakt definierte Kategorien von Daten zugreifen. So weiß zum einen der Bürger, mit wem er Geschäfte machen kann. Zum anderen kann auch der Diensteanbieter sicher sein, dass er korrekte Angaben erhält. Das Prinzip der Authentifizierung beider beteiligten Parteien, eines der Kernelemente sicherer Online-Transaktionen, ist erfüllt.

RECHTSVERBINDLICHE UNTERSCHRIFT

Die Qualifizierte Elektronische Signatur (QES) macht es möglich, online rechtsverbindlich Verträge, Vollmachten oder Anträge zu unterschreiben. Sie ist der eigenhändigen Unterschrift rechtlich gleichgestellt. Anders als die Online-Ausweisfunktion (eID), mit der man sich sozusagen vorstellt („Das bin ich"), dient die QES dazu, sein Einverständnis mit einem Sachverhalt zu bekunden („Damit bin ich einverstanden").

Um sie nutzen zu können, muss man die Online-Ausweisfunktion aktiviert haben. Außerdem benötigt man eine individuelle eID-PIN sowie eine zusätzliche Signatur-PIN. Diese und das nötige Signaturzertifikat kann der Anwender bei einem akkreditierten Zertifizierungsdiensteanbieter (ZDA) wie etwa D-TRUST, dem Trustcenter der Bundesdruckerei, erwerben. Während für die Nutzung der Online-Ausweisfunktion ein Basislesegerät ausreicht, braucht man für die QES ein Komfortlesegerät. Auf dieses Gerät legt der Anwender während des Signiervorgangs seinen neuen Personalausweis und gibt die Signatur-PIN ein.

EINDEUTIGE IDENTIFIKATION

Die hoheitlichen Ausweisfunktionen sind ausschließlich für den Umgang mit staatlich autorisierten Instanzen von Bedeutung. So hat niemand außer Polizei-, Grenz- und Zollkontrollbehörden, den Steuerfahndungsstellen der Länder sowie den Meldebehörden Zugriff auf sie. Allerdings können selbst diese Instanzen die Daten nicht ohne Wissen ihres Besitzers quasi „im Vorbeigehen" auslesen: Auch hier ist wieder ein entsprechendes Berechtigungszertifikat nötig, das die ZDA ausstellen. Der Ausweisinhaber muss für das Auslesen der Daten zudem persönlich anwesend sein und sein Dokument vorlegen. Erst dann kann ein Mitarbeiter mit einem speziellen Lesegerät die aufgedruckte Zugangsnummer erfassen. Zum Einsatz kommt dieses Verfahren zum Beispiel bei Passkontrollen an der Grenze oder bei der Eingabe von Adressänderungen auf den Meldeämtern.

Den Diensteanbietern stehen verschiedene Optionen offen, wenn sie ihren Kunden die Online-Ausweisfunktion oder die QES ermöglichen möchten. Grundsätzlich können sie auch selbst die entsprechende Hard- und Software entwickeln und somit die gesamte Kommunikation mit der AusweisApp der Kunden und die dazugehörigen Verwaltungsprozesse in Eigenregie steuern. Voraussetzung dafür ist, dass sie dabei die entsprechenden technischen Richtlinien einhalten.[8]

Das wäre für die meisten Online-Anbieter allerdings mit einem erheblichen personellen und materiellen Aufwand verbunden. Daher entscheiden sich viele für den so genannten eID-Service, den akkreditierte ZDA wie D-TRUST, das Trustcenter der Bundesdruckerei, bereitstellen. Die ZDA verfügen über umfangreiche Erfahrungen mit dem Management von digitalen Identitäten. Sie stellen hierfür eine leistungsfähige Infrastruktur zur Verfügung. Der Diensteanbieter muss keinen eigenen eID-Server aufbauen, um seinen Kunden die Anwendung der Online-Ausweisfunktion oder der QES zu ermöglichen. Vielmehr regelt der eID-Service die gesamte Kommunikation mit dem Personalausweis-Chip und stellt sicher, dass sowohl Berechtigungszertifikate als auch Sperrlisten stets auf dem neuesten Stand sind. So bleiben dem Diensteanbieter umfangreiche Investitionen in die entsprechenden Systeme und deren Betrieb erspart. Zugleich sind seine Transaktionen mit Kunden optimal abgesichert. Der eID-Service lässt sich kurzfristig in die IT-Systemarchitektur des Diensteanbieters integrieren, sodass der Online-Shop die Vorteile der neuen Ausweisanwendungen komfortabel und kostengünstig nutzen kann.

KAPITEL 3
DIE TECHNIK IM DETAIL

Der neue Personalausweis ist Teil einer komplexen und hoch sicheren eID-Systemarchitektur. Zu den Eckpfeilern dieses Systems gehören, abgesehen von dem Identitätsdokument, das Lesegerät, die AusweisApp und so genannte Berechtigungszertifikate. Der eID-Service verknüpft diese Bausteine und ermöglicht es Bürgern und Diensteanbietern, auf Basis der Online-Ausweisfunktion miteinander zu kommunizieren und Geschäfte abzuschließen. Er stellt den beteiligten Parteien also gewissermaßen die Räumlichkeiten zur Verfügung, in denen sie sich begegnen.

Vereinfacht dargestellt läuft der Dialog zwischen den Beteiligten wie folgt ab:

1. Der Bürger möchte beispielsweise ein Produkt in einem Online-Shop erwerben und sich mittels seiner Online-Ausweisfunktion gegenüber dem Diensteanbieter zu erkennen geben. Er sendet daher eine Anfrage an den Diensteanbieter.

2. Um die Identität des Käufers eindeutig zu authentifizieren, wird die Anfrage an den eID-Service weitergeleitet.

3. Der eID-Service authentifiziert zunächst den Diensteanbieter, dann übermittelt er dem Nutzer das Berechtigungszertifikat des Diensteanbieters (siehe unten). Erst dann ermittelt er die freigegebenen Daten für den Diensteanbieter, die auf dem Chip hinterlegt sind.

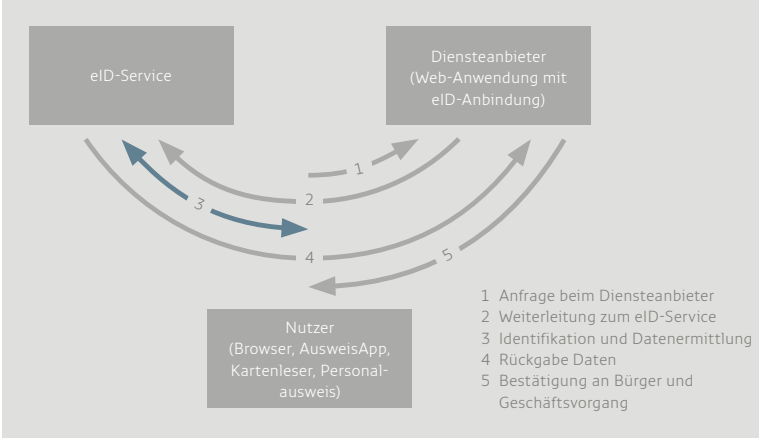
4. Dem Bürger wird in einer Maske auf seinem Bildschirm die Auswahl der zu übermittelnden Daten angezeigt. Er schränkt die Daten gegebenenfalls ein. Der eID-Service übermittelt daraufhin die ausgewählten Informationen an den Diensteanbieter.

5. Anschließend bestätigt dieser die Anfrage des Käufers und leitet die weiteren Schritte ein – etwa den Versand der Ware und die Rechnungstellung.

Der eID-Service ermöglicht also eine gegenseitige Authentifikation im Internet.

Um den Komfort der Online-Ausweisfunktion zu nutzen, müssen Bürger und Diensteanbieter die entsprechenden Voraussetzungen schaffen. Sie benötigen zum einen spezielle Hard- und Software, um auf dem Chip gespeicherte Daten auslesen zu können. Zum anderen müssen sie ihre Berechtigung mittels geeigneter Zertifikate nachweisen.

ABBILDUNG 3: DER eID-SERVICE



STARTER-KIT AUSWEISINHABER

Der Bürger entscheidet selbst, ob er Online-Ausweisfunktion und QES des Dokuments nutzen möchte. Falls er sich dafür entscheidet, braucht er Folgendes, um sie bei Transaktionen im Internet zu verwenden:

> **PIN:** Der Ausweisinhaber muss jede Datenübermittlung mit seiner sechsstelligen Geheimnummer (PIN) autorisieren. Nachdem der Bürger den neuen Personalausweis beantragt hat, erhält er, bevor er das Dokument abholt, zunächst einen PIN-Brief von der Bundesdruckerei. Dieser enthält die fünfstellige Transport-PIN, die Entsperrnummer (PUK) und ein Sperrkennwort. Der Ausweisinhaber sollte die Transport-PIN sofort nach Erhalt durch eine selbst gewählte Geheimnummer ersetzen.

> **PUK:** (Personal Unblocking Key, auch Entsperrnummer)
Die PUK ist zehnstellig und nur dem Ausweisinhaber bekannt. Er besteht ausschließlich aus Ziffern. Wird die PIN des Personalausweises dreimal falsch eingegeben, so wird sie gesperrt. Durch Eingabe des PUK kann die Sperrung aufgehoben werden.

> **Sperrkennwort:** Das Sperrkennwort ist ein leicht zu merkendes Wort (z. B. Lokomotive). Geht der Personalausweis verloren oder wird er gestohlen, muss der Inhaber den Ausweis nebst seinen Funktionen mithilfe des Sperrkennworts sperren lassen. Den jeweiligen Begriff wissen nur der Ausweisinhaber und die ausstellende Meldestelle. Das Sperrkennwort gibt der Anwender – anders als PIN und PUK – nicht am Computer ein. Vielmehr fragen Mitarbeiter der Sperrhotline oder der Personalausweisbehörde es ab.

> **Lesegerät:** Im Handel sind vom BSI zugelassene Lesegeräte erhältlich. Der Bürger kann sie am aufgedruckten kreisförmigen grün-blauen Logo des neuen Personalausweises erkennen.

> **Zertifikat:** Um die QES des Ausweises anwenden zu können, benötigt der Bürger ein Zertifikat. Dieses Zertifikat kann er bei einem Zertifizierungsdiensteanbieter (ZDA), wie z. B. der Bundesdruckerei, erwerben.

> **Signatur-PIN für QES:** Die Signatur-PIN verwendet der Ausweisinhaber, wenn er ein Dokument elektronisch unterschreiben möchte.

> **Treibersoftware:** Die so genannte AusweisApp ermöglicht die Kommunikation zwischen Ausweis und Computer. Sie steht für die Betriebssysteme Windows, Linux und Mac OS zur Verfügung und ist unter www.ausweisapp.bund.de kostenlos herunterzuladen.

STARTER-KIT DIENSTEANBIETER

Diensteanbieter müssen klar definierte Vorgaben gemäß §21 des deutschen Personalausweisgesetzes (PAuswG) erfüllen und dies schriftlich nachweisen. Darüber hinaus brauchen sie Folgendes, um die Online-Ausweisfunktion oder die QES in ihr Angebot zu integrieren.

> **Berechtigung:** Die Vergabestelle für Berechtigungszertifikate (VfB), ein Referat des Bundesverwaltungsamts, fordert vom Anbieter eine freiwillige Selbsterklärung zum Datenschutz. Außerdem benötigt sie einen Nachweis, inwieweit die Daten, die der Diensteanbieter auslesen möchte, für sein Angebot erforderlich sind. Die erteilte Berechtigung der VfB ist maximal drei Jahre gültig.

> **Berechtigungszertifikate:** Ist die Berechtigung erteilt, kann das Unternehmen einen individuellen Bereitstellungsvertrag mit einem ZDA abschließen. D-TRUST, das Trustcenter der Bundesdruckerei, ist ein solcher ZDA. Die Berechtigungszertifikate authentifizieren den Diensteanbieter, sind nur wenige Tage gültig und werden automatisch regelmäßig erneuert. Besteht ein Verdacht auf Datenmissbrauch, werden die Zertifikate nicht weiter ausgestellt.

> **eID-Service:** Er wird von Hochsicherheitsunternehmen bereitgestellt, mit denen der Diensteanbieter einen Vertrag schließen kann. Der eID-Service der Bundesdruckerei ermöglicht es, mithilfe des Berechtigungszertifikats die auf dem Chip des Personalausweises gespeicherten Daten zu lesen.

> **SAML 2.0 Token:** SAML steht für Security Assertion Markup Language und ist ein Standard für den sicheren Austausch von Authentifizierungen und Autorisierungen zwischen Domains. SAML Assertions sind Aussagen, anhand derer ein eID-Service-Provider Zugang zu bestimmten Dienstleistungen gewährt. Der SAML-Token beinhaltet die Informationen vom Ausweis und wird dem Diensteanbieter zur Weiternutzung zur Verfügung gestellt.

> **Token-Zertifikate:** Sie erlauben dem Diensteanbieter den Zugriff auf den eID-Service. Der zugehörige private Diensteanbieter-Schlüssel ist nur dem Diensteanbieter bzw. der eID-Service-Schlüssel der Bundesdruckerei bekannt. Mit diesen Schlüsseln werden die SAML 2.0 Token signiert sowie anschließend für den Empfänger verschlüsselt. So wird innerhalb des SSL-Tunnels eine zweite individuell gesicherte Verbindung aufgebaut.

> **SSL-Zertifikate:** SSL steht für Secure Sockets Layer und ist ein Sicherheitsprotokoll. Es ermöglicht sichere Datenübertragungen im Internet. SSL-Zertifikate benötigen Diensteanbieter, um die Kommunikation mit Nutzern ihrer Website zu verschlüsseln. Die Zertifikate können sie bei einem ZDA erwerben.

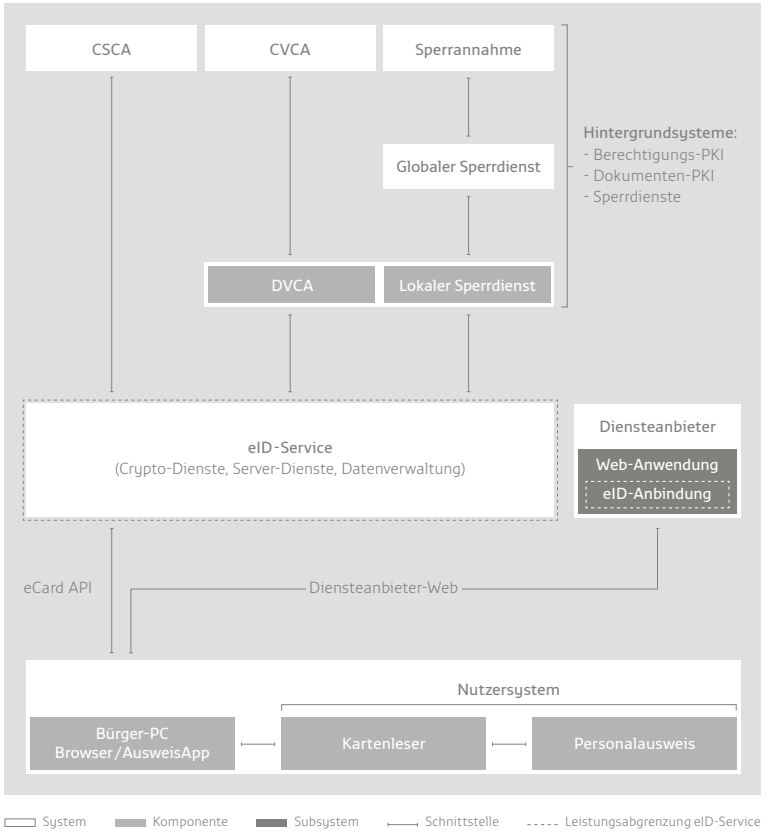
VORTEILE DES eID-SERVICE

So gerüstet, können Diensteanbieter die Vorzüge des eID-Service in vollem Umfang nutzen und sich im Wettbewerb positionieren. Banken und Versicherungen haben die Möglichkeit, Antragsteller eindeutig und entsprechend den Anforderungen des Geldwäschegesetzes (GWG) zu identifizieren. Bei einer Kontoeröffnung oder dem Abschluss einer Versicherungspolice kann die Legitimation des Vertragspartners am PC erfolgen, ein persönliches Vorsprechen ist nicht mehr nötig. Die elektronische Identifikation ist sowohl für den Bürger als auch für den Diensteanbieter attraktiv. Denn sie funktioniert medienbruchfrei, ist zeitsparend und kostengünstig. Manche Anbieter sind aufgrund ihres altersbeschränkten Angebots gesetzlich verpflichtet, das Alter ihrer Kunden zu erfragen. Dies ist problemlos mit der Altersverifikation des eID-Service möglich.

Die bereits genannten Anwendungen Altersverifikation oder aber auch die Wohnortbestätigung sowie die Pseudonymfunktion (siehe Kapitel 2, Seite 15) sind weitere interessante Angebote, die Diensteanbieter für ihre potenziellen Nutzer auf ihrer Website bereitstellen können. Der eID-Service übernimmt das Auslesen der dafür erforderlichen Daten.

Herzstück des eID-Service ist ein spezieller Server (der eID-Server). Als Hard- und Softwarekomponente ermöglicht er die Kommunikation zwischen dem PC des Ausweisinhabers, dessen Auslese-terminal und dem Diensteanbieter. Er übermittelt und verwaltet die Berechtigungszertifikate des Diensteanbieters, prüft die Echtheit des Chips im neuen Personalausweis und gleicht Sperrlisten ab. Der eID-Service verfügt über zwei Schnittstellen: eine innere und eine äußere. Die innere Schnittstelle ist mit dem eCard API Framework des BSI (TR-03112) konform und ermöglicht den Informationsaustausch mit dem Personalausweis. Sie umfasst kryptografische Protokolle sowie die Zugriffskontrollen PACE und EAC. Die äußere Schnittstelle liefert über einen international standardisierten Token (SAML 2.0 Assertion) die auf dem Chip des neuen Personalausweises gespeicherten Daten an den Diensteanbieter.

ABBILDUNG 4: SYSTEMÜBERSICHT



BEWÄHRTE SICHERHEITSMECHANISMEN

Verschiedene Protokolle und Verfahren schützen die personenbezogenen Daten, die auf dem Chip hinterlegt sind. Sie prüfen darüber hinaus die Echtheit des neuen Personalausweises und machen ihn fälschungssicher. Dabei kommt den Lösungen, die die kontaktlose Schnittstelle zwischen Ausweis und Lesegeräten absichern, eine besondere Bedeutung zu.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert folgende Protokolle und Maßnahmen:

> **PACE:** Password Authenticated Connection Establishment
Zugriffskontrolle, schützt vor Auslesen des kontaktlosen Chips

> **EAC:** Extended Access Control
Erweiterte Zugriffskontrolle, bestehend aus den zwei Subprotokollen CA (Chip Authentication) und TA (Terminal Authentication)

> **PA:** Passive Authentication
Prüfung der Echtheit und Unverfälschtheit der Daten auf dem Chip

> **RI:** Restricted Identification
Erzeugung von chip- und anwenderspezifischen Pseudonymen

> **PKI:** Public Key Infrastructure
Hierarchie von digitalen Zertifikaten: CSCA (Country-Signing-Certification-Authority) und CVCA (Country-Verifying-Certification-Authority)

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI): „Innovationen für eine eID-Architektur in Deutschland"

> **PACE**
Password Authenticated Connection Establishment
PACE stellt zum einen sicher, dass der kontaktlose Chip im neuen Personalausweis nicht ohne Eingabe der sechsstelligen eID-PIN ausgelesen werden kann. Diese PIN ist nur dem Ausweisinhaber bekannt. Zum anderen gewährleistet die Zugriffskontrolle, dass die Daten verschlüsselt an das Lesegerät übertragen werden.

> **EAC**
Extended Access Control
EAC beinhaltet verschiedene Protokolle. EAC umfasst die Subprotokolle Chip Authentication (CA) und Terminal Authentication (TA). Diese werden zusammen mit PACE und Passive Authentication (PA, siehe unten) ausgeführt. CA baut eine sichere Verbindung zum Chip auf und erkennt geklonte Chips. TA schützt die sensiblen Daten des neuen Personalausweises vor dem Zugriff durch Unbefugte. Der Chip gibt bestimmte Daten nur dann zum Lesen frei, wenn das Lesegerät eine Berechtigung für den Zugang zu genau diesen Daten nachweist.

> **PA**
Passive Authentication
PA prüft die Echtheit und Unverfälschtheit der Daten auf dem kontaktlosen Chip. Nur der offiziell vom BMI beauftragte Ausweishersteller, die Bundesdruckerei, ist befugt, Daten auf dem Chip des neuen Personalausweises zu speichern. In den Meldestellen können diese Daten mithilfe der Änderungsterminals bearbeitet werden. Bei der Herstellung signiert die Bundesdruckerei die gespeicherten Daten digital mit dem so genannten Document-Signing-Zertifikat. Dieses wiederum ist mit dem Country-Signing-Certification-Authority-Certificate (CSCA-Zertifikat) der Nation signiert, die das Ausweisdokument ausstellt. Beim Auslesen des neuen Personalausweises wird mithilfe der PA die Signatur des Chips geprüft und bis zum CSCA-Zertifikat zurückverfolgt.

> **RI**
Restricted Identification
RI erzeugt automatisch Pseudonyme für einen individuellen Chip und einen bestimmten Anbieter. Sie ermöglichen es einem Diensteanbieter, den Chip basierend auf dem zuvor erhaltenen Pseudonym wiederzuerkennen – und zwar ohne personenbezogene Daten auszulesen. Dabei werden für verschiedene Diensteanbieter unterschiedliche Pseudonyme generiert. Es ist daher nicht möglich, dass verschiedene Anbieter Pseudonyme untereinander abgleichen und Informationen über Nutzer austauschen. Dieses Verfahren dient dem Datenschutz.

Das BMI hat verschiedene Studien in Auftrag gegeben, um die Sicherheit der verwendeten Protokolle zu prüfen. Die Technische

Universität Darmstadt hat etwa im Rahmen ihrer Studie „Sicherheitsanalyse des EAC-Protokolls[9]" geprüft, ob die sensiblen Daten durch die Ausführung der Protokolle vertraulich bleiben und sich authentische Teilnehmer erfolgreich dem Partner gegenüber ausweisen können. In ihrem Abschlussbericht stellen die Studienleiter fest: „Die kryptografischen Verfahren gewährleisten ausreichende Sicherheit diesbezüglich." Und die auf Internetsicherheit spezialisierte Fachhochschule Gelsenkirchen hält im Ergebnis ihrer Studie zu „Restrisiken beim Einsatz der AusweisApp auf dem Bürger-PC zur Online-Authentisierung mit Penetration-Test[10]" fest: „Die eID-Funktion weist im Vergleich zur herkömmlichen Authentisierung mit Passwörtern ein höheres Sicherheitsniveau auf."

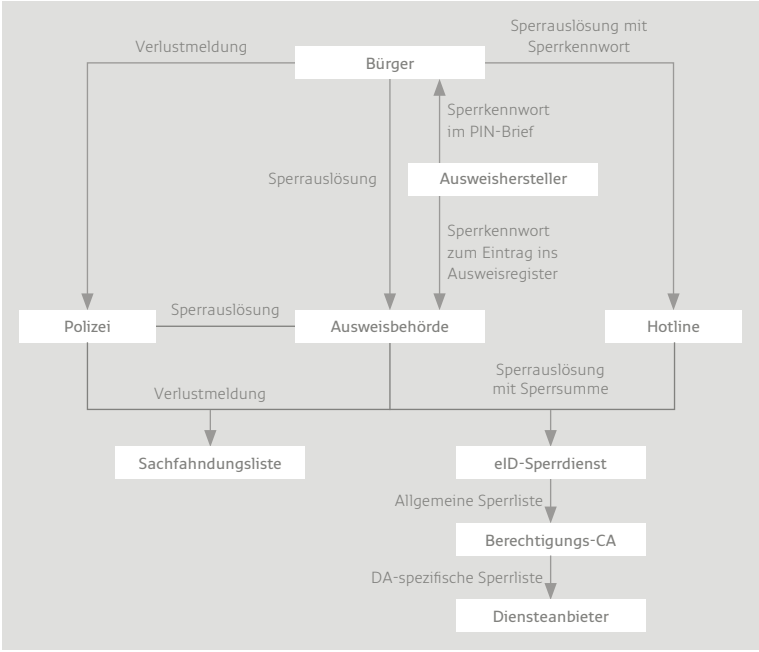
SPERRMANAGEMENT

Was aber passiert, wenn Unbefugte einen gestohlenen oder gefundenen neuen Personalausweis einsetzen? In diesem Fall greift das Sperrmanagement des elektronischen ID-Dokuments. Der Ausweisinhaber ist verpflichtet, die zuständige Personalausweisbehörde über den Verlust des Personalausweises zu informieren. Diese veranlasst die Sperrung beim Sperrlistenbetreiber, trägt sie in das Personalausweisregister ein und meldet den Verlust gemäß § 11 Absatz 5 Personalausweisgesetz unverzüglich der Polizei. Nach Eintrag in die Sperrliste lässt sich die Online-Ausweisfunktion nicht mehr nutzen. Auf diese Weise ist sichergestellt, dass keine Dienste für den aktuellen Besitzer des Ausweises erbracht werden. Eine gegebenenfalls genutzte QES-Funktion muss der Ausweisinhaber beim ZDA sperren lassen, bei dem er das Signaturzertifikat erworben hat. Die so genannte globale Sperrliste wird vom Bundesverwaltungsamt (BVA) geführt, regelmäßig aktualisiert und den ZDA zur Verfügung gestellt.

Die Sperrung der gängigen Chipkarten, wie zum Beispiel von Karten für die QES, erfolgt in der Regel über einen chipindividuellen öffentlichen Schlüssel. Dieser wird über eine Sperrliste abgeglichen. Dieses Merkmal ist personenbezogen, da es den Chip und seinen Inhaber eindeutig identifiziert. Die datenschutzfreundliche Konzeption der elektronischen Ausweisfunktion verbietet einen solchen Mechanismus.

Vor diesem Hintergrund werden diensteanbieterspezifische Sperrlisten erzeugt. Jeder Ausweis übersendet im Zuge des elektronischen Identitätsnachweises ein dienste- und kartenspezifisches Sperrmerkmal an den Diensteanbieter. Dieser gleicht das Sperrmerkmal gegen die individuelle, diensteanbieterspezifische Sperrliste ab. ZDA übernehmen es, für jeden Dienst aus einer globalen Sperrliste eine diensteanbieterspezifische Sperrliste zu erstellen. Dieses Verfahren erlaubt es, Personalausweise effektiv zu sperren, ohne dass in einem zentralen Register personenbezogene Daten gespeichert werden müssen. Auch dank der Leistungen des eID-Service und der ZDA schützt das Gesamtsystem „neuer Personalausweis" nicht nur die personenbezogenen Daten der Bürger, sondern bewahrt Bürger und Diensteanbieter auch vor wirtschaftlichem Schaden durch missbräuchlich eingesetzte Identitätsdokumente.

ABBILDUNG 5: SPERRMANAGEMENT – GESAMTÜBERSICHT



KAPITEL 4
IDENTITÄTSMANAGEMENT IN DER PRAXIS – ANWENDUNGSBEISPIELE

So hochkomplex die Funktionsweise des eID-Service auch ist: Für Bürger und die nicht mit IT-Aufgaben betrauten Verantwortlichen bei den Diensteanbietern bleibt diese Komplexität im Alltag unsichtbar.

Die im Hintergrund ablaufenden technischen Prozesse sind vollständig automatisiert. Dank eines im hohen Maße selbsterklärenden Verfahrens und der intuitiven Benutzerführung können sowohl Bürger als auch Anbieter die Funktionen des neuen Personalausweises online wie offline unkompliziert nutzen. Drei Beispiele zeigen, was dabei im Detail passiert.

BEISPIEL 1
Identifikation personenbezogener Daten: Frau Mustermann eröffnet ein Konto

Um ein Konto bei einer Bank eröffnen zu können, müssen Kunden sich bei dem Kreditinstitut mit einem hoheitlichen Identitätsdokument ausweisen. Das ist in Deutschland im Geldwäschegesetz und in der Abgabenverordnung verbindlich festgeschrieben. Bislang suchten Kunden dafür direkt eine Filiale auf, wo ein Kundenberater ihre persönlichen Daten anhand des Dokuments in die entsprechenden Bankformulare eintrug. Einzige Alternative zum Termin bei der Bank war das Postident-Verfahren, bei dem man sich statt zur Bank zur örtlichen Postfiliale begeben musste. Mit der Online-Ausweisfunktion, deren Nutzung immer mehr Finanzdienstleister auf ihren Websites anbieten, lässt sich dieses Prozedere deutlich bequemer und kundenfreundlicher gestalten.

Eine Kundin, im Folgenden Erika Mustermann genannt, hat zunächst im örtlichen Einwohnermeldeamt ihre Online-Ausweisfunktion freischalten lassen und auf ihrem PC die AusweisApp installiert. Zusätzlich hat sie sich im Handel ein vom BSI zugelassenes Komfortlesegerät besorgt und an ihren PC angeschlossen. Sie ruft am Rechner die Seite ihrer künftigen kontoführenden Bank auf und sieht dort nach, ob und für welche Geschäfte das Institut die Identifikation mit dem elektronischen Identitätsnachweis anbietet. Anhand des angezeigten Zertifikats stellt Frau Mustermann fest, dass das Unternehmen eine Berechtigung für Kontoeröffnungen mithilfe des neuen Personalausweises erhalten hat: Die Bank darf auf die Datenkategorien Familienname und Vorname, Tag und Ort der Geburt, Anschrift sowie auf die Wohnortverifikation zugreifen, sofern der Bürger, in diesem Fall Frau Mustermann, es zulässt.

Frau Mustermann klickt sich nun durch das Produktangebot der Bank und wählt ein spezielles Privatkonto aus. Auf dem Bildschirm erscheint eine Aufforderung, sich für eine Anfrage zur Kontoeröffnung mithilfe eines ID-Dokuments mit Online-Ausweisfunktion zu erkennen zu geben. Dafür legt Frau Mustermann ihren Ausweis auf das Lesegerät, damit die Daten auf dem integrierten Chip ausgelesen werden können. Noch bevor der Ausleseprozess startet, prüft der eID-Server als Vermittlungsinstanz zwischen Nutzer und Anbieter, ob die Bank das nötige Berechtigungszertifikat für die Abfrage der Daten hat. Am PC von Frau Mustermann erscheint eine Maske mit den vom Diensteanbieter gewünschten Daten. Frau Mustermann wählt die Informationen ab, die sie nicht übermitteln möchte, und schaltet ihre Auswahl durch Eingeben der PIN zur Übermittlung an den eID-Server frei. Über PACE- und EAC-gesicherte Verbindungen werden die Daten aus dem Chip gelesen und an den Diensteanbieter in einem SAML 2.0 Token sicher übermittelt. Für die Kundin ist der Prozess damit vorerst abgeschlossen. Sie nimmt ihren Ausweis vom Lesegerät, wählt bei Bedarf

besondere Optionen für ihr Konto in der Online-Anfrage der Bank aus und schickt sie per Mausklick ab. Jetzt kann das Kreditinstitut ihre Anfrage bearbeiten und davon ausgehen, dass die Identität seiner potenziellen Kundin korrekt ist.

BEISPIEL 2
Online-Authentisierung mithilfe von Restricted Identification: Frau Mustermann tritt in einem sozialen Netzwerk unter einem Pseudonym auf

Wer häufig auf Online-Portalen oder in sozialen Netzwerken unterwegs ist, kennt das Problem: Als Nutzer muss man sich eine Vielzahl von Passwörtern und Benutzernamen merken, um sich auf diesen Websites einloggen zu können. Die Online-Ausweisfunktion des neuen Personalausweises eröffnet Frau Mustermann auch hier eine Möglichkeit, sich den Alltag zu erleichtern. Mithilfe der Pseudonymfunktion kann sie sich bequem in Portale einloggen, ohne dabei persönliche Daten angeben zu müssen. Wie genau sie dabei vorgeht, hängt vom Angebot des jeweiligen Diensteanbieters ab. Dieser kann innerhalb eines gewissen Rahmens selbst festlegen, wie das Verfahren zum Einloggen mithilfe der Pseudonymfunktion gestaltet sein soll. Zur Illustration der Mechanik wird daher im Folgenden nur ein fiktiver, beispielhafter Vorgang beschrieben.

Frau Mustermann möchte in einem sozialen Netzwerk ihre Identität schützen. Dafür prüft sie zunächst auf dessen Website anhand des dort einsehbaren Zertifikats, ob der Diensteanbieter die Online-Ausweisfunktion unterstützt und auch den Einsatz der Pseudonymfunktion akzeptiert. Ist das der Fall, wählt sie im Menü des Diensteanbieters die Option „Anmelden" aus. Sie legt, sobald die entsprechende Aufforderung am Bildschirm erscheint, ihren neuen Personalausweis auf das Lesegerät. Der eID-Server prüft zunächst, ob der Diensteanbieter alle nötigen aktuellen Zertifikate für den Anmeldeprozess besitzt. Erfüllt er die Voraussetzungen, wird Frau Mustermann zur Eingabe ihrer persönlichen eID-PIN aufgefordert. Erst wenn sie diese eingetippt hat, liest das Lesegerät ihre Daten aus.

Auf einer Bildschirmmaske wählt Frau Mustermann daraufhin bis auf die Pseudonymfunktion alle Kategorien ab: Je nachdem, auf was für einem Portal sie sich anmelden möchte, kann sie auf die Preisgabe persönlicher Daten vollständig verzichten. Soweit der Diensteanbieter eine Anmeldung allein über ein Pseudonym zulässt, schaltet Frau Mustermann durch Eingabe der eID-PIN die Kategorie „Pseudonym" zur Übertragung an den eID-Server frei. So ist sichergestellt, dass dieses Netzwerk Frau Mustermanns Chip jederzeit wiedererkennen kann – ohne dass die Ausweisinhaberin dafür persönliche Daten freigeben müsste.

Da das Pseudonym vom eID-Server individuell für dieses spezielle Angebot erzeugt wurde, kann das soziale Netzwerk auch keinerlei Abgleich mit weiteren Pseudonymen desselben Nutzers für andere Anbieter durchführen. Frau Mustermanns Identität ist so gut wie derzeit technisch möglich geschützt: Sofern sie beim Surfen im sozialen Netzwerk nicht selbst Angaben über sich macht, die diese Identität enthüllen, bleibt sie für den Diensteanbieter und andere Nutzer anonym. Loggt Frau Mustermann sich das nächste Mal in das Netzwerk ein, wiederholt sie den beschriebenen Vorgang einfach – das authentisierte Terminal des Anbieters erkennt sie automatisch wieder. Dieses Verfahren vereinfacht nicht nur für die Nutzer, sondern auch für den Diensteanbieter die Abläufe: Weil es zum Beispiel überflüssig wird, vergessene Passwörter oder Benutzernamen zurückzusetzen, sinkt der administrative Aufwand. Diensteanbieter können glaubhaft darauf verweisen, dass sie den Datenschutz bestmöglich gewährleisten und ihr Angebot strengsten Anforderungen an die Sicherheit gerecht wird.

BEISPIEL 3
Altersverifikation beim Online-Kauf: Frau Mustermann bestellt Wein über das Internet

Ob ein Nutzer, der im Netz Spirituosen, Filme für Erwachsene oder ähnliche Produkte bestellt, die Altersvorgaben dafür erfüllt, lässt sich für Anbieter nur schwer überprüfen. Meist müssen sie sich auf die Ehrlichkeit ihrer Kunden verlassen. Die Online-Ausweisfunktion des neuen Personalausweises macht eine sichere Altersverifikation für die Anbieter deutlich einfacher.

Der Online-Shop, bei dem Frau Mustermann Wein bestellt, hat bei einem Zertifikateanbieter ein Berechtigungszertifikat dafür erworben, neben Namen und Adresse auch die Volljährigkeit seiner Kunden per Online-Ausweisfunktion überprüfen zu können. Statt des genauen Geburtsdatums übermittelt der eID-Server in diesem Fall bei Bestellungen nur, ob die Altersvorgabe erfüllt wird oder nicht.

Wie in den bereits erläuterten Beispielen wählt Frau Mustermann zunächst ein Angebot aus, in diesem Fall eine Kiste Wein. Sie legt, sobald die entsprechende Aufforderung am Bildschirm erscheint, ihren neuen Personalausweis auf das Lesegerät. Der eID-Server prüft zunächst, ob der Diensteanbieter alle nötigen aktuellen Zertifikate für die Datenübermittlung besitzt. Auf der Bildschirmmaske erscheinen jetzt diejenigen Datenkategorien, die der Weinhändler gerne abrufen möchte. Frau Mustermann wählt diejenigen ab, die sie nicht übermitteln möchte, und gibt ihre persönliche eID-PIN über die Tastatur ein.

Über PACE- und EAC-gesicherte Verbindungen werden die Daten aus dem Ausweis ausgelesen. Der Weinhändler erhält die Daten in einem SAML 2.0 Token vom eID-Service. Jetzt kann der Anbieter mit großer Sicherheit darauf vertrauen, dass Frau Mustermann die Altersgrenze für den Erwerb von Alkohol bereits erreicht hat. Sobald ihre Bestellung abgeschlossen ist, kann der Händler die Ware versenden.

KAPITEL___5
AUSBLICK: eGOVERNMENT OHNE GRENZEN

Wäre es nicht komfortabel, wenn sich Menschen europaweit mit ihren nationalen Identitätsnachweisen zu erkennen geben und grenzübergreifende Dienste nutzen könnten? Diese Vision wollen die Teilnehmer des EU-Projekts STORK Realität werden lassen.

STORK steht für Secure idenTity acrOss boRders linKed.[11] Ziel des Projekts, an dem 17 europäische Länder und 32 Konsortialpartner beteiligt sind, ist es, im Rahmen des IKT-Förderprogramms der Europäischen Union eine EU-weite Plattform einzuführen. Diese soll es den Bürgern ermöglichen, ihre nationalen elektronischen Ausweise auch in anderen Ländern der EU zu nutzen.

Bereits Ende 2010 verwendeten zwölf Länder der Europäischen Union elektronische Identitätsnachweise. Finnland war 1999 der erste Staat, der einen elektronischen Personalausweis einführte. Belgien und Estland folgten 2003.

Der neue deutsche Personalausweis, der seit November 2010 erhältlich ist, gilt in Expertenkreisen als die technisch anspruchsvollste und sicherste eID-Karte weltweit. Ende 2011 werden sich voraussichtlich Bürger von 16 europäischen Staaten elektronisch zu

erkennen geben können. Allerdings basieren nicht alle Karten auf den europäischen Standards der Internationalen Zivilluftfahrtorganisation (International Civil Aviation Organization, ICAO) und/oder des Europäischen Komitees für Normung (Comité Européen de Normalisation, CEN), die seit 2004 verfügbar sind. Speziell die Vorreiter Finnland, Belgien und Estland, die ihre eID-Karten vor 2004 eingeführt haben, verwenden bisher keinen internationalen Standard.

Die unterschiedlichen Karten- und Systemarchitekturen in den europäischen Ländern verhindern bisher einen grenzübergreifenden Einsatz der nationalen eIDs. STORK hat verschiedene Pilotprojekte ins Leben gerufen, in denen Bürger verschiedener Staaten ihre Personalausweise für eGovernment-Dienste in mehreren europäischen Ländern nutzen können. Das Bundesamt für Sicherheit

ABBILDUNG 6: eID-LÖSUNGEN IN EUROPA

Land[1] Jahr der Einführung	eID	eGov	eSignature[3]	Travel	eHealth	Sonstiges
Finnland 1999	■	■	■	■		eBanking
Belgien 2003	■	■	■	■		
Estland 2003	■	■	■	■		
Österreich 2004	■	■	■		■	eTax und eBanking
Schweden 2005	■[2]	■	■	■		
Italien 2006	■	■	■		■	eTicketing
Spanien 2006	■	■	■	■		
Portugal 2007	■	■	■	■	■	eTax
Serbien 2007	■	■				
Großbritannien 2009/2010	■[2]			■		
Frankreich 2010	■	■	■	■		
Deutschland 2010	■[2]	■	■	■		
Tschechien 2011	■	■		■		weitere in Planung
Polen 2011	■	■		■	■	Social-Service und EHIC[4]

1 Nicht alle Länder haben eine Ausweispflicht.
2 Elektronische Variante ist freiwillig.
3 QES ist freiwillig, Ausnahme Estland.
4 EHIC = EU Auslandskrankenschein in elektronischer Form.

in der Informationstechnik vertritt innerhalb des Projekts die Interessen der Bundesrepublik Deutschland und möchte den Bürgern die Nutzung des neuen Personalausweises für Internetangebote in ganz Europa ermöglichen. Insgesamt stehen für das EU-Projekt im Laufe von drei Jahren 20 Millionen Euro bereit. Sechs Pilotprojekte sind seit Oktober 2010 für die Öffentlichkeit zugänglich: „Grenzüberschreitende Authentifizierung für elektronische Dienste", „Safer Chat", „Studenten-Mobilität", „Grenzüberschreitende elektronische Zustellung", „Adressänderung" und „Kommissionsdienste".

GRENZÜBERSCHREITENDE AUTHENTIFIZIERUNG FÜR ELEKTRONISCHE DIENSTE

Das von der Bundesrepublik Deutschland koordinierte Pilotprojekt testet, wie Bürger ihren nationalen elektronischen Identitätsnachweis einsetzen können, um die Online-Behördendienste anderer Mitgliedstaaten zu nutzen. In diesem Zusammenhang werden auch Leistungsfähigkeit und Anwenderfreundlichkeit grenzübergreifender eID-Services geprüft.

SAFER CHAT

Das isländische Finanzministerium koordiniert das Pilotprojekt Safer Chat. Es soll grenzüberschreitendes eLearning ermöglichen. Schüler sollen mit ihren Altersgenossen aus anderen Ländern zusammenarbeiten. Um die Internetsicherheit für Kinder und Jugendliche zu verbessern, entwickeln Lehrer innerhalb der verschiedenen Altersgruppen Aufgaben und definieren sichere Chatrooms für die minderjährigen Anwender. Besondere Bildungspakete für die junge Zielgruppe schärfen das Bewusstsein für Internetsicherheit.

STUDENTEN-MOBILITÄT

Mithilfe dieser Anwendung können Studenten ihren nationalen elektronischen Ausweis (Personalausweis, digitale Zertifikate) verwenden, um sich zu authentifizieren und entsprechende akademische Dienste zu nutzen – beispielsweise können sie sich für ein Erasmus-Programm[12] bewerben. Das Projekt stellt einen ersten Meilenstein für die Analyse des künftigen Datenaustauschs zwischen Universitäten der verschiedenen EU-Länder dar. Dieser

Datenaustausch ist zur Anrechnung von Studienleistungen, die Studierende in anderen Ländern erbracht haben, notwendig. Die Universität Jaume I in Castelló de la Plana steuert dieses Teilprojekt im Auftrag der Rektorenkonferenz der spanischen Universitäten.

GRENZÜBERSCHREITENDE ELEKTRONISCHE ZUSTELLUNG

Bei diesem Pilotprojekt können Bürger Portale anderer EU-Länder für elektronische Zustellungen (eDelivery) nutzen, indem sie ihren nationalen elektronischen Identitätsnachweis einsetzen. Darüber hinaus werden öffentliche Verwaltungen in die Lage versetzt, Dokumente an Bürger verschiedener Länder direkt über das eDelivery-Portal des jeweiligen Landes zu senden. Die Technische Universität Graz koordiniert dieses Projekt.

ADRESSÄNDERUNG

Dieses Pilotprojekt wird es ausländischen Bürgern ermöglichen, Adressänderungen mithilfe ihres nationalen elektronischen Identitätsnachweises vorzunehmen und alle relevanten Stellen über diese Änderung zu informieren. Die in den einzelnen Mitgliedstaaten geltenden Verfahren müssen hierfür nicht geändert werden, da die von STORK entwickelte Plattform interoperabel ist, das heißt, sie ist für verschiedene Kartentypen und länderspezifische Infrastrukturen anwendbar. Aktuell sind zwei Szenarien vorgesehen: die Abfrage und die Aktualisierung einer Adresse. Die Agência para a Modernização Administrativa in Portugal zeichnet für dieses Projekt verantwortlich.

KOMMISSIONSDIENSTE

Der European Commission Authentication Service (ECAS) erlaubt es Mitarbeitern der EU-Kommission, sich für eine Vielzahl von Anwendungen anzumelden. Das Pilotprojekt Kommissionsdienste verbindet STORK und ECAS. So ist es den Mitarbeitern in den Mitgliedstaaten möglich, ihre nationalen eIDs einzusetzen, um die elektronischen Dienste der Europäischen Kommission zu nutzen. ECAS stellt beispielsweise Authentifizierungsdienste für die Kommunikation zwischen den Mitgliedstaaten (Internal Market Information System, IMI) und das Teilnehmerportal für europäische Forschungsprogramme zur Verfügung. Neun Staaten nehmen an diesem von der Technischen Universität Graz koordinierten Pilotprojekt teil: Österreich, Belgien, Estland, Deutschland, Island, Italien, Portugal, Slowenien und Spanien.

Die geschilderten Anwendungsszenarien eröffnen für Bürger und staatliche Stellen neue Möglichkeiten. „Die Pilotprojekte werden den Bürgerinnen und Bürgern und auch den öffentlichen Verwaltungen zeigen, dass eine Interoperabilität von elektronischen Identitäten in eGovernment-Diensten möglich ist. Sie werden den Mehrwert einer elektronischen Identität in einem geschützten, sicheren und privaten Umfeld deutlich machen", so Professor Antonio Lioy vom Politecnico di Torino in Italien und stellvertretender STORK-Vorsitzender.[13] Das eID-Netz werde öffentliche Mittel einsparen, den Zeitaufwand sowohl für Behörden als auch für Bürger verringern, die Risiken von Missbrauch und Betrug reduzieren sowie eine Vielzahl von Möglichkeiten schaffen. „Es ist ein weiterer Schritt in Richtung eines grenzenlosen EU-Markts." Zugleich wird es mit dieser Entwicklung für den Bürger immer selbstverständlicher, die eID-Funktion seines Ausweises zu nutzen – auch im privatwirtschaftlichen Bereich. Daraus ergeben sich Marktpotenziale für Online-Diensteanbieter, die frühzeitig die elektronische Ausweisfunktion in ihr Angebot integrieren.

FRAGEN UND ANTWORTEN

Bei dem eID-Service handelt es sich um eine neue Technologie. Wie kann ein Diensteanbieter sicher sein, dass der Service hält, was er verspricht?

Die Bundesdruckerei hat bereits erfolgreich einen umfangreichen Anwendungstest durchgeführt und ihren eID-Service für über 40 Firmen und Institutionen bereitgestellt.

Woher bezieht ein interessierter Diensteanbieter weitere Informationen zum eID-Service?

Der Diensteanbieter kann die Experten der Bundesdruckerei unter der Rufnummer +49 (0) 30 – 25 98 0 oder per Mail an info@bundesdruckerei.de kontaktieren. Allgemeine Informationen zum eID-Service stehen auf folgenden Seiten zur Verfügung:
www.bundesdruckerei.de
www.personalausweisportal.de

Welche IT-Komponenten benötigt ein Diensteanbieter, wenn er die Online-Ausweisfunktion (eID-Funktion) in sein Angebot integrieren möchte?

Der Diensteanbieter tauscht mittels Webservice-Kommunikation Daten mit der Bundesdruckerei aus. Dafür erhält er neben der Schnittstellen-Beschreibung auch eine Beispiel-Implementation.

Welche Voraussetzungen müssen Unternehmen oder Behörden (Diensteanbieter) erfüllen, um eine Berechtigung für die Nutzung der Online-Ausweisfunktion in ihrem Angebot zu erhalten?

Die Berechtigung wird auf Antrag durch die Vergabestelle für Berechtigungszertifikate (VfB), ein Referat des Bundesverwaltungsamts, mittels Berechtigungsbescheid erteilt. Im Antragsverfahren sind vom Anbieter verschiedene Unterlagen und Informationen einzureichen, wie z. B. der Nachweis, inwieweit die Daten, die der Diensteanbieter auslesen möchte, für sein Angebot erforderlich sind. Der erteilte Bescheid der VfB ist maximal drei Jahre gültig.

Welche Berechtigungszertifikate braucht ein Diensteanbieter, um die Online-Ausweisfunktion in sein Angebot zu integrieren?

Sobald die Vergabestelle für Berechtigungszertifikate die Berechtigung erteilt hat, kann die Behörde oder das Unternehmen einen individuellen Bereitstellungsvertrag mit einer Berechtigungs-CA (BerCA) abschließen: D-TRUST, das Trustcenter der Bundesdruckerei, ist eine solche BerCA. Die Berechtigungszertifikate authentifizieren den Diensteanbieter gegenüber dem Ausweisinhaber. Sie sind nur wenige Tage gültig und werden automatisch regelmäßig erneuert.

Welche Vorteile hat ein eID-Service gegenüber einem vom Diensteanbieter selbst betriebenen Server?

Sollte ein Diensteanbieter einen eigenen Server betreiben wollen, muss er die strengen Anforderungen erfüllen, die in der Technischen Richtlinie BSI TR-03127 „Architektur elektronischer Personalausweis und elektronische Aufenthaltstitel" des Bundesamts für Sicherheit in der Informationstechnik (BSI) dargestellt sind. Das wäre mit einem erheblichen personellen und materiellen Aufwand verbunden. Daher entscheiden sich viele für den so genannten eID-Service, den akkreditierte Zertifizierungsdiensteanbieter (ZDA) wie D-TRUST, das Trustcenter der Bundesdruckerei, bereitstellen. Die Vorteile auf einen Blick:

> ZDA verfügen über umfangreiche Erfahrungen mit dem Management von digitalen Identitäten
> ZDA stellen leistungsfähige Infrastrukturen bereit
> Der eID-Service übernimmt die gesamte Kommunikation mit dem Personalausweis-Chip

> Berechtigungszertifikate und Sperrlisten sind stets auf dem neuesten Stand
> Optimale Absicherung der Transaktionen
> Kurzfristige Integration des eID-Service in die IT-Systemarchitektur des Diensteanbieters ist möglich
> Nutzung des eID-Service ist kostengünstig und ressourcenschonend im Vergleich zum Aufbau eines eigenen Servers

Welche Leistungen übernehmen eID-Service-Anbieter für staatliche Stellen und privatwirtschaftliche Unternehmen, die den neuen Personalausweis online als Authentifizierungsdokument akzeptieren?

Der eID-Service-Anbieter liest die für den Diensteanbieter freigegebenen Daten aus dem neuen Personalausweis aus. Diese Freigabe ist abhängig von den Vorgaben der Vergabestelle für Berechtigungszertifikate (VfB), von den Anforderungen des Diensteanbieters und natürlich vom Inhaber des Ausweises, der jede Datenübermittlung mit seiner eID-PIN autorisieren muss.

Wie hoch sind die Kosten für den Diensteanbieter?

Die Kosten für die Anbindung eines eID-Service können in Abhängigkeit von den konkreten Anforderungen des Kunden und der vorliegenden IT-Infrastruktur variieren. Der Diensteanbieter kann bei der Bundesdruckerei ein individualisiertes Angebot erfragen.

Was passiert bei Verdacht auf Datenmissbrauch?

Datenmissbrauch läge vor, wenn der Diensteanbieter sein Berechtigungszertifikat für Geschäfte nutzen würde, die er zuvor bei der Beantragung der Berechtigung nicht genannt hat, oder wenn er die Kundendaten an Dritte weitergeben würde. Die Vergabestelle für Berechtigungszertifikate kann bei Verdacht auf Datenmissbrauch die Berechtigung widerrufen. Die technischen Berechtigungszertifikate der ZDA sind nur zwei Tage gültig und würden in diesem Fall nicht erneuert werden.

Was passiert, wenn ein Nutzer sich weigert, vom Diensteanbieter abgefragte Datenkategorien freizugeben?

In diesem Fall werden die Daten nicht ausgelesen und nicht übermittelt, denn der Inhaber des neuen Personalausweises muss die Datenübermittlung mit seiner PIN bestätigen und ihr so zustimmen. Grundsätzlich besitzt der Diensteanbieter eine Berechtigung der Vergabestelle für Berechtigungszertifikate für die Abfrage bestimmter Daten. Wenn der Ausweisinhaber diese nicht vollständig übermitteln möchte, entscheidet der Diensteanbieter, ob er den Vorgang fortsetzen möchte oder nicht.

Wie finden Diensteanbieter einen leistungsfähigen eID-Service-Anbieter?

Auf der Website www.personalausweisportal.de sind die verfügbaren eID-Service-Anbieter aufgeführt.

Für welche Branchen bietet der eID-Service der Bundesdruckerei seine Leistungen an?

Grundsätzlich können Unternehmen aus allen Branchen, die für ihr Internetangebot die Online-Ausweisfunktion anbieten möchten, den eID-Service der Bundesdruckerei nutzen.

Welche Vorteile hat das Integrieren der Online-Ausweisfunktion (und damit verbunden das Anbinden an einen eID-Service) gegenüber der Verwendung von Passwort und PIN für Online-Angebote?

Das Nutzen der Online-Ausweisfunktion hat sowohl für den Bürger als auch für den Diensteanbieter entscheidende Vorteile:

> Der Kunde muss sich nur ein Passwort merken statt viele; das macht den Online-Dienst deutlich komfortabler
> Es entstehen geringere Kosten für das Zurücksetzen von Passwörtern und den damit verbundenen Versand von Passwortbriefen
> Phishing- und Trojaner-Angriffe werden erschwert, das bringt höhere Sicherheit für den Betreiber des Kundenportals
> Auch die Daten des Kunden des Diensteanbieters sind so besser geschützt
> Der Diensteanbieter erfüllt automatisch die Anforderungen der Kommission für Jugendmedienschutz der Landesanstalten
> Darüber hinaus wird den Anforderungen des Geldwäschegesetzes Genüge getan

Können Diensteanbieter den eID-Service im Vorfeld testen?

Ja, die Möglichkeit besteht in verschiedenen Phasen des Projekts. Wenn sich ein Diensteanbieter für die Anbindung eines eID-Service interessiert, empfiehlt die Bundesdruckerei zunächst den Einsatz in einer Testumgebung: Dabei wird der Kanal für den Datenaustausch zwischen Diensteanbieter und Bundesdruckerei bereits abgebildet. Vordefinierte Nachrichten und Fehlercodes werden versendet, sodass sich der Diensteanbieter auf die Liveschaltung umfassend vorbereiten kann. Beispielsweise werden folgende Szenarien durchgespielt: Der Ausweisinhaber gibt die falsche PIN ein oder erteilt keine Datenfreigabe. Identitätskarten kommen in der Testumgebung nicht zum Einsatz. Dies findet im Rahmen eines Tests in der so genannten Referenzumgebung statt. Ein Testlauf in der Referenzumgebung entspricht zu nahezu 100 Prozent der tatsächlichen Umsetzung und ist beispielsweise für das Vorführen der eID-Service-Anwendung innerhalb des Unternehmens zu empfehlen. Grundsätzlich ist es möglich, bereits nach der Probe in der Testumgebung den eID-Service livezuschalten.

Datenschutz spielt für Diensteanbieter eine besondere Rolle. Wie werden bei Anwendung der Online-Ausweisfunktion Datenschutz und Datensicherheit gewährleistet?

Der neue Personalausweis bietet maximale Sicherheit für die Daten des Bürgers. Er schützt vor Identitätsdiebstahl und verhindert mithilfe von Sicherheitsprotokollen und -mechanismen, dass Unbefugte Informationen unberechtigt auslesen, kopieren oder verändern können. Bevor Daten übertragen werden, prüft der Ausweis, ob der anfragende Dienst oder die anfragende Behörde dazu berechtigt sind, diese Informationen abzufragen. Ein unbemerktes Auslesen der Daten ist nicht möglich. Darüber hinaus sind alle Informationen und Übertragungen mit international anerkannten und etablierten technischen Verfahren (Verschlüsselung und Signatur) geschützt.

Auch im Internet sind die persönlichen Informationen des Bürgers sicher: Nur wer den Ausweis besitzt und die sechsstellige PIN kennt, kann Informationen zur Übermittlung freigeben. Daten werden nur zwischen dem Ausweisinhaber und dem Diensteanbieter ausgetauscht.

Das Gesamtsystem, das die Daten des neuen Personalausweises vor unberechtigten Zugriffen schützt, ist auf einem sehr hohen technischen Sicherheitsniveau. Auch der Chip genügt höchstmöglichen Sicherheitsstandards. Das konkrete Niveau der Sicherheit hängt ebenso wie bei anderen Anwendungen, etwa dem Online-Banking oder Internetshopping, von der Computerumgebung des Nutzers ab.

GLOSSAR/ SCHLAGWORTVERZEICHNIS

A

Altersverifikation
Feature innerhalb der >Online-Ausweisfunktion des neuen Personalausweises. Ermöglicht es zu prüfen, ob der Besitzer des Dokuments eine bestimmte Altersgrenze erreicht hat. Im Sinne einer sparsamen Datenerfassung wird das genaue Geburtsdatum des Bürgers dabei nicht übermittelt.

Äußere Schnittstelle
Bestandteil des eID-Servers. Liefert bei Transaktionen mit dem neuen Personalausweis die auf dem Chip gespeicherten Daten über den international standardisierten >Token (SAML 2.0 Assertion) an den Diensteanbieter.

AusweisApp
Spezielle Treibersoftware, die auf dem PC des Bürgers installiert sein muss, damit er die >Online-Ausweisfunktion nutzen kann. Sie ermöglicht die Kommunikation zwischen Lesegerät und Ausweis. Diensteanbieter, die ihren Kunden Zugang zur AusweisApp verschaffen möchten, sollten auf das offizielle Portal https://www.ausweisapp.bund.de/pweb/index verweisen. Der Vertrieb über andere Anbieter und Websites ist nicht gestattet.

Authentifizierung
Überprüfung und Bestätigung der Identität eines Internetnutzers, der sich zuvor >authentisiert hat. Wird bei der Nutzung der Online-Ausweisfunktion durch Besitz, den Personalausweis und Kenntnis der PIN über den >eID-Server gewährleistet. Das Prinzip der Authentifizierung beider beteiligten Parteien durch eine unabhängige dritte Instanz, einen >ZDA, ist eines der Kernelemente sicherer Online-Transaktionen.

Authentisierung
Nachweis der eigenen Identität, etwa mithilfe von Wissen (z. B. Eingabe eines Codes), Besitz (Vorzeigen eines Ausweises) oder biometrischen Merkmalen. Ein Besitzer des neuen Personalausweises kann sich physisch zum Beispiel über das Vorzeigen seines neuen Personalausweises authentisieren oder im Internet über das Auslesen der auf dem >Sicherheits-Chip des neuen Personalausweises gespeicherten Daten.

B

BerCA
Berechtigungs-Certification Authority (BerCA); wird vom >ZDA betrieben und setzt technisch die Ausgabe des Berechtigungszertifikats um.

Berechtigung
Erlaubnis für Diensteanbieter, die Online-Ausweisfunktion oder die >Qualifizierte Elektronische Signatur (QES) in ihr Angebot zu integrieren. Wird von der >Vergabestelle für Berechtigungszertifikate (VfB) erteilt, einem Referat des Bundesverwaltungsamts. Voraussetzung dafür sind eine freiwillige Selbsterklärung zum Datenschutz und ein Nachweis darüber, dass die Daten, die der Diensteanbieter auslesen möchte, für sein Angebot erforderlich sind. Die erteilte Berechtigung der VfB ist maximal drei Jahre gültig und muss danach neu beantragt werden. Auf Wunsch kann ein eID-Service-Anbieter vollständig im Namen des Antragstellers handeln und ihn bei der Beantragung beim VfB unterstützen.

Berechtigungszertifikat
Erhalten Diensteanbieter, die einen individuellen Bereitstellungsvertrag mit einem >ZDA abschließen. Diese Zertifikate authentifizieren den Anbieter und ermöglichen ihm den Zugriff auf zuvor festgelegte Datenkategorien. Sie sind nur wenige Tage gültig und werden regelmäßig erneuert, sofern kein Verdacht auf Datenmissbrauch besteht.

BMI
Bundesministerium des Innern.

BSI
>Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Nationale, dem >BMI nachgeordnete Sicherheitsbehörde, zuständig für Fragen zur Sicherheit in der Informationsgesellschaft. Das BSI verantwortet unter anderem die Zulassung der Lesegeräte, mit denen der Chip des neuen Personalausweises ausgelesen werden kann, und die Akkreditierung der >ZDA.

C

CA
>Certification Authority.

Certification Authority (CA)
Zertifizierungsstelle, die digitale Zertifikate vergibt; alternative englische Bezeichnung für ZDA und >Trustcenter.

CSCA-Zertifikat
Country-Signing-Certification-Authority-Zertifikat; enthält die Landeskennung der ausstellenden Behörde. Bestandteil der >PKI und damit wesentliches Element der zahlreichen Sicherheitsmechanismen in elektronischen Ausweisdokumenten.

CVCA-eID
Country-Verifying-Certification-Authority-eID, Zertifizierungsstelle beim >BSI; stellt die nötigen Zertifikate für >ZDA wie etwa >D-TRUST aus. Mit diesen Zertifikaten erhalten ZDA die Möglichkeit, ihrerseits Berechtigungszertifikate an autorisierte Diensteanbieter und Betreiber von Visualisierungs- und Änderungsterminals auszugeben (vgl. Internet-Angebot des BSI dazu).

D

D-TRUST
Akkreditierter >ZDA, der im speziell abgesicherten Wertdruckgebäude der Bundesdruckerei betrieben wird; bietet Unternehmen und Behörden bewährte interoperable Signaturprodukte, Zertifizierungsdienstleistungen und elektronische Notariatsservices.

E

EAC
Extended Access Control; erweiterter Zugriffsschutz für die auf dem Chip des neuen Personalausweises gespeicherten Daten, der verschiedene Protokolle bündelt. Dazu gehören etwa die Protokolle „Chip Authentication" (CA), das eine sichere Verbindung zum Chip aufbaut und geklonte Chips erkennt, und „Terminal Authentication" (TA), das die sensiblen Daten des neuen Personalausweises vor dem Zugriff durch Unbefugte schützt. Beide Protokolle werden zusammen mit >PACE und >PA ausgeführt.

eGovernment 2.0
Im Jahr 2006 von der damaligen Bundesregierung verabschiedete Strategie zur Modernisierung der IT-Strukturen in der deutschen Verwaltung. Die Einführung des neuen Personalausweises und die Erarbeitung von eIdentity-Konzepten zählen zu den Kernelementen der Strategie. Die Federführung für die Umsetzung liegt beim >BMI.

eID
Electronic Identity; deutsch: elektronische Identität.

eID-PIN
Selbst gewählte sechsstellige Geheimnummer, mit der ein Nutzer jede Übertragung von Daten aus seinem neuen Personalausweis an einen >eID-Server autorisieren muss. Ohne PIN-Eingabe kann außer der Gültigkeit des Ausweises keine andere Datenkategorie übermittelt werden. Die Transport-PIN aus dem PIN-Brief der Bundesdruckerei, den alle Inhaber eines neuen Personalausweises zum Start erhalten, müssen sie sofort durch eine persönliche, nur ihnen bekannte PIN ersetzen, wenn sie die Online-Ausweisfunktion nutzen möchten. Erst dann sind Online-Transaktionen möglich.

eID-Server
Hard- und Softwareinfrastruktur, die die Kommunikation zwischen Bürgern und Diensteanbietern auf Basis der Online-Ausweisfunktion technisch ermöglicht. Diensteanbieter können entweder selbst einen eID-Server einrichten, sofern sie dabei die technischen Richtlinien des BSI beachten, oder den eID-Server eines >eID-Service nutzen.

eID-Service
Regelt die gesamte Kommunikation mit dem Personalausweis-Chip und sorgt für eine optimale Absicherung der Transaktionen. Dafür überprüft er beispielsweise die Aktualität der >Berechtigungszertifikate und hält die >Sperrlisten ungültiger Ausweise auf dem neuesten Stand.

Elektronische Signatur
Auch digitale Signatur genannt; bezeichnet elektronische Daten, die einer Mitteilung beigefügt oder mit ihr verbunden sind. Die elektronische Signatur garantiert die Echtheit und Integrität der Mitteilung. Sie stellt sicher, dass der Absender auch der ist, der er zu sein vorgibt, und dass die Mitteilung nicht auf dem Übertragungsweg vom Absender zum Empfänger verändert wurde.

ENISA
European Network and Information Security Agency; Europäische Agentur für Netz- und Informationssicherheit; berät EU-Gremien und Mitgliedstaaten und setzt sich für die Harmonisierung der unterschiedlichen ID-Konzepte innerhalb der Europäischen Union ein.

ePass
Elektronischer Reisepass, wurde in Deutschland 2005 eingeführt. Auf dem integrierten Sicherheits-Chip des ePasses der ersten Generation ist das digitale Passfoto als biometrisches Merkmal gespeichert. Beim ePass der zweiten Generation, der seit 2007 erhältlich ist, sind zusätzlich zwei Fingerabdrücke des Ausweisinhabers auf dem Chip hinterlegt. Anders als beim neuen Personalausweis ist seit dem 1. November 2007 die Speicherung der Fingerabdrücke bei Passanträgen gesetzlich vorgeschrieben und keine freiwillige Option. Damit bietet der ePass ein Höchstmaß an Fälschungssicherheit. Alte Reisepässe behalten aber ihre vorgesehene Gültigkeit. Allerdings ist für die Einreise in bestimmte Länder, zum Beispiel die USA, der ePass Voraussetzung. Seit 2005 sind drei verschiedene Passtypen in Umlauf: Reisepässe ohne Chip, elektronische Reisepässe der ersten Generation, die nur das Passfoto auf dem Chip enthalten, sowie elektronische Reisepässe der zweiten Generation, die das Passfoto und zwei Fingerabdrücke auf dem Chip speichern.

F

Fortgeschrittene elektronische Signatur
>Elektronische Signatur, die gemäß §2 >Signaturgesetz
a) ausschließlich dem Inhaber des >Signaturschlüssels zugeordnet ist,
b) die Identifizierung des Signaturschlüssel-Inhabers ermöglicht,
c) mit Mitteln erzeugt wird, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

H

Hoheitliche Ausweisfunktion
Ermöglicht es, sich gegenüber staatlich autorisierten Instanzen auszuweisen. Zugriff auf die entsprechenden Daten haben ausschließlich Polizei-, Grenz- und Zollkontrollbehörden, die Steuerfahndungsstellen der Länder sowie die Meldebehörden. Auch sie benötigen zum Auslesen spezielle >Berechtigungszertifikate, die von den >ZDA ausgestellt werden. Zudem muss der Ausweisinhaber während des Auslesevorgangs persönlich anwesend sein.

I

ID1
International gebräuchlichstes Format für Identitätskarten, von der International Organization for Standardization (ISO) unter ISO 7815 standardisiert. ID1-Karten haben die Maße 85,60 x 53,98 x 0,76 mm. Das Format wird unter anderem für Führerscheine, Bank-, Kredit- und Debitkarten eingesetzt – und seit November 2010 auch für den neuen Personalausweis.

Identitätsdiebstahl
Straftat, bei der jemand unbefugt die Identität eines anderen nutzt, um etwa dessen Ansehen zu schädigen oder in seinem Namen Geschäfte zu tätigen. Liegt vor, wenn man anhand der vom Betrüger verwendeten Daten das Opfer in einem bestimmten Zusammenhang eindeutig identifizieren kann. Gelangen Unbefugte in den

Besitz persönlicher Daten eines Bürgers wie Name, Kreditkartendaten, Anschrift und Geburtsdatum, könnten sie diese für kriminelle Zwecke verwenden.

Identitätsmanagement
Fachbegriff, der das professionelle Handling von Identitäten beschreibt. Dazu gehören etwa die sichere Verwaltung von Identitäten und der Prozess, mit dem Personen, Gruppen oder Organisationen identifiziert und ggf. authentisiert werden.

ID-Systeme
Zusammenspiel von Hochsicherheitstechnologien (Hard- und Software), das sensible Daten von Identitätsdokumenten wirksam vor dem Zugriff durch Unbefugte schützt und den Datenaustausch zwischen autorisierten Nutzern managt.

Innere Schnittstelle
Element des eID-Servers, das den Informationsaustausch mit dem neuen Personalausweis ermöglicht. Die innere Schnittstelle ist mit dem eCard API Framework des BSI (TR-03112) konform und umfasst neben mehreren kryptografischen Protokollen die Zugriffskontrollen >PACE und >EAC.

L

Lesegerät
Gehört für Bürger und für autorisierte staatliche Stellen zur Grundausstattung, um Daten aus dem neuen Personalausweis auslesen zu können. Während Standard- und Komfortkartenleser über eine eigene Tastatur („PIN-Pad") zur PIN-Eingabe verfügen, müssen Nutzer eines Basislesegeräts dafür auf ihre Computertastatur oder eine Bildschirmtastatur zurückgreifen. Um die >Qualifizierte Elektronische Signatur (QES) verwenden und die dafür nötige >Signatur-PIN eingeben zu können, benötigt der Ausweisinhaber ein Komfortlesegerät mit eigenem Display. Das BSI empfiehlt, ausschließlich zertifizierte Kartenleser einzusetzen. Man erkennt sie am kreisförmigen grün-blauen Logo des neuen Personalausweises, das auf ihnen angebracht ist.

N

Neuer Personalausweis (nPA)
Neuer Identitätsnachweis im >ID1-Format für Bürger der Bundesrepublik Deutschland; seit November 2010 verfügbar. Der nPA enthält einen >Sicherheits-Chip und dient nicht nur als Sichtausweis, sondern auf Wunsch des Bürgers auch als elektronischer Identitätsnachweis im Internet.

O

Online-Ausweisfunktion
Auch elektronische Ausweisfunktion des neuen Personalausweises; erlaubt es dem Bürger erstmals, sich mit seinem Identitätsnachweis im Internet zu erkennen zu geben. Dabei entscheidet allein der Ausweisinhaber, welche Informationen er mit seiner sechsstelligen >eID-PIN für jede einzelne Transaktion freigeben möchte. Um die Online-Ausweisfunktion nutzen zu können, muss der Dokumenteninhaber sie aktiviert haben, die >Ausweis-App auf seinem PC installiert haben und mindestens 16 Jahre alt sein. Darüber hinaus muss der Geschäftspartner im Internet den elektronischen Identitätsnachweis ausdrücklich anbieten und sich zunächst selbst als berechtigter Online-Partner zu erkennen geben.

P

PA
>Passive Authentication.

PACE
Password Authenticated Connection Establishment; Sicherheitsprotokoll, das den kontaktlosen >Sicherheits-Chip im neuen Personalausweis vor unbefugten Zugriffen schützt: Dank PACE kann er erst ausgelesen werden, wenn der Inhaber seine sechsstellige >eID-PIN eingegeben hat. Außerdem sorgt PACE für die Verschlüsselung der Daten, die an das Lesegerät übertragen werden.

Passive Authentication (PA)
Prüft, ob die Daten auf dem kontaktlosen Chip des neuen Personalausweises echt und unverfälscht sind. Das trifft nur dann zu, wenn sie mit dem digitalen Document-Signing-Zertifikat der Bundesdruckerei signiert sind. Nur die Bundesdruckerei hat die offizielle Befugnis des >BMI, Daten auf dem Chip des neuen Personalausweises zu speichern. Das Document-Signing-Zertifikat selbst ist außerdem mit einem weiteren Zertifikat ausgezeichnet, dem >CSCA-Zertifikat. Während der nPA ausgelesen wird, überprüft die Software mithilfe der PA die Signatur des Chips und verfolgt sie zurück bis zum CSCA-Zertifikat.

PAuswG
>Personalausweisgesetz.

Personalausweisgesetz (PAuswG)
Im Jahr 2009 vom Bundestag verabschiedetes Gesetz, das alles Rechtliche rund um den neuen Personalausweis und den elektronischen Identitätsnachweis regelt. Es umfasst unter anderem die mit der neuen Rechtslage verbundenen Änderungen des Passgesetzes, des Melderechtsrahmengesetzes, der Signaturverordnung und des Geldwäschegesetzes und kann zum Beispiel unter
http://www.personalausweisportal.de/SharedDocs/Downloads/DE/pauswg.pdf?__blob=publicationFile
aus dem Netz heruntergeladen werden.

PIN
Personal Identification Number bzw. persönliche Identifikationsnummer oder Geheimnummer; mit ihr authentisiert sich eine natürliche Person gegenüber einer Maschine.

PKI
Public Key Infrastructure; bezeichnet ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann. Im Mittelpunkt eines PKI-Aufbaus steht stets eine Software zum Betrieb der Zertifizierungsstelle (>Certification Authority, CA).

Pseudonymfunktion
Feature des neuen Personalausweises, das es ermöglicht, sich ohne Eingabe persönlicher Daten zum Beispiel in Online-Portale einzuloggen. Sofern der Diensteanbieter die Online-Ausweisfunktion unterstützt und den Einsatz der Pseudonymfunktion akzeptiert, erzeugt der eID-Server ein Pseudonym speziell für das jeweilige Online-Angebot. Es kann nicht mit anderen Pseudonymen des jeweiligen Nutzers abgeglichen werden.

PUK
Personal Unblocking Key bzw. Entsperrnummer, die der Bürger mit dem PIN-Brief der Bundesdruckerei erhält und unzugänglich für andere aufbewahren sollte. Dient zum Entsperren der Online-Ausweisfunktion, falls versehentlich drei Mal hintereinander die falsche eID-PIN eingegeben wurde. Ein PUK kann bis zu zehn Mal verwendet werden.

Q

Qualifizierte Elektronische Signatur (QES)
Besondere Form der >fortgeschrittenen elektronischen Signatur, die gemäß >Signaturgesetz a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht und b) mit einer sicheren Signaturerstellungseinheit erzeugt wird. Für manche Willenserklärung (bspw. Darlehensverträge) wird die Schriftform gemäß §126 BGB gefordert. Damit ist gemäß §126 a BGB im Fall des elektronischen Datenaustauschs eine QES erforderlich. Zusätzlich schreiben verschiedene Gesetze ohne Verweis auf die gesetzliche Schriftform bereits explizit eine QES (manchmal mit Anbieterakkreditierung oder langfristiger Überprüfbarkeit) zur Unterzeichnung von elektronischen Dokumenten vor.

Um die QES nutzen zu können, benötigt der Bürger ein Komfortlesegerät sowie ein >Signaturzertifikat und eine >Signatur-PIN, die beide bei einem >ZDA zu beziehen sind. Die QES ist der persönlichen Unterschrift rechtlich gleichgestellt.

R

Restricted Identification (RI)
Sicherheitsprotokoll zur Erzeugung von chip- und anwenderspezifischen Pseudonymen.

RI
>Restricted Identification.

S

SAML 2.0 Token
Security-Assertion-Markup-Language-2.0-Token; Standard für den sicheren Austausch von Authentifizierungen und Autorisierungen zwischen Domains. SAML Assertions sind Aussagen, anhand derer ein eID-Service-Provider Zugang zu bestimmten Dienstleistungen gewährt. Der SAML- Token beinhaltet die Informationen vom Ausweis und wird dem Diensteanbieter zur Weiternutzung zur Verfügung gestellt.

Sicherheits-Chip
Berührungslos lesbarer Computerchip, der in den neuen Personalausweis integriert ist. Auf ihm sind folgende Informationen in digitalisierter Form gespeichert: die Daten der aufgedruckten maschinenlesbaren Zone (Rückseite), Familien- und Geburtsname, Vorname(n), Doktorgrad, Tag und Ort der Geburt, Foto, Anschrift, Staatsangehörigkeit, Seriennummer sowie Ordens- oder Künstlername. Auf Wunsch des Ausweisinhabers können im Chip zusätzlich die Daten von zwei Fingerabdrücken und die Zertifikatinformation zur Nutzung einer >Qualifizierte Elektronische Signatur (QES) hinterlegt werden.

Sicherheitsprotokoll
Festgelegte Schemata von Datenabfolgen für die Kommunikation zwischen einem Chip und einem Lesegerät. Sicherheitsprotokolle wie >EAC oder >PACE gewährleisten Datenschutz, Fälschungssicherheit und Authentizität der Daten im neuen Personalausweis.

SigG
>Signaturgesetz.

Signaturgesetz (SigG)
Gesetz über Rahmenbedingungen für elektronische Signaturen, kurz SigG oder SigG 2001, vom 16. Mai 2001; definiert Regeln für die Verwendung >elektronischer Signaturen.

Signatur-PIN
Vom >ZDA vergebene Geheimnummer, die der Ausweisinhaber benötigt, um ein Dokument elektronisch zu unterschreiben.

Signaturschlüssel
Gemäß § 2 >SigG einmalige elektronische Daten wie private kryptografische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden.

Signaturzertifikat
Elektronisches Zertifikat, das der Bürger benötigt, um die Qualifizierte Elektronische Signatur (QES) anwenden zu können. Es ist bei einem >ZDA zu erwerben.

Sperrdienst
Sperrt die elektronische Ausweisfunktion des neuen Personalausweises, um einen Missbrauch bei Diebstahl oder Verlust auszuschließen; wird von der >VfB betrieben. Zu den zentralen Aufgaben des Sperrdienstes gehören die zentrale Führung und Speicherung einer Sperrliste mit den Sperrschlüsseln der abhandengekommenen Personalausweise mit eingeschalteter >Online-Ausweisfunktion, die Bereitstellung von Schnittstellen zum Ausweishersteller, zur Hotline und zu den Personalausweisbehörden sowie die Weitergabe der Sperrlisten an die Zertifizierungsdienste.

Sperrhotline
Telefonnummer, unter der Bürger den Verlust ihres neuen Personalausweises unter Angabe von Name, Vorname, Geburtsdatum und >Sperrkennwort melden müssen, sofern sie die >Online-Ausweisfunktion aktiviert haben. Parallel ist die zuständige Personalausweisbehörde zu verständigen, da kein automatischer Austausch zwischen der Sperrhotline und den Ausweisbehörden stattfindet.

Sperrkennwort
Leicht zu merkendes Kennwort (z. B. Lokomotive), das der Bürger benötigt, um seinen >nPA bei Verlust oder Diebstahl sperren zu lassen. Das Sperrkennwort wissen nur der Ausweisinhaber und die ausstellende Meldestelle. Der Anwender gibt es – anders als PIN und PUK – nicht am Computer ein. Vielmehr fragen Mitarbeiter der Sperrhotline oder der Personalausweisbehörde es ab.

Sperrliste
Verzeichnis der aufgrund von Diebstahl oder Verlust gesperrten Personalausweise; wird von der >VfB betrieben.

Sperrmanagement
Prozess der Sperrung eines elektronischen Identifikationsdokuments, zum Beispiel eines neuen Personalausweises.

SSL-Verschlüsselung
Secure Sockets Layer; dieses Sicherheitsprotokoll ermöglicht sichere Datenübertragungen im Internet.

SSL-Zertifikat
Verschlüsselt die Kommunikation von Diensteanbietern mit Nutzern ihrer Website. SSL-Zertifikate können Diensteanbieter bei einem >ZDA erwerben.

STORK
Secure Identity Across Borders Linked; EU-Projekt mit dem Ziel, eine EU-weite Plattform für die Interoperabilität von >eIDs einzuführen. Diese Plattform soll es den Bürgern ermöglichen, ihre nationalen eIDs für eGovernment-Dienste in mehreren europäischen Ländern zu nutzen. Weitere Informationen unter https://www.eid-stork.eu/.

T

Token-Zertifikat
Erlaubt dem Diensteanbieter den Zugriff auf den >eID-Service.

Trustcenter
Akkreditierter Zertifizierungsdiensteanbieter (>ZDA).

V

Vergabestelle für Berechtigungszertifikate (VfB)
Referat des Bundesverwaltungsamts; kontrolliert die Vergabe von Berechtigungszertifikaten, betreibt die >Sperrlisten und kümmert sich um das >Sperrmanagement. Diensteanbieter müssen klar definierte Vorgaben gemäß § 21 des deutschen >PAuswG erfüllen und diese der VfB gegenüber schriftlich nachweisen sowie eine freiwillige Selbsterklärung zum Datenschutz beibringen, um eine >Berechtigung zur Abfrage von Personalausweisdaten zu erhalten. Die erteilte Berechtigung der VfB ist maximal drei Jahre gültig. Sie ist zwingend erforderlich, damit der Diensteanbieter einen individuellen Bereitstellungsvertrag mit einem >ZDA abschließen und technische >Berechtigungszertifikate erwerben kann.

VfB
>Vergabestelle für Berechtigungszertifikate.

W

Wohnortverifikation
Funktion innerhalb der Online-Ausweisfunktion des neuen Personalausweises; bestätigt oder verneint eine Wohnortanfrage des Diensteanbieters. Im Sinne einer sparsamen Datenerfassung wird die vollständige Anschrift des Bürgers nicht übermittelt.

Z

ZDA
>Zertifizierungsdiensteanbieter.

Zertifizierungsdiensteanbieter (ZDA)
Certification Authority (CA); von der Bundesnetzagentur nach dem >SigG in der Fassung vom 17. Juli 2009 angezeigter Dienstleister, der qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen darf. Ausschließlich akkreditierte ZDA sind befugt, >Berechtigungszertifikate für Diensteanbieter auszustellen. Die Liste der ZDA ist unter http://www.nrca-ds.de/ZDAliste.htm einzusehen.

FUSSNOTEN

01 Vgl.: http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung.

02 Security-Monitor des IT-Dienstleisters Unisys, vgl. http://www.unisys.de/about__unisys/presse/10102701.htm.

03 Vgl.: BSI-Studie „Identitätsdiebstahl und Identitätsmissbrauch im Internet – Rechtliche und technische Aspekte".

04 Vgl.: http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung.

05 GO SMART 2012: Always-In-Touch, Studie zur Smartphonenutzung 2012. Hrsg. Google, Otto Group, TNS Infratest und Trendbüro.

06 Repräsentative Forsa-Umfrage im Auftrag von BITKOM im November 2010, vgl. http://www.bitkom.org/65912_65908.aspx.

07 Security-Monitor des IT-Dienstleisters Unisys, vgl. http://www.unisys.de/about__unisys/presse/10102701.htm.

08 In der Technischen Richtlinie BSI TR-03127 „Architektur elektronischer Personalausweis und elektronische Aufenthaltstitel" des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist ein Überblick zu allen technischen Spezifikationen zu finden.

09 Technische Universität Darmstadt, Projekt 826, Studie „Sicherheitsanalyse des EAC-Protokolls", 11. Oktober 2010.

10 Institut für Internet-Sicherheit an der Fachhochschule Gelsenkirchen, Zwischenbericht „Restrisiken beim Einsatz der AusweisApp auf dem Bürger-PC zur Online-Authentisierung mit Penetration-Test", Oktober 2010.

11 https://www.eid-stork.eu/.

12 Das Erasmus-Programm wurde am 15. Juni 1987 durch den Beschluss 87/327/EWG des Ministerrats gegründet. Ziel des Programms ist es, die Zusammenarbeit von Hochschulen innerhalb der EU und anderen europäischen Ländern sowie die Mobilität von Studenten und Dozenten zu fördern.

13 STORK-Pressemitteilung vom 25. Oktober 2010 und Bundesamt für Sicherheit in der Informationstechnik (BSI).

Bundesdruckerei GmbH
Unternehmenskommunikation
Oranienstraße 91
10969 Berlin
www.bundesdruckerei.de

Stand August 2011

www.bundesdruckerei.de