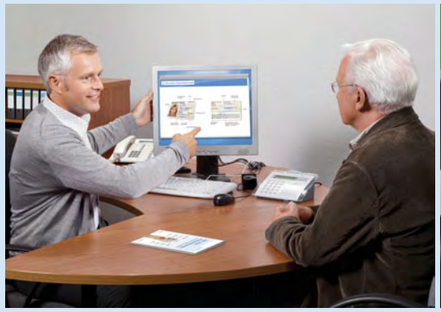
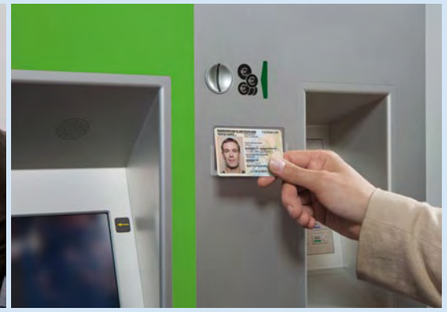
Der neue Personalausweis
Meine wichtigste Karte.

Der Personalausweis

Anwenderhandbuch für Wirtschaft und Verwaltung

Bundesministerium des Innern

Herausgegeben vom Bundesministerium des Innern

Inhalt

Abbildungsverzeichnis

1 Einleitung

Seit dem 1. November 2010 wird auf Grundlage des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis ein neuer Personalausweis ausgegeben. Mit diesem neuen Ausweisdokument setzt Deutschland neue Maßstäbe im Identitätsmanagement.

Heute werden immer mehr Dienstleistungen von Unternehmen und Behörden über das Internet angeboten. Diesen Schritt geht der neue Personalausweis mit und eröffnet damit neue Möglichkeiten in der Interaktion von Geschäftspartnern in der Online-Welt. Bisherige Hürden in der Umsetzung von Geschäftsprozessen im Internet werden damit überwunden. Neue Anwendungen werden insbesondere dort realisiert, wo die Überprüfung der Identität gesetzlich vorgeschrieben ist oder Geschäftsprozesse noch der Schriftform bedürfen.

Der neue Personalausweis leistet einen Beitrag zur sicheren Abwicklung von Geschäftsprozessen. Für die öffentliche Verwaltung und die Wirtschaft ist der neue Personalausweis ein Katalysator: Er vereinfacht bestehende Geschäftsprozesse, stößt neue an und trägt zu effizienteren Abläufen bei und sorgt für eine sichere Kommunikation und Abwicklung von Dienstleistungen zwischen Nutzern und Anbietern von Dienstleistungen.

Das hier vorliegende Dokument richtet sich dabei in erster Linie an Entscheidungsträger in Unternehmen aller Branchen und Verwaltungsinstitutionen. Ihnen soll eine Entscheidungshilfe für folgende Fragestellungen gegeben werden:

- Was leisten die innovativen Funktionen des neuen Personalausweises?
- Wofür kann ich den neuen Personalausweis einsetzen?
- Kann ich den neuen Personalausweis auch in die Dienste meines Unternehmens und meiner Behörde integrieren?

In drei Abschnitten werden schrittweise sowohl die Anwendungen als auch die hierfür benötigten Infrastrukturkomponenten des neuen Personalausweises erläutert. In einem ersten Schritt soll ein Überblick über den neuen Personalausweis und seine Funktionen gegeben werden (Kapitel 1 und 2). In den sich daran anschließenden Kapiteln 3 und 4 werden die technischen und infrastrukturellen Voraussetzungen für Unternehmen und Behörden dargestellt. In den Kapiteln 5 bis 9 wird die Umsetzung erläutert. Abschließend werden die wichtigsten Informationen und Fragestellungen nochmals zusammengefasst.

Der hier vorliegende Leitfaden soll Ihnen dabei einen Überblick verschaffen, welche Möglichkeiten mit dem neuen Personalausweis bestehen und was bei einer Umsetzung und Integration in die Geschäftsprozesse zu beachten ist. Anhand von Anwendungsbeispielen werden Ihnen diese Möglichkeiten anschaulich dargestellt. Dabei ist der Leitfaden nicht als Anleitung zu verstehen, wie Anwendungen mit dem neuen Personalausweis konkret bei Anbietern von Diensten umgesetzt und implementiert werden können. Allerdings können Sie nach dem Studium dieses Leitfadens eine qualifizierte Entscheidung darüber treffen, welcher Nutzen mit dem Einsatz des neuen Personalausweises für Ihre bestehenden Geschäfts- und Verwaltungsprozesse verbunden sein kann.

2 Der Personalausweis mit seinen neuen Funktionen

2.1 Die Ausweiskarte

Der neue Personalausweis enthält einen kontaktlos lesbaren Chip, in dem die Daten des Besitzers elektronisch abgelegt sind.

Der neue Personalausweis hat nicht nur das praktische Format einer Scheckkarte, sondern bietet darüber hinaus auch noch weitere wesentliche Innovationen an. Im Vergleich zum bisherigen Ausweis sind zwei neue Datenfelder hinzugekommen: die Zugangsnummer auf der Vorderseite und der Ordens- und Künstlername auf der Rückseite. Eine weitere wichtige Neuerung ist die Ergänzung der Anschrift um die Postleitzahl. Hierüber ist es für den Anbieter eines Dienstes erstmals möglich, die vollständige Anschrift eines Geschäftspartners über die Daten des Personalausweises zu erhalten.

Abbildung 1: Vorder- und Rückseite des neuen Personalausweises

Das Logo zeigt an, wo Dienstleistungen mit dem neuen Personalausweis angeboten werden.

Im Innern des neuen Personalausweises ist ein kontaktlos lesbarer Computerchip integriert. Auf dem Chip sind die folgenden Daten des Ausweisinhabers digital abgelegt:

- Familienname und Geburtsname
- Vornamen
- Doktorgrad
- Tag und Ort der Geburt
- Lichtbild
- Anschrift, bei Anschrift im Ausland die Angabe „keine Hauptwohnung in Deutschland“
- Staatsangehörigkeit
- Seriennummer
- Ordensname, Künstlername
- ggf. die digitalen Fingerabdrücke
- Daten der maschinenlesbaren Zone
- Daten zur Nutzung der Signaturfunktion

Zum Design des neuen Personalausweises gehört auch ein Logo, das sich auf der Rückseite des Ausweises befindet. Mit diesem Logo können Anbieter einer Dienstleistung mit dem neuen Personalausweis zeigen, dass bei ihnen der Ausweis für die Dienstleistung eingesetzt werden kann. Die zwei sich ergänzenden Halbkreise des Logos stehen für das Prinzip des gegenseitigen Ausweisens von Nutzer und Anbieter und symbolisieren die Verwendung des Ausweises in Online- und Offline-Welt.

2.2 Identitätsnachweis mit der Online-Ausweisfunktion

Was ist die Online-Ausweisfunktion?

Der Identitätsnachweis erfolgt nach dem Prinzip der Gegenseitigkeit: Auf der einen Seite können Bürgerinnen und Bürger mit der Online-Ausweisfunktion ihre Identität nachweisen, auch ohne persönlich anwesend zu sein. Dies erfolgt ebenso einfach und sicher wie das Vorzeigen eines Ausweises im Alltag. Auf der anderen Seite können Anbieter von Online-Dienstleistungen diese Funktion in ihre Prozesse einbinden, um sicher zu sein, wer ihr Partner in einem Geschäftsprozess ist. Weitere Anstrengungen bezüglich der Identitätsüberprüfung entfallen.

Folgende Abbildung veranschaulicht das Prinzip der Gegenseitigkeit:

Abbildung 2: Die gegenseitige Authentisierung der Online-Ausweisfunktion

Anbieter können die Identität einer Person prüfen. Bürgerinnen und Bürger können im Gegenzug verlässlich feststellen, bei welchem Unternehmen oder welcher Behörde sie sich mit dem neuen Personalausweis anmelden.

Die elektronische Identität kann bei allen Anbietern von Leistungen mit dem Ausweis eingesetzt werden. Die Online-Ausweisfunktion kann erst mit Erreichen der Ausweispflicht – also ab 16 Jahren – verwendet werden. Voraussetzung für die Übermittlung der Daten ist die Eingabe einer PIN durch den Nutzer. Ebenso haben Bürgerinnen und Bürger die Möglichkeit, die Online-Ausweisfunktion in der Personalausweisbehörde ausschalten zu lassen. In diesem Fall können sie allerdings keinen Gebrauch mehr von der Online-Ausweisfunktion machen.

Die Vorteile auf einen Blick

- Service für den Kunden
- Sichere Datenübermittlung und hohe Datenqualität
- Sicherheit über Identität des Geschäftspartners
- Schlankere Prozesse
- Stärkeres Vertrauen in der Geschäftsbeziehung

Mit der Online-Ausweisfunktion können sich Unternehmen und Behörden einer hohen Qualität der Daten aus dem Personalausweis sicher sein. Sie können die Identität einer Person bzw. eines Kunden eindeutig überprüfen. Dabei kann der Authentisierungsmechanismus für viele verschiedene Anwendungen in den unterschiedlichsten Bereichen eingesetzt werden. Es können neue Dienste angeboten werden, die zuvor nicht möglich waren. Hier profitieren die Unternehmen und Behörden von einer sicheren Datenübermittlung sowie einem besseren Service für ihre Kunden und Bürger. Diese müssen sich nicht mehr Benutzernamen und Passwörter merken, sondern melden sich mit dem neuen Personalausweis an.

Unternehmen und Behörden, die die Online-Ausweisfunktion nutzen, können zudem von schlankeren automatisierten Prozessen profitieren. Geschäftsvorfälle und Bürgerdienste können medienbruchfrei und unabhängig von Öffnungszeiten im Internet abgewickelt werden. Hinzu kommt, dass zukünftig nahezu jede Bürgerin und jeder Bürger einen neuen Personalausweis besitzen wird. Ab 2011 wird ebenfalls der elektronische Aufenthaltstitel mit der gleichen Technik wie der neue Personalausweis erstellt, so dass sich ab diesem Zeitpunkt auch in Deutschland lebende Bürgerinnen und Bürger aus Nicht-EU-Staaten sicher authentisieren können. Zeit- und ressourcenintensives persönliches Vorstellen, Identitätsprüfung oder der Versand von Dokumenten entfallen. Dabei ist der Integrationsaufwand überschaubar. Die angebotenen Webanwendungen können eine standardisierte Schnittstelle verwenden, um den elektronischen Identitätsnachweis zu unterstützen.

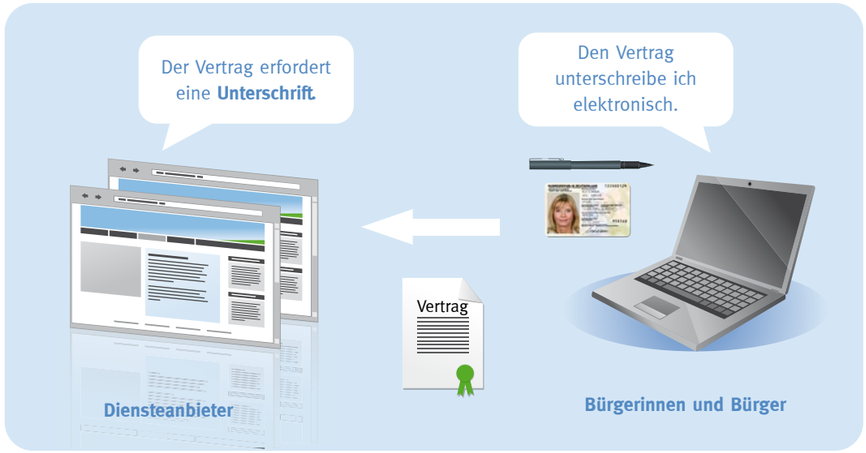
Um Dienstleistungen mit dem neuen Personalausweis anbieten zu können, benötigt ein Unternehmen nicht nur die technische Infrastruktur, sondern auch eine staatliche Berechtigung (siehe auch Abschnitt 4.1). Der Zugriff auf die Daten des Personalausweises ist möglich, sofern die Erforderlichkeit der Datenverwendung im Geschäftsprozess des Diensteanbieters gegeben ist.

2.3 Die Unterschriftsfunktion mit der qualifizierten elektronischen Signatur

Der neue Personalausweis ist mit der Unterschriftsfunktion (wird auch als Signaturfunktion bezeichnet) für die qualifizierte elektronische Signatur (QES) vorbereitet. Während die Online-Ausweisfunktion durch den Staat zur Verfügung gestellt wird, erfolgt die Ausgabe von Signaturzertifikaten durch private Anbieter. Das bedeutet, dass der Personalausweisinhaber ein Signaturzertifikat bei einem privaten Anbieter eigenständig erwirbt und nachlädt. Eine Liste aller aktuellen Zertifizierungsdiensteanbieter findet sich im Verzeichnisdienst der Bundesnetzagentur unter http://www.nrca-ds.de. Voraussetzung für das Nachladen ist, dass die Online-Ausweisfunktion eingeschaltet ist.

Mit der Unterschriftsfunktion können Dokumente elektronisch signiert werden. Die QES erfüllt alle rechtlichen Anforderungen einer Unterschrift nach dem Signaturgesetz und ist damit der persönlichen eigenhändigen Unterschrift nach § 126 a des Bürgerlichen Gesetzbuches sowie nach § 3 a Nr. 2 des Verwaltungsverfahrensgesetzes gleichgestellt. Eine solche dient dem rechtssicheren Nachweis z. B. der Willenserklärung in Verträgen, die die Schriftform erfordern, oder bei Anträgen und Auskünften im Verwaltungsverfahren.

Folgende Abbildung verdeutlicht den Einsatz der Unterschriftsfunktion mit dem neuen Personalausweis:



Mit der Unterschriftsfunktion können digitale Dokumente rechtsverbindlich unterschrieben werden.

Abbildung 3: Abschluss rechtskräftiger Verträge mit der Unterschriftsfunktion

Der Unterzeichner bestätigt durch seine digitale Unterschrift, dass er das Dokument gelesen hat und den Regelungen zustimmt. Zusätzlich kann bei einem signierten Dokument erkannt werden, ob dieses nachträglich geändert worden ist. Unternehmen und Behörden können auf diese Weise ihren Kunden anbieten, Dokumente wie z.B. Verträge oder Vollmachten elektronisch und somit medienbruchfrei rechtsverbindlich zu unterzeichnen.

Die Vorteile auf einen Blick

- Rechtsverbindliche Unterschrift elektronischer Dokumente
- Keine separate Signaturkarte beim Kunden erforderlich
- Unmittelbarer und schneller Abschluss von Verträgen, die der Schriftform bedürfen
- Abwicklung von Diensten rund um die Uhr
- Unterstützung der elektronischen Archivierung

Die Einbindung der Unterschriftsfunktion kann Geschäftsprozesse, die heute noch den persönlichen oder postalischen Austausch von Dokumenten erfordern, vollständig ins Internet verlagern. Dokumente können weitgehend rechtlich gleichgestellt elektronisch unterzeichnet werden. Anschließend lässt sich anhand der elektronischen Signatur zweifelsfrei erkennen, ob Dokumente nach dem Signieren verändert worden sind. Das ermöglicht insbesondere die schnellere und durchgängig elektronische Abwicklung von Diensten und den vollständig elektronischen Abschluss von formbedürftigen Verträgen.

Bürgerinnen und Bürger profitieren von einer unmittelbaren Abwicklung ihrer Dienste im Internet rund um die Uhr. Eine Beschränkung durch Öffnungs- oder Bürozeiten entfällt.

Für Behörden und Unternehmen sind Einsparungen durch die Umsetzung automatisierter elektronischer Geschäftsprozesse von Vorteil. Weiterhin unterstützt die qualifizierte elektronische Signatur in elektronischen Dokumenten-Managementsystemen die sichere langfristige Archivierung der Datenbestände in Behörden und Unternehmen.

Der neue Personalausweis kann mit der Unterschriftsfunktion somit einen wichtigen Beitrag zur weiteren Etablierung der QES bei Bürgerinnen und Bürgern sowie in Wirtschaft und Verwaltung leisten.

2.4 Was sind die Unterschiede zwischen Online-Ausweis- und Unterschriftsfunktion?

Das elektronische Signieren und die Integritätsprüfung elektronisch signierter Dokumente erfordern gemäß Signaturgesetz für qualifizierte elektronische Signaturen eine sichere Signaturerstellungseinheit und eine sichere Signaturanwendungskomponente. Als Signaturerstellungseinheit ist der neue Personalausweis geeignet und als Signaturanwendungskomponente die AusweisApp.

Die Online-Ausweisfunktion und die Unterschriftsfunktion folgen dabei zwei unterschiedlichen Logiken. Die Online-Ausweisfunktion stellt einen Nachweis der Identität im Internet dar, im Sinne von „Das bin ich“. Die Unterschriftsfunktion zeigt: „Das habe ich unterschrieben.“

	Online-Ausweisfunktion	Unterschriftsfunktion
Logik	„Das bin ich“	„Das habe ich unterschrieben“
Zweck	Sicherer Identitätsnachweis	Rechtsverbindliche Unterschrift
Anbieter	Staat	Zertifizierungsdiensteanbieter
Aktivierung	Personalausweisbehörde	Zertifizierungsdiensteanbieter
Anzeige	Identität des Diensteanbieters und angeforderte Daten	Zu unterzeichnendes Dokument
Zugriffsschutz	eID-PIN	Signatur-PIN

Abbildung 4: Die Unterschiede zwischen der Online-Ausweis- und der Unterschriftsfunktion

Die Online-Ausweisfunktion umfasst den gegenseitigen Identitätsnachweis des Diensteanbieters mit einem staatlichen Berechtigungszertifikat und des Personalausweisinhabers mit einem Personalausweis, dessen Online-Ausweisfunktion von einer Personalausweisbehörde aktiviert wurde.

Die Unterschriftsfunktion wird im Unterschied dazu von Zertifizierungsdiensteanbietern im Wettbewerb angeboten. Der neue Personalausweis ist für die Nutzung dieser Funktion lediglich vorbereitet. Das Nachladen des Zertifikats übernimmt der Nutzer selbst über den gewählten privaten Anbieter.

3 Infrastruktur und Technik

Für die technische Umsetzung der neuen Funktionen wird eine reibungslos funktionierende Personalausweis-Infrastruktur vorausgesetzt, die Datenschutz und Datensicherheit gewährleistet. Sowohl Bürgerinnen und Bürger als auch die Diensteanbieter müssen technische Voraussetzungen erfüllen, um in diese Infrastruktur eingebunden werden zu können. Diese Voraussetzungen werden im Folgenden erläutert.

Generell basiert die gesamte Infrastruktur auf der Ausweiskarte mit Chip und auf einer Public-Key-Infrastruktur (PKI) für Berechtigungszertifikate sowie dem Sperrmanagement. An der Infrastruktur sind eine Reihe von Behörden und Unternehmen beteiligt. Dazu gehören insbesondere:

- das Bundesamt für Sicherheit in der Informationstechnik (BSI) als oberste Zertifizierungsstelle (Root-CA)
- das Bundesverwaltungsamt (BVA) mit der Vergabestelle für Berechtigungszertifikate (VfB) und dem Sperrdienst
- die Zertifizierungsdiensteanbieter (BerCA), die die technische Ausstellung der Berechtigungszertifikate übernehmen
- die Bundesdruckerei als Hersteller der neuen Ausweise
- die Anbieter von Hardware, Software und Diensten für die Anwendung des neuen Personalausweises (z. B. eID-Service-Anbieter)

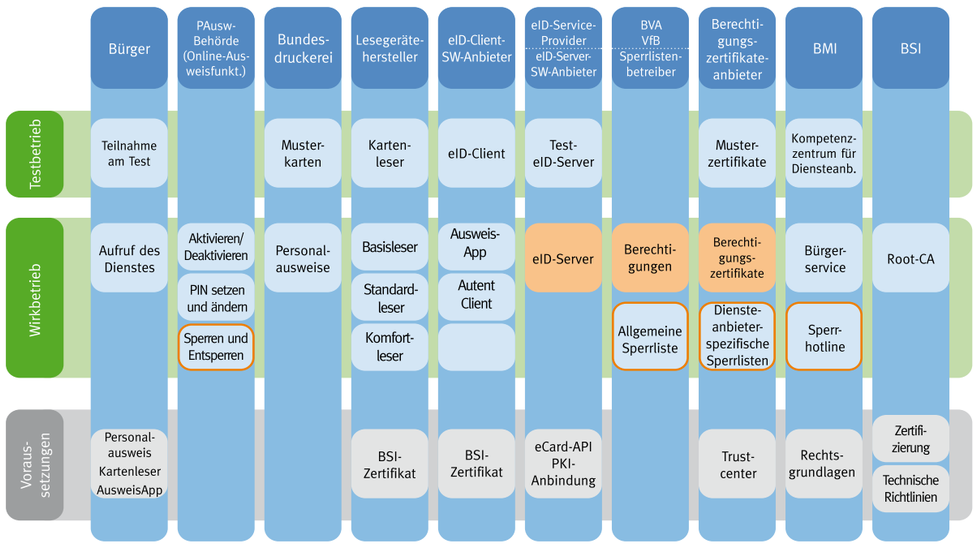


Abbildung 5: Übersicht über die Infrastruktur und Technik

- der Service für Personalausweisinhaber in Kommunen und im telefonischen Bürgerservicezentrum, einschließlich der Sperrhotline

In Abbildung 5 werden die an der Personalausweis-Infrastruktur beteiligten Akteure, d. h. die Ausweisinhaber, Hard-, Software- und IT-Diensteanbieter sowie Behörden, einschließlich ihrer Hauptaufgaben im Test- und Wirkbetrieb dargestellt. Der Testbetrieb dient potenziellen Anwendern aus Wirtschaft und öffentlicher Verwaltung zur Erprobung neuer Dienste. Er wird in Abschnitt 7.2 näher erläutert. Für den Wirkbetrieb sind die Komponenten farblich hervorgehoben, die die Diensteanbieter benötigen: die Berechtigung von der VfB (siehe auch Kapitel 4), das Berechtigungszertifikat von einem Zertifizierungsdiensteanbieter (siehe auch Abschnitt 3.2.1) und einen eID-Server bzw. eID-Service (siehe auch Abschnitt 2.2.2), der auch die diensteanbieterspezifischen Sperrlisten abruft und prüft.

Ein vereinfachtes Infrastrukturmodell, das die wesentlichen Beziehungen zwischen den Beteiligten an der Online-Ausweisfunktion veranschaulicht, enthält die Anlage 1.

3.1 Infrastruktur bei Bürgerinnen und Bürgern

Um sich mit dem neuen Personalausweis im Internet ausweisen zu können, muss die Online-Ausweisfunktion eingeschaltet sein. Für die Nutzung am eigenen Computer werden benötigt:

- **der Personalausweis mit eingeschalteter Online-Ausweisfunktion.** Diese kann bei der zuständigen oder ausstellenden Personalausweisbehörde ein- und ausgeschaltet werden.
- **das Kartenlesegerät.** Es wird empfohlen, ein handelsübliches Kartenlesegerät für Karten mit kontaktlosen Chips zu nutzen, das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert ist. Obwohl der neue Personalausweis auch in Verbindung mit einfachen Basislesegeräten deutlich mehr Schutz vor Identitätsmissbrauch bietet als die üblichen Anmeldeverfahren per Nutzername und Passwort, wird darauf hingewiesen, dass für die Sicherheit des PCs ein jeweils aktueller Virenscanner, das Betriebssystem mit allen sicherheitsrelevanten Updates und eine Firewall verwendet werden sollten.
- **Anwendungs-Software.** Zur Nutzung der Online-Ausweisfunktion ist eine Software nötig, die die Kommunikation zwischen Anbietersystem und Personalausweis ermöglicht. Es wird empfohlen, nur Client-Software zu verwenden, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert ist. Als Anwendungs-Software kann beispielsweise die sogenannte AusweisApp genutzt werden, die den Bürgerinnen und Bürgern kostenfrei vom Bund bereitgestellt wird.
- **die eID-PIN (PIN für die Online-Ausweisfunktion).** Eine sechsstellige Geheimnummer, mit der der Personalausweisinhaber bestätigt, dass die Daten aus seinem Personalausweis übermittelt werden dürfen. Die eID-PIN ist personengebunden.

Das Nachladen der Unterschriftsfunktion erfordert einmalig die Online-Ausweisfunktion, um sich beim Zertifikateanbieter für die qualifizierte elektronische Signatur sicher zu authentisieren. Der weitere Gebrauch der Unterschriftsfunktion ist von der Online-Ausweisfunktion unabhängig. Beide Funktionen besitzen unterschiedliche PINs. Zusätzlich werden folgende Komponenten für die Unterschriftsfunktion benötigt:

- **die Signatur-PIN (Unterschriftsfunktion).** Eine sechsstellige Geheimnummer, mit der der Personalausweisinhaber bestätigt, dass die qualifizierte elektronische Signatur von ihm stammt. Die Signatur-PIN ist personenbezogen und wird vom Personalausweisinhaber über die AusweisApp oder eine andere Client-Software vor dem Nachladen des Signaturzertifikats auf den Ausweis-Chip selbständig gesetzt.

- **das Signaturzertifikat.** Signaturzertifikate werden nicht von den Personalausweisbehörden ausgestellt, sondern von speziellen Dienstleistern, die nach dem Signaturgesetz (SigG) staatlich zugelassen sind. Das Signaturzertifikat kann auf den Personalausweis gemäß der Anleitung des Signaturanbieters nachgeladen werden. Beim Nachladen wird ein privater Signierschlüssel auf dem Ausweis-Chip erzeugt und abgelegt und ein öffentlicher Signierschlüssel beim Signaturanbieter hinterlegt. Eine aktuelle Liste dieser Anbieter wird im Internet durch die Bundesnetzagentur (http://www.nrca-ds.de/) veröffentlicht.

- **das Komfortlesegerät.** Durch das BSI zertifizierter Kartenleser mit Eingabetastatur und Display für Karten mit kontaktlosem Chip.

3.1.1 Anwendungs-Software zur Authentisierung

Auf Seiten des Nutzers wird eine Client-Software benötigt, mit deren Hilfe eine sichere Verbindung zwischen dem verwendeten Kartenlesegerät, dem Ausweis-Chip und einem Diensteanbieter (konkret: dem vom Diensteanbieter genutzten eID-Server) hergestellt wird. Die Übertragung der Daten erfolgt dabei in einem sicheren Kanal mit etablierten Verschlüsselungsverfahren.

Eine solche Client-Software gemäß eCard-API (siehe Abschnitt 3.4.3) wird durch den Bund kostenfrei zur Verfügung gestellt: die „AusweisApp“. Diese integriert neben der Auslesefunktionalität für den neuen Personalausweis auch eine Signaturanwendungskomponente und kann daher auch für die Unterschriftsfunktion eingesetzt werden. Sowohl das Setzen der Signatur-PIN als auch das Nachladen eines qualifizierten Signaturzertifikats, das Anzeigen von Dokumenten, das Signieren von Dokumenten und das Prüfen von digitalen Signaturen werden von der AusweisApp unterstützt.

Dabei ist die AusweisApp nicht nur auf die Verwendung mit dem neuen Personalausweis beschränkt, sondern sie ist in der Lage, mit beliebigen Chipkarten – also auch sämtlichen gängigen Signaturkarten – zusammenzuarbeiten. Dafür muss der Herausgeber der jeweiligen Chipkarte ein sogenanntes CardInfo-File bereitstellen, das die AusweisApp verarbeiten kann.

Die AusweisApp des Bundes kann im Internet vom Downloadportal des BSI für die AusweisApp www.ausweisapp.bund.de kostenfrei heruntergeladen werden. Bitte laden Sie die Software nur unter der genannten Adresse herunter. Diensteanbieter wie Webshops oder Kommunen werden für den Download immer auf www.ausweisapp.bund.de verlinken.

Für einen Großteil der Behörden steht alternativ dazu kostenfrei die Software „Autent Client PA“ auf Basis der Sicherheitsmiddleware Governikus zur Verfügung (http://www.governikus.de), mit der ebenfalls die Authentisierung mit dem neuen Personalausweis im Internet erfolgen kann. Governikus Autent – bestehend aus dem Autent Server sowie den drei alternativen Autent Clients PA, PWD und CERT – implementiert das eCard-API-Framework, das plattformunabhängige Schnittstellen umfasst und somit die Kommunikation zwischen Anwendungen und Chipkarten vereinheitlicht.

3.1.2 Kartenleser

Für den neuen Personalausweis ist ein Kartenleser für Karten mit kontaktlos lesbaren Chips erforderlich. Drei Arten von Kartenlesegeräten mit unterschiedlicher Ausstattung werden in der technischen Richtlinie BSI TR-03119 spezifiziert:

- Basisleser (Cat-B) besitzen weder Eingabetastatur noch Display
- Standardleser (Cat-S) sind mindestens mit einer Eingabetastatur ausgestattet
- Komfortleser (Cat-K) haben eine Eingabetastatur, ein Display und ein Kryptografie-Modul. Sie sind gemäß Signaturgesetz als Signaturterminal für die Unterschriftsfunktion über die kontaktlose Schnittstelle zugelassen

Für die Online-Ausweisfunktion reichen Basisleser aus. Standardleser bieten einen zusätzlichen Schutz gegen das mögliche Abhören von Tastatureingaben durch Keylogger. Für die Nutzung der Unterschriftsfunktion des neuen Personalausweises ist immer ein Komfortleser erforderlich.

In Lesegeräten, die sowohl für den neuen Personalausweis als auch für kontaktbehaftete Chipkarten, z. B. Signaturkarten mit Kontaktchip, verwendet werden, muss parallel zur kontaktlosen NFC-Schnittstelle auch eine kontaktbehaftete Schreib-Lese-Einheit verbaut sein.

Achtung: Die Kategorien der BSI TR-03119 sind nicht identisch mit den Chipkarten-Sicherheitsklassen I bis IV, die vom Zentralen Kreditausschuss spezifiziert sind.

Unabhängig von der Art des genutzten Kartenlesers und der Verwendung des neuen Personalausweises rät das BSI dazu, dass der Bürger-PC über die grundlegenden Sicherheitsmaßnahmen verfügt. Hierzu zählen neben einer Personal Firewall und einem leistungsfähigen Virenscanner auch die regelmäßigen Sicherheitsupdates des verwendeten Betriebssystems.

Eine Übersicht über ausgewählte Kartenleser, die für die Anwendung des neuen Personalausweises geeignet sind, veröffentlicht das BSI im Zusammenhang mit der AusweisApp unter www.ausweisapp.bund.de.

3.1.3 PIN/PUK

Grundsätzlich gibt es zwei verschiedene PINs, die im Zusammenhang mit dem neuen Personalausweis Verwendung finden:

- eine PIN für die Online-Ausweisfunktion (eID-PIN)
- eine PIN für die Unterschriftsfunktion (Signatur-PIN)

Jedes Mal, wenn Bürgerinnen und Bürger die Online-Ausweisfunktion anwenden, wird ihre sechsstellige eID-PIN (Geheimnummer) abgefragt.

Nach Beantragung ihres neuen Personalausweises erhalten die Bürgerinnen und Bürger vom Ausweishersteller einen fünfstelligen Aktivierungscode – die Transport-PIN – zusammen mit der PUK (Entsperrnummer) und dem Sperrkennwort per Post. Die Transport-PIN muss vom Ausweisinhaber durch eine selbst gewählte sechsstellige eID-PIN ersetzt werden. Erst danach kann die Online-Ausweisfunktion genutzt werden kann. Die PIN kann – z. B. mit der AusweisApp – auch von zu Hause jederzeit neu gesetzt werden.

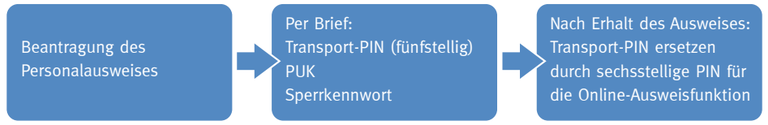


Abbildung 6: PIN-Übermittlung

Wurde die PIN beim Verwenden der Online-Ausweisfunktion einmal falsch eingegeben, kann ein zweiter Eingabeversuch erfolgen. Wenn die eID-PIN zweimal hintereinander falsch eingegeben wurde, muss ein dritter Versuch durch das Eingeben der Zugangsnummer freigeschaltet werden. Die Zugangsnummer ist auf der Vorderseite des Personalausweises aufgedruckt. Wenn die eID-PIN dreimal falsch eingegeben wurde, wird sie blockiert. Die PUK dient dazu, diese Blockierung aufzuheben. Sie kann bis zu zehn Mal verwendet werden.

Falls der Ausweisinhaber seine eID-PIN vergessen hat, kann er in der Personalausweisbehörde gegen eine Gebühr eine neue setzen lassen.

Ebenso wie für die Online-Ausweisfunktion benötigen die Bürgerinnen und Bürger auch für die Nutzung der Unterschriftsfunktion eine Geheimnummer, die Signatur-PIN. Diese muss vor dem Nachladen des Signaturzertifikats vom Ausweis- und Signaturinhaber ebenfalls selbst gesetzt werden. Den Umgang mit der Signatur-PIN regelt der Signaturzertifikateanbieter.

3.1.4 Sperrkennwort

Wenn der Personalausweis gestohlen wird oder anderweitig abhandenkommt, müssen Ausweis und Online-Ausweisfunktion gesperrt werden. Das hierzu notwendige Sperrkennwort wird den Bürgerinnen und Bürgern im gleichen Brief zugestellt, in dem auch die Transport-PIN und die PUK mitgeteilt werden. Es ist ein leicht zu merkendes Wort (z. B. „Lokomotive“). Das Sperrkennwort kennen nur der Ausweisinhaber persönlich und die ausstellende Personalausweisbehörde, die es im Personalausweisregister speichert.

Das Sperrkennwort wird im Gegensatz zu PIN und PUK nicht von den Nutzern am Computer eingegeben, sondern von den Mitarbeitern des Sperrnotrufs oder der Personalausweisbehörde direkt abgefragt.

Der Verlust des Personalausweises muss in jedem Fall bei der zuständigen oder ausstellenden Personalausweisbehörde gemeldet werden. Dabei kann auch die eingeschaltete Online-Ausweisfunktion gesperrt werden. Die Online-Ausweisfunktion kann aber auch jederzeit über den telefonischen Sperrnotruf (0180 1 33 33 33[1]) gesperrt werden.

Entscheidet sich die Bürgerin oder der Bürger für die telefonische Sperrung, muss sie/er am Telefon ihr/sein Sperrkennwort mitteilen. Ist der Bürgerin oder dem Bürger das Sperrkennwort nicht bekannt, kann die Sperrung nur über die zuständige oder ausstellende Personalausweisbehörde veranlasst werden.

Das Sperren der Unterschriftsfunktion erfolgt nicht automatisch, sondern muss separat beim gewählten Signaturanbieter erfolgen.

3.2 Infrastruktur beim Diensteanbieter

Um die Online-Ausweisfunktion einfach in bereits existierende Dienste einzubinden, benötigt ein Diensteanbieter ein Berechtigungszertifikat für den kontrollierten Zugriff auf Daten des neuen Personalausweises und einen eID-Server bzw. eID-Service, der die sichere Kommunikation mit dem Personalausweis und die Anbindung an die Personalausweis-Infrastruktur übernimmt. Im Folgenden wird die Infrastruktur für die Online-Ausweisfunktion näher erläutert.

3.2.1 Berechtigungszertifikat

Das Berechtigungszertifikat ist eine elektronische Bescheinigung, die vom Chip des Personalausweises bei der Online-Ausweisfunktion vor jedem Lesevorgang überprüft wird. Ein Diensteanbieter benötigt für jeden seiner Dienste ein Berechtigungszertifikat. Darin ist festgelegt, welche personen- und ausweisbezogenen Daten vom Dienst aus dem Personalausweis abgefragt werden dürfen. Voraussetzung ist die Erteilung einer Berechtigung der staatlichen Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt. Erst mit dieser staatlichen Berechtigung können dann nach Wahl bei einem Zer-

[1] 3,9 ct/min aus dem dt. Festnetz, max. 42 ct/min aus dem Mobilfunknetz.

tifizierungsdiensteanbieter (auch Berechtigungszertifikateanbieter, kurz BerCA genannt) die entsprechenden technischen Berechtigungszertifikate erworben werden. In Kapitel 4 werden der Prozess und die Voraussetzungen für die Beantragung von Berechtigungen und Berechtigungszertifikaten ausführlich erläutert. Die Berechtigungsvergabe richtet sich nach den Grundsätzen der Erforderlichkeit und Sparsamkeit des Personendatenschutzes.

Als Anlage 3 ist die Leitlinie der Vergabestelle für Berechtigungszertifikate für die Vergabe von Berechtigungen für Diensteanbieter nach § 21 Abs. 2 PAuswG beigefügt.

3.2.2 eID-Server bzw. eID-Service

Die Hard- und Software-Komponente zur Nutzung des elektronischen Identitätsnachweises ist auf Seiten des Diensteanbieters der eID-Server. Erst der eID-Server ermöglicht es Diensteanbietern, die Online-Ausweisfunktion in ihre IT-Systeme zu integrieren. Er bildet das Herzstück der Integration auf Seiten des Unternehmens oder der Behörde. Er steuert die elektronische Kommunikation zwischen dem Online-Angebot des Unternehmens oder der Behörde und der Authentifizierungskomponente der Bürgerin oder des Bürgers. So wird das Berechtigungszertifikat, mit dem sich der Diensteanbieter gegenüber dem Nutzer seines Online-Angebotes authentifiziert, vom eID-Server bereitgestellt. Die Authentifizierungskomponente, die die Bürgerin oder der Bürger verwendet, sendet die freigegebenen Daten aus dem neuen Personalausweis an den eID-Server, der diese wiederum zum Online-Angebot des Unternehmens oder der Behörde überträgt. Eine genauere Beschreibung der einzelnen Ablaufschritte erfolgt im nachfolgenden Kapitel 3.3.

Ein Diensteanbieter kann dabei den eID-Server selbst technisch betreiben, sei es als ausgelagertes Service-Zentrum seines eigenen Hauses oder Unternehmens-/Behördenverbundes, oder auf einen IT-Dienstleister übertragen. Die technische Richtlinie des BSI TR-03130 definiert die Schnittstellen und Sicherheitsanforderungen an die Hard- und Software-Systeme des eID-Servers.

Übernimmt ein IT-Dienstleister die Aufgaben des elektronischen Identitätsnachweises, wird diese Dienstleistung „eID-Service“ und der Dienstleister „eID-Service-Provider“ genannt. Dabei handelt es sich um eine Auftragsdatenverarbeitung nach § 11 des Bundesdatenschutzgesetzes.

In jedem Fall ist der Diensteanbieter der Inhaber der Berechtigung, die die Vergabestelle für Berechtigungszertifikate (VfB) ausstellt, und damit für die Einhaltung sämtlicher Vorgaben und Anforderungen im eigenen Haus sowie im Falle der Aufgabenübertragung an einen Dritten vollständig verantwortlich.

3.3 Technischer Ablauf der Online-Ausweisfunktion

Der funktionale Ablauf der Online-Ausweisfunktion und die beteiligten Systeme sind in Abbildung 7 dargestellt.

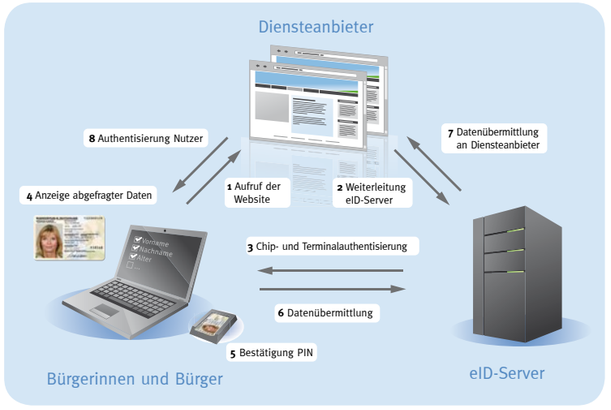


Abbildung 7: Authentisieren mit der Online-Ausweisfunktion

Die Kommunikation zwischen Personalausweis und Diensteanbieter erfolgt nicht direkt, sondern über den eID-Server.

Die Authentisierung wird schrittweise am Beispiel eines Webangebots beschrieben:

1. Der Ausweisinhaber ruft den Webdienst des Diensteanbieters auf, der eine Online-Authentisierung benötigt

2. Der Dienst leitet eine Authentisierungsanfrage an den eID-Server weiter

3. Zwischen dem eID-Server sowie der Client-Software (z. B. AusweisApp), dem Lesegerät und dem Ausweis-Chip wird ein sicherer Kanal aufgebaut und die Authentizität des Diensteanbieters sowie die Authentizität und Integrität (Fälschungssicherheit) des Ausweises geprüft

4. Die Client-Software zeigt dem Ausweisinhaber das Berechtigungszertifikat des Diensteanbieters und die angefragten Ausweisdatenkategorien an. Der Ausweisinhaber entscheidet, welche Ausweisdaten er übermitteln möchte

5. Durch Eingabe der PIN bestätigt der Ausweisinhaber die Übermittlung der Daten

6. Die Ausweisdaten werden an den eID-Server übermittelt

7. Der eID-Server sendet eine Authentisierungsantwort und die Ausweisdaten an den Dienst

8. Die Authentisierungsantwort und die Ausweisdaten werden ausgelesen. Der Dienst prüft die Authentisierungsergebnisse und entscheidet, ob die Authentisierung als erfolgreich anzusehen ist. Abschließend erfolgt eine Ergebnisantwort an den Nutzer bzw. die Ausführung des Dienstes

3.4 Der eID-Server

Der eID-Server hat dabei die folgenden Aufgaben:

- Er übernimmt die sichere Kommunikation mit der Client-Software, dem Personalausweis und dem PC der Bürgerinnen und Bürger
- Er stellt die Authentizität und die Gültigkeit des Personalausweises fest, prüft, ob dieser von der Ausweisinhaberin oder dem -inhaber gesperrt wurde, und übermittelt die Ergebnisse der eID-Funktion an die weiteren Systeme des Diensteanbieters
- Er bezieht von dem Anbieter für Berechtigungszertifikate regelmäßig neue Berechtigungszertifikate sowie aktualisierte Sperrlisten

Die Software des eID-Servers für die Personalausweisanwendung muss der eCard-API-Spezifikation gemäß technischer Richtlinie des BSI TR-03112 entsprechen. Spezielle Festlegungen dazu enthält die technische Richtlinie eID-Server des BSI TR-03130.

Bei Beauftragung eines eID-Service müssen die kryptografischen Schlüssel für die Kommunikation zwischen dem Diensteanbieter und dem eID-Service auf beiden Seiten auf dem gleichen sicheren Schutzniveau gespeichert werden.

Um diesen Anforderungen gerecht zu werden, sind im eID-Server mehrere modulartige Funktionseinheiten integriert (siehe Abbildung 8). Die Einheiten werden in den folgenden Abschnitten kurz vorgestellt.

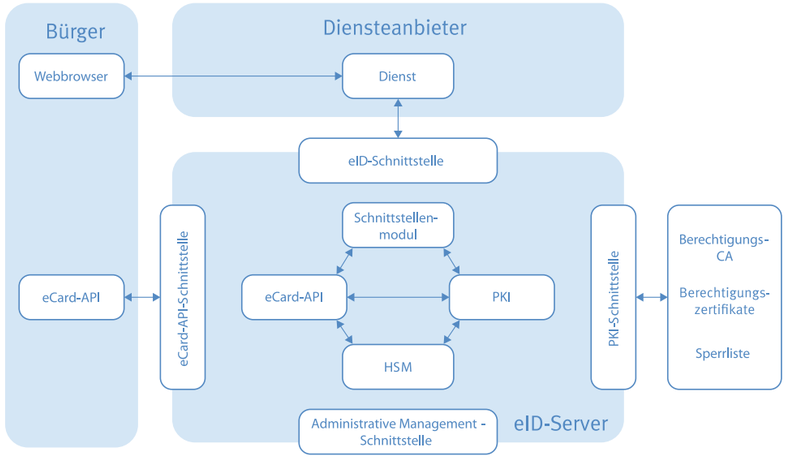


Abbildung 8: Funktionseinheiten eID-Server (Quelle: BSI TR-03130)

3.4.1 eID-Schnittstelle

Um die eID-Schnittstelle eines Dienstes zum eID-Server einfach zu gestalten, stellt der eID-Server gemäß TR-03130 einen Webservice zur Verfügung, der die Komplexität der verwendeten Protokolle und Komponenten kapselt. In der technischen Richtlinie wird einerseits eine eID-Schnittstelle in der Web Services Description Language (WSDL) formal beschrieben (eID.wsdl), andererseits ist aber auch eine Anbindung mit SAML-Token (Security Assertion Markup Language) möglich. Die konkrete eID-Anbindung ist mit dem eID-Server-Betreiber bzw. eID-Service-Provider abzustimmen.

3.4.2 Administrative Management-Schnittstelle

Damit der eID-Server die spezifizierten Funktionen bereitstellen kann, benötigt er initiale Einstellungen und Schlüssel. Diese Parameter werden über die administrative Management-Schnittstelle konfiguriert, die betreiberspezifisch ausgelegt ist. Ein eID-Service kann gegebenenfalls auch weitere Serviceleistungen beinhalten.

3.4.3 eCard-API-Schnittstelle

Das Ziel des eCard-API-Frameworks (TR-03112) ist das Bereitstellen einer einfachen und homogenen Schnittstelle, um in verschiedenen Anwendungen eine einheitliche Nutzung von unterschiedlichen Chipkarten (eCards) zu ermöglichen. Eine dieser Chipkarten ist der neue Personalausweis.

Für die Nutzung des Personalausweises wird an zwei Stellen auf eine eCard-API-Implementierung zurückgegriffen: auf Client-Seite (auf dem PC des Bürgers) und auf Server-Seite (eID-Server des Diensteanbieters). Die Client-Software reagiert auf Authentisierungsanfragen, die durch den Browser des Benutzers geleitet werden, und verbindet sich daraufhin mit der eCard-API-Schnittstelle des eID-Servers. Diese Verbindung nutzt der eID-Server, um die Daten aus dem neuen Personalausweis zu lesen.

3.4.4 Schnittstelle zur Public-Key-Infrastruktur und Berechtigungszertifikateanbieter

Über die PKI-Schnittstelle stellt der Berechtigungszertifikateanbieter dem eID-Server die Berechtigungszertifikate, die diensteanbieterspezifischen Sperrlisten sowie alle im Verifikationsprozess nach der technischen Richtlinie BSI TR-03110 benötigten Zertifikate, Sperr- und Defect-Listen bereit.

Berechtigungszertifikate

Der Berechtigungszertifikateanbieter stellt einem Diensteanbieter auf Basis der durch die Vergabestelle für Berechtigungszertifikate im Verwaltungsverfahren erteilten Berechtigung die Berechtigungszertifikate mit kurzzeitiger Gültigkeit zur Verfügung. Der eID-Server verwaltet die Berechtigungszertifikate, die regelmäßig zu erneuern sind. Daher bestellt der eID-Server automatisiert entsprechend neue Zertifikate bei der zuständigen BerCA gemäß den technischen Richtlinien BSI TR-03128 und TR-03129. Dieser automatisierte Abruf muss mit Hilfe von Authentisierungszertifikaten (SSL-Zertifikaten) abgesichert werden.

eID-Sperrliste

Um die missbräuchliche Nutzung gestohlener oder verloren gegangener Personalausweise zu verhindern, kann die Online-Ausweisfunktion gesperrt werden. Das nachträgliche

Tracking von gesperrten Ausweisen wird durch diensteanbieterspezifische eID-Sperrlisten, errechnet aus einer zentralen Sperrliste, verhindert. Das bei der Online-Authentisierung übermittelte dienste- und kartenspezifische Sperrmerkmal darf nur zum Abgleich mit einer diensteanbieterspezifischen eID-Sperrliste verwendet werden. Die zentrale Sperrliste wird zentral bei der Vergabestelle für Berechtigungszertifikate betrieben, die diensteanbieterspezifischen Sperrlisten werden den Diensteanbietern vom zuständigen Berechtigungszertifikateanbieter bereitgestellt.

3.4.5 Hardware-Sicherheits-Modul (HSM)

Jeder Zertifikatsnehmer der eID-PKI und damit jeder Besitzer eines Berechtigungszertifikates muss sein eigenes Schlüsselpaar generieren. Dabei sind kryptografische Algorithmen gemäß BSI TR-03110 zu verwenden. Das jeweils erzeugte kryptografische Schlüsselpaar muss gemäß Anforderungen der Certificate Policy in einem sicheren Kryptografiemodul generiert, gespeichert und genutzt werden. Als Kryptografiemodule geeignet sind dabei Chipkarten oder High Security Module (HSM), die nach Common Criteria Protection Profiles (PPs) durch das BSI zertifiziert worden sind.[2]

3.4.6 Kryptografische Protokolle für die Datenübermittlung zwischen Ausweis-Chip und eID-Server

Die kryptografischen Protokolle für den mehrstufigen Aufbau eines sicheren Kanals zwischen Ausweis-Chip und Kartenleser sowie anschließend zwischen Ausweis-Chip und Diensteanbieter (bzw. dessen eID-Server) sind in der technischen Richtlinie BSI TR-03110 beschrieben.

Die Ausführung der Protokolle hinterlässt im Ausweis-Chip einen definierten Sicherheitszustand, der bei einem Abbruch der Karten-Session (z. B. durch Herunternehmen der Karte vom Kartenleser) aus Sicherheitsgründen sofort gelöscht wird.

PACE (Password Authenticated Connection Establishment)

Das PACE-Protokoll dient der sicheren PIN-Eingabe und dem Aufbau eines verschlüsselten und integritätsgesicherten Kanals zwischen dem lokalen Kartenlesegerät oder der AusweisApp (abhängig vom verwendeten Kartenleser) und dem kontaktlosen Chip.

Terminalauthentisierung

Ist der sichere Kanal aufgebaut, kann der Ausweis-Chip mit Hilfe der Terminalauthentisierung verifizieren, ob das Lesegerät (z. B. bei der Unterschriftsfunktion) bzw. der Diensteanbieter berechtigt ist, auf Daten im Personalausweis zuzugreifen. Dies erfolgt durch die Prüfung des Berechtigungszertifikats. Die Berechtigungszertifikate sind CV-Zertifikate (Card Verifiable Certificates) nach ISO 7816.

Chipauthentisierung

Die Chipauthentisierung dient dem Aufbau eines sicheren Ende-zu-Ende-Kanals zwischen Ausweis und Diensteanbieter (bzw. dessen eID-Server). Erst wenn dieser Kanal aufgebaut ist, kann auf die Daten im Chip zugegriffen werden.

[2] Vgl. „Certificate Policy für die eID-Anwendung des ePA – Elektronischer Identitätsnachweis mit dem elektronischen Personalausweis“, in seiner aktuellsten Fassung zu finden unter www.bsi.bund.de.

Ebenfalls erfolgt die Prüfung des Ausweis-Chips auf Echtheit. Die Authentizität der ausgelesenen Daten wird implizit über den Echtheitsnachweis des Chips gesichert.

3.5 Die Sperrung der Online-Ausweisfunktion

Um Unternehmen und Behörden vor Missbrauch ihres Online-Angebotes mit gestohlenen Personalausweisen mit eingeschalteter Online-Ausweisfunktion zu schützen, sieht der Gesetzgeber die Einrichtung und den Betrieb eines zentralen Sperrdienstes vor, der allen Anbietern von Online-Diensten eine jederzeit verfügbare Liste (Sperrliste) aller abhandengekommenen und gesperrten Personalausweise (mit eingeschalteter Online-Ausweisfunktion) zur Verfügung stellt.

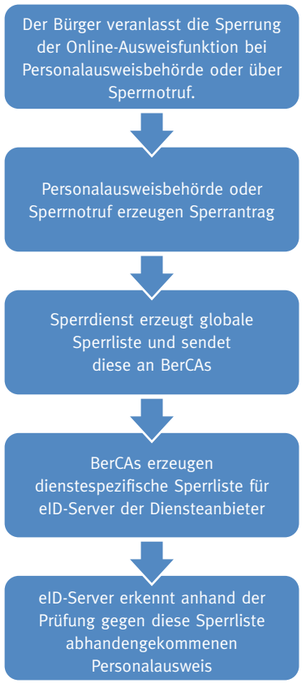


Abbildung 9: Sperrprozess Online-Ausweisfunktion

Der Bürger hat die Möglichkeit, im Falle des Verlustes seines Personalausweises mit eingeschalteter Online-Ausweisfunktion diese unverzüglich durch die ausgebende Personalausweisbehörde oder den Sperrnotruf sperren zu lassen.

Im Rahmen des Authentifizierungsprozesses über den eID-Server können Personalausweise mit gesperrter Online-Ausweisfunktion zuverlässig identifiziert werden.

Die nebenstehende Darstellung (Abbildung 9) zeigt den vereinfachten Ablauf der Sperrung inkl. der Bereitstellung der Sperrliste an den eID-Server des Unternehmens oder der Behörde.

3.6 Anbindung eines Dienstes an die Infrastruktur

Um die Online-Ausweisfunktion als Diensteanbieter in die eigenen Geschäftsprozesse einbinden zu können, sind bestimmte Umsetzungsschritte erforderlich, die in der folgenden Abbildung 10 dargestellt und anschließend erläutert werden:

1. Dienst konzipieren:

Verschiedene Dienste benötigen für den elektronischen Identitätsnachweis unterschiedliche Datenfelder des neuen Personalausweises. Die zwingend erforderlichen Datenfelder für den jeweiligen Geschäftsprozess sind zu ermitteln, um im Antrag für ein Berechtigungszertifikat die angeforderten Datenfelder begründen zu können. Gegebenenfalls sind mehrere Berechtigungszertifikate für unterschiedliche Dienste zu beantragen. Bei der Konzeption des Dienstes sollte auf eine barrierefreie Darstellung der Webinhalte geachtet werden (siehe auch Abschnitt „Barrierefreiheit“).

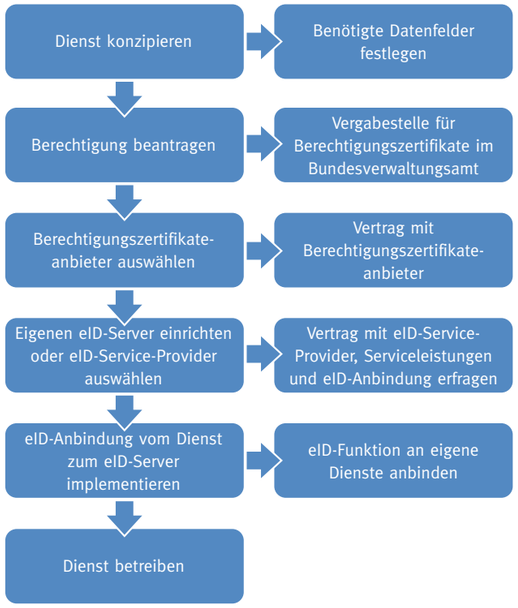


Abbildung 10: Schritte zur Umsetzung eines Dienstes[3]

Soll die Online-Ausweisfunktion in einem Dienst verwendet werden, so hat der Diensteanbieter dies dem Nutzer gegenüber auf einfache Art und Weise zu verdeutlichen. In jedem Fall ist dazu das Personalausweis-Logo („Zwei Welten“) zu verwenden. In der Richtlinie gemäß § 29 Abs. 2 PAuswV ist beschrieben, auf welche Art und Weise das Logo Verwendung finden darf.

2. Berechtigung beantragen:

Die Beantragung der Berechtigung bei der Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt wird detailliert in Kapitel 4 beschrieben.

3. Berechtigungszertifikateanbieter auswählen:

Aufgrund des positiven Bescheides der Vergabestelle für Berechtigungszertifikate kann ein Berechtigungszertifikateanbieter ausgewählt und auf dieser Basis ein Vertrag über den Bezug der Berechtigungszertifikate und der diensteanbieterspezifischen Sperrlisten abgeschlossen werden. Der eID-Server bzw. eID-Service-Provider muss die Anbindung an den ausgewählten Berechtigungszertifikateanbieter unterstützen, da die neuen Berechtigungszertifikate und Sperrlisten regelmäßig online bereitgestellt werden.

4. Eigenen eID-Server einrichten oder eID-Service-Provider auswählen:

Ein Diensteanbieter kann einen eigenen eID-Server betreiben oder einen Dienstleister als eID-Service-Provider auswählen. Die Aufgaben des eID-Servers wurden in Abschnitt 3.4 erläutert. Wird ein eID-Service-Provider beauftragt, so unterstützt dieser gegebenenfalls auch bei anderen Umsetzungsschritten.

Eine Übersicht über die aktuell bekannten eID-Service-Provider wird auf http://www.personalausweisportal.de veröffentlicht.

5. eID-Anbindung vom Dienst zum eID-Server implementieren:

In Abhängigkeit vom eID-Server kann die eID-Anbindung als eID-Schnittstelle oder die SAML-Anbindung (siehe Abschnitt 3.4.1) für die Kommunikation zwischen Dienst und eID-Server genutzt werden. Diensteanbieter sollten sich bei ihrem eID-Service-Provider informieren, wie die eID-Anbindung technisch erfolgt und welche Software-Unterstützung für welche Plattformen bereitgestellt wird.

6. Dienst betreiben:

Bei der Verwendung der Online-Ausweisfunktion ist durch den jeweiligen Diensteanbieter sicherzustellen, dass sich die Authentisierung mit der AusweisApp durchführen lässt.

Barrierefreiheit

Ältere Menschen oder Menschen mit Behinderung können besonders auf Dienste im Internet angewiesen sein, weil beispielsweise das persönliche Erscheinen auf Ämtern nur mit sehr viel Aufwand möglich ist. Der neue Personalausweis und die AusweisApp unterstützen den barrierefreien Zugang zu personalisierten Internetdiensten grundsätzlich.

Eine barrierefreie Ausführung eines Dienstes insgesamt obliegt jedoch den Diensteanbietern. Die Richtlinien für barrierefreie Webinhalte (WCAG) 2.0[4] (W3C-Empfehlung 11. Dezember 2008) definieren Prinzipien, Richtlinien und testbare Erfolgskriterien, um Webinhalte barrierefreier zu gestalten. Damit sind auch Techniken zur Umsetzung, zum Beispiel in Form von Programmierbeispielen, Codelistings und Screenshots, dokumentiert.

Im Bereich der öffentlichen Verwaltung geben Bundes- oder Landesverordnungen für die IT-Barrierefreiheit Regelungen für die barrierefreie und nutzerfreundliche Gestaltung hauptsächlich für Webangebote der Verwaltung vor.

[3] Die Schritte zur Umsetzung müssen nicht zwingend nacheinander erfolgen. Insbesondere können die Schritte zwei bis vier auch zeitgleich initiiert werden.

[4] Richtlinien für barrierefreie Webinhalte (WCAG) 2.0, autorisierte deutsche Übersetzung vom 29.10.2009, http://www.w3.org/Translations/WCAG20-de/

4 Der Zertifikatsprozess

4.1 Das Berechtigungszertifikat

Wenn Sie als Diensteanbieter die eID-Funktion des neuen Personalausweises nutzen möchten, müssen die Vorgaben des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis (PAuswG) eingehalten werden. Das heißt unter anderem, dass Sie eine Berechtigung benötigen, Daten aus dem neuen Personalausweis auslesen zu dürfen. Berechtigungszertifikate dienen gegenüber dem Personalausweisnutzer als Nachweis, dass ein Anbieter von Diensten berechtigt ist, auf einige oder alle der im § 18 Abs. 3 Satz 2 PAuswG genannten Datenfelder zuzugreifen.

Diese Berechtigung, die sich aus § 21 Abs. 2 des Personalausweisgesetzes ableiten lässt, muss bei der Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt beantragt werden.

Der Vergabeprozess ist in Abbildung 11 dargestellt:

Um Dienste mit dem neuen Personalausweis anbieten zu können, ist eine Berechtigung erforderlich. Eine solche kann bei der Vergabestelle für Berechtigungszertifikate beantragt werden.

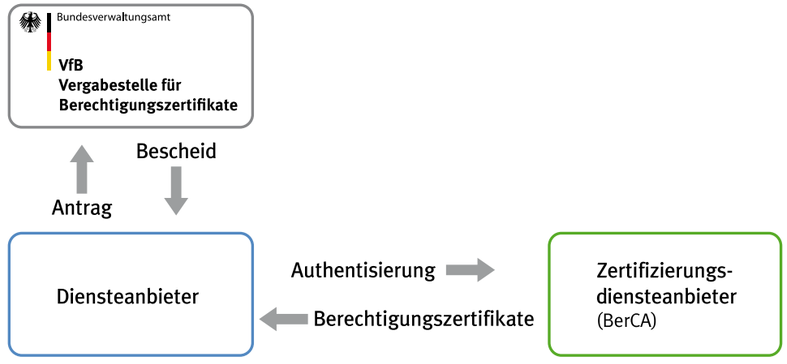


Abbildung 11: Vergabeprozess

Nach einem positiven Bescheid der Vergabestelle erhält der Diensteanbieter das elektronische Berechtigungszertifikat von einem Berechtigungszertifikateanbieter (BerCA). Im folgenden Abschnitt wird das Antragsverfahren bei der Vergabestelle für Berechtigungszertifikate erläutert.

Anlage 3 enthält die Leitlinie der Vergabestelle für Berechtigungszertifikate im BVA, einschließlich der betreffenden Abschnitte des PAuswG und der PAuswV sowie der PAuswGebV.

4.2 Der Prozess der Beantragung

Die Beantragung eines Berechtigungszertifikates ist auf drei Wegen möglich:

- elektronisch mit der Client-Software
- schriftlich per Postident
- persönliche Vorsprache im BVA in Köln

Für den Antrag werden benötigt:

- Erklärung zu Datenschutz und Datensicherheit
- Nachweis der Erforderlichkeit der Datenfelder nach § 18 Abs. 3 des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis (PAuswG)
- für E-Business-Anwendungen: Handelsregisterauszug

Eine detaillierte Beschreibung des Antragsverfahrens findet sich im Internet unter www.personalausweisportal.de/anbieter. Dort sind auch die Antragsformulare hinterlegt.

4.3 Gesetzliche Vergabevoraussetzungen

Nachdem im ersten Schritt der Antrag bei der Vergabestelle für Berechtigungszertifikate eingereicht wurde, wird der Antrag nach den Voraussetzungen des § 21 Absatz 2 Nr. 1 bis 4 PAuswG geprüft.

Bei der Beantragung einer Berechtigung steht eine Erläuterung zur Erforderlichkeit der Datenübermittlung für den vorgesehenen Geschäftszweck im Vordergrund.

Im Einzelnen wird geprüft, dass:

- der angegebene Zweck nicht rechtswidrig ist (Nr. 1),
- der Zweck nicht in der geschäftsmäßigen Übermittlung der Daten besteht und keine Anhaltspunkte für die geschäftsmäßige oder unberechtigte Vermittlung der Daten vorliegen (Nr. 2),
- der antragstellende Diensteanbieter die Erforderlichkeit der zu übermittelnden Angaben für den beschriebenen Zweck nachgewiesen hat (Nr. 3) und
- die Anforderungen, insbesondere an Datenschutz und Datensicherheit, gemäß der Rechtsverordnung nach § 34 Nr. 7 erfüllt sind (Nr. 4).

Es ist insbesondere wichtig, dass die Erforderlichkeit der personenbezogenen Daten für den vorgesehenen Geschäftszweck begründet und die Maßnahmen zum Datenschutz und zur Datensicherheit erläutert werden. Die Erforderlichkeit besagt, dass keine überflüssigen personenbezogenen Daten erhoben, verwendet oder genutzt werden dürfen. Es sind in jedem Einzelfall, nach den Vorgaben des Gesetzes, das Interesse des Diensteanbieters als verantwortliche Stelle und das schutzwürdige Interesse des Personalausweisinhabers als Betroffener abzuwägen. Der Diensteanbieter als verantwortliche Stelle darf die personenbezogenen Daten des Personalausweisinhabers nur verarbeiten, wenn er diese

- für ein berechtigtes Interesse auch wirklich benötigt (Erforderlichkeit) und
- schutzwürdige Interessen des Betroffenen nicht überwiegen.

Die wesentliche Vorarbeit liegt in der Analyse der eigenen Geschäftsprozesse, die der Vergabestelle im Antragsverfahren zu erläutern sind. Weitere Erläuterungen zur Prüfung der Vergabestelle für Berechtigungszertifikate können Sie den Durchführungshinweisen entnehmen.

Im positiven Fall wird dem Antragsteller der Bescheid über das Ausstellen der Berechtigung zugestellt. Im negativen Fall erhält der Antragsteller eine Ablehnung bzw. eine Aufforderung zur Neubeantragung.

4.4 Berechtigungszertifikateanbieter

Der Diensteanbieter kann sich nach Erhalt des Berechtigungszertifikats für einen Berechtigungszertifikateanbieter seiner Wahl entscheiden.

Nach positivem Bescheid ist seitens des Diensteanbieters ein Berechtigungszertifikateanbieter für die Bereitstellung der Berechtigungszertifikate auszuwählen, mit dem auf Basis des positiven Berechtigungsbescheides ein Vertrag abgeschlossen wird. Die Vertragsverhandlungen zwischen dem Diensteanbieter und dem Zertifizierer sollten frühzeitig beginnen, damit der Wirkbetrieb zeitnah nach Ausstellung des Bescheides aufgenommen werden kann. Eine Übersicht über die Anbieter, die sich bei der Vergabestelle registriert haben, sowie weitere Informationen zur technischen Infrastruktur finden sich auf http://www.personalausweisportal.de.

4.5 Rechtsgrundlagen

Zusammenfassend kann festgehalten werden, dass Anbieter für Dienste mit dem neuen Personalausweis eine Reihe von Vorgaben und Vorschriften einhalten müssen, um das Auslesen der Personalausweisdaten für die Bürgerinnen und Bürger sicher und gesetzeskonform zu gestalten. Dies sind:

- die Leitlinie der Vergabestelle für Berechtigungszertifikate gemäß § 29 Abs. 2 PAuswV. Hier werden die technischen und organisatorischen Anforderungen für die Nutzung von Berechtigungszertifikaten beschrieben (Leitlinie siehe Anlage 3)
- das unter 4.4 genannte Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PAuswG) insbesondere mit den §§ 10–22 (Auszug im Anhang zu Anlage 3)
- die Personalausweisverordnung (PAuswV) vom 22.04.2010: Darin sind wichtige Voraussetzungen für die Nutzung der Online-Ausweisfunktion beschrieben (Auszug im Anhang zu Anlage 3)
- die Durchführungshinweise der Vergabestelle für Berechtigungszertifikate
- die technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI): Diese liefern alle relevanten Vorgaben und Informationen zu technischen Umsetzungen und den damit verbundenen Sicherheitsbestimmungen

4.6 Kosten

Die Kosten für ein Berechtigungszertifikat werden durch die Verordnung über Gebühren für Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgebührenverordnung/PAuswGebV) geregelt.

Die Kosten schließen nicht die Bereitstellung der Berechtigungszertifikate durch den Berechtigungszertifikateanbieter ein. Diese Preise regelt der Markt selbst.

Gebühren für Berechtigungen

Für Berechtigungen sind folgende Gebühren nach § 3 PAuswGebV zu erheben:

- 102 Euro für die Erteilung einer Berechtigung nach § 21 Absatz 1 Satz 2 des Personalausweisgesetzes
- 80 Euro für die Versagung einer Berechtigung
- 115 Euro für die Rücknahme oder den Widerruf einer Berechtigung

Behörden können ggf. von den Gebühren befreit werden. Einzelheiten hierzu finden sich im § 8 VwKostG (http://bundesrecht.juris.de/vwkostg/__8.html).

5 Anwendungsbeispiele

Die folgenden Anwendungsbeispiele mit dem neuen Personalausweis bei Unternehmen und Behörden werden aus Sicht von Erika Mustermann beschrieben. Frau Mustermann hat ihren neuen Personalausweis vor einigen Wochen erhalten und berichtet von ausgewählten Erlebnissen mit ihrer neuen Karte.

5.1 Kundenmanagement

Ich möchte bei meiner Versicherung einen verbindlichen Antrag zum Abschluss einer privaten Haftpflichtversicherung für mich und meine Familie stellen. Die Versicherung darf als Diensteanbieter diejenigen Daten auslesen, die für die Annahme des Antrags und damit für den Vertragsabschluss notwendig sind. Tippfehler werden vermieden und meine Identität als neue Versicherungsnehmerin ist sichergestellt.

Hierzu gehe ich auf das Internetportal meiner Versicherung und informiere mich über passende Produkte und Tarife. Dies erfolgt vollkommen anonym und unverbindlich. Die Familienhaftpflichtversicherung mit dem erweiterten Schutz PHV-Sorglos passt sehr gut zu meiner Situation und meinen Anforderungen. Ich möchte diesen Schutz erwerben und kann den Antrag direkt im Internetportal stellen. Hierzu muss ich mich gegenüber der Versicherung authentifizieren, denn das Unternehmen muss ja wissen, mit wem es den Vertrag abschließen wird. Ich möchte sichergehen, dass ich elektronisch mit der Versicherung kommuniziere und nicht mit einer gefälschten Webseite. Wie praktisch, dass die Versicherung die Antragstellung mit Hilfe des neuen Personalausweises ermöglicht. Damit können sich meine Versicherung und auch ich selbst sicher sein, dass wir jeweils mit dem richtigen Partner kommunizieren. Bislang musste ich in solchen Fällen meine persönlichen Angaben stets manuell eingeben oder gar ein entsprechendes Formular herunterladen, ausfüllen und per Post verschicken. Das war in jedem Fall sehr umständlich. Tippfehler ließen sich nicht immer vermeiden und außerdem war ich mir nicht sicher, bei wem meine Daten landen – da habe ich es lieber gleich gelassen.

Zur Antragstellung lege ich meinen Personalausweis auf mein Lesegerät und nach einem Klick auf „Antrag stellen mit dem neuen Personalausweis“ sehe ich in einem Fenster, das von der AusweisApp auf meinem PC erzeugt wird, die Angaben aus dem Berechtigungszertifikat der Versicherung. Ich entnehme diesen Angaben, dass ich tatsächlich mit meiner Versicherung kommuniziere und dass sie die Berechtigung dafür besitzt, dass ich mich ihr gegenüber mit dem neuen Personalausweis zum Zweck des Abschlusses von Versicherungsverträgen authentifizieren kann. Ich klicke auf „Weiter“ und die AusweisApp zeigt mir diejenigen Datenkategorien an, die das Unternehmen aus meinem Ausweis auslesen möchte: Familienname, Vornamen, Doktorgrad, Tag der Geburt und Anschrift. Die Übermittlung dieser Datenkategorien wurde von der Vergabestelle für Berechtigungszertifikate im BVA für den Geschäftszweck der Beantragung eines Versicherungsvertrags genehmigt (siehe Kap. 4). Auch aus meiner Sicht ist das in Ordnung. Da es mehr als eine Erika Mustermann gibt, ist es für mich nachvollziehbar, dass neben meinem Namen auch weitere persönliche Daten zur eindeutigen Identifizierung übermittelt werden. Schließlich hat die Versicherung mehrere Millionen Kunden. Da ich mit der Übermittlung der Daten einverstanden bin, wähle ich keine der gewünschten Datenkategorien ab. Danach gebe ich noch meine PIN ein, um mein Einverständnis zur Übermittlung der persönlichen Daten zu bestätigen.

Die erfolgreiche Übermittlung meiner Daten wird von der AusweisApp bestätigt. Nun bin ich authentifiziert und beantworte online noch weitere antragsrelevante Fragen. Abschließend bestätigt mir die Versicherung den Erhalt meiner Angaben und sichert mir zu, dass ich umgehend nach der Antragsbearbeitung meine Versicherungspolice erhalten werde. Aufgrund der hochgradigen Validität meiner Daten aus dem Personalausweis kann die Antragsbearbeitung bis zur Policierung weitgehend automatisiert erfolgen, so dass mir bereits in wenigen Tagen die Police zugestellt werden kann.

Die Vorteile auf einen Blick

Die Versicherung hatte sich schon früh entschieden, die elektronische Authentifizierung in ihre Online-Antragsprozesse zu integrieren. Als ein Unternehmen, das konsequent den Vertriebskanal Internet ausbaut, möchte sie aus strategischen Gründen die zukunftsorientierte Sicherheitstechnologie des neuen Personalausweises im Unternehmen etablieren und dabei rechtssicher in der digitalen Welt agieren. Weiterhin können aufgrund einer medienbruchfreien Abwicklung und der hohen Datenqualität der personenbezogenen Daten aus dem Personalausweis Kosten eingespart werden. Eine Kontrolle der manuell vom Kunden eingegebenen Informationen wird eingespart.

5.2 Altersbestätigung

Vor Kurzem hat mein 17-jähriger Sohn Max einen Shop im Internet gefunden, bei dem er seine Musik, Filme und Computerspiele online bestellen und sich anschließend per Post zuschicken lässt. Natürlich hatte ich anfangs die Befürchtung, dass er sich auch Filme kauft, die erst ab einem Alter von 18 Jahren freigegeben sind. Bisher wurde beim Einkauf an der Kasse immer sein Ausweis kontrolliert, um festzustellen, wie alt er ist. Hier war mir nicht klar, ob so eine Prüfung auch in der neuen Online-Welt funktioniert.

Die Bedenken konnte mein Sohn mit seinem neuen Personalausweis schnell zerstreuen. Er erklärte mir, dass er im Rahmen seines Bestellprozesses vom Verkäufer dazu aufgefordert wird, sich mit der Online-Ausweisfunktion des neuen Personalausweises im Internet auszuweisen. Bei Waren ab 18 Jahren wird bei der Bestellung zusätzlich eine Altersüberprüfung anhand des Geburtsdatums im Ausweis durchgeführt. Er legt dazu lediglich seinen Ausweis auf das Kartenlesegerät, schaut sich in der AusweisApp an, ob die Berechtigung des Online-Shops zum Internetangebot passt, und bestätigt die Ausweisdaten, die

an den Online-Händler übermittelt werden sollen. Die Datenübermittlung gibt er mit der sechsstelligen PIN frei. Dabei wird auch nicht das genaue Geburtsdatum meines Sohnes übermittelt, sondern bei Waren ab 18 Jahren nur die Angabe, ob er dieses Mindestalter erreicht hat oder nicht. Für Waren ab 16 Jahren kann diese Prüfung ganz entfallen, da die Online-Ausweisfunktion erst ab dem 16. Lebensjahr auf dem Ausweis bereitgestellt wird. Für die Bestellung nicht altersbeschränkter Waren reicht dem Online-Händler schon die Abfrage des Pseudonyms aus, um das Risiko einer Fehllieferung oder Rückforderung zu senken. Dieses datensparsame Verfahren war mir sehr wichtig, da ich nicht möchte, dass jedem Online-Händler sein Geburtsdatum bekannt ist, und bei Online-Lieferungen auch die Adresse nicht unbedingt genannt werden muss. Für das Sparschwein meines Sohnes wirkt sich die Ausweisabfrage bei der Bestellung in Form eines kleinen Rabatts auf den Rechnungspreis aus, die der Händler bei diesem Bestellweg einräumt. Die Befugnis zur Abfrage des Altersnachweises hat sich der Online-Händler durch einen entsprechenden Antrag bei der Vergabestelle für Berechtigungszertifikate genehmigen lassen müssen. (Vgl. Kap. 4)

Die Vorteile auf einen Blick

Mit der Altersbestätigung leistet der Händler einen erheblichen Beitrag zum Jugendschutz und damit zu Renommee und Glaubwürdigkeit seines Geschäfts, aber auch zur Wirtschaftlichkeit. Er kann davon ausgehen, dass er keine jugendgefährdenden Inhalte an junge Kunden unter 18 abgibt. Auch werden komplizierte papiergebundene Verfahren des Altersnachweises hinfällig, die der Online-Händler mit eigenen Mitarbeiterinnen und Mitarbeitern bearbeiten müsste. Der neue Personalausweis schafft auf diese Weise Vertrauen bei seinen Kunden und zusätzliche Sicherheit. Erst durch den neuen Personalausweis mit seiner Altersfunktion konnte der Online-Händler sein Angebot im Internet auch auf Inhalte für Personen über 18 Jahre ausweiten, da er diese nun eindeutig und sicher identifizieren kann.

5.3 Wohnortbestätigung

Schon seit einigen Jahren wohne ich mit meinem Mann und unseren Kindern im schönen Wellnesshofen. Bis jetzt hat es meine Freundin mit ihren Kindern aber noch nie geschafft, mich hier zu besuchen, obwohl diese Region sich auch für einen erholsamen Kurzurlaub eignet. Vergangenes Wochenende war es dann aber so weit. Endlich hatte sie es geschafft. Sie war auch ganz begeistert von den Wellness-Möglichkeiten und den Vergünstigungen, z. B. dem ermäßigten Eintritt in unsere Thermalquellen, die sie als auswärtige Besucherin hier bekommen hat. Hierfür musste sie sich lediglich vorab auf der Homepage des örtlichen Tourismusvereins anmelden und vorab ihre Kurtaxe entrichten. Dadurch hatte sie einige Bonusgutscheine vor ihrem Urlaubsantritt zugesandt bekommen. Leider sind diese Gutscheine nur für auswärtige Touristen gedacht, daher werden wir wohl nicht in diesen Genuss kommen. Dennoch wollte ich wissen, wie der Tourismusverein sicherstellt, dass diese Gutscheine nicht auch an Einheimische versendet werden. Nachdem meine Freundin mir den Bestellprozess erklärt hat, ist mir nun auch klar, wie das funktioniert:

Bei der Bestellung dieser Gutscheine setzt der Verein auf die Wohnortbestätigung der Online-Ausweisfunktion. Da die Gutscheine meiner Freundin elektronisch zugestellt wurden, benötigt der Verein aber nicht die volle Adresse meiner Freundin, sondern muss nur wissen, ob sie innerhalb des Gemeindebezirkes von Wellnesshofen gemeldet ist. Hierzu hat der Verein eine Abfrage in seinen Bestellprozess integriert, die aus dem neuen Personalausweis die Gemeindekennzahl erfragt und mit denen von Wellnesshofen vergleicht. Hierzu musste meine Freundin bei der Bestellung der Bonusgutscheine ihren Ausweis auf den Kartenleser legen und über die AusweisApp die Wohnortbestätigung zulassen. Dabei werden nicht die vollständigen Adressdaten des Ausweisinhabers übertragen, sondern es wird lediglich überprüft, ob die Adressdaten auf dem Ausweis mit einem angefragten Datensatz übereinstimmen oder nicht. Für den Zugriff auf den Ausweis hat der Verein die Erlaubnis bei der Vergabestelle für Berechtigungszertifikate bekommen.

Die Vorteile auf einen Blick

Für den Tourismusverein hat sich der Einsatz der Wohnortbestätigung gelohnt. Sie hat den Vorteil, dass mittels valider Daten festgestellt werden kann, ob ein Interessent berechtigt ist, in den Genuss von Vergünstigungen zu kommen, die nur für Touristen gelten. Somit können Gutscheine auch elektronisch und nicht mehr nur über den postalischen Versand zugestellt werden. Dies spart u. a. Portokosten und erfolgt fast in Echtzeit.

5.4 Zugang mit einem „Pseudonym“

Je intensiver ich das Internet nutze, umso mehr Login-Namen und Passwörter muss ich mir merken. Es wird ja immer wieder empfohlen, Passwörter nicht mehrfach zu vergeben. Also verwende ich für meine diversen Online-Bankkonten, Internetshops und Versicherungsportale jeweils unterschiedliche Passwörter. Dabei fällt es sicher nicht nur mir schwer, die vielen Login-Namen und Passwörter im Kopf zu behalten. Hier bietet der neue Personalausweis mit seiner neuen Funktion eines pseudonymen Zugangs Abhilfe.

Diensteanbieter, die Leistungen mit dem neuen Personalausweis anbieten, kann ich sofort am Logo des neuen Personalausweises erkennen. Um mich bei ihnen künftig anmelden zu können, benötige ich nur meinen neuen Personalausweis und meine sechsstellige PIN für den Online-Ausweis. Wenn ich mich zuvor z. B. bei einer Bank oder einem Online-Shop mit dem neuen Personalausweis registriert und meine PIN eingegeben habe, werden die erforderlichen persönlichen Daten und ein sogenanntes Pseudonym (der offizielle Name ist „karten- und dienstespezifisches Kennzeichen“) ausgelesen.
Dieses Pseudonym ist ein Wiedererkennungszeichen, das für jeden von mir angewählten Internetdienst (z. B. Bankportal oder Internetshop), den ich mit meinem Ausweis

verwende, neu festgelegt wird. Wenn ich mich später bei diesen Diensteanbietern wieder anmelden möchte, dann reicht es aus, dass nur das Pseudonym zur Datenübertragung ausgewählt wird. Nach der PIN-Eingabe wird nur mein für jeden Dienst spezielles Pseudonym übertragen, mit dem der jeweilige Diensteanbieter mich als seinen Kunden „wiedererkennt“. Übrigens, da Pseudonyme für jeden Dienst neu berechnet werden, können mehrere Diensteanbieter nicht durch einfachen Abgleich der Pseudonyme erkennen, dass ich bei ihnen Kunde bin. Ein guter Beitrag zum Datenschutz, schließlich möchte ich nicht, dass jemand mitverfolgt, welche Internetdienste ich nutze und welche nicht.

Es gibt noch einen Fall, in dem ich das Pseudonym nutzen kann: Wenn ich z. B. in einem Chatroom, der den neuen Personalausweis unterstützt, aufgefordert werde, zur Registrierung einen Nickname wie z. B. „Erika64“ anzugeben, dann kann gleichzeitig ein Pseudonym mit dem neuen Personalausweis für diesen Dienst gespeichert werden. Früher hätte ich zusätzlich noch ein Passwort vergeben und mir merken müssen. Mit dem neuen Personalausweis reicht es, bei Anmeldungen im Chatportal nur das Pseudonym des Ausweises zu übertragen, und ich werde automatisch als „Erika64“ erkannt. Damit sind meine Einträge sicher und nur ich kann sie ändern oder neue anlegen.

Die Vorteile auf einen Blick

Der pseudonyme Zugang mit dem neuen Personalausweis erleichtert Anmeldeprozesse, indem die Nutzerin oder der Nutzer nach einer initialen Anmeldung wiedererkannt werden kann. Damit trägt er in hohem Maße zur Sparsamkeit von Daten bei. Firmen müssen bei der Verwendung eines pseudonymen Zugangs keine neuen Passwörter mehr generieren und versenden, sofern diese dem Nutzer nicht mehr bekannt sind. Die Nutzerfreundlichkeit kann verbessert und die Benutzerverwaltung von Internetportalen vereinfacht werden.

5.5 Unterschriftsfunktion

Berufsbedingt werde ich die kommenden zwei Jahre öfter in Berlin sein. Daher habe ich mir überlegt, dort ein kleines Apartment anzumieten. Ich war auch schon vergangenes Wochenende in unserer Hauptstadt und habe mir einige Wohnungen angesehen. Leider konnte ich mich aber noch nicht entscheiden, und ich wollte auch mit meinem Mann nochmals darüber sprechen. Nun habe ich mich für das kleine moderne Apartment in Prenzlauer Berg entschieden. Die Wohnungsgesellschaft hat mir angeboten, den Vertrag elektronisch per Mail zuzuschicken, und ich kann ihn mit der elektronischen Unterschriftsfunktion auf meinem neuen Personalausweis rechtswirksam unterschreiben und anschließend wieder per Mail an sie zurücksenden.

Zum Glück hatte ich vor einiger Zeit meinen Personalausweis schon mit einer qualifizierten elektronischen Signatur ausgestattet. Das war eigentlich ganz einfach. Zuerst hatte ich den Ausweis über die AusweisApp mit Hilfe der eingeschalteten Online-Ausweisfunktion für die qualifizierte elektronische Signatur vorbereitet. Hierzu musste ich mir eine Signatur-PIN ausdenken (ich habe natürlich nicht mein Geburtsdatum genommen). Anschließend habe ich mich über die Online-Ausweisfunktion meines neuen Personalausweises bei einem Zertifizierungsdiensteanbieter registriert. Dieser hat dann für mich ein elektronisches Zertifikat erstellt, das ich über das Internet im Chip meines Ausweises ablegen konnte.

Um nun den Mietvertrag unterschreiben zu können, habe ich das mir zugesandte Dokument und die AusweisApp geöffnet und diesen nach dem gründlichen Durchlesen über den Befehl „Dokument signieren“ mit meiner Signatur-PIN unterschrieben.

Zuvor hatte ich bereits die kontaktlose Verbindung zwischen meinem Ausweis als Signaturkarte und dem Lesegerät zugelassen. Dazu musste ich meinen Ausweis aufs Lesegerät auflegen und die sechsstellige Zugangsnummer, die – leicht zu finden – auf der Vorderseite des Ausweises steht, eingeben. Der ganze Prozess ist besonders sicher, da ich den Komfortkartenleser mit integriertem Zahlenblock und Display nutze, wie es gesetzlich vorgeschrieben ist.

Die Vorteile auf einen Blick

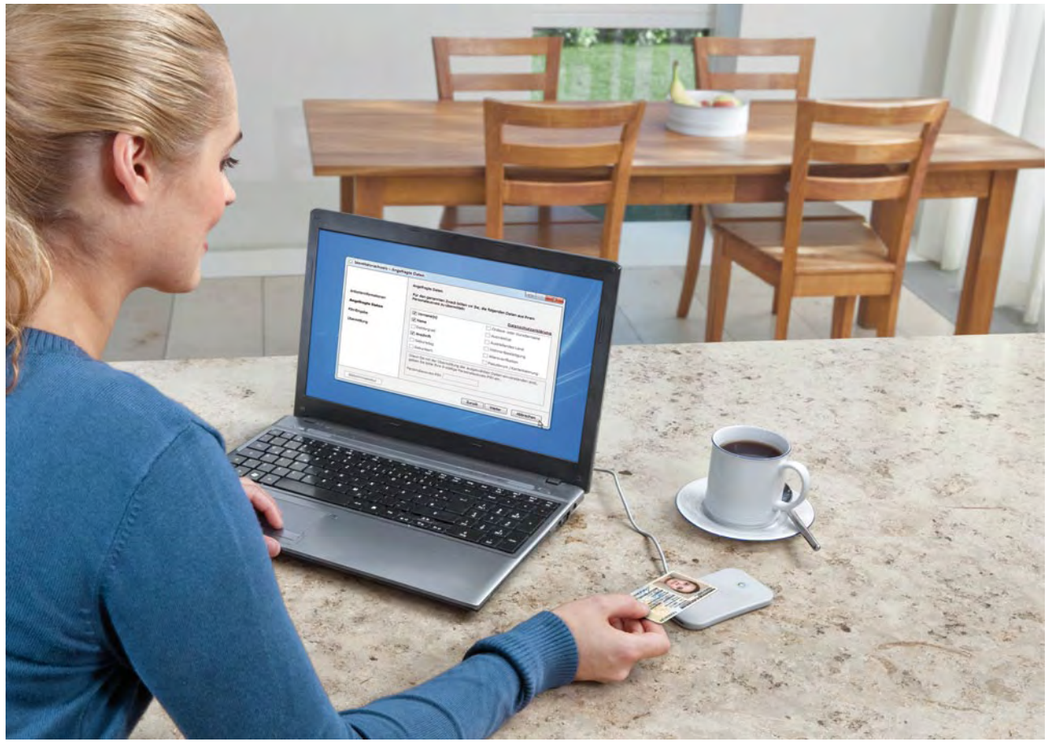
Mit der Unterschriftsfunktion konnte ich den Mietvertrag elektronisch unterschreiben und per E-Mail an die Berliner Wohnungsgesellschaft zurücksenden. Auch für die Wohnungsbaugesellschaft war dies von Vorteil, da sie den unterschriebenen Vertrag sofort vorliegen hatte und nachweisen kann, dass wirklich ich den Vertrag unterschrieb.

5.6 Online-Behördengänge

Endlich habe ich mir einen Traum erfüllt und mir einen kleinen Hund angeschafft. Natürlich muss ich nun, damit alles rechtmäßig läuft, Hundesteuer entrichten. Früher hätte ich dazu zum Bürgeramt gehen und mich in die Schlange stellen müssen, aber dank des neuen Personalausweises kann ich das nun bequem von zu Hause aus machen.

Ich rufe also die Internetseite meiner Stadt auf und registriere mich erst einmal als Bürger bei meiner Stadt, damit die wissen, mit wem sie es überhaupt zu tun haben. Ich muss das nicht unbedingt tun, aber da ich später noch weitere Dienste meiner Stadt in Anspruch nehmen will und vor allem auch noch wesentlich umfangreichere Dienstleistungen nutzen möchte, entscheide ich mich für diesen Weg.

Für diese Registrierung erlaube ich der Stadt, meinen Namen, Vornamen, mein Geburtsdatum und meine Anschrift aus meinem neuen Personalausweis auszulesen. Und ich schaue mir genau das Berechtigungszertifikat meiner Stadt an. Nur so können beide Seiten sicher sein, mit vertrauenswürdigen Daten zu arbeiten. Ich bin sicher, meine persönlichen Daten wirklich nur meiner Stadt übermittelt zu haben und nicht einer kriminellen, falschen Seite.



Die Stadt legt für mich ein Bürgerkonto an. Nun werde ich mit Namen begrüßt und kann zwischen den Diensten „Hundesteuer anmelden“ und „Hundesteuer abmelden“ auswählen. Natürlich wähle ich „Hundesteuer anmelden“. Meine Stadt zeigt mir nun ein Formular an, in dem bereits meine Namen, mein Geburtsdatum und meine Anschrift voreingetragen sind. Diese Daten entstammen meinem Personalausweis und sind folglich korrekt. Ich muss nur noch ein paar andere Daten zu meinem neuen Hund eintragen und schicke das Formular ab. Wenn ich möchte, kann ich jetzt noch weitere Dienste nutzen. Ich kann zum Beispiel noch das Formular „Antrag auf Ausgabe einer Reitplakette“ für mein Pferd oder „Fernleihe Bücher“ bei der Stadtbücherei anwählen und mich auch noch für die Fernleihe für Bücher, die ich für meine Doktorarbeit brauche, anmelden. Ich könnte auch beim Standesamt meine Heiratsurkunde anfordern, die ich verloren habe.

Wenn ich nicht möchte, dass meine Stadt ein Benutzerkonto für mich anlegt, und ich auch nur einfache Prozesse online nutzen möchte, gibt es eine weitere Möglichkeit. Dazu gehe ich auch auf die Seite meiner Stadt, klicke auf „Hundesteuer anmelden mit dem neuen Personalausweis“, bekomme wie oben das Formular angezeigt, erlaube meiner Stadt, meine Daten aus dem Personalausweis auszulesen und in das Formular zu übertragen. Ich trage weitere Daten zu meinem Hund in das Formular ein und sende es ab. Die Daten, die meine Stadt aus meinem Personalausweis ausgelesen hat, werden sofort wieder gelöscht. Die Stadt legt kein Bürgerkonto für mich an.

Die Vorteile auf einen Blick

Der Weg in die Behörde und die Beschränkung durch Öffnungszeiten entfallen. Daten, die übernommen werden, sind zu 100 % korrekt, da sie einem hoheitlichen Dokument (Ausweis) entnommen sind. Dies bedeutet auch, dass aufgrund einer medienbruchfreien Abwicklung und der hohen Datenqualität der personenbezogenen Daten aus dem Personalausweis Kosten bei der Stadt eingespart werden können. Eine Kontrolle manuell vom Kunden eingegebener Informationen erübrigt sich. An Bürgerinnen und Bürger adressierte Schreiben erreichen diese zuverlässig, da die Anschrift verifiziert ist.

5.7 Sichere E-Mail/De-Mail

Erst kürzlich bin ich von meinem E-Mail-Provider angeschrieben worden, ob ich mir nicht einen De-Mail-Account einrichten möchte. Von De-Mail hatte ich schon gehört und die kurze De-Mail-Beschreibung meines Providers überzeugte mich rasch von den Vorteilen.

Der De-Mail-Dienst ermöglicht das rechtssichere und vertrauliche Versenden von Dokumenten und Nachrichten über das Internet. Jeder Bürger, aber auch jede Institution kann sich einen dafür erforderlichen De-Mail-Account zulegen. Mein E-Mail-Provider hat sich kürzlich als De-Mail-Provider akkreditieren lassen und bietet diesen Dienst nun an.

Um einen De-Mail-Account einzurichten, muss ich mich allerdings einmalig und eindeutig identifizieren und damit nachweisen, dass es mich gibt. Bisher war dies nur persönlich oder mittels Postident-Verfahren möglich. Mit meinem neuen Personalausweis und der Online-Ausweisfunktion kann ich das aber jetzt auch bequem von zu Hause aus erledigen.

Doch damit nicht genug. Mit meinem neuen Personalausweis kann ich mich auch an meinem De-Mail-Account anmelden – und das ist viel sicherer als nur mit Benutzerkennung und Passwort. Wenn ich dann De-Mails versende, kann der Empfänger sicher sein, dass sie von mir stammen.

Von meinem De-Mail-Account aus kann ich verschlüsselt und sicher Nachrichten und Dokumente übers Internet versenden und empfangen. Außerdem kann ich wählen, ob ich eine Versand- oder sogar eine Eingangsbestätigung haben möchte. Dies finde ich prima, da ich erst neulich schlechte Erfahrungen gemacht habe, als ich ein Abonnement schriftlich kündigte. Da bestritt die Firma, meine Kündigung erhalten zu haben, und so verlängerte sich mein Vertrag um ein weiteres Jahr. Das kann mir nun mit De-Mail nicht mehr passieren. Auf meinen Wunsch hin erstellt nämlich der De-Mail-Provider des Empfängers eine Eingangsbestätigung. Damit kann ich nachweisen, dass der Empfänger die Nachricht bekommen hat.

Viele Schriftstücke lasse ich mir jetzt auch elektronisch per De-Mail zuschicken und archiviere sie gleich sicher im De-Safe bei meinem De-Mail-Provider. So finde ich sie schneller und spare Platz und Arbeit.

Auch meine Stadtverwaltung, mit der ich ab und zu im Schriftverkehr stehe, profitiert davon. Man hat mir erklärt, dass diese zukünftig auf diesem Wege auch offizielle Dokumente an mich zustellen lassen kann und somit Geld und Zeit spart. Darüber hinaus kann die Verwaltung Antragsdaten direkt aus meinen Dokumenten elektronisch übernehmen und muss diese nicht erst aufwändig vom Papierantrag übertragen.

Die Vorteile auf einen Blick

Mit dem neuen Personalausweis komme ich schnell und vor allem online zu meinem De-Mail-Account. Dabei kann ich mich auf einem hohen Sicherheitsniveau beim De-Mail-Konto anmelden. Damit gelte ich gegenüber meinen Kommunikationspartnern als besonders vertrauenswürdig. Sowohl Bürgerinnen und Bürger als auch Behörden und Unternehmen sparen mit De-Mail Zeit und Kosten, wenn sie den Service für ihre jeweiligen Kommunikationsprozesse nutzen.

5.8 Was geht nicht?

Die oben aufgeführten Beispiele aus meinem täglichen Leben haben mir gezeigt, wie unterschiedlich und vielfältig die Einsatzmöglichkeiten meines neuen Ausweises sind. Ich habe aber auch erfahren können, dass ich für einige Anwendungen die elektronische Identifikationsfunktion nicht einsetzen kann. Dies hat unterschiedliche, aber stets nachvollziehbare Gründe. Grundsätzlich gibt es für den Diensteanbieter kein Berechtigungszertifikat, wenn er die persönlichen Ausweisdaten auslesen möchte, nur um Bürgerinnen und Bürgern allgemein zugängliche Informationen zu präsentieren, z. B. innerhalb eines Online-Shops, wenn ich mir den Warenkatalog aus Interesse nur einmal anschauen möchte. Darüber hinaus wird keine Berechtigung zum Auslesen des Ausweises erteilt, sofern rechtliche Bestimmungen gegen das Erheben von Daten sprechen oder auch wenn die rechtliche Grundlage zum Erheben meiner persönlichen Daten fehlt.

Sobald der Verdacht besteht, dass das Erheben meiner persönlichen Daten aus dem Ausweis u. a. dem Zweck dienen soll, diese (Adress-)Daten gewerblich oder gegen Entgelt an Dritte weiterzugeben, wird zum Glück und zu meinem besonderen Schutz dafür ebenfalls keine Berechtigung bewilligt. Der Diensteanbieter, der meine Ausweisdaten verwenden möchte, muss mir klar und deutlich am Anfang des Ausleseprozesses mitteilen, wann und zu welchem Zweck er meine Daten benötigt und wie er sie verwenden möchte.

6 Wirtschaftlichkeit

Unternehmen und Behörden erhalten in diesem Kapitel Informationen, um Aufwand und Nutzen einer Personalausweisanwendung selbst abschätzen zu können. Dabei werden einmalige Investitionen und die laufenden Kosten für den späteren Betrieb unterschieden. Neben Kosten- und Ertragsauswirkungen werden auch positive Effekte für Kundenservice, Image und Compliance erläutert. Zum Schluss wird der voraussichtliche Verbreitungsgrad des neuen Personalausweises dargestellt, damit Mengengrößen für eine Wirtschaftlichkeitsrechnung über mehrere Jahre geschätzt werden können.

6.1 Investitionsbedarf

Für die Einführung eines Dienstes mit dem neuen Personalausweis wird die Durchführung in Form eines Organisations- und IT-Projektes empfohlen. Abbildung 12 zeigt den internen Aufwand in Personentagen (PT) für ein solches Investitionsprojekt als Ergebnis einer Befragung unter den Teilnehmern des Anwendungstests für den neuen Personalausweis 2009 bis 2010. Die Prozentangaben zeigen den Anteil der Unternehmen mit dem jeweiligen Aufwand.

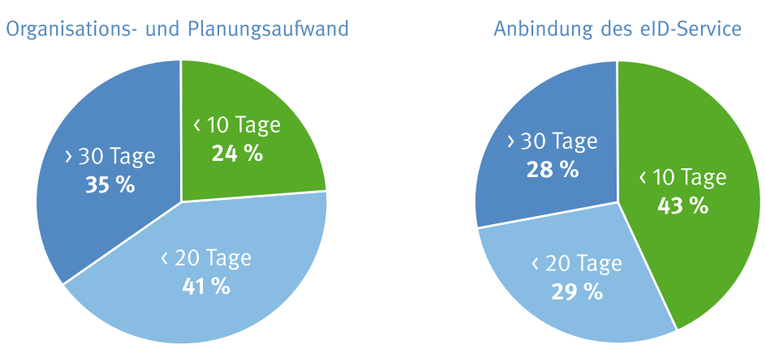


Abbildung 12: Interner Projektaufwand von Diensteanbietern im Anwendungstest (Quelle: Kompetenzzentrum neuer Personalausweis)

Demnach gab ein Großteil der Diensteanbieter an, für Organisation und Planung weniger als 20 Tage zu benötigen. Ebenso wurden für die Anbindung des eID-Service mehrheitlich weniger als 20 Tage in Anspruch genommen.

Neben dem Aufwand für die Analyse der Geschäftsprozesse, deren Neugestaltung und die technische Integration sollten ausreichende Ressourcen für die Abstimmung mit dem Datenschutzbeauftragten und die Beantragung des Berechtigungszertifikats bei der Vergabestelle für Berechtigungszertifikate eingeplant werden.
Für den Fall, dass ein eigener eID-Server betrieben werden soll, sind Investitionen in Hardware und den Erwerb der Software-Lizenz zu berücksichtigen, ggf. auch längere Vorlaufzeiten für eID-Server-Eigenentwicklung nach der eCard-API und Software-Zertifizierung. Software-Lizenzen für eID-Server und eID-Services werden von mehreren Firmen angeboten. Nähere Informationen finden Sie auf der Seite www.personalausweisportal.de unter den Menüpunkten „Partner werden“ und „Technische Infrastruktur“.

Bei entsprechenden Rahmenverträgen kann es sich z. B. für Behörden lohnen, beim eigenen IT-Service-Provider nachzufragen, ob eine Bereitstellung einer Software-Lizenz für einen eigenen eID-Server kostenfrei erfolgen kann.

Manche Firmen bieten Komponenten an, bei denen die notwendige Hard- und Software für den Betrieb eines eigenen eID-Servers bereits fertig integriert ist. Dabei kann eine bestimmte Verfügbarkeit des Gesamtsystems garantiert werden.

Weitere Investitionskosten entstehen durch die individuellen Anforderungen jedes Diensteanbieters an Geräte und Software-Anwendungen. Im Fall von Online- oder Stand-alone-Automaten kann der Einbau von Kartenlesern und Eingabetastaturen für die Eingabe der eID-PIN notwendig werden.

6.2 Laufende Kosten

Für Software-Lizenzen eines eigenständig betriebenen eID-Servers fallen bei den bisher am Markt auftretenden Anbietern neben den Lizenzkosten auch jährliche Gebühren für Wartung und Updates an.
Wenn sich ein Diensteanbieter für einen eID-Service von einem externen eID-Service-Provider entscheidet, entfallen die Investitionskosten und es fallen nur Servicegebühren an.

Die Preisgestaltung hängt in diesem Fall davon ab, welche Anzahl von Auslesevorgängen erwartet wird, welche Auslastungsschwankungen bestehen und welche Verfügbarkeit der Systeme garantiert werden muss. Erste Preisindikatoren am Markt Ende des Jahres 2010 zeigen, dass für 100.000 Auslesevorgänge ein Preis von unter 6.000 Euro im Jahr erwartet werden kann.
Alle drei Jahre sind 102 Euro Gebühren nach § 3 der PAuswGebV an die Vergabestelle für Berechtigungszertifikate für die Prüfung und Erteilung eines Berechtigungszertifikates zu entrichten. Diese Gebühr entfällt für Diensteanbieter der öffentlichen Verwaltung.
Weitere Kosten fallen jährlich an, um die technischen Berechtigungszertifikate und die notwendigen SSL-Zertifikate von den Trustcentern zu erhalten. Erste Preisindikatoren Ende des Jahres 2010 zeigen jährliche Kosten für technische Berechtigungszertifikate von unter 2.000 und für SSL-Zertifikate von unter 600 Euro an.
Weitere laufende IT-Betriebskosten ergeben sich aus den individuellen Anforderungen der Diensteanbieter an ihre Geräte und Anwendungen.

Es ist davon auszugehen, dass sich der Markt der Anbieter von Berechtigungszertifikaten und eID-Services weiter ausdifferenziert. Daher kann erwartet werden, dass weitere attraktive Preismodelle für verschiedene Bedarfslagen bei kleinen, mittleren und großen Unternehmen und Behörden angeboten werden.

6.3 Nutzen

6.3.1 Kostenreduktion und Umsatzsteigerung

Der neue Personalausweis erlaubt es, Geschäftsprozesse vollständig in das Internet zu verlagern, für die bisher ein persönlicher Kontakt etwa in einer Behörde, ein Vertreterbesuch oder ein Laden erforderlich waren. In diesen Fällen können bei den Diensteanbietern Personal- und Standortkosten reduziert werden.

Der Einsatz des neuen Personalausweises bietet Chancen zur Senkung von Sach- und Prozesskosten.

Auch bereits bestehende Online-Geschäftsprozesse werden durch den Personalausweis attraktiver, da durch die gegenseitige Authentifizierung ein hochwertiges Vertrauensverhältnis aufgebaut wird und beide Seiten bereit sind, auf dieser Grundlage mehr Transaktionen im Internet abzuwickeln. In diesen Fällen entsteht der Nutzen für Diensteanbieter durch Umsatzsteigerungen. In Fällen, in denen auf papiergebundenen Schriftverkehr verzichtet werden kann, ergeben sich Einsparungen bei Versand- und Portokosten. Im Bereich der Bezahlverfahren können das Zahlungsausfallrisiko und der Aufwand für den Forderungseinzug z. B. bei Lieferung auf Rechnung oder im ELV weiter begrenzt werden. Durch das Auslesen einer verifizierten Adresse aus dem neuen Personalausweis werden Falschlieferungen verhindert und im Fall eines Zahlungsverzugs können Mahnungen rechtskräftig zugestellt werden. Rückstellungen für diese Risiken können reduziert werden. Durch eine Altersüberprüfung können Geschäfte mit beschränkt oder nicht geschäftsfähigen Personen abgelehnt und das Unternehmen und seine Mitarbeiter vor unerwünschten Rechtsfolgen bewahrt werden.

Nicht zuletzt erhöht sich durch den neuen Personalausweis die Qualität der Stammdaten für den Diensteanbieter. Prozesse und Ressourcen zur Kontrolle und Stammdatenpflege können reduziert werden.

6.3.2 Erhöhung von Kundenservice, Image und Compliance

Für die Kunden von Diensteanbietern ist es ein Vorteil, wenn ihnen Wege auf Ämter oder in die Kundenservicebereiche von Dienstleistern einschließlich der dort anfallenden Wartezeiten erspart bleiben und sie stattdessen ein Leistungsangebot bzw. einen Dienst jederzeit, medienbruchfrei und schnell vom eigenen Computer zu Hause abwickeln können. Durch das automatische Ausfüllen von Formularen steigt zudem die Kundenfreundlichkeit der Dienstleistung. Entsprechend attraktiv wird der Diensteanbieter aus Kundensicht und kann sich ansprechend im Markt differenzieren.

Der Einsatz des neuen Personalausweises mit Online-Ausweisfunktion und ggf. Unterschriftsfunktion zeigt den Kunden die technische Kompetenz des Diensteanbieters. Die Kunden werden den Sicherheitsgewinn durch einen hohen Datenschutz und die Selbstbestimmung über ihre Daten begrüßen. Durch den Wegfall von schriftlicher Korrespondenz sparen die Kunden Portokosten und erkennen den umweltfreundlichen Aspekt der Einsparung von Briefsendungen.

Unternehmen können durch den Einsatz des neuen Personalausweises viele gesetzliche Auflagen erfüllen und damit ihre Compliance verbessern. Dies wird deutlich z. B. bei der Einhaltung von Jugendschutzbestimmungen an Automaten und beim Internetverkauf oder bei der Erfüllung von Formerfordernissen durch den Einsatz der Unterschriftsfunktion.

6.4 Verbreitung des neuen Personalausweises

Alle Bürgerinnen und Bürger können seit dem 1. November 2010 ausschließlich den neuen Personalausweis beantragen. Durchschnittlich werden pro Jahr acht Millionen neue Ausweise ausgestellt. Da der neue Personalausweis für viele Bürgerinnen und Bürger besonders attraktiv ist, wird davon ausgegangen, dass im ersten Jahr bis zu zehn Millionen neue Ausweise ausgegeben werden.

Pro Jahr werden rund acht Millionen neue Personalausweise ausgestellt.

Für Ausländer, die dauerhaft in der Bundesrepublik Deutschland leben, ist für 2011 die Einführung eines elektronischen Aufenthaltstitels geplant, der ebenfalls die Online-Ausweisfunktion des neuen Personalausweises besitzen wird.

Für EU-Bürger, die selbst bereits im Besitz einer eigenen staatlich geprüften elektronischen Identität und Signatur sind, sollen über ein EU-Projekt die technischen Voraussetzungen geschaffen werden, dass sie ebenfalls Dienste in Deutschland elektronisch nutzen können. Für EU-Bürger mit ständigem Wohnsitz in Deutschland wird zudem die Einführung einer gesonderten eCard in Deutschland geprüft.

Für die Unterschriftsfunktion mit der qualifizierten elektronischen Signatur fallen nur noch die Kosten für das Zertifikat an und nicht mehr die Kosten für eine gesonderte Trägerkarte. Das Zertifikat kann in Zukunft direkt auf den neuen Personalausweis geladen werden.

7 Unterstützung von Diensteanbietern

7.1 Kompetenzzentrum neuer Personalausweis

Die Unterstützung für aktive und neue Diensteanbieter im „Kompetenzzentrum neuer Personalausweis“ wird fortgeführt, um auch nach dem 1. November 2010 eine neutrale Plattform für Infrastruktur- und Diensteanbieter, Verbände und die Fachgemeinschaft anzubieten. Das Angebot umfasst mehrere Bausteine, die im Folgenden beschrieben werden.

7.1.1 Wissens- und Kommunikationsplattform

Die Wissens- und Kommunikationsplattform www.ccepa.de dient als zentrale Plattform für fachliche und technische Informationen und den Erfahrungs- und Meinungsaustausch zum neuen Personalausweis, hauptsächlich zur Online-Ausweisfunktion. Es ist die Verlängerung des Personalausweisportals für Partner des neuen Personalausweises. Mit Infobriefen, Newslettern und einem Forum werden die registrierten Interessenten informiert oder unmittelbar am Wissens- und Erfahrungsaustausch der Kompetenzträger beteiligt.

7.1.2 Test- und Demonstrationszentrum (TDZ)

Das Test- und Demonstrationszentrum (TDZ) dient der Unterstützung aktiver und neuer Diensteanbieter in Wirtschaft und Verwaltung zur Einbindung des neuen Personalausweises in die verschiedenen IT-Systeme und Geschäftsprozesse, zur verstärkten Förderung der Verfügbarkeit von Diensten, zur Erhöhung der Akzeptanz und zur weiteren Entwicklung neuer Geschäftsmodelle rund um den neuen Personalausweis. Das TDZ fördert durch die Demonstration erfolgreicher Anwendungen und Tests, durch eine Erstberatung bzw. eine vertiefende Beratung die gezielte Betreuung und Begleitung der Einführungsphase des neuen Personalausweises in verschiedenen Geschäftsprozessen und dient als zentraler Anlauf- und Informationspunkt für interessierte Besucher aus öffentlicher Verwaltung und Wirtschaft. In Teststellungen und Workshops werden insbesondere die Personalausweis-Infrastruktur, unterschiedliche Komponenten sowie innovative Szenarien und Anwendungen erprobt und demonstriert. Zusätzlich werden die technischen Komponenten wie die AusweisApp und die eID-Server oder Lesegeräte verschiedener Anbieter präsentiert.

7.1.3 Fachberatung

Im Rahmen einer branchenorientierten Fachberatung werden Diensteanbieter auf Grundlage einer laufenden Potenzialanalyse für die Anwendung der elektronischen Ausweisfunktionen gewonnen und bei der Evaluation, Konzeption und Umsetzung von Anwendungsszenarien zielgerichtet unterstützt. Dabei können sowohl organisatorische als auch technische Fragestellungen wie beispielsweise zur technischen Integration des neuen Personalausweises, darunter seiner eID-Client- und eID-Server-Komponenten, in die IT-Prozesse und IT-Infrastruktur des Diensteanbieters beantwortet werden. Die organisatorische Beratung umfasst hier vor allem die Geschäftsmodellentwicklung, Prozessdefinitionen und Prozessmodellierung, Organisationsberatung, Wirtschaftlichkeitsprüfungen, Kommunikationsstrategie und Kommunikationsmaßnahmen. Mit der technischen Beratung werden Dienste- und Infrastrukturanbieter in die Lage versetzt, über die Tiefe ihres technischen Engagements oder die Drittbeauftragung z.B. eines eID-Service-Providers zu entscheiden. Anwendungstests der elektronischen Ausweisfunktionen führen Diensteanbieter anschließend in der Regel mit ihren selbst ausgewählten und ggf. beauftragten IT-Partnern und nicht mehr mit dem Kompetenzzentrum durch.

7.1.4 Sicherheitsberatung

Mit der Sicherheitsberatung unterstützt das Kompetenzzentrum Diensteanbieter und eID-Service-Provider bei der Evaluation vorhandener und geplanter Prozesse, der Integration der eID- und QES-Funktion, dem Parallelbetrieb mehrerer Authentisierungsmechanismen, Penetrationstests und durch ein Testlabor.

7.2 Test-Infrastruktur für neue Dienste

Um die Funktionalitäten des neuen Personalausweises testen zu können, wird eine Test-Infrastruktur von den jeweiligen eID-Service-Providern angeboten. Daher wenden sich Diensteanbieter zur Nutzung einer Test-Infrastruktur direkt an entsprechende eID-Service-Provider.

Für die Test-Infrastruktur wurden fünf verschiedene Berechtigungen vordefiniert, d. h. Berechtigungen für unterschiedliche Zwecke, wie Altersbestätigung, Online-Handel, Bankkontoeröffnung, Anmeldung für ein Internetportal und Pseudonym. Die entsprechenden Musterzertifikate werden von den BerCAs den Diensteanbietern und eID-Services zur Verfügung gestellt. Die Musterzertifikate werden nicht für die einzelnen Diensteanbieter personalisiert, sondern enthalten vordefinierte Dienstedaten. Besitzt ein Diensteanbieter die Genehmigung der VfB für die Ausstellung eines Berechtigungszertifikats, kann er sich auch in der Test-Infrastruktur ein entsprechendes Zertifikat mit den genehmigten Datengruppen und Funktionen ausstellen lassen.

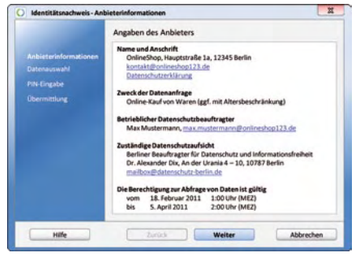
Zum Testen werden von der Bundesdruckerei GmbH sogenannte Musterkarten mit unterschiedlichen Datensätzen (männlich/weiblich, verschiedene Namen, Geburtsdaten, Geburtsorte usw.) für interessierte Diensteanbieter gegen eine Gebühr angeboten. Die Musterkarten können von den Diensteanbietern über die eID-Service-Provider beantragt werden.

8 Weitere Informationen und Kontakte

Das Bundesministerium des Innern hat unter www.personalausweisportal.de seit Mai 2010 ein Informations- und Serviceportal zum neuen Personalausweis eingerichtet. Hier sind aktuelle Informationen rund um den neuen Personalausweis erhältlich. In einer umfangreichen Bibliothek sind u. a. auch Anträge für die Erteilung von Berechtigungszertifikaten bei der Vergabestelle für Berechtigungszertifikate erhältlich.

Das Bundesministerium des Innern hat seit Oktober 2009 ein Kompetenzzentrum neuer Personalausweis eingerichtet. Dieses steht Ihnen als Ansprechpartner bei allen Fragen zum Testen der neuen Funktionen zur Verfügung. Ein zentrales Medium ist die Wissens- und Kommunikationsplattform unter www.ccepa.de. Hier finden Bürger und Diensteanbieter zahlreiche Informationen. Auskünfte erhalten Sie auch per E-Mail unter info@ccepa.de.

Das Schaufenster für den neuen Personalausweis befindet sich im Test- und Demonstrationszentrum in Berlin und ist Teil des Kompetenzzentrums neuer Personalausweis. Dort werden Szenarien und Anwendungen mit dem neuen Personalausweis demonstriert. Darüber hinaus stehen dort Experten bereit, die Informationen rund um den Personalausweis je nach Interesse der Besuchergruppe vermitteln. Um einen Eindruck zu erhalten, können Sie das Test- und Demonstrationszentrum auch virtuell im Rahmen einer Flash-Animation besuchen. Sie erreichen es unter http://www.ccepa.de/Unternehmen/Verwaltung ➔ Unterstützung ➔ Test- und Demozentrum.



Die Vergabestelle für Berechtigungszertifikate (VfB) erreichen Sie im Internet unter

http://www.personalausweisportal.de ➔ Partner werden.

Dort erhalten Sie Informationen sowohl zu Berechtigungszertifikaten als auch zum Sperrdienst und Sperrmanagement.

Das Bundesamt für Sicherheit in der Informationstechnik ist für die technischen Sicherheitsspezifikationen des neuen Personalausweises verantwortlich, erstellt Spezifikationen, Schutzprofile und Konformitätstests für die einzelnen Komponenten und führt Zertifizierungen durch.

Es ist unter
https://www.bsi.bund.de/ElektronischeAusweise
➔ Der neue Personalausweis
zu erreichen.

9 Häufig gestellte Fragen

Wo erhalte ich Unterstützung bei der Durchführung von Testmaßnahmen?

Das Bundesministerium des Innern hat für die Unterstützung der Testmaßnahmen ein Kompetenzzentrum neuer Personalausweis eingerichtet. Dort stehen Ansprechpartner für alle Fragen bereit. Das Kompetenzzentrum betreibt in Berlin ein Test- und Demonstrationszentrum. Dort werden Szenarien entwickelt und Anwendungen mit dem neuen Personalausweis gezeigt.

Wo finde ich die für den neuen Personalausweis relevanten Richtlinien für die technische Umsetzung?

Das Bundesamt für Sicherheit in der Informationstechnik legt Richtlinien für elektronische Ausweisdokumente fest. Diese sind unter https://www.bsi.bund.de einsehbar.

Wo bekomme ich Personalausweise, um Anwendungen testen zu können?

Um die Funktionalitäten des neuen Personalausweises testen zu können, wird eine Test-Infrastruktur von den jeweiligen eID-Service-Providern angeboten. Von der Bundesdruckerei GmbH werden sogenannte Musterkarten mit unterschiedlichen Datensätzen (männlich/weiblich, verschiedene Namen, Geburtsdaten, Geburtsorte usw.) gegen eine Gebühr bereitgestellt. Diese Musterkarten können über die eID-Service-Provider beantragt werden.

Wo kann ich zertifizierte Kartenleser erhalten?

Zertifizierte Kartenleser werden von mehreren Herstellern angeboten. Eine Auflistung ist unter https://www.bsi.bund.de oder www.ausweisapp.bund.de erhältlich. Eine Liste von weiteren Lesegeräten, die für die Nutzung mit dem neuen Personalausweis geeignet sind, finden Sie unter www.ccepa.de.

Welche Informationen benötige ich für die Beantragung eines Berechtigungszertifikats?

Um eine Berechtigung bei der Vergabestelle für Berechtigungszertifikate zu beantragen, ist anzugeben, welche Datenfelder ausgelesen werden sollen. Dabei ist auch der jeweilige Geschäftszweck darzustellen. Darüber hinaus sind Angaben zum Datenschutz erforderlich.

Wie lange ist ein Berechtigungszertifikat gültig?

Die Vergabestelle für Berechtigungszertifikate stellt eine Berechtigung für maximal drei Jahre aus.

Wie erhalte ich ein Signaturzertifikat?

Der neue Personalausweis ist für die Nutzung der Unterschriftsfunktion lediglich vorbereitet. Das heißt, der Personalausweisinhaber erwirbt selbständig ein Signaturzertifikat bei einem Anbieter. Eine vollständige Liste über akkreditierte und angezeigte Signaturanbieter wird im Verzeichnisdienst der Bundesnetzagentur unter http://www.nrca-ds.de veröffentlicht.

Wie erhalte ich Zugang zu technischen Richtlinien?

Technische Richtlinien zum neuen Personalausweis finden Sie auf den Internetseiten des Bundesamtes für Sicherheit in der Informationstechnik unter der Rubrik „Elektronische Ausweise“, „TRs und Schutzprofile“ (https://www.bsi.bund.de/ElektronischeAusweiseTR).

Können Unbefugte Zugriff auf die Personalausweisdaten erhalten?

Die Übertragung der Daten auf dem Personalausweis erfolgt nach hohen Sicherheitsstandards. Vertraulichkeit, Fälschungssicherheit und Authentizität der Daten im neuen Personalausweis werden technisch durch Protokolle und Verfahren gewährleistet. Zudem können die Daten nur übertragen werden, sofern der Personalausweisinhaber durch die Eingabe einer PIN seine Zustimmung erteilt hat.

10 Glossar

AusweisApp

Die AusweisApp ist eine Software, die die Kommunikation zwischen dem Personalausweis und dem Diensteanbieter (bzw. dessen eID-Service) übernimmt. Die AusweisApp wird kostenfrei zur Verfügung gestellt.

Berechtigungs-zertifikat

Ein Berechtigungszertifikat stellt sicher, dass ein Diensteanbieter die Erlaubnis hat, auf die Daten des neuen Personalausweises zuzugreifen. Dort wird genau festgelegt, um welche Datenfelder es sich handelt. Der Diensteanbieter weist über das Berechtigungszertifikat dem Nutzer seine Identität nach. Eine Berechtigung kann bei der Vergabestelle für Berechtigungszertifikate beantragt werden. Die Zertifikate sind in ihrer Gültigkeit beschränkt.

Berechtigungs-zertifikateanbieter

Ein Berechtigungszertifikateanbieter stellt die Berechtigungszertifikate für einen Diensteanbieter bereit. Der Diensteanbieter schließt hierfür einen Vertrag mit dem Berechtigungszertifikateanbieter ab. Voraussetzung ist, dass dem Diensteanbieter eine entsprechende Berechtigung von der Vergabestelle für Berechtigungszertifikate erteilt worden ist. Berechtigungszertifikateanbieter werden auch als Zertifizierer oder BerCA bezeichnet.

eCard-API

Das Ziel des eCard-API-Frameworks ist das Bereitstellen einer einfachen und homogenen Schnittstelle, um in verschiedenen Anwendungen eine einheitliche Nutzung von unterschiedlichen Chipkarten (eCards) zu ermöglichen. Eine dieser Chipkarten ist der neue Personalausweis.

eID-Server

Die Kommunikation erfolgt zwischen dem Diensteanbieter bzw. dem von ihm genutzten eID-Server und dem Ausweis-Chip des Personalausweisinhabers. Dabei werden die Daten an den jeweiligen Diensteanbieter weitergegeben.

eID-Service

Sofern Diensteanbieter keinen eigenen eID-Server einrichten möchten, haben sie die Möglichkeit, auf externe Anbieter zurückzugreifen, die einen eID-Server betreiben. In diesem Fall wird ein eID-Service in Anspruch genommen.

Entsperrnummer (PUK)

Wenn die Geheimnummer für den Identitätsnachweis dreimal falsch eingegeben wurde, kann mit der Entsperrnummer der Fehlbedienungszähler zurückgesetzt werden.

Geheimnummer (PIN)

Für die Nutzung der Online-Ausweisfunktion ist die Eingabe einer sechsstelligen personengebundenen Geheimnummer erforderlich. Durch die Eingabe bestätigt der Personalausweisinhaber, dass er mit der Übermittlung der Daten an den Diensteanbieter einverstanden ist.

Online-Ausweisfunktion

Die Online-Ausweisfunktion ermöglicht es dem Personalausweisinhaber, sich gegenüber einem Anbieter eines Dienstes auszuweisen. Gleichzeitig weist der Diensteanbieter über sein Berechtigungszertifikat gegenüber dem Personalausweisinhaber nach, dass er eine staatliche Berechtigung hat, auf die Daten des neuen Personalausweises zuzugreifen.

Pseudonymer Zugang

Der pseudonyme Zugang stellt als einen Anwendungsfall das Wiedererkennen eines Benutzers nach erfolgreicher Erstregistrierung sicher. Das Pseudonym besteht aus einer speziellen Zeichenfolge, die sich nicht nur von Nutzer zu Nutzer unterscheidet, sondern auch von Dienst zu Dienst unterschiedlich ist. Hierüber ist eine vollständige Übermittlung der Personalausweisdaten nicht erneut erforderlich, sondern es wird lediglich das Pseudonym übermittelt.

Public-Key-Infrastruktur

Die gesamte Personalausweis-Infrastruktur basiert auf einer Public-Key-Infrastruktur (PKI) für Berechtigungszertifikate und Sperrmanagement. Daran sind mehrere Behörden beteiligt, insbesondere das Bundesamt für Sicherheit in der Informationstechnik, das Bundesverwaltungsamt (inkl. Sperrdienst), Zertifizierungsdiensteanbieter und die Bundesdruckerei.

Signaturzertifikat

Zur Nutzung der Unterschriftsfunktion ist ein Signaturzertifikat erforderlich. Dieses wird von privaten Signaturanbietern zur Verfügung gestellt und kann nach Anforderung des Personalausweisinhabers vom Zertifizierungsdiensteanbieter auf den Personalausweis aufgespielt werden.

Sperrkennwort

Das Sperrkennwort dient dazu, den elektronischen Identitätsnachweis zu sperren oder zu entsperren.

Sperrliste

Wird der Personalausweis gesperrt, erfolgt ein Eintrag in eine Sperrliste. Jeder Diensteanbieter verfügt über eine aktuelle Sperrliste. Auf dieser Sperrliste eingetragene Sperrmerkmale werden erkannt und der Einsatz der Online-Ausweisfunktion ist dann nicht mehr möglich.

Technische Richtlinie

Technische Richtlinien werden vom Bundesamt für Sicherheit in der Informationstechnik herausgegeben und enthalten technische und organisatorische Vorgaben für die Verbreitung eines angemessenen IT-Sicherheitsstandards.

Trustcenter

Ein Trustcenter ist eine Zertifizierungsstelle, die ein Zertifikat für die qualifizierte elektronische Signatur ausstellt.

Unterschriftsfunktion

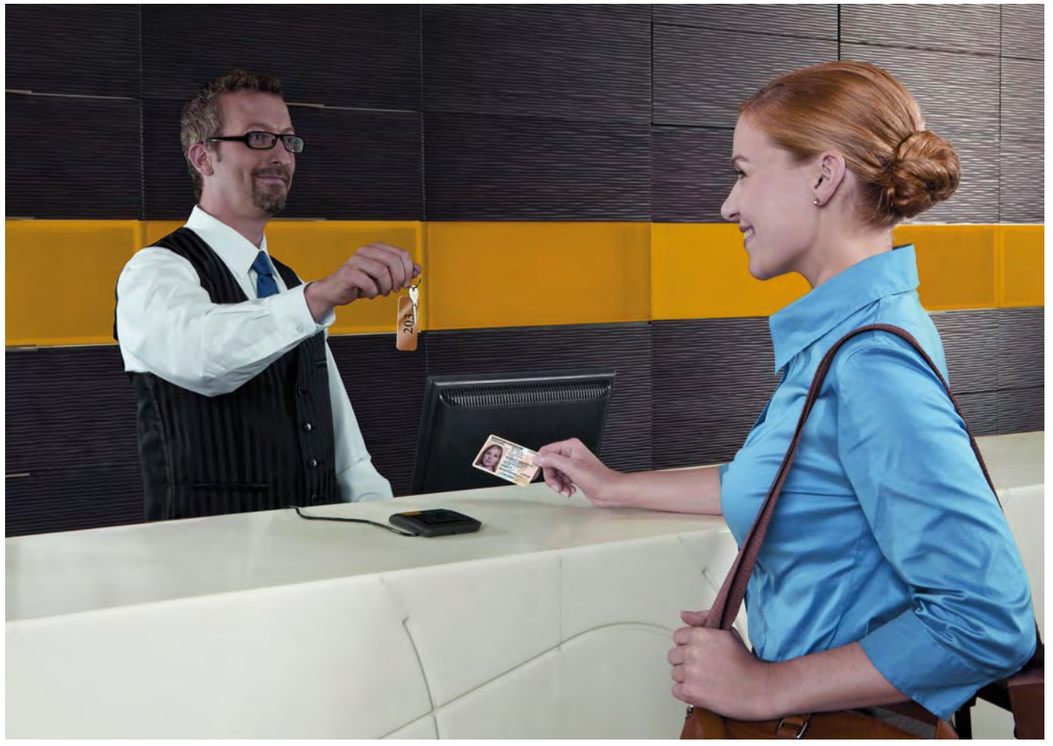
Die Unterschriftsfunktion erlaubt es dem Personalausweisinhaber, Dokumente auf elektronischem Weg rechtssicher zu unterschreiben. Voraussetzung hierfür sind die Aktivierung der Online-Ausweisfunktion und ein Signaturzertifikat, das der Personalausweisinhaber selbständig bei einem privaten Anbieter erwirbt. (Die Vergabestelle für Berechtigungszertifikate entscheidet über die Berechtigung der Diensteanbieter, die erforderlichen Daten im Wege des elektronischen Identitätsnachweises beim Inhaber des Personalausweises anzufragen.)

Zertifizierungsdiensteanbieter

Zertifizierungsdiensteanbieter, die nach dem Signaturgesetz zugelassen sind, stellen sowohl Signaturzertifikate als auch Berechtigungszertifikate aus. Die Zertifizierungsdiensteanbieter, die Signaturzertifikate ausstellen, werden auch Signaturanbieter genannt.

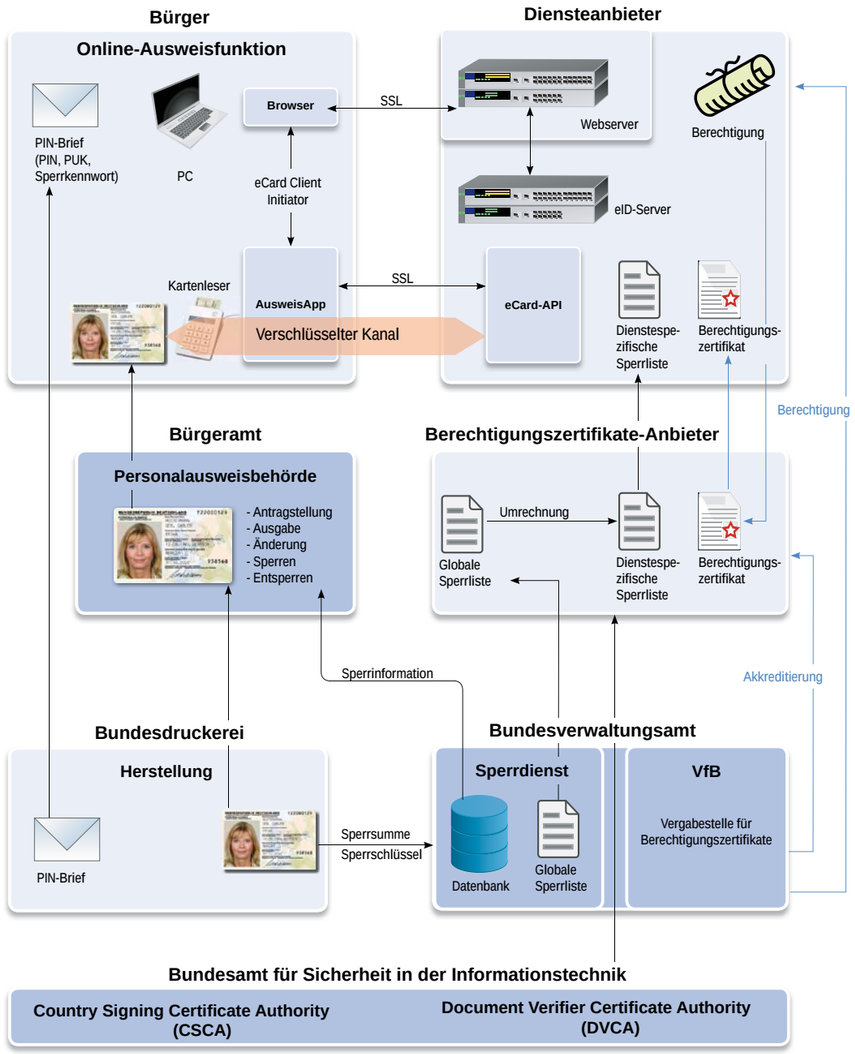
Zugangsnummer

Die Zugangsnummer ist auf der Vorderseite des Personalausweises abgedruckt. Die Zugangsnummer wird bei Falscheingabe der PIN, der Identitätsprüfung, dem Zugang zur Signatur und dem Änderungsdienst verwendet.



Anlage 1

Vereinfachtes Infrastrukturmodell für die Online-Ausweisfunktion



Anlage 2

Testanwendungen

(Stand der Registrierung bis 31. Oktober 2010)

Nr.	Registrierter Diensteanbieter	Name der Testanwendung
1*	**]init[AG** in Zusammenarbeit mit der Arbeitsgruppe **Extrapol** der Polizeien des Bundes und der Länder	Unterstützung der länderübergreifenden Zusammenarbeit der Polizeien durch geschlossene Benutzergruppen im Rahmen der gemeinsamen Plattform Extrapol
2	**achelos GmbH**	Unterstützung aller Dienste und Verfahren
3	**ac-Media Inc, deutsche Niederlassung**	Authentifizierung der Nutzer unseres Online-ERP-Systems
4	**ADDISON Software und Service GmbH**	ELSTER. Signieren und Verschlüsseln von E-Mails, Anmeldung am eigenen Online-Portal
5	**adesso AG**	Entwicklung und Testbetrieb des Single-Sign-on-Portals des GDV (Gesamtverband der Deutschen Versicherungswirtschaft e. V.)
6	**AHB Systeme GmbH**	Zutrittskontrolle und Zeiterfassung
7*	**Air Berlin PLC & Co. Luftverkehrs KG**	Fluggastabfertigung
8	**Akademische Arbeitsgemeinschaft, Wolter Kluwer Deutschland GmbH**	Authentifizierung für ELSTER und für Banking-Anwendungen
9*	**AKDB Anstalt für Kommunale Datenverarbeitung in Bayern**	Kfz-Zulassungsverfahren OK.VORFAHRT; Zentrale Einfache Melderegisterauskunft ZEMA; Führerscheinverfahren OK.EFA; Einwohnerwesen OK.EWO
10*	**Allianz Deutschland AG**	Kundenserviceprozesse im Versicherungsportal

11	**allyve GmbH**	Individuell konfigurierbares Internetportal zur Verwaltung der eigenen Passwörter für das Internet
12	**AOK Systems GmbH**	GKV-Online-Geschäftsstelle
13	**Applied Security GmbH**	Online-Banking für Geschäftskunden
14*	**ARGE** Deutsche Verwaltungsagentur (bestehend aus **]init[AG, Fraunhofer FOKUS, Christoph Kroschke GmbH, subreport, LABO Berlin, Daimler Benz Berlin, Bundesdruckerei** u. a.) c/o]init[AG	Teilprojekt E-Kfz, Kfz-An-, -Um- und -Abmeldung und andere Geschäftsprozesse im Kfz-Wesen
15	**arvato systems GmbH**	Kommunales Bürgerportal
16	**Ärztekammer Nordrhein**	Heilberufsausweisnutzung (HBA) nach § 291 a SGB V
17	**Atos Worldline Processing GmbH**	Identitätsnachweis bei Kartenzahlungen
18	**AXA Konzern AG**	Authentifizierungsverfahren im Maklerportal/ Extranet der AXA
19	**B+S Banksysteme Aktiengesellschaft**	Online-Banking (Authentifizierung), Kontoeröffnung (Identifikation)
20	**Baltech AG**	Einsatz diverser Kartenlesegeräte zur Nutzung des neuen Personalausweises
21	**Bardenheuer GmbH**	Zutrittskontrolle und Portalzugang
22	**Bayerische Versorgungskammer**	Versicherten- und Mitgliederportal
23*	**Bayerisches Landesamt für Steuern,** Bereich IUK, Verfahrens-Management ELSTER	Registrierungsverfahren mit Personalausweis für die Teilnahme am Verfahren ELSTER (elektronische Steuererklärung) über das ElsterOnline-Portal
24	**bbg Betriebsberatungs GmbH**	Single-Sign-on in der Versicherungswirtschaft
25	**Beschaffungsamt des BMI**	E-Vergabe
26	**BG System Ltd**	Single-Sign-on
27	**Bibliothek der TH (FH) Wildau** (Land Brandenburg)	Bibliotheksbenutzerausweis für externe Nutzer, nicht der TH Wildau angehörige Bibliothekskunden
28	**BIG Gesundheit** – Die Direktkrankenkasse	BIGexclusiv
29	**BillSAFE GmbH**	Rechnungskauf
30*	**bol Behörden Online Systemhaus GmbH**	Diverse Online-Antragsverfahren im Rahmen bereits existierender E-Government-Anwendungen
31	**Boll und Partner Software GmbH**	E-Government-Lösungen
32	**Bonk Consulting GmbH**	ORWELL-DMS-(Direktmarketingserver-) Provider
33*	**Bundesamt für Sicherheit in der Informationstechnik/STORK**	Europäische E-Government-Portale und in Deutschland mein.service-BW
34*	**Bundesdruckerei GmbH**	ID-Provider
35	**Bundesministerium des Innern,** Geschäftsstelle Deutschland-Online	Wissensplattform für den IT-Planungsrat
36	**Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen**	Aufsichtsbehörde für qualifizierte elektronische Signaturen
37	**BÜROTEX GMBH SYSTEMHAUS**	Online-Shop
38	**BV Zahlungssysteme GmbH**	Nutzung des Personalausweises als Log-in beim Online-Banking
39	**CETECOM ICT Services GmbH**	Durchführung von Tests nach BSI TR-03119
40	**Clavid AG**	Internet Identity Provider (OpenID und SAML)
41	**comdirect bank AG**	Kontoeröffnung
42	**communal.cc GmbH**	Wissens- und Kontaktmanagementsystem
43	**CompuGROUP Holding AG**	Elektronische Gesundheitsakten
44	**CONET Solutions GmbH**	Online-Antragsmanagement

45*	**CosmosDirekt**	Authentisierte Willenserklärungen/Mitteilungen
46	**Cybits AG**	Personenidentifikation, Altersverifikation
48	**DAIMLER TSS**	car2go-Benutzeridentifikation und -registrierung
49	**DAKO Unternehmensgruppe**	Mobiles Erfassungsgerät ME3 zur Prüfung und Erfassung von Personaldokumenten
50	**DATA BECKER GmbH & Co KG**	shop to date: Software zur Erstellung von Online-Shops; Nutzung des Verfahrens für den hauseigenen Online-Shop
51*	**Datenzentrale Baden-Württemberg (DZBW)**	Online-Gewerbeanzeige des Kommunalen Gewerbemanagements (KoGeMa)
52*	**DATEV eG**	Online-Zugriff auf Lohn- und Gehaltsabrechnungen
53	**Defense AG**	Informationssicherheit, Content sowie Websecurity, Zugangskontrolle
54*	**Deutsche Emissionshandelsstelle (DEHSt)** im Umweltbundesamt	Antrag auf Zuteilung von Emissionszertifikaten und Emissionsberichterstattung
55*	**Deutsche Kreditbank AG**	Direktbank
56	**Deutsche Post IT Services GmbH**	Rentenantragsverfahren, Anwartschaftsinformationsdienst
57*	**Deutsche Rentenversicherung**	E-Service der Deutschen Rentenversicherung
58	**Deutsches Forschungszentrum für Künstliche Intelligenz GmbH**	Zugriff auf digitale Daten im Internet der Dinge
59	**DFN-Verein**	DFN-PKI
60	**DGN Deutsches Gesundheitsnetz Service GmbH**	Online-Beantragung qualifizierter Signaturen und Anmeldung am Online-Dienst „Deutsches Gesundheitsnetz“
61	**d-Hosting/Institut E-Inclusion**	Erstellung barrierefreier Internetdienste für Menschen mit Behinderung für mehr soziale Teilhabe, Sicherheit und Datenschutz

62	**digitronic computersysteme gmbh**	Internetzugang in Computerpools von Hochschulen
63	**doubleSlash Net-Business GmbH**	Unterstützung der QES- und eID-Funktion in Web-Applikationen und Software-Produkten
64	**Dr. Ing. Wandrei GmbH**	Elektronisches Abfallnachweisverfahren (eANV)
65	**Dr. Thomas Fricke**	Zugangskontrolle für virtuelle Maschinen
66	**D-TRUST GmbH**	Beantragung und Ausgabe von QES-Karten am Online-Registrierungsarbeitsplatz (Online-RA)
67	**Duale Hochschule Baden-Württemberg** Mannheim	Zugangskontrolle für Netzwerke und User Self-Services
68*	**Duisburger Verkehrsgesellschaft AG/Verkehrsverbund Rhein- Ruhr (VRR)**	Customer-Self-Care Terminals (CSC Terminals) und E-Ticketsystem
69	**easy Login GmbH**	Single-Sign-on in der Finanz- und Versicherungswirtschaft
70	**e-data GmbH**	Zutrittskontrolle
71	**ERGO Versicherungsgruppe**	1) Internet-Login, 2) Online-Anfrage für Lebens- und Rentenversicherungen
72	**F1 GmbH in Zusammenarbeit mit der Euronorm GmbH**	Identitätsnachweis unter Nutzung des Personalausweises bei der Anmeldung und Nutzung des Portals PROTON
73	**Fabasoft Distribution GmbH**	Fabasoft Folio Cloud
74	**Fachhochschule Gelsenkirchen,** Institut für Internet-Sicherheit	OpenID-Proxy für die Online-Ausweisfunktion (Verwalter für Internetidentitäten)
75	**Fachhochschule Trier,** Umwelt-Campus Birkenfeld, Institut für Softwaresysteme	Elektronisches Abfallnachweisverfahren
76	**FaxLogic Gesellschaft für Kommunikationslösungen mbH**	Single-Sign-on im Gesundheitswesen und Single-Sign-on im Versicherungswesen
77	**FEIG ELECTRONIC GmbH**	Hersteller/Lieferant für Kartenleser

78	**Fidelity Information Services KORDOBA GmbH**	Kontoeröffnungsverfahren im Online-Banking
79*	**Finanzbehörde Hamburg**	Identitätsnachweis
80	**FlexSecure GmbH**	InSel – Informationelle Selbstbestimmung in Dienstenetzen
81	**Frank Industrie GmbH**	Zugangskontrolle und Zeiterfassung
82	**Fraunhofer Innovationscluster „Sichere Identität“**	Identifizierung mit dem elektronischen neuen Personalausweis für die effiziente Verbundforschung innerhalb der Fraunhofer Gesellschaft
83	**Fraunhofer Institut SIT**	Sicheres VoIP zur Eröffnung eines Bankkontos (nur für Demonstrationszwecke)
84*	**FRITZ & MACZIOL GmbH**	Abwicklung des gesetzlich vorgeschriebenen elektronischen Abfallnachweisverfahrens (eANV)
85	**fr-wlan GmbH**	Verwaltung von lokalen WLAN-Netzwerken
86*	**Fujitsu Technology Solutions**	Online-Shop (Kundenregistrierung, Bereitstellung personalisierter Serviceangebote wie Tracking und beschleunigter Bestellvorgang)
87	**fun communications GmbH**	Kombination von benutzerzentrierten Identitätsverfahren mit dem neuen Personalausweis zur erweiterten Identifikation
88	**FunDorado GmbH**	Altersverifikationssystem
89	**Funk-Sicherungs-Club NRW e. V.**	Überprüfung der Zugangsberechtigung auf Veranstaltungen
90	**GAD eG**	Einsatz des Personalausweises in bankfachlichen Anwendungen
91	**GDV Dienstleistungs-GmbH & Co. KG**	Single-Sign-on für die Deutsche Versicherungswirtschaft
92	**Gemalto GmbH**	Authentisierungs-Gateway
93	**Gerrit Albrecht**	API zur Nutzung der Funktionen des neuen Personalausweises
94*	**Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV)**	Single-Sign-on für ungebundene Vermittler
95*	**Gothaer Allgemeine Versicherung AG**	Antragstellung
96	**GS computerservice**	PC-KLAUS, Gewerbe- und Fundbüro-Software
97	**Gutwirth, Lauterbach u. Liebig GbR**	Online-Shop, Bestellung von Fashion- bzw. Sportprodukten
98	**Haas IT GmbH, Jarosch & Haas Ges. mbH**	E-Ticketing im ÖPNV, Zutrittskontrolle bei Events
99*	**Hagener E-Government-Konsortium,** bestehend aus der **Stadt Hagen,** dem **Hagener Betrieb für Informationstechnologie,** dem **Lehrstuhl für Informationssysteme und Datenbanken der Fernuniversität Hagen** sowie dem **Institut für Kooperative Systeme GmbH** (IKS) der Stadt Hagen	Bestehende kommunale Verwaltungsdienstleistungen aus dem E-Government-Framework Rathaus21
100	**Handwerkskammer Rheinhessen**	One Stop Shop, Gewerbean-, -ab-, -ummeldung, Anmeldung Meisterkurse
101	**Hannoversche Lebensversicherung AG**	Online-Antragsverfahren für Versicherungen
102	**Hasso-Plattner-Institut**	Universitärer Single-Sign-on und Authentisierungsdienst
103	**Hessisches Ministerium des Innern und für Sport**	Online-Antragstellung im Rahmen des Vorhabens zur Einführung von Formularmanagement auf dem Internetportal des Landes Hessen
104	**HID Global GmbH**	Innerbetriebliche Anwendungen
105	**highQ Computersysteme GmbH**	Ticketing für den öffentlichen Personenverkehr (ÖPV)
106	**HITEC-Team GmbH**	Altersverifikation im Internet
107	**HKS Systeme GmbH**	Identifizierung und bargeldlose Nutzung von City-Card-Diensten

108	**HOB GmbH & Co. KG**	HOB RD VPN
109	**Hochschule Coburg**	Hochschulweites Single-Sign-on
110	**Hochschule Darmstadt,** Fachbereich Informatik	eID-Authentifizierung für vertrauliche Voice-over-IP-Telefonate
111	**Hochschule Harz – Netzwerklabor** (netlab)	eCampus - Services und Infrastrukturen für gesicherte und verbindliche elektronische Hochschulverwaltung
112	**HORATIO GmbH Zeit Daten Systeme**	Zeiterfassung und Zutrittskontrolle
113*	**HSH Soft- und Hardware Vertriebs GmbH**	E-Bürgerservice
114*	**HUK24 AG**	Online-Versicherung
115	**Humboldt-Universität zu Berlin,** Institut für Informatik	Einschreibung zum Informatikstudium und Accountverwaltung mit Passwortrecovery
116	**IBM Deutschland GmbH**	eID-Service-Integration in IBM-SSO-Sicherheitslösungen
117	**IBTC**	Software für Bibliotheken
118	**iC Consult GmbH**	Authentisierungsdienste in Unternehmensverzeichnissen
119	**ICT Europe GmbH**	Jugendschutz an Verkaufsautomaten wie z. B. Zigarettenautomaten
120	**IMP Computersysteme AG** in Zusammenarbeit mit dem **Institut für Transfusionsmedizin der Universitätsklinik Köln**	Blutspender-Identifizierung
121	**impuls systems GmbH**	Rechtsgültiger Abschluss von Versicherungen on- und offline
122	**infinity3 GmbH**	SSO für Online-Handel
123	**Ingenieuris GmbH**	Zertifizierungs-/Akkreditierungsstellen nach ISO 9001, Dokumentation sicherheitsrelevanter/-kritischer Daten und Vorgänge in Produktionsbereichen

124	**Innenministerium Mecklenburg-Vorpommern**	Kommunale Online-Dienste im Dienstleistungsportal M-V, Kontaktperson zentraler kommunaler Online-Dienste, Testperson für Pilotierung und technische Abnahmen neuer kommunaler Online-Services im Land M-V, Verfahrensprüfstelle EU-geförderter E-Government-Vorhaben
125	**intarsys consulting GmbH**	Elektronische Patientenakte – Arzt zu Arzt, Arzt zu Patient
126*	**InterCard AG**	Kundenkarte mit Zahlfunktion
127	**intermedi8 GmbH**	Zutrittskontrolle
128	**INTERNET AG**	Online-Bestelldienst
129	**Inveda.net GmbH**	Abschluss von Versicherungen
130	**IT Science Center Rügen gGmbH**	Accessibility-Test des Bürgerclients für blinde und sehbehinderte Menschen
131	**ITSG GmbH**	ELENA – Registratur Fachverfahren (vorbehaltlich des Abschlusses im Gesetzgebungsverfahren)
132	**Kästner Sicherheitstechnik**	Zutrittskontrolle
133	**KKH-Allianz Gesetzliche Krankenversicherung**	Anträge auf Versicherungen
134	**Klinikum Ingolstadt**	Patientenaufnahme, -identifikation
135	**Kommunale Datenverarbeitungszentrale Citkomm,** Iserlohn	E-Government-Portal
136	**Kommunales Rechenzentrum Minden-Ravensberg/Lippe**	Registrierung/Authentifizierung an Portalen für E-Government-Anwendungen
137	**komuna GmbH**	Rathaus-Service-Portal
138	**Landeshauptstadt Stuttgart, Kommunales Rechenzentrum der Region Stuttgart, KIND w. V.**	Einmal registrieren, immer identifizieren (ERII) – Interoperabilität portalübergreifender Identifizierung
139	**Landratsamt Calw**	E-Bürgerdienste (Führerschein online, Online-Kfz-Zulassung, Online-Bauantrag)

140	**Lehrstuhl für eingebettete Sicherheit, Ruhr-Universität Bochum, Horst Görtz Institut für IT-Sicherheit**	Zugangskontrolle und Benutzerauthentifikation
141	**LOTTO Hamburg GmbH**	1) Einmalige Kundenregistrierung/-identifizierung 2) Laufende Authentisierung (offline/online) 3) Personalisierte Serviceangebote (offline/online) 4) Öffentliche elektronische Infrastruktur
142*	**LVM-Versicherungen**	Authentifizierung, Portalzugang, Adressübernahme
143	**MATERNA GmbH Information & Communications**	Unternehmensweites Identitätsmanagement für den Mittelstand
144	**MATESO GmbH**	Zugang zur Software – zu den gespeicherten Daten – nach Identifizierung des Anwenders mittels der Personalausweisdaten
145	**Mazda Motor Europe GmbH**	Nutzung im Rahmen des „Dealer Management System“ MACS
146	**media transfer AG (mtG)**	Altersverifikation im Internet gem. KJM- Anforderungen, Registrierung/Identifizierung bei Portalen
147	**mediaBEAM GmbH**	Stadtnetz – soziales Netzwerk auf Kommunalebene
148	**Mentana-Claimsoft AG**	Sichere Identifizierung für De-Ident und andere Plattformen
149	**Ministerium des Innern des Landes Sachsen-Anhalt**	E-Shop-System Landesverwaltung Sachsen-Anhalt
150	**mps public solutions gmbh**	E-Bürgerdienste, u. a. Online-Wahlscheinantrag, einfache Melderegisterauskunft
151	**Net of Trust an der Universität der Bundeswehr München**	Zugang zu Informationsportalen
152	**NetzWerkPlan GmbH**	Planverwaltung im Projektkommunikationsraum, hier „verbindliche Freigabe von planungsrelevanten Plänen und Dokumenten“
153	**new-in-town GmbH**	Anmeldung bei new-in-town.com

154	**Nokia Siemens Networks GmbH & Co KG**	Mobile Nutzung des neuen Personalausweises
155	**Nordrheinische Ärzteversorgung**	2-Faktor-Authentifizierung mit Personalausweis
156	**novedia finance software ag**	Identifizierung im Online-Banking
157	**NÜRNBERGER Versicherungsgruppe**	Authentifizierung – Registrierung ExtraNet
158	**PCS Systemtechnik GmbH**	Zutrittskontrolle für Gebäude und Räume
159	**petaFuel GmbH**	Prepaid MasterCard
160	**PixelPlanet GmbH**	Software für qualifizierte elektronische Rechnungs-/Dokumentsignatur
161	**PPI AG Informationstechnologie**	Authentifizierung und Autorisierung im Umfeld E-Banking
162	**procilon IT-Logistics GmbH**	Bauantragsverfahren, Registrierungs- und Metadatendienst EU-DLR, Authentifizierung, Kfz-Auskunft
163*	**Provinzial Rheinland AG**	Versicherungsbeantragung
164	**PSS Software & Services GmbH**	Zeiterfassung, Zutrittskontrolle, Personalstammdatenanlage
165	**quattro research GmbH**	Personenidentifikation zum Erfindungsnachweis für Patente
166	**Reiner Kartengeräte GmbH & Co. KG**	Individualshops für Banken, Sparkassen, Trustcenter etc.
167	**RESISTO IT GmbH**	Altersverifikation im Internet
168	**Ricoh International B.V.**	Digitale Kopier- und Druckmaschinen
169	**RISER ID Services GmbH**	RISER ID Check
170	**Rudolf Linsenbarth (NETWORK)**	Portalzugriff
171	**RWSoft Thomas Wegener**	Primus Web: bargeldloses Bezahlsystem für Menschen und Unternehmen

172	**S&N AG**	CETIS Cash Handling: Selbstbedienungslösung zum Einsatz von Bankautomaten in Gerichtskassen
173	**Sagem Monetel GmbH**	Zertifikatseinbringung für ELENA-Verfahren
174	**SAP Deutschland AG & Co. KG**	Integration in SAP Identity Management: sichere Registrierung und Anmeldung an SAP-Systemen für interne und externe Benutzer
175	**Sascha Diebel EK**	Internetidentifikation für Webseiten mit Altersverifikation
176	**Scholz Systemprogrammierung GmbH**	Zugangs- und Alterskontrolle für Gebäude und Automaten
177*	**Schufa Holding AG**	Verbraucher-Online-Portal „meineschufa.de“ und Online-Beantragung von Eigenauskünften
178	**SCM Microsystems GmbH**	Internetbestellservice
179	**Secaron AG**	Authentisierungsdienste/Identifizierungsdienste in Netzwerkinfrastrukturen, generische Anwendungen
180	**SecCommerce Informationssysteme GmbH**	Integration des Personalausweises in Produkte zur elektronischen Authentifizierung und qualifizierten elektronischen Signatur
181	**SECUDE IT Security GmbH**	Authentisierung für EDV-Systeme und Datenverschlüsselung bei Unternehmen
182	**SEIB Software Engineer Information Broker**	Kundenidentifikation für Nutzung der Dienstleistungen
183	**SERVODATA GmbH** und **Sperr e. V. Verein zur Förderung der Sicherheit in der Informationsgesellschaft**	Sperrnotruf 116 116
184*	**Siemens AG, Siemens IT Solutions and Services (SIS)**	Showcase Formularmanagementsystem
185	**signalkontor GmbH**	Passwort-Manager für Windows und den Internet Explorer
186	**SIPATEC Prozessautomations GmbH**	Zutrittskontrollsystem

187*	**SIZ – Informatikzentrum der Sparkassenorganisation GmbH**	Online-Beantragung von qualifizierten elektronischen Signaturen
188	**Softceed GmbH**	Neuer PA in Internetanwendungen: sicheres Registrieren, Anmelden und Lesen von Daten
189	**Sparkasse Jena-Saale-Holzland**	Erfassung von Kundendaten zur Kundenanlage und Legitimationsprüfung bei Geldgeschäften
190	**SSOCircle**	Identity Provider as a Service
191	**Stadt Dortmund**	Virtuelles Rathaus
192	**Stadt Herzogenrath**	Elektronische Formulare
193	**Stadt Köln** – E-Government und Online-Dienste	Authentifizierung an städtischen Dienstleistungen (Portal)
194	**Stadt Münster, citeq**	Verschiedene kommunale Antragsverfahren (Mülltonnenummeldung, Anmeldung zur Musikschule etc.)
195	**Stadt Wolfsburg**	Selbstregistrierung am Portal der Stadt Wolfsburg zur Nutzung von E-Government-Diensten/-Antragsverfahren
196	**Stadtverwaltung Markranstädt**	Einwohnermeldeamt
197	**Stadtverwaltung Wiesbaden,** Informationsmanagement, Online-Rathaus	Beantragung eines Führungszeugnisses mit Personalausweis
198	**Star Finanz – Software Entwicklung und Vertriebs GmbH**	Authentifizierung zur sicheren Benutzeranmeldung
199	**StepOver GmbH**	Handgeschriebene E-Signatur von Anträgen, Verträgen mit automatischer Adressdatenerfassung
200	**Stollmann E+V GmbH**	Kompatibilität und Einsatz der kontaktlosen Funktionen im NFC-Umfeld, u. a. auf Mobiltelefonen
201	**Stuttgarter Lebensversicherung a. G.**	Single-Sign-on

202	**SYNCHRONITY GmbH**	Integration des Personalausweises in E-Government-, E-Commerce- und E-Business-Portale
203	**TeamDrive Systems GmbH**	Virtuelle Server für die sichere Zusammenarbeit und den verschlüsselten Dokumentenaustausch für Unternehmen und Privatpersonen
204	**Technische Universität Darmstadt**	Personalausweis-gestützte Authentisierung mit dem Handy
205	**Telecomputer GmbH**	Fahrzeug-Zulassung (IKOL-KFZ), Fahrerlaubniswesen (IKOL-FS)
206*	**Tönjes Holding AG**	Identitätsnachweis bei Kfz-Online-Zulassungen
207	**TOPiCO Handels-GmbH & Co. KG**	Werbemittelbestellservice
208*	**T-Systems Enterprise Services GmbH** in Kooperation mit **Innenministerium Baden-Württemberg**	EU-DLR/mein.service-bw (Teilbereich des Verwaltungsdiensteportals Baden-Württemberg)
209	**T-Systems International GmbH** (Projekt SiXFORM)	SiXFORM (signierbare XML-Formulare)
210	**ubinova UG (haftungsbeschränkt) & Co. KG**	Event-ID-Management
211	**Universität Bremen**	Strukturierte Sicherheitsuntersuchung der Kommunikationsverbindungen
212	**Universität des Saarlandes,** Lehrstuhl für Sicherheit und Kryptographie, Prof. Dr. Michael Backes	Anonyme Beweistechniken auf der Basis der im digitalen Personalausweis gespeicherten Daten
213	**Universität Koblenz-Landau**	Registrierung von digitalen Signaturzertifikaten
214	**Universität Siegen,** Institut für Digitale Kommunikationssysteme	Zugriffskontrolle
215	**van den Berg Consulting & Service AG**	Bereitstellung der Middleware (eCard-API-Middleware) durch das van den Berg Service Bureau
216	**Vasco Data Security BV**	Authentifizierungsservice
217	**Verlag für Standesamtswesen GmbH**	Online-Urkundenservice
218	**Versicherungswirtschaftlicher Datendienst GmbH**	Authentifizierung
219	**vita-X AG**	Zugangsschlüssel zur elektronischen Gesundheitsakte
220	**Vodafone D2 GmbH**	Auftragsformular für Telekommunikationsverträge
221	**VOICETRUST AG**	Self-Service PIN Reset
222	**Volksbank Euskirchen eG**	Erfassung von Kundendaten zur Kundenanlage und Legitimationsprüfung bei Geldgeschäften
223	**Volkswagen Bank GmbH**	Einsatz Personalausweises in Bankanwendungen
*224	**VZnet Netzwerke Ltd. Berlin**	Soziale Netzwerke schülerVZ, studiVZ und meinVZ
225	**WIBU-SYSTEMS Aktiengesellschaft**	Vertrieb und Lizenzierung von Software, Dokumenten und Medien mit anwenderfreundlichem digitalem Rechtemanagement
*226	**Willi Weber GmbH & Co. KG**	Altersverifikation an Zigarettenautomaten
*227	**Wincor Nixdorf International GmbH**	Nutzung des Personalausweises an Geldautomaten oder an Transaktionsterminals bei Banken, Behörden und Industrie
228	**Wrocklage Intermedia GmbH Aloaha Software**	Software für Smartcards
229	**Württembergische Gemeinde-Versicherung a. G.** und die **WGV-Versicherung AG**	Authentifizierung bei Portalzugang, Antragstellung und Online-Versicherung
230	**Zentraler IT-Betrieb der niedersächsischen Justiz,** Fachverfahrensteam Justizvollzug	Erfassung der Personalausweisdaten
231	**Zurich Versicherung**	Kunden-Selbstservice-Portal

* Mitglieder des Anwenderbeirats für den neuen Personalausweis bei der Bundesbeauftragten für IT.

Anlage 3

Leitlinie für die Vergabe von Berechtigungen für Diensteanbieter

nach § 21 Abs. 2 PAuswG der Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt
Version 1.0 vom 16.11.2010

Inhalt

I. Einleitung

§ 4 Abs. 1 PAuswG lässt die Verwendung des Personalausweises als Ausweis- und Legitimationspapier auch im nichtöffentlichen Bereich ausdrücklich zu. Im Unterschied zur Identifizierung in hoheitlichen Verfahren existiert aber bei der Identifizierung bzw. Autorisierung gegenüber privaten Stellen wie bspw. Wirtschaftsunternehmen keine Ausweispflicht i. S. d. § 1 Abs. 1 PAuswG; es liegt vielmehr in der freien Entscheidung des Personalausweisinhabers, seine Identität dem Diensteanbieter zu offenbaren. Zur technischen und rechtlichen Absicherung dieser Entscheidungsfreiheit ist die gegenseitige Authentisierung von Diensteanbieter und Ausweisinhaber auf ein Verfahren festgelegt, das die berechtigten Interessen beider Parteien berücksichtigt. Dieses Verfahren ist als elektronischer Identitätsnachweis im Personalausweisgesetz ausdrücklich geregelt.

Diensteanbieter erhalten unter den Voraussetzungen von § 21 Abs. 2 PAuswG auf schriftlichen Antrag die Berechtigung, die für die Wahrnehmung ihrer Aufgaben oder Geschäftszwecke erforderlichen Daten im Wege des elektronischen Identitätsnachweises beim Inhaber eines Personalausweises mittels eines Berechtigungszertifikats anzufragen.

Die nachfolgende Darstellung beschreibt das Prüfungsverfahren zur Erlangung einer Berechtigung bei der Vergabestelle für Berechtigungszertifikate. Der Schwerpunkt der Darstellung liegt dabei auf der Erforderlichkeit der zu übermittelnden Daten nach § 21 Abs. 2 Nr. 3 PAuswG.

II. Grundlagen

Diensteanbieter

Diensteanbieter sind natürliche und juristische Personen, die zur Wahrnehmung von Aufgaben der öffentlichen Verwaltung oder zur Erfüllung eigener Geschäftszwecke den Nachweis der Identität oder einzelner Identitätsmerkmale des Ausweisinhabers benötigen (§ 2 Abs. 3 PAuswG). Diensteanbieter treten gegenüber Personalausweisinhabern als Anbieter von Waren oder Dienstleistungen auf. Man unterscheidet Diensteanbieter im E-Government und solche im E-Business.

Zur Durchführung des elektronischen Identitätsnachweises muss sich zunächst der Daten anfragende Diensteanbieter (Behörde oder private Stelle) gegenüber dem Personalausweisinhaber authentisieren und die Berechtigung zum Zugriff auf bestimmte Datenfelder des neuen Personalausweises nachweisen. Dies geschieht auf technischem Wege durch Vorweisen eines Berechtigungszertifikats. Die Daten werden nur übermittelt, wenn der Diensteanbieter ein gültiges Berechtigungszertifikat an den Personalausweisinhaber übermittelt und dieser in der Folge seine Geheimnummer eingibt.

Berechtigung und Berechtigungszertifikat

Ein Berechtigungszertifikat ist eine elektronische Bescheinigung, die es einem Diensteanbieter ermöglicht,

- seine Identität dem Personalausweisinhaber nachzuweisen und
- die Übermittlung personen- und ausweisbezogener Daten aus dem Personalausweis anzufragen (§ 2 Abs. 4 PAuswG).

Berechtigungszertifikate dürfen von (privaten) Berechtigungszertifikateanbietern (§ 1 Abs. 3 PAuswV) ausgestellt werden, wenn der Diensteanbieter eine Berechtigung der Vergabestelle für Berechtigungszertifikate (§ 7 Abs. 4 S. 1 PAuswG) vorlegt. Berechtigungszertifikateanbieter werden auf der Webseite www.personalausweisportal.de veröffentlicht.

Bei der Berechtigung handelt es sich um einen (öffentlich-rechtlichen) Verwaltungsakt, der auf Antrag eines Diensteanbieters erlassen wird und ihn berechtigt, bestimmte Datenkategorien zum angegebenen Zweck aus dem Personalausweis auszulesen.

Vergabestelle für Berechtigungszertifikate

Für die Erteilung und Aufhebung von Berechtigungen ist die Vergabestelle für Berechtigungszertifikate (VfB) beim Bundesverwaltungsamt zuständig (vgl. http://www.personalausweisportal.de/anbieter).

Die Vergabestelle für Berechtigungszertifikate prüft die Voraussetzungen, ob dem Diensteanbieter eine Berechtigung, die für die Wahrnehmung seiner Aufgaben oder Geschäftszwecke erforderlichen Daten beim Inhaber des Personalausweises mittels eines Berechtigungszertifikates anzufragen, erteilt werden kann. Der Prüfmaßstab, ob ein Diensteanbieter berechtigt ist, Ausweisdaten aus dem Personalausweis auszulesen, ergibt sich aus § 21 Abs. 2 Personalausweisgesetz in Verbindung mit konkretisierenden Vorschriften der Personalausweisverordnung.

Datenfelder des elektronischen Identitätsnachweises

Gemäß § 18 Abs. 3 Satz 2 PAuswG können im Rahmen des elektronischen Identitätsnachweises maximal folgende Daten übermittelt werden:

1. Familienname
2. Vornamen
3. Doktorgrad
4. Tag der Geburt
5. Ort der Geburt
6. Anschrift
7. Dokumentenart
8. dienste- und kartenspezifisches Kennzeichen
9. Abkürzung „D“ für Bundesrepublik Deutschland
10. Angabe, ob ein bestimmtes Alter über- oder unterschritten wird
11. Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht
12. Ordensname, Künstlername

Das Sperrmerkmal und die Angabe, ob der Personalausweis gültig ist, sind zur Überprüfung, ob ein gesperrter oder abgelaufener Personalausweis vorliegt, immer zu übermitteln (§ 18 Abs. 3 S. 1 PAuswG). Alle anderen Kategorien müssen für den vom Diensteanbieter angegebenen Zweck der Datenerhebung erforderlich sein.

Die Datenfelder Nr. 1–6 und 12 enthalten in elektronischer Form die Informationen, wie sie auf dem Ausweisdokument aufgedruckt sind. Die Übermittlung der Dokumentenart (Nr. 7) kann erforderlich sein, um den Personalausweis von anderen Dokumenten unterscheiden zu können. So wird in Zukunft z. B. auch der elektronische Aufenthaltstitel mit der Funktion des elektronischen Identitätsnachweises ausgestattet werden. Die Übermittlung der Abkürzung des Landes, das den Personalausweis ausgibt (Nr. 9), kann im Hinblick auf andere Länder erforderlich sein, die einen technisch identischen elektronischen Identitätsnachweis auf eigene Dokumente aufbringen könnten.

Die Angaben zur Über- oder Unterschreitung eines bestimmten Alters (Nr. 10) und zur Bestätigung eines bestimmten Wohnortes (Nr. 11) dienen der datenschutzfreundlichen Ausgestaltung bestimmter Dienste, die über diese Angaben hinaus keine weiteren – insbesondere keine den Ausweisinhaber identifizierenden – Angaben benötigen.

Anforderungen an Datenschutz und Datensicherheit

Der elektronische Identitätsnachweis erfolgt durch Übermittlung von Daten auf elektronischem Weg aus dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises an einen sogenannten eID-Server auf Anbieterseite. Dabei ist konzeptionell sichergestellt, dass die Übertragung aufgrund technischer Vorgaben immer gegen Zugriff durch Dritte gesichert ist.

Die technischen und organisatorischen Anforderungen, die Diensteanbieter zu erfüllen haben, um für die Nutzung von Berechtigungszertifikaten zugelassen zu werden, legt die Vergabestelle für Berechtigungszertifikate gemäß § 29 Abs. 2 S. 2 PAuswV in Richtlinien fest, die im elektronischen Bundesanzeiger und unter www.personalausweisportal.de veröffentlicht werden.

III. Antragsvoraussetzungen

Zur Erlangung einer Berechtigung ist ein Antrag an die Vergabestelle für Berechtigungszertifikate zu richten, der den formalen und inhaltlichen Anforderungen des § 28 PAuswV entspricht.

Antragsformulare mit Erläuterungen finden interessierte Dienstleister unter http://www.personalausweisportal.de/anbieter.

IV. Erteilung und Aufhebungen von Berechtigungen für Diensteanbieter

Die Prüfung des Antrags erfolgt nach den Vorgaben des § 21 PAuswG, wie nachfolgend erläutert:

Rechtmäßigkeit des Abrufzwecks, § 21 Abs. 2 Nr. 1 PAuswG

Der angegebene Zweck der Datenverarbeitung darf nicht rechtswidrig sein, § 21 Abs. 2 Nr. 1 PAuswG. Gemäß § 21 Abs. 1 Satz 1 PAuswG muss es sich dabei entweder um die Wahrnehmung einer (öffentlichen) Aufgabe (öffentliche Diensteanbieter) oder um die Wahrnehmung von Geschäftszwecken (nichtöffentliche Diensteanbieter) handeln. Der Geschäftszweck darf insbesondere nicht darin bestehen, personenbezogene Daten des Ausweisinhabers ohne bestehende Rechtsgrundlage zu erheben und zu verwenden. Rechtsgrundlagen in diesem Sinne sind gesetzliche Regelungen oder wirksame Einwilligungen des Ausweisinhabers nach den §§ 4 und 4a BDSG oder strengeren spezialgesetzlichen Normen z. B. im Telemediengesetz. Geschäftszwecke sind alle Prozesse, die als „Mittel zum Zweck“ zur Erfüllung anderer, außerhalb der Datenverarbeitung liegender Geschäftszwecke dienen.

Geschäftsmäßige Übermittlung von Daten an Dritte, § 21 Abs. 2 Nr. 2 PAuswG

Der Zweck der Datenerhebung darf nicht in der geschäftsmäßigen Übermittlung der Daten bestehen, und es dürfen keine Anhaltspunkte für die geschäftsmäßige oder unberechtigte Übermittlung der Daten vorliegen, § 21 Abs. 2 Nr. 2 PAuswG. Es soll verhindert werden, dass der elektronische Identitätsnachweis als Datenerhebungswerkzeug für Adresspools und andere geschäftsmäßige Datenübermittler verwendet wird und so das Vertrauen der Ausweisinhaber in den elektronischen Identitätsnachweis geschwächt wird, weil dessen Einsatz z. B. mit einer erhöhten Anzahl unverlangt übersandter Werbeschreiben einhergeht oder einen Kontrollverlust über die eigenen Daten mit sich bringt.

Diensteanbieter können allerdings einen elektronischen Dienst für den Ausweisinhaber bereitstellen, in den dieser verifizierte Daten im Wege des elektronischen Identitätsnachweises einstellen und auf bewusster, informierter Basis an Dritte im Netz weiterleiten kann. Voraussetzung dafür, dass hier keine geschäftsmäßige Datenübermittlung vorliegt, ist jedoch, dass der Ausweisinhaber selbst für jede Übermittlung an einen Dritten aktiv eine eigene Freigabe seiner Daten erteilen muss. Diese Freigabe wird regelmäßig die Voraussetzungen des § 13 Telemediengesetz erfüllen müssen.

Die Datenerhebung durch den Diensteanbieter fällt unter die Privilegierung des § 28 Abs. 1 Satz 1 Nr. 1 BDSG, soweit der Diensteanbieter nach seinem Geschäftsmodell bei der Datenerhebung und -speicherung eigene Geschäftszwecke verfolgt und das Verfahren der

Freigabe durch den Betroffenen sichergestellt ist. Im Rahmen der Berechtigungsvergabe wird im Einzelfall geprüft, ob das Verfahren diesen Vorgaben genügt.

Erforderlichkeit der Angaben für den beschriebenen Zweck,
§ 21 Abs. 2 Nr. 3 PAuswG
Grundsätzlich gilt nach allgemeinem Datenschutzrecht das Gebot der Datensparsamkeit. Danach sollen nur so viele personenbezogene Daten verarbeitet werden, wie für die Zweckerreichung unbedingt erforderlich sind (Erforderlichkeitsgrundsatz). Der Diensteanbieter muss die Erforderlichkeit der von ihm beantragten Datenkategorien für seinen konkreten Geschäftszweck nachweisen. Was konkret für einen Zweck erforderlich ist, ist im Einzelfall in einer Abwägung zu bestimmen. Die Abwägung berücksichtigt die konkrete Notwendigkeit eines Datums für den angestrebten (legalen) Zweck sowie die schutzwürdigen Interessen des Personalausweisinhabers.

Der Grundsatz der Erforderlichkeit kommt sowohl im Hinblick auf die Frage, ob ein Identitätsnachweis für den konkreten Zweck überhaupt benötigt wird, als auch hinsichtlich des Umfangs der zu erhebenden Daten zur Anwendung. Insoweit ist für die Erforderlichkeitsprüfung eine Zweckbestimmung auf der Basis einer Gesamtschau der Ausgestaltung des Dienstes und seiner rechtlichen Rahmenbedingungen vorzunehmen.

Ist festgestellt, dass eine Erhebung verifizierter Daten erforderlich ist, ist der Umfang der Daten zu bestimmen. Der Datenumfang wird sich regelmäßig an dem Datenbedarf des gesamten Dienstes orientieren, unabhängig davon, ob in einzelnen Prozessen, z. B. bei Wiederanmeldung mittels karten- und dienstespezifischen Kennzeichens, bei einem Dienst nur Auszüge des Datenbedarfs übermittelt werden müssen. Der Diensteanbieter sollte in den einzelnen Abrufverfahren eines Dienstes nur die tatsächlich verwendeten Daten anfordern (als „ausgewählt“ in der AusweisApp anzeigen lassen), auch wenn das Zertifikat für den gesamten Dienst weiter gehende Anfrageberechtigungen enthält. Davon unabhängig kann nach § 18 Abs. 5 Satz 2 PAuswG der Personalausweisinhaber die Übermittlung einzelner durch die Berechtigung freigegebener Datenkategorien im Einzelfall ausschließen.

Es wird eine Vielzahl von Geschäftsvorfällen geben, bei denen ein Auslesen aller Datenkategorien nach Maßgabe von § 18 Abs. 3 PAuswG für den Diensteanbieter nicht erforderlich ist. Eine gleichwohl verlangte Übermittlung der Daten durch den Diensteanbieter darf nicht durch das Verlangen einer entsprechenden Einwilligung herbeigeführt werden, da damit der Erforderlichkeitsgrundsatz ausgehöhlt würde.

Ein Dienst kann mehrere Geschäftsprozesse in verschiedenen (chronologischen) Stufen umfassen, die charakteristisch für bestimmte Phasen sind, z. B. eine vorgelagerte allgemeine Informationsphase, eine Phase, in der beschränkt zugängliche Informationen nach Abfrage der Legitimation (z. B. des Altersnachweises) bereitgestellt werden, sowie schließlich den Vertragsschluss (z. B. den Produktkauf mit Vorleistung durch den Verkäufer) mit einer umfassenden Identifizierung des Käufers.

Praktische Anwendungsbeispiele

Die Vergabestelle für Berechtigungszertifikate hat in Zusammenarbeit mit Diensteanbietern aus dem koordinierten Anwendungstest und den Beauftragten für den Datenschutz des Bundes und der Länder Anwendungsbeispiele entwickelt, die die „Erforderlichkeit“ im Sinne von § 21 Abs. 2 Nr. 3 PAuswG definieren.

Folgende Fallgestaltungen sind derzeit geprüft:
Use Case 1 **„Allgemeine Informationen“**
Use Case 2 **„Alters- und Wohnortbestätigung“**
Use Case 3 **„Dienste- und kartenspezifisches Kennzeichen (DKK)“**
Use Case 4 **„Wiedererkennbarkeit“**
Use Case 5 **„Anwendungen mit Identifikationsbedarf in der privaten Wirtschaft“**
Use Case 6 **„ID Safe“**
Use Case 7 **„Selbstauskunft“**
Use Case 8 **„Anwendungen mit Identifikationsbedarf in der öffentlichen Verwaltung“**

Use Case 1: „Allgemeine Informationen“

Beabsichtigt der Personalausweisnutzer, außerhalb einer bestehenden Kundenbeziehung allgemein zugängliche Informationen wie etwa einen Online-Warenkatalog oder das Informationsangebot einer öffentlichen Stelle einzusehen, so ist die Nutzung der Daten des elektronischen Identitätsnachweises nicht erforderlich.

Use Case 2: „Alters- und Wohnortbestätigung“, § 18 Abs. 3 Nr. 10 u. 11 PAuswG

Anstelle der Bekanntgabe des Geburtsdatums kann eine „Anfrage“ an den elektronischen Personalausweis gerichtet werden, ob der Ausweisinhaber vor oder nach einem bestimmten Geburtsdatum geboren ist. Insbesondere bei den folgenden Beispielen besteht eine Erforderlichkeit für die Datenübermittlung hinsichtlich der Angabe, ob ein bestimmtes Alter über- oder unterschritten wird:

- Erwerb von Tabakwaren oder Spirituosen an einem Automaten
- Erwerb von Tabakwaren oder Spirituosen im Versand- und Online-Handel
- Online-Zugriff auf Filme und Filmvorschauen mit Altersbeschränkungen (Ü16 und Ü18)
- Inanspruchnahme von altersspezifischen Angeboten

Ob ein Wohnort dem abgefragten Wohnort entspricht, wird anhand des amtlichen Gemeindeschlüssels des Wohnortes verifiziert. Die Abfrage kann dabei auf bestimmte Sequenzen beschränkt werden (Gemeinde, Kreis, Bundesland), so dass der Diensteanbieter die Möglichkeit hat, nur bestimmten Personen seine Leistungen anzubieten.

- Kurtaxe: Die Benutzung von gemeindlichen Einrichtungen oder Strandabschnitten wird in einigen Gemeinden von der Zahlung einer Kurtaxe abhängig gemacht. Personen mit Hauptwohnsitz in der Gemeinde werden nicht zur Zahlung einer Kurtaxe herangezogen. Im Falle einer Automatisierung des Verfahrens könnte die Gemeinde als öffentlicher Diensteanbieter eine Wohnortverifikation vornehmen.

- Bereitstellung nur örtlich lizenzierter Inhalte für die Bürgerinnen und Bürger einer Gemeinde durch die Stadtbibliothek

Use Case 3: „Dienste- und kartenspezifisches Kennzeichen“ (DKK), § 18 Abs. 3 Nr. 8 PAuswG

Zur eindeutigen elektronischen Wiedererkennung eines Personalausweises durch den Diensteanbieter kann ein dienste- und kartenspezifisches Kennzeichen („DKK“) verwendet werden, § 2 Abs. 5 PAuswG.

Insbesondere bei den folgenden Beispielen besteht die Erforderlichkeit für die Datenübermittlung nur für dieses Pseudonym, ohne dass üblicherweise weitere Daten aus dem neuen Personalausweis auszulesen sind:

- Nutzung von Prepaid-Angeboten
- Anmeldung bei „sozialen Netzwerken“ oder sonstigen Telemediendiensten
- Ersatz-Alternativzugang für Username und Passwort bei Diensten

Use Case 4: „Wiedererkennbarkeit“

Hier kann im Rahmen einer bestehenden Kundenbeziehung – aber ohne bestehendes Kundenkonto – ein Zugriff auf die durch den Vertragspartner vorgehaltenen Kundeninformationen mittels Ausweisverifikation ermöglicht werden. Dabei wird davon ausgegangen, dass Familienname, Vorname und Anschrift des Kunden (Ausweisinhaber) dem Dienstanbieter bereits bekannt sind und z. B. im Rahmen der erstmaligen Identifikation ausgelesen werden dürfen. Bei künftigen Zugriffen auf seine durch den Diensteanbieter vorgehaltenen personenbezogenen Daten kann das DKK zum Login genutzt werden. Mit der Übermittlung des DKK soll unter dem Gesichtspunkt der Datensparsamkeit bei jeder weiteren Anmeldung nur ein Datum bereitgestellt werden, das der Wiedererkennung des Ausweisinhabers dient.

Use Case 5: „Anwendungen mit Identifikationsbedarf in der privaten Wirtschaft“ (Online-Shopping, Informationsdienste)

Zahlreiche Geschäftsvorfälle dürften einmalige Austauschgeschäfte in der privaten Wirtschaft betreffen, wie dies beispielsweise im Online- und Versandhandel als Massengeschäft der Fall ist. Neben spezialgesetzlichen Anforderungen an die Identifizierung der Nutzer (z. B. GwG, GewO, JSchG, sonstige rechtlich bindende Vorgaben für den beschriebenen Geschäftszweck des Diensteanbieters) ist der Rückgriff auf verifizierte Daten unter besonderer Abwägung der berechtigten Interessen des Diensteanbieters und der schutzwürdigen Interessen des Personalausweisinhabers zulässig. Dabei ist die Absicherung konkret vorhandener kreditorischer Risiken der Diensteanbieter im Rahmen eines Austauschverhältnisses „Ware/Dienstleistung gegen Geld“ als ein Merkmal für das Vorliegen einer Erforderlichkeit anzusehen.

In diesen Fällen kommt die Nutzung insbesondere folgende Datenfelder in Betracht:
- Familienname
- Vorname
- Anschrift
- Tag und Ort der Geburt (für ggf. erforderliche Einwohnermeldeamtsanfragen zur Ermittlung einer ladungsfähigen Anschrift)

Use Case 6: „ID Safe“

Diensteanbieter können zum Zwecke eines weiter gehenden elektronischen Identitätsmanagements einen „ID Safe“ für den Ausweisinhaber bereitstellen, in den dieser verifizierte Daten im Wege des elektronischen Identitätsnachweises einstellen und auf bewusster, informierter Basis an Dritte im Netz als durch den Dienstleister verifizierte Daten weiterleiten kann. Dabei ist vorzusehen, dass der Ausweisinhaber selbst für jede Übermittlung an einen Dritten aktiv eine eigene Freigabe seiner Daten erteilen muss (Zäsur zwischen elektronischem Identitätsnachweis und benutzerkontrollierter Weiterverwendung). Die Freigabe muss regelmäßig die Voraussetzungen des § 13 Telemediengesetz erfüllen.

Use Case 7: „Selbstauskunft“

§ 34 BDSG bezweckt eine kostenfreie und ohne besondere Erschwernisse zugängliche Auskunft über die bei einer verantwortlichen Stelle verarbeiteten personenbezogenen Daten. Dabei ist der Betroffene zu identifizieren, um eine Bekanntgabe personenbezogener Daten an unberechtigte Dritte auszuschließen. Soll der Nutzer für eine Auskunft nach § 34 BDSG identifiziert werden, sind hierfür in der Regel Name, Vorname, Anschrift und evtl. Geburtsdatum erforderlich. Durch die Wahrnehmung datenschutzrechtlicher Betroffenenrechte sollen Anbieter keine zusätzlichen Daten erlangen. Eine Berechtigung zu diesem Zweck ist daher auf die zur eindeutigen Identifizierung erforderlichen, in der Datenbank des Betreibers enthaltenen Datenfelder zu beschränken. Beispiel: Ein Internetportal für berufliches Networking erhebt von allen Nutzern Vor- und Familiennamen sowie das Geburtsdatum. Dass Nutzer auch freiwillig Anschrift und weitere Daten eingeben können, ist nicht relevant. Übermittelt werden dürfen in diesem Fall die allgemein von allen Nutzern erhobenen Daten.

Use Case 8: „Anwendungen mit Identifikationsbedarf in der öffentlichen Verwaltung“

Eine Nutzung des elektronischen Identitätsnachweises durch die Verwaltung kann erfolgen, wenn eine Rechtsgrundlage für den Zugriff besteht und dies für den konkreten Vorgang erforderlich ist. Ein bloßes Auskunftsersuchen für nicht personenbezogene Daten (Einsicht in Bebauungsplan oder in eine Satzung) rechtfertigt daher ebenso wenig die Erhebung der Identität des Betroffenen wie z. B. eine kostenpflichtige, aber per Vorkasse

bezahlte und an jedermann zu erteilende Auskunft.

Sieht das Verfahren vor, dass sich der Bürger ausweist, darf dies aus datenschutzrechtlicher Sicht mittels des elektronischen Identitätsnachweises erfolgen. Daneben ist eine Identitätsfeststellung auch bei allen Verfahren möglich, die bisher eine Unterschrift des Bürgers erforderten, aber nicht der Schriftform bedürfen. Hier wird die Behörde auch bisher nur tätig, wenn die Identität anhand des Antragstellers geprüft wurde. Art und Umfang der Daten, die mittels Personalausweis erhoben werden dürfen, richten sich danach, welche der Daten im Verwaltungsverfahren benötigt werden.

V. Anforderungen an Datenschutz und Datensicherheit

Die Erteilung der Berechtigung setzt weiterhin voraus, dass die Einhaltung der erforderlichen Maßnahmen zu Datenschutz und Datensicherheit (§ 21 Abs. 2 Nummer 4) erfüllt sind. Der Diensteanbieter gibt in seinem Antrag hierzu eine Erklärung ab, die insbesondere die Existenz eines Datenschutz- und eines Datensicherheitskonzepts für die Systemkomponenten, die Personalausweisdaten verarbeiten, betreffen.

Weiterhin dürfen keine Anhaltspunkte für eine missbräuchliche Verwendung der Berechtigung (§ 21 Abs. 2 Nummer 5) vorliegen. Die möglichen Anhaltspunkte können unterschiedlichster Art sein. Solche Anhaltspunkte können z. B. in früheren Rechtsverstößen des Antragstellers liegen, aber auch ohne bereits nachgewiesene Rechtsverstöße gegeben sein. Die Richtigkeit der die Anhaltspunkte begründenden Tatsachen ist zu überprüfen.

VI. Antragsunterlagen und weitere Informationen

Alle Unterlagen für den Antrag eines Diensteanbieters sind auf www.personalausweisportal.de/anbieter veröffentlicht.

Die Richtlinie gem. § 29 Abs. 2 S. 2 PAuswV zu Art und Umfang der Datenschutz- und Datensicherheitsanforderungen an Systemkomponenten, eine Liste der berechtigten Diensteanbieter und der angezeigten Berechtigungszertifikateanbieter ist auf www.personalausweisportal.de veröffentlicht.

Anhang

Personalausweisgesetz
(Auszug), Stand 01.11.2010

§ 2 Begriffsbestimmungen

(3) Diensteanbieter sind natürliche und juristische Personen, die zur Wahrnehmung von Aufgaben der öffentlichen Verwaltung oder zur Erfüllung eigener Geschäftszwecke den Nachweis der Identität oder einzelner Identitätsmerkmale des Ausweisinhabers benötigen und ihren Wohn-, Geschäfts- oder Dienstsitz innerhalb des Geltungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie in Staaten, in denen ein vergleichbarer Datenschutzstandard besteht, haben.

(4) Ein Berechtigungszertifikat ist eine elektronische Bescheinigung, die es einem Diensteanbieter ermöglicht,

1. seine Identität dem Personalausweisinhaber nachzuweisen und

2. die Übermittlung personen- und ausweisbezogener Daten aus dem Personalausweis anzufragen.

Berechtigte Diensteanbieter erhalten Berechtigungszertifikate. Zur Identitätsfeststellung berechtigte Behörden erhalten hoheitliche Berechtigungszertifikate, die ausschließlich für die hoheitliche Tätigkeit der Identitätsfeststellung zu verwenden sind.

(5) Ein dienste- und kartenspezifisches Kennzeichen ist eine Zeichenfolge, die im Speicher- und Verarbeitungsmedium des Personalausweises berechnet wird. Es dient der eindeutigen elektronischen Wiedererkennung eines Personalausweises durch den Diensteanbieter, für den es errechnet wurde, ohne dass weitere personenbezogene Daten übermittelt werden müssen.

§ 4 Eigentum am Ausweis; Ausweishersteller; Vergabestelle für Berechtigungszertifikate

(3) Das Bundesministerium des Innern bestimmt den Ausweishersteller, die Vergabestelle für Berechtigungszertifikate und den Sperrlistenbetreiber und macht deren Namen im Bundesanzeiger bekannt.

§ 7 Sachliche Zuständigkeit

(4) Für die Erteilung und Aufhebung von Berechtigungen nach § 21 ist die Vergabestelle für Berechtigungszertifikate nach § 4 Abs. 3 zuständig. Für das Führen einer Sperrliste nach § 10 Abs. 4 Satz 1 ist der Sperrlistenbetreiber nach § 4 Abs. 3 zuständig.

(5) Für Diensteanbieter in Deutschland sind die für die Einhaltung der Vorgaben des Datenschutzes zuständigen Stellen zuständig. Haben Diensteanbieter ihren Wohn-, Geschäfts- oder Dienstsitz nicht in Deutschland, so ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständige Datenschutzaufsichtsbehörde im Sinne des § 21 Abs. 5 Satz 3.

§ 18 Elektronischer Identitätsnachweis

(2) Der elektronische Identitätsnachweis erfolgt durch Übermittlung von Daten aus dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises. Dabei sind dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten gewährleisten. Im Falle der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden. Die Nutzung des elektronischen Identitätsnachweises durch eine andere Person als den Personalausweisinhaber ist unzulässig.

(3) Das Sperrmerkmal und die Angabe, ob der Personalausweis gültig ist, sind zur Überprüfung, ob ein gesperrter oder abgelaufener Personalausweis vorliegt, immer zu übermitteln. Folgende weitere Daten können übermittelt werden:

1. Familienname
2. Vornamen
3. Doktorgrad
4. Tag der Geburt
5. Ort der Geburt
6. Anschrift
7. Dokumentenart
8. dienste- und kartenspezifisches Kennzeichen
9. Abkürzung „D“ für Bundesrepublik Deutschland
10. Angabe, ob ein bestimmtes Alter über- oder unterschritten wird
11. Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht, und
12. Ordensname, Künstlername

(4) Die Daten werden nur übermittelt, wenn der Diensteanbieter ein gültiges Berechtigungszertifikat an den Personalausweisinhaber übermittelt und dieser in der Folge seine Geheimnummer eingibt. Vor Eingabe der Geheimnummer durch den Personalausweisinhaber müssen insbesondere die folgenden Angaben aus dem Berechtigungszertifikat zur Anzeige übermittelt werden:

1. Name, Anschrift und E-Mail-Adresse des Diensteanbieters,
2. Kategorien der zu übermittelnden Daten nach Absatz 3 Satz 2,
3. Zweck der Übermittlung,
4. Hinweis auf die für den Diensteanbieter zuständigen Stellen, die die Einhaltung der Vorschriften zum Datenschutz kontrollieren,
5. letzter Tag der Gültigkeitsdauer des Berechtigungszertifikats.

(5) Die Übermittlung ist auf die im Berechtigungszertifikat genannten Datenkategorien beschränkt. Der Personalausweisinhaber kann die Übermittlung auch dieser Datenkategorien im Einzelfall ausschließen.

§ 21 Erteilung und Aufhebung von Berechtigungen für Diensteanbieter

(1) Diensteanbieter erhalten unter den Voraussetzungen des Absatzes 2 auf schriftlichen Antrag die Berechtigung, die für die Wahrnehmung ihrer Aufgaben oder Geschäftszwecke erforderlichen Daten im Wege des elektronischen Identitätsnachweises beim Inhaber des Personalausweises mittels eines Berechtigungszertifikats anzufragen. Die zuständige Stelle nach § 7 Abs. 4 Satz 1 stellt hierzu den Diensteanbietern Berechtigungen gemäß den nachstehenden Bestimmungen aus und stellt den Diensteanbietern entsprechende Berechtigungszertifikate über jederzeit öffentlich erreichbare Kommunikationsverbindungen zur Verfügung. In dem Antrag sind die Daten nach § 18 Abs. 4 Satz 2 Nr. 1 bis 4 anzugeben.

(2) Die Berechtigung nach Absatz 1 ist zu erteilen, wenn

1. der angegebene Zweck nicht rechtswidrig ist,
2. der Zweck nicht in der geschäftsmäßigen Übermittlung der Daten besteht und keine Anhaltspunkte für die geschäftsmäßige oder unberechtigte Übermittlung der Daten vorliegen,
3. der antragstellende Diensteanbieter die Erforderlichkeit der zu übermittelnden Angaben für den beschriebenen Zweck nachgewiesen hat,
4. die Anforderungen, insbesondere an Datenschutz und Datensicherheit, gemäß der Rechtsverordnung nach § 34 Nr. 7 erfüllt sind und
5. keine Anhaltspunkte für eine missbräuchliche Verwendung der Berechtigung vorliegen.

Der Diensteanbieter hat durch Selbstverpflichtung die Anforderungen nach Nummer 4 schriftlich zu bestätigen und auf Anforderung nachzuweisen.

(3) Die Berechtigung ist zu befristen. Die Gültigkeitsdauer darf einen Zeitraum von drei Jahren nicht überschreiten. Die Berechtigung darf nur von dem im Berechtigungszertifikat angegebenen Diensteanbieter und nur zu dem darin vorgesehenen Zweck verwendet werden. Die Berechtigung kann mit Nebenbestimmungen versehen und auf entsprechenden Antrag wiederholt erteilt werden.

(4) Änderungen der Daten und Angaben nach Absatz 1 Satz 3 sind der zuständigen Stelle gemäß § 7 Abs. 4 Satz 1 unverzüglich mitzuteilen.

(5) Die Berechtigung ist zurückzunehmen, wenn der Diensteanbieter diese durch Angaben erwirkt hat, die in wesentlicher Beziehung unrichtig oder unvollständig waren. Sie ist zu widerrufen, wenn sie nicht oder nicht im gleichen Umfang hätte erteilt werden dürfen. Die Berechtigung soll zurückgenommen oder widerrufen werden, wenn die für den Diensteanbieter zuständige Datenschutzaufsichtsbehörde die Rücknahme oder den Widerruf verlangt, weil Tatsachen die Annahme rechtfertigen, dass der Diensteanbieter die aufgrund der Nutzung des Berechtigungszertifikates erhaltenen personenbezogenen Daten in unzulässiger Weise verarbeitet oder nutzt.

(6) Mit Bekanntgabe der Rücknahme oder des Widerrufs der Berechtigung darf der Diensteanbieter vorhandene Berechtigungszertifikate nicht mehr verwenden. Dies gilt nicht, solange und soweit die sofortige Vollziehung (§ 30) ausgesetzt worden ist.

§ 32 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer

6. entgegen § 19 Abs. 1 Nr. 1 oder Nr. 2 erster Halbsatz, Abs. 2, 3 oder Abs. 4 Satz 1 ein Sperrmerkmal, ein Sperrkennwort oder Daten speichert,

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 21 Abs. 1 Satz 3 eine in § 18 Abs. 4 Satz 2 Nr. 1, 3 oder Nr. 4 genannte Angabe nicht richtig macht,
2. entgegen § 21 Abs. 3 Satz 3 eine Berechtigung verwendet,
3. entgegen § 21 Abs. 4 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht oder
4. entgegen § 21 Abs. 6 Satz 1 ein Berechtigungszertifikat verwendet.

(3) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nr. 6, 7 und 8 mit einer Geldbuße bis zu dreihunderttausend Euro, in den Fällen des Absatzes 1 Nr. 5 und des Absatzes 2 Nr. 2, 3 und 5 mit einer Geldbuße bis zu dreißigtausend Euro und in den übrigen Fällen mit einer Geldbuße bis zu fünftausend Euro geahndet werden.

§ 33 Bußgeldbehörden

Verwaltungsbehörden im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten sind, soweit dieses Gesetz von Bundesbehörden ausgeführt wird,

2. in den Fällen des § 32 Abs. 1 Nr. 6 bis 8 der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
4. in den Fällen des § 32 Abs. 2 Nr. 1 bis 4 die Vergabestelle für Berechtigungszertifikate nach § 7 Abs. 4 Satz 1.

§ 34 Verordnungsermächtigung

Das Bundesministerium des Innern wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates und im Benehmen mit dem Auswärtigen Amt

5. Einzelheiten zum elektronischen Identitätsnachweis nach § 18 zu regeln,
7. die Einzelheiten der Vergabe der Berechtigungen und Berechtigungszertifikate festzulegen

Personalausweisverordnung,
(Auszug), Stand 01.11.2010

§ 1 Begriffsbestimmungen

(3) Berechtigungszertifikateanbieter im Sinne dieser Verordnung ist eine natürliche oder juristische Person, die Berechtigungszertifikate im Sinne des § 2 Absatz 4 Satz 1 des Personalausweisgesetzes ausstellt.

§ 28 Antrag

(1) Um das Vorliegen der Voraussetzungen des § 21 Absatz 2 Satz 1 des Personalausweisgesetzes überprüfen zu können, muss ein Antrag nach § 21 Absatz 1 Satz 1 des Personalausweisgesetzes enthalten:

1. Angaben zur Identitätsfeststellung von juristischen und natürlichen Personen; bei natürlichen Personen sind dies insbesondere der Familienname, die Vornamen, der Tag und der Ort der Geburt sowie die Anschrift der Hauptwohnung; bei juristischen Personen sind dies insbesondere der Name, die Anschrift des Sitzes, die Rechtsform und die Bevollmächtigten; außerdem ist in diesem Fall eine Kopie des Handelsregisterauszugs oder der Errichtungsurkunde beizulegen;
2. Kontaktdaten, insbesondere die Telefon- und Faxnummer sowie die E-Mail-Adresse;
3. Angaben zu antragstellenden Personen mit Wohnung oder Sitz außerhalb Deutschlands, soweit zur eindeutigen länderspezifischen Identifizierung erforderlich, einschließlich einer ladungsfähigen Anschrift; soweit eine Niederlassung in Deutschland besteht, sind auch deren Angaben nach den Nummern 1 und 2 aufzunehmen;
4. eine Beschreibung des Diensteanbieters und seiner Tätigkeitsfelder sowie die Angabe der Unternehmenswebsite, soweit vorhanden;
5. eine Beschreibung des Diensteangebots, für das das Berechtigungszertifikat gelten soll, einschließlich einer Angabe der Internetseite, auf der das Berechtigungszertifikat genutzt wird, oder des Standortes bei Automaten und eines Verweises auf die für das Angebot geltende Datenschutzerklärung;
6. eine hinreichende Beschreibung des Zwecks der Datenerhebung, für den die Berechtigung ausgestellt werden soll;
7. eine Angabe der Datenkategorien nach § 18 Absatz 3 des Personalausweisgesetzes, auf die die antragstellende Person zugreifen möchte; hierbei ist für jede Datenkategorie zu begründen, warum es für den dargelegten Zweck erforderlich ist, die Daten zu erheben;
8. Angaben zum oder zur betrieblichen oder behördlichen Datenschutzbeauftragten nach § 4 f des Bundesdatenschutzgesetzes (Name, Anschrift, Telefonnummer, E-Mail-Adresse) und zur zuständigen Datenschutzaufsichtsbehörde (Name, Sitz, Anschrift, Telefonnummer, E-Mail-Adresse);
9. die Angabe, ob die antragstellende Person sich eines Auftragnehmers nach § 11 des Bundesdatenschutzgesetzes zur Durchführung des elektronischen Identitätsnachweises bedienen wird, und gegebenenfalls die Angaben nach Nummer 1 für diesen Auftragnehmer; ist diese Angabe zum Zeitpunkt des Antrages noch nicht bekannt, so ist sie sobald bekannt unverzüglich nachzuliefern.

(2) Der Antrag ist von der antragstellenden Person zu unterschreiben oder mit einer qualifizierten elektronischen Signatur zu versehen. Die antragstellende Person ist zu identifizieren durch:

1. persönliches Erscheinen und Vorlage eines amtlichen Lichtbildausweises der antragstellenden Person, bei juristischen Personen einer vertretungsberechtigten Person bei der Vergabestelle für Berechtigungszertifikate oder geeigneten Dritten,
2. eine qualifizierte elektronische Signatur oder
3. den elektronischen Identitätsnachweis. Die Vergabestelle für Berechtigungszertifikate bestimmt, welche der genannten Arten des Identitätsnachweises genutzt werden können.

§ 29 Anforderungen an Datenschutz und -sicherheit

(1) Anforderungen im Sinne des § 21 Absatz 2 Satz 1 Nummer 4 des Personalausweisgesetzes liegen insbesondere nicht vor, wenn

1. der Zweck der Datenerhebung ausschließlich in der Auslesung oder Bereitstellung personenbezogener Daten aus dem Personalausweis für den Ausweisinhaber oder Dritte besteht,
2. der Staat des Wohnsitzes oder des Sitzes der antragstellenden Person kein angemessenes Datenschutzniveau gewährleistet entsprechend der Richtlinie 95/46/EG des

Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31),
3. der elektronische Identitätsnachweis für den Diensteanbieter durch einen Auftragnehmer nach § 11 des Bundesdatenschutzgesetzes durchgeführt wird und hierbei kein wirksames Auftragsverhältnis nach § 11 des Bundesdatenschutzgesetzes zwischen dem Diensteanbieter und dem Auftragnehmer besteht,
4. der Diensteanbieter einen Auftragnehmer nach § 11 des Bundesdatenschutzgesetzes gewählt hat, der die technischen und organisatorischen Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik für die sichere Bereitstellung des elektronischen Identitätsnachweises nicht erfüllt.

(2) Die Anforderungen an die Datensicherheit im Sinne des § 21 Absatz 2 Satz 1 Nummer 4 des Personalausweisgesetzes sind durch die Diensteanbieter nach dem Stand der Technik zu erfüllen. Art und Umfang der einzusetzenden Systemkomponenten legt die Vergabestelle für Berechtigungszertifikate in der Berechtigung fest. Die Vergabestelle für Berechtigungszertifikate legt in Richtlinien die weiteren technischen und organisatorischen Anforderungen fest, die ein Diensteanbieter zu erfüllen hat, um für die Nutzung von Berechtigungszertifikaten zugelassen zu werden. Die Richtlinien gelten in der jeweils im elektronischen Bundesanzeiger veröffentlichten Fassung.

(3) Vor Erteilung einer Berechtigung für einen nichtöffentlichen Diensteanbieter kann die Vergabestelle für Berechtigungszertifikate eine Stellungnahme der zuständigen Datenschutzaufsichtsbehörde einholen, ob dort Umstände bekannt sind, aus denen sich Anhaltspunkte für eine missbräuchliche Verwendung der Berechtigung ergeben.

§ 30 Öffentliche Liste der Berechtigungen
Die Vergabestelle für Berechtigungszertifikate veröffentlicht eine Liste aller erteilten gültigen Berechtigungen. Dabei sind die Angaben nach § 18 Absatz 4 Satz 2 Nummer 1 bis 4 des Personalausweisgesetzes und die Gültigkeitsdauer der Berechtigung zu veröffentlichen. Die Daten dürfen ausschließlich für Zwecke des elektronischen Identitätsnachweises verwendet werden.

§ 31 Anzeige der Ausgabe von Berechtigungszertifikaten
Berechtigungszertifikateanbieter dürfen Berechtigungszertifikate für den elektronischen Identitätsnachweis bereitstellen, wenn sie vor Aufnahme dieser Tätigkeit
1. der zuständigen Behörde nach § 3 des Signaturgesetzes die Aufnahme des Betriebs eines Zertifizierungsdienstes nach § 4 Absatz 3 des Signaturgesetzes angezeigt haben oder nach § 15 des Signaturgesetzes akkreditiert worden sind,
2. der Vergabestelle für Berechtigungszertifikate die Anzeige nach Nummer 1 vorgelegt und ihr gegenüber die in § 28 Absatz 1 Nummer 1 bis 3, 8 und 9 sowie Absatz 2 aufgeführten Angaben gemacht haben.

§ 32 Beachtung der Anforderungen des Inhabers der Wurzelzertifikate
Das Bundesamt für Sicherheit in der Informationstechnik ist Inhaber der Wurzelzertifikate für Berechtigungszertifikate zum elektronischen Identitätsnachweis. Die Zertifikatsrichtlinien des Bundesamtes für Sicherheit in der Informationstechnik für die technischen und organisatorischen Voraussetzungen für die Ausstellung von Berechtigungszertifikaten sind vom Berechtigungszertifikateanbieter einzuhalten. Die Richtlinien gelten in der jeweils im elektronischen Bundesanzeiger veröffentlichten Fassung.

§ 33 Beachtung der Berechtigung durch den Berechtigungszertifikateanbieter
Vor der Ausgabe von Berechtigungszertifikaten hat der Berechtigungszertifikateanbieter zu überprüfen, ob eine Berechtigung der Vergabestelle für Berechtigungszertifikate vorliegt. Er hat Auflagen, Beschränkungen und Nebenbestimmungen der Berechtigung zu beachten. Bei Zweifeln über den Inhaber, die Gültigkeit oder den Umfang einer Berechtigung hat er vor der Ausstellung von Berechtigungszertifikaten die Vergabestelle für Berechtigungszertifikate zu informieren. Wird ein Berechtigungszertifikat widerrufen oder zurückgenommen, informiert die Vergabestelle für Berechtigungszertifikate den vom Diensteanbieter beauftragten Berechtigungszertifikateanbieter.

§ 34 Gültigkeitsdauer von Berechtigungszertifikaten
Die Vergabestelle für Berechtigungszertifikate legt mit Erteilung der Berechtigung die Gültigkeitsdauer der Berechtigungszertifikate fest. Das Bundesamt für Sicherheit in der Informationstechnik legt angemessene Höchstgrenzen für die Gültigkeitsdauer von Berechtigungszertifikaten fest. Es hat sich dabei am Risiko des Einsatzumfeldes und an den beantragten Datenkategorien zu orientieren.

§ 35 Speicherung, Abrufund Verwendung von Daten durch Berechtigungszertifikateanbieter
(1) Berechtigungszertifikateanbieter sind verpflichtet, sich zur Erzeugung von Listen, die Sperrmerkmale im Sinne des § 2 Absatz 7 des Personalausweisgesetzes enthalten, der jeweils aktuellen Liste der allgemeinen Sperrmerkmale nach § 1 Absatz 4 zu bedienen. Dazu rufen sie regelmäßig die Liste der allgemeinen Sperrmerkmale ab, rechnen die allgemeinen Sperrmerkmale in Sperrmerkmale um und stellen sie für die Diensteanbieter bereit.

(2) Berechtigungszertifikateanbieter dürfen die allgemeinen Sperrlisten, die vom Sperrlistenbetreiber bereitgestellt worden sind, nur bis zum Abruf einer neueren Sperrliste speichern und verwenden.

(3) Die Daten aus der allgemeinen Sperrliste dürfen nur dazu verwendet werden, dienstespezifische Sperrlisten mit Sperrmerkmalen zu erstellen.

Personalausweisgebühren-verordnung, (Auszug), Stand 01.11.2010

§ 3 Gebühren für Berechtigungen
Für Berechtigungen sind folgende Gebühren zu erheben:
1. 102 Euro für die Erteilung einer Berechtigung nach § 21 Absatz 1 Satz 2 des Personalausweisgesetzes,
2. 80 Euro für die Versagung einer Berechtigung,
3. 115 Euro für die Rücknahme oder den Widerruf einer Berechtigung.

Bundesministerium
des Innern

Kompetenzzentrum neuer Personalausweis

Herausgeber:
Bundesministerium des Innern
11014 Berlin

www.personalausweisportal.de
www.ccepa.de

Gestaltung:
Steria Mummert Consulting AG

Bildnachweise:
BMI

Stand:
Dezember 2010

Erstellt in Zusammenarbeit
mit dem

Kompetenzzentrum
neuer Personalausweis,

dem Bundesverwaltungsamt

und dem
Bundesamt für Sicherheit
in der Informationstechnik