



Digitale Identifizierung mit dem deutschen Online-Ausweis

Informationen für Unternehmen und Behörden



Impressum

Herausgeber

Bundesministerium des Innern, für Bau und Heimat
Referat Identifizierungssysteme, Pass- und Ausweiswesen
Alt-Moabit 140, 10557 Berlin
www.personalausweisportal.de

Stand

September 2019

Gestaltung

ORCA Affairs GmbH, Berlin

Bildnachweis

Seite 6: Bundesamt für Sicherheit in der Informationstechnik
Seite 8, 9: Bundesministerium des Innern, für Bau und Heimat

Digitale Identifizierung mit dem deutschen Online-Ausweis

Informationen für Unternehmen und Behörden

Vorwort

Sehr geehrte Damen und Herren,

der Personalausweis im Scheckkartenformat, den inzwischen über 61 Millionen Deutsche erhalten haben, ermöglicht Ihnen die sichere und schnelle Identifizierung von Personen im Internet, an Automaten und am Point of Sale.

Über die gleichen Funktionen verfügen der elektronische Aufenthaltstitel und ab November 2020 auch die eID-Karte für Unionsbürger.

Dieser Leitfaden informiert Sie über die verschiedenen Einsatzmöglichkeiten der Ausweiskarten in Ihren digitalen Geschäftsprozessen. Sie erhalten unter anderem Antworten auf folgende Fragen:

- **Was gibt es Neues** beim elektronischen Identitätsnachweis?
- Über **welche Funktionen** verfügen die Ausweiskarten?
- **Wofür** kann ich diese Funktionen **einsetzen** und **was brauche ich** dazu?
- Wo finde ich **weitere Informationen und Unterstützung**?

Der Leitfaden soll Ihnen einen guten Überblick über den Online-Ausweis bieten.

Detailliertere Informationen erhalten Sie auf www.personalausweisportal.de. Auf dieser Internetseite informiert das Bundesministerium des Innern, für Bau und Heimat (BMI) in den Rubriken „Bürgerinnen und Bürger“, „Wirtschaft“ und „Verwaltung“ aktuell und ausführlich über die elektronischen Funktionen der Ausweiskarten. An vielen Stellen auf den nachfolgenden Seiten wird daher auf die Unterseiten des Personalausweisportals verlinkt und verwiesen.

Für Ihre Fragen steht Ihnen das im BMI für den Online-Ausweis zuständige Fachreferat DG I 2 gern zur Verfügung. Bitte wenden Sie sich bei Bedarf an DG12@bmi.bund.de.

Inhalt

I.	Neues über den elektronischen Identitätsnachweis	6
	A. Erhalt der Berechtigungszertifikate vereinfacht	6
	B. Identifizierungsdienstleistungen für Dritte zugelassen	6
	C. Mobiles Online-Ausweisen möglich	6
	D. Online-Ausweisfunktion stets eingeschaltet	7
	E. Online-Ausweis für ausländische Personen bereitgestellt	7
	F. Vor-Ort-Auslesen eingeführt	7
	G. Qualifizierte elektronische Fernsignatur ermöglicht	7
	H. Auslandsadressen im Personalausweis eingetragen	7
II.	Der Personalausweis im Überblick	8
	A. Die Daten auf dem Chip des Personalausweises	8
	B. Die maschinenlesbare Zone des Personalausweises	9
	C. Fotokopien und Scans	9
III.	Die digitalen Funktionen im Überblick	10
	A. Der Online-Ausweis	10
	B. Das Vor-Ort-Auslesen	10
	C. Die Biometriefunktion	11
IV.	Geeignete Geräte für das mobile Online-Ausweisen	12
V.	Technik beim Online-Ausweisen und Vor-Ort-Auslesen	13
	A. Der technische Ablauf beim Online-Ausweisen	13
	B. Die Komponenten der eID-Infrastruktur	15
	C. Das Vor-Ort-Auslesen: Voraussetzungen und Ablauf	16
	D. Identifizierungsdienstleistungen nutzen	17
	E. Identifizierungsdienstleister werden	17
VI.	Der deutsche Online-Ausweis in Europa	18
VII.	Nutzerkonten mit Online-Ausweis für Bürger und Unternehmen	19
VIII.	Die Online-Signatur	20
	A. Kartenbasierte Signaturen	20
	B. eIDAS-konforme Fernsignaturen	20
	C. Die „On-the-Fly“-Signatur mit dem Online-Ausweis	21
IX.	Informationsquellen und Ansprechpartner	22
	A. Im Internet	22
	B. Broschüren und Leitfäden	22
	C. Beantragung von Berechtigungszertifikaten	23
	D. Testkonzept für die eID-Infrastruktur	23
	E. Pilotprojekt Fernsignaturverfahren	23

I. Neues über den elektronischen Identitätsnachweis

Den Personalausweis im praktischen Scheckkartenformat gibt es seit 1. November 2010, den elektronischen Aufenthaltstitel seit 1. September 2011. Mit beiden Ausweiskarten erhalten ihre Inhaberinnen bzw. Inhaber die Möglichkeit, ihre Online-Ausweisfunktion, d. h. ihren ‚Online-Ausweis‘, zu nutzen.

Im Sommer 2017 wurden wichtige Neuerungen für den Online-Ausweis mit Inkrafttreten des Gesetzes zur Förderung des elektronischen Identitätsnachweises eingeführt. Für Unternehmen und Behörden, die elektronische Dienste mit dem Online-Ausweis anbieten oder künftig anbieten möchten, hat der Gesetzgeber zahlreiche Erleichterungen sowie neue Einsatzmöglichkeiten geschaffen. Zudem konnten die technischen Möglichkeiten des mobilen Online-Ausweises deutlich weiterentwickelt werden.

A. Erhalt der Berechtigungszertifikate vereinfacht

Früher brauchten Sie zum Auslesen der Ausweisdaten stets je ein Berechtigungszertifikat für jeden einzelnen Geschäftszweck. Jetzt können Sie ein Berechtigungszertifikat für mehrere Dienste erhalten.

B. Identifizierungsdienstleistungen für Dritte zugelassen

Noch einfacher wird es für Sie als Anbieter von Online-Diensten, wenn Sie einen Anbieter von Identifizierungsdienstleistungen mit der Identifizierung Ihrer Kundinnen und Kunden beauftragen (siehe Abschnitt V.D).



C. Mobiles Online-Ausweisen möglich

Für Ausweisinhaberinnen und Ausweisinhaber ist die Nutzung des Online-Ausweises deutlich einfacher geworden und auch mobil möglich. Sie können zwischen verschiedenen Softwareangeboten wählen, die ihnen jeweils einen nutzerfreundlichen Identifizierungsclient für stationäre Systeme (Windows, Mac) sowie für Smartphones und Tablets (Android, iOS) zur Verfügung stellen, z. B. die kostenlose AusweisApp2 des Bundes. Immer mehr Smartphones können zudem durch Kopplung per WLAN mit einem stationären System das Kartenlesegerät ersetzen (siehe Kapitel IV.).



Das Angebot an Software und Dienstleistungen für das Online-Ausweisen wächst stetig. Nicht alle Angebote können hier aufgeführt werden.

Auf www.personalausweisportal.de finden Sie aktuelle Informationen über Identifizierungsclients und Identifizierungsdienste.

D. Online-Ausweisfunktion stets eingeschaltet

Personalausweise werden seit Juli 2017 immer mit eingeschalteter Online-Ausweisfunktion ausgegeben. Seitdem steigt der Anteil der eingeschalteten Online-Ausweise jährlich um rund 8 Millionen. Kaum eine andere Chipkarte erreicht eine so hohe Verbreitung in Deutschland.

E. Online-Ausweis für ausländische Personen bereitgestellt

In Deutschland lebende Ausländerinnen und Ausländer, die nicht die Staatsangehörigkeit eines Mitgliedstaats der Europäischen Union besitzen und von den Behörden sicher identifiziert wurden, verfügen mit dem elektronischen Aufenthaltstitel häufig ebenfalls über den Online-Ausweis. Jährlich werden 1,3 Millionen elektronische Aufenthaltstitel ausgegeben.

Ab 1. November 2020 wird zudem eine eID-Karte mit dem Online-Ausweis für Bürgerinnen und Bürger der Europäischen Union sowie der Staaten des Europäischen Wirtschaftsraums ausgegeben.

Aufgrund der EU-weiten Notifizierung der Online-Ausweisfunktion gemäß eIDAS-Verordnung kann diese eID-Karte auch von Bürgerinnen und Bürgern eines EU-Mitgliedstaates genutzt werden, der noch nicht über ein notifiziertes eID-System verfügt. Auf diese Weise setzt die deutsche eID-Funktion neue Maßstäbe im europaweiten Wettbewerb der sicheren eID-Systeme (siehe Kapitel VI.).



Der Online-Ausweis funktioniert bei dem Personalausweis, dem elektronischen Aufenthaltstitel sowie der eID-Karte für Unionsbürger identisch.

Wird der Online-Ausweis im Folgenden erläutert, gelten die Informationen daher für alle drei Chipkarten. Der Personalausweis wird in Kapitel II. ausführlicher vorgestellt.

F. Vor-Ort-Auslesen eingeführt

Neue Nutzungsmöglichkeiten bietet auch das Vor-Ort-Auslesen. Daten aus dem Personalausweis können jetzt vor Ort am Kundenschalter oder an Verkaufsstellen (Point of Sale, PoS) ohne PIN und Unterschrift der Ausweisinhaberin oder des Ausweisinhabers elektronisch und fehlerfrei in das Kassen- oder Hintergrundsystem übernommen werden (siehe Abschnitt III.B).

G. Qualifizierte elektronische Fernsignatur ermöglicht

Bei der neuen Fernsignatur wird eine qualifizierte elektronische Signatur (QES) nicht mehr mit einer Signaturkarte erstellt, sondern im Auftrag der unterzeichnenden Person von einem qualifizierten Vertrauensdiensteanbieter über einen zugelassenen Signatur-Serverdienst (SigS). Der Vorteil des neuen Verfahrens liegt darin, dass keine zusätzliche technische Ausstattung (Signaturkarte, Lesegerät) für das Erstellen einer qualifizierten elektronischen Signatur benötigt wird (siehe Abschnitt VIII.B).

H. Auslandsadressen im Personalausweis eingetragen

Auch deutsche Staatsbürgerinnen und Staatsbürger mit ständigem Wohnsitz im Ausland und ohne Wohnsitz im Inland können künftig die Online-Ausweisfunktion mit ihrer Anschrift nutzen, da anstelle der Angabe „keine Wohnung in Deutschland“ die Wohnadresse im Ausland im Personalausweis eingetragen werden kann.

B. Die maschinenlesbare Zone des Personalausweises

Die maschinenlesbare Zone (englisch: Machine Readable Zone, MRZ) befindet sich im unteren Bereich der Rückseite des Personalausweises. Sie entspricht den Vorgaben der Internationalen Zivilluftfahrt-Organisation (ICAO). Dadurch ist sichergestellt, dass die deutschen Ausweise und Pässe zum Beispiel bei Grenzkontrollen analog zu internationalen Reisepässen maschinell gelesen werden können. Wegen der begrenzt verfügbaren Zeichenzahl werden lange Namen in der MRZ nach festen Regeln gekürzt dargestellt.

Beförderungsunternehmen dürfen personenbezogene Daten aus der maschinenlesbaren Zone des Personalausweises elektronisch nur auslesen und verarbeiten, soweit sie aufgrund internationaler Abkommen oder Einreisebestimmungen zur Mitwirkung an Kontrolltätigkeiten im internationalen Reiseverkehr und zur Übermittlung personenbezogener Daten verpflichtet sind.

C. Fotokopien und Scans

Personalausweise dienen ausschließlich der Identifizierung. Kopien sind nur mit dem Einverständnis der Ausweisinhaberin bzw. des Ausweisinhabers erlaubt.

Sofern das Ausweisdokument im Original vorgelegt wurde und die Identifizierung erfolgte (siehe § 20 Absatz 1 PAuswG), genügt in vielen Fällen

die Anfertigung eines entsprechenden Vermerks, zum Beispiel „Personalausweis hat vorgelegen“. Eine zusätzliche Kopie des Ausweises ist in diesen Fällen grundsätzlich nicht erforderlich.

Der Ausweisinhaberin bzw. dem Ausweisinhaber steht es jedoch frei, Kopien ihres bzw. seines Ausweises anzufertigen. Die Ablichtung muss eindeutig und dauerhaft als Kopie erkennbar sein. Die Weitergabe einer Ausweiskopie ist nur durch die Ausweisinhaberin bzw. den Ausweisinhaber zulässig. Auch die Erhebung und Verarbeitung personenbezogener Daten durch Ablichtung darf nur mit ausdrücklicher Zustimmung der Ausweisinhaberin bzw. des Ausweisinhabers erfolgen.

Mit Zustimmung der Ausweisinhaberin bzw. des Ausweisinhabers kann auch eine andere Person eine Ausweiskopie anfertigen. Die Weitergabe der Ausweiskopie durch die andere Person an Dritte ist nicht zulässig.

Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten sind zu beachten.

Es gibt gesetzlich geregelte Fälle, in den Kopien von Ausweisen erstellt werden dürfen oder müssen, geregelt z. B. in § 8 Absatz 2 Satz 2 des Geldwäschegesetzes (einschließlich der Seriennummer); § 95 Absatz 4 Satz 3 des Telekommunikationsgesetzes oder § 64 Absatz 1 Nummer 2 der Fahrerlaubnisverordnung.

Die MRZ des Personalausweises besteht aus drei Zeilen:



1. Zeile: ID = Personalausweis, D = Ländercode der Bundesrepublik Deutschland, Seriennummer mit Prüfziffer
 2. Zeile: Geburtsdatum mit Prüfziffer, Gültigkeitsdatum mit Prüfziffer, Ländercode, Gesamtprüfziffer
 3. Zeile: Familienname, Vorname(n)
- Leerstellen werden mit „<“ dargestellt

III. Die digitalen Funktionen im Überblick

Der Chip des Personalausweises im Scheckkartenformat ermöglicht die Nutzung von drei digitalen Funktionen, die im Folgenden erläutert werden.

A. Der Online-Ausweis

Die Online-Ausweisfunktion ist der Ausweis für die digitale Welt. Mit ihr weisen sich die Nutzerinnen und Nutzer sicher im Internet oder an Automaten aus und erledigen ihre Behördengänge oder ihre geschäftlichen Angelegenheiten einfach online. Das spart Ihnen sowie Ihren Kundinnen und Kunden Zeit, Kosten und Wege.

Dabei sind die persönlichen Daten der Ausweisinhaberinnen und Ausweisinhaber immer zuverlässig vor Diebstahl und Missbrauch geschützt:

- Vor der Übermittlung der Daten kann die Nutzerin bzw. der Nutzer sehen, welche Behörde oder welches Unternehmen die angezeigten Daten erhält und dass eine staatliche Zulassung (Berechtigung) der Vergabestelle für Berechtigungszertifikate (VfB, <https://www.bva.bund.de>) im Bundesverwaltungsamt für diesen Geschäftszweck vorliegt (gegenseitige Identifizierung).
- Durch Eingabe der persönlichen Geheimnummer (PIN) stimmt die Nutzerin bzw. der Nutzer der digitalen Übermittlung der Ausweisdaten zu. Ohne Besitz der Ausweiskarte und Kenntnis der PIN ist der Online-Ausweis nicht verwendbar (Zwei-Faktor-Authentifizierung). Sollte der Verdacht bestehen, dass die PIN nicht mehr nur der Ausweisinhaberin bzw. dem Ausweisinhaber bekannt ist, sollte diese bzw. dieser die PIN unverzüglich ändern.
- Die Ausweisdaten werden vom Chip des Ausweises bis zum eID-Server des Diensteanbieters ausschließlich Ende-zu-Ende-verschlüsselt übermittelt.

Details über die Sicherheitsmechanismen für den Schutz der Daten finden Sie auf <https://www.personalausweisportal.de/sicherheit>

Eine Übersicht über die Elemente der eID-Infrastruktur finden Sie in siehe Abschnitt V.B

B. Das Vor-Ort-Auslesen

Das Vor-Ort-Auslesen bezeichnet die medienbruchfreie Übernahme von Ausweisdaten in ein elektronisches Formular. Die Identifizierung erfolgt vorher per Lichtbild- und Personendatenabgleich von der Ausweiskarte vor Ort durch eine Mitarbeiterin oder einen Mitarbeiter des Dienstleisters. Anstelle der PIN wird die Zugangsnummer (englisch: Card Access Number, CAN) verwendet, die auf der Vorderseite des Ausweises aufgedruckt ist.

Überall dort, wo Personendaten wie Name und Adresse fehlerfrei in ein Formular übernommen werden sollen, bietet sich ein Vor-Ort-Auslesen an. Insbesondere ist das Vor-Ort-Auslesen für die in der Kreditwirtschaft gemäß Abgabenordnung und Geldwäschegesetz notwendige Legitimationsprüfung natürlicher Personen in deren Filialen geeignet sowie für die Identitätsprüfung beim Erwerb von Prepaid-SIM-Karten bzw. bei Abschluss von Mobilfunkverträgen nach Telekommunikationsgesetz.

Die technischen Details des Vor-Ort-Auslesens und der Ablauf vor Ort werden in Abschnitt V.C erklärt.

C. Die Biometriefunktion

Die Biometriefunktion dient der hohen Bindung der Ausweiskarte an ihre Inhaberin bzw. ihren Inhaber und ermöglicht anhand der auf dem Chip gespeicherten biometrischen Daten die sichere Zuordnung des Ausweisdokuments zu der Person, die sich damit ausweisen möchte.

Als biometrisches Merkmal wird beim Personalausweis derzeit das Lichtbild verwendet. Zusätzlich können zwei Fingerabdrücke der Ausweis-

inhaberin bzw. des Ausweisinhabers gespeichert werden. Voraussichtlich ab Mitte 2021 sind aufgrund einer EU-Verordnung die Fingerabdrücke verpflichtend in den Personalausweis aufzunehmen, wie dies beim elektronischen Aufenthaltstitel bereits der Fall ist.

Die Biometriefunktion kommt ausschließlich bei hoheitlichen Personenkontrollen an Grenzen oder im Inland zum Einsatz. Diensteanbieter können darauf nicht zugreifen.

IV. Geeignete Geräte für das mobile Online-Ausweisen

Immer mehr Smartphones oder Tablets sind in der Lage, den Online-Ausweis auszulesen. Geeignete Geräte können

- mobil für das Online-Ausweisen genutzt werden (ohne Kartenlesegerät) oder
- als Kartenlesegerät im gleichen WLAN mit einem stationären System (Windows, Mac) gekoppelt werden.

Smartphones und Tablets mit den Betriebssystemen Android (ab Version 5.0) oder iOS (ab Version 13.1) eignen sich unter folgenden Voraussetzungen für das mobile Online-Ausweisen:

- Das Modell ist mit einem Chip ausgestattet, der die Technologie „Near Field Communication“ (NFC) unterstützt.
- Der eingebaute NFC-Chip und die Software des Geräteherstellers für diesen NFC-Chip unterstützen den vom Chip des Personalausweises benötigten Kommunikationsstandard (Extended Length gemäß ISO 14449).

- Für eine stabile Verbindung während der Datenübertragung muss der im mobilen Endgerät eingebaute NFC-Chip über eine ausreichende Feldstärke verfügen.
- Eine App für die Online-Ausweisfunktion muss auf dem mobilen Endgerät installiert sein, z. B. die AusweisApp2 des Bundes.



Die Anbieter der Apps für den Online-Ausweis informieren auf ihren Internetseiten sowie in den Apps über erfolgreich mit der Online-Ausweisfunktion getestete Smartphones und Tablets.

Da die Gerätehersteller kontinuierlich Updates für die Software des in ihren Geräten eingebauten NFC-Chips bereitstellen, kann der Online-Ausweis nach einem Update häufig auch mit Modellen genutzt werden, mit denen das vorher nicht ging.

Online-Ausweisen wird immer mobiler und einfacher

heute

Online-Ausweisen mit dem Personalausweis am Smartphone (Android oder iOS)



Smartphone ersetzt den NFC-Kartenleser am PC oder MAC



Smartphone ersetzt den NFC-Kartenleser am Tablet-PC ohne NFC-Schnittstelle

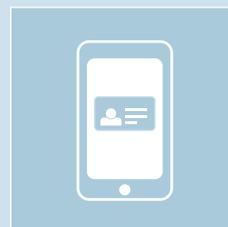


Smartphone als Webclient mit NFC-Schnittstelle



morgen

Online-Ausweisen mit dem Smartphone

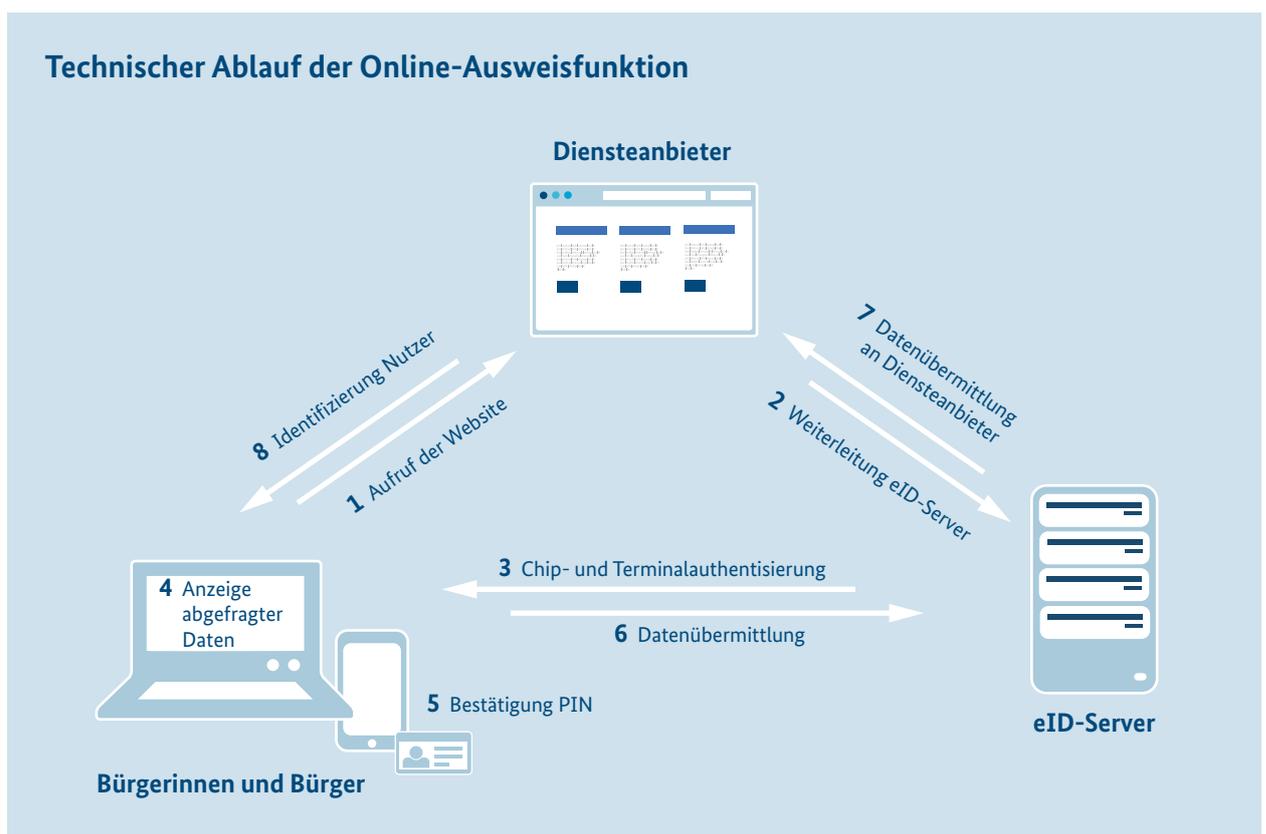


Smartphone wird zum Online-Ausweis

V. Technik beim Online-Ausweisen und Vor-Ort-Auslesen

In diesem Kapitel finden Sie technische Details über das Online-Ausweisen und das Vor-Ort-Auslesen.

A. Der technische Ablauf beim Online-Ausweisen

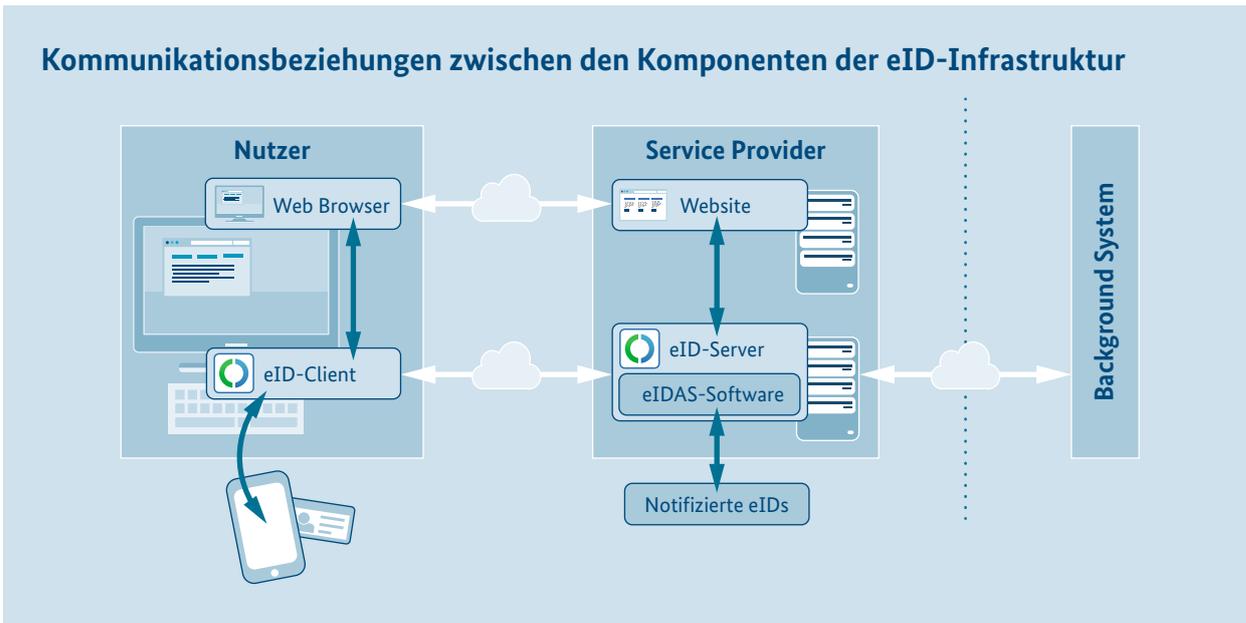


Die Authentisierung am Beispiel eines Online-Dienstes

- 1 Die Ausweisinhaberin bzw. der Ausweisinhaber ruft den Online-Dienst des Diensteanbieters auf, der eine Online-Identifizierung benötigt.
- 2 Der Dienst leitet eine Identifizierungsanfrage an den eID-Server weiter.
- 3 Zwischen dem eID-Server sowie dem Identifizierungsclient (bzw. dem Kartenlesegerät oder mobilen Endgerät und dem Chip des Ausweises) wird ein sicherer Kanal aufgebaut. Die Authentizität des Diensteanbieters sowie die Authentizität und Integrität (Fälschungssicherheit) des Ausweises werden geprüft. Zugleich erfolgt ein Abgleich des Online-Ausweises mit der Liste der gesperrten Ausweise im eID-Server (Sperrliste). Dadurch wird sichergestellt, dass kein Ausweis mit gesperrter Online-Ausweisfunktion verwendet wird.
- 4 Wenn gewünscht, kann sich die Nutzerin bzw. der Nutzer das Berechtigungszertifikat des Diensteanbieters und die angefragten Ausweisdatenkategorien im Identifizierungsclient anzeigen lassen.
- 5 Durch Eingabe der PIN stimmt die Ausweisinhaberin bzw. der Ausweisinhaber der Übermittlung der angefragten Ausweisdaten zu.
- 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 Ergebnisse und entscheidet, ob die Identifizierung erfolgreich war. Abschließend erfolgt eine Ergebnisantwort an die Nutzerin bzw. den Nutzer.

Weitere Informationen über den technischen Ablauf der Online-Ausweisfunktion sowie die benötigten Infrastrukturkomponenten finden

- Unternehmen auf https://www.personalausweisportal.de/Wirtschaft_Technik
- und Behörden auf https://www.personalausweisportal.de/Verwaltung_Technik



B. Die Komponenten der eID-Infrastruktur

Die eID-Infrastruktur ist die für eine sichere elektronische Identifizierung notwendige Infrastruktur, die bei den Ausweisinhaberinnen und Ausweisinhabern sowie dem Serviceprovider (Dienstanbieter, eID-Serviceprovider, Identifizierungsdienstleister) vorhanden sein muss.

Die Nutzerumgebung besteht aus einem Computer oder einem mobilen Endgerät, der eID-Client-Software und einem für die physische Kommunikation mit dem Chip auf der Ausweis-karte geeigneten Gerät (Kartenlesegerät oder Smartphone).

Die eID-Client-Software koordiniert den Identifizierungsvorgang in der Nutzerumgebung zwischen dem Online-Ausweis, der Ausweisinhaberin bzw. dem Ausweisinhaber und dem Serviceprovider.

Als Dienstanbieter benötigen Sie für die Identifizierung mit der Online-Ausweisfunktion einen eID-Server, den sie entweder selbst einrichten oder betreiben lassen. Dieser Server kommuniziert mit Ihrer Anwendung, der eID-Client-Software der Ausweisinhaberin bzw. des Ausweisinhabers und dem Hintergrundsystem.

Für den Zugang zu Online-Diensten der Verwaltung mit notifizierten Identifizierungsmitteln anderer EU-Staaten gleichwertig zum deutschen Online-Ausweis ist der eID-Server um die eIDAS-Software erweitert.

Das Hintergrundsystem besteht in Verlängerung des eID-Servers aus der Public-Key-Infrastruktur (Zugriffsschlüssel für die eID) und den Sperrlisten für verlorene oder gestohlene und daher gesperrte Personalausweise.

Die mit der Online-Ausweisfunktion eingeführte sichere Datenübertragung und die gegenseitige Authentisierung zwischen dem Chip des Ausweises und der auslesenden Gegenstelle werden auch beim Vor-Ort-Auslesen verwendet.

Zum Testen der verschiedenen Komponenten vor Übernahme in das Wirksystem steht Herstellern und Anwendern der eID-Infrastruktur ein Testkonzept zur Verfügung, mit dem primär die Interoperabilität der Komponenten in der eID-Infrastruktur sichergestellt werden soll: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/Testkonzept_eID-Infrastruktur.pdf?blob=publicationFile&v=4

C. Das Vor-Ort-Auslesen: Voraussetzungen und Ablauf

Ihre Kundinnen und Kunden benötigen für das Vor-Ort-Auslesen nur ihren Personalausweis. Ihre PIN müssen sie nicht kennen, da zum Auslesen der Ausweisdaten die Zugangsnummer (englisch: Card Access Number, CAN) des Ausweises erfasst wird. Die CAN steht auf der Vorderseite des Personalausweises rechts neben dem Gültigkeitsdatum.

Die Technische Richtlinie TR-03128 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gibt Vor-Ort-Anbietern IT-Sicherheitsempfehlungen sowie einen Überblick über die rechtlichen und technischen Voraussetzungen für das Vor-Ort-Auslesen: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03128/TR-03128_node.html.



Für das Vor-Ort-Auslesen benötigen Sie:

- eine Berechtigung der Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt sowie ein technisches Berechtigungszertifikat,
- eine geeignete Software für die Datenübernahme (z. B. das integrierbare Software Development Kit (SDK) für die AusweisApp2 oder Authada onsite),
- einen eID-Server oder einen eID-Service und
- ein Kartenlesegerät für den Personalausweis oder ein NFC-fähiges Mobilgerät (Android, iOS).

Vor-Ort-Auslesen in fünf schnellen Schritten

1

Ihr Personal fragt die Kundin bzw. den Kunden nach ihrem bzw. seinem Personalausweis, führt den Lichtbildabgleich zur Identifizierung durch und bittet um ihr bzw. sein Einverständnis zur Datenübernahme.



2

Ihr Personal öffnet den Identifizierungsclient und verbindet die Ausweiskarte mit dem Kartenlesegerät oder dem mobilen Endgerät.



3

Die Zugangsnummer (CAN) wird erfasst.

4

Die Datenübertragung an den eID-Server erfolgt.



5

Die Daten werden fehlerfrei an das Formular und Ihr System übergeben.



D. Identifizierungsdienstleistungen nutzen

Die Anbieter von Identifizierungslösungen bieten Ihnen Dienste an, die von der Vergabestelle für Berechtigungszertifikate (VfB) zugelassen wurden und die Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) einhalten.

Zu den ersten Identifizierungslösungen auf diesem noch neuen Markt zählt z. B. der Dienst AusweisIDent von Bundesdruckerei und Governikus.

Für die Nutzung von Identifizierungsdienstleistungen stehen Ihnen zwei Wege zur Verfügung:

- Der Identifizierungsdienst wird direkt in Ihr Online-Angebot integriert, sodass sich Ihre Kundinnen und Kunden scheinbar gegenüber Ihrem Online-Angebot identifizieren und Ihr Identifizierungsdienstleister nur anhand des Berechtigungszertifikats erkennbar ist.
- Ihre Kundinnen und Kunden werden für das Online-Ausweisen auf die Internetseite Ihres Identifizierungsdienstleisters weitergeleitet und kehren nach der Identifizierung wieder zu Ihrer Internetpräsenz zurück.

In beiden Fällen benötigen Sie keine eigene eID-Infrastruktur für das Online-Ausweisen.

Durch den schnellen und komfortablen elektronischen Identifizierungsdienst können Sie die Abbruchquote verringern und mit Ihren Kundinnen und Kunden einfach online rechtssichere Geschäfte vereinbaren sowie Verträge abschließen.

Weitere Informationen über Anbieter von Identifizierungslösungen finden

- Unternehmen auf https://www.personalausweisportal.de/Wirtschaft_Anwendungsbeispiele_identifizierungsloesungen
- und Behörden auf https://www.personalausweisportal.de/Verwaltung_Anwendungsbeispiele_identifizierungsloesungen

E. Identifizierungsdienstleister werden

Als Identifizierungsdienstleister bieten Sie einzel-fallbezogene Identifizierungsdienstleistungen für Dritte mithilfe des Online-Ausweises an (siehe § 2 Abs. 3a PAuswG, <https://www.gesetze-im-internet.de/pauswg/2.html>). Die planmäßig wiederholt vorgenommene Identifizierung für ein- und denselben Auftraggeber, wie es beispielsweise im Rahmen eines Login- bzw. Account-Managements der Fall ist, ist davon ausgenommen.

Auf https://www.personalausweisportal.de/Wirtschaft_identifizierungsdiensteanbieter_werden erfahren Sie, wie Sie Identifizierungsdienstleister werden können.

VI. Der deutsche Online-Ausweis in Europa

Mit der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910>) gelten in allen Mitgliedstaaten einheitliche, rechtliche Rahmenbedingungen für die grenzüberschreitende Nutzung elektronischer Identifizierungsmittel und Vertrauensdienste.

Die EU-Verordnung sieht vor, dass die grenzüberschreitende Identifizierung auf Basis der gegenseitigen Anerkennung der elektronischen Identifizierungsmittel der Mitgliedstaaten erfolgt. Der deutsche Online-Ausweis wurde 2017 von den Mitgliedstaaten der EU anerkannt. Die Notifizierung erfolgte für das Vertrauensniveau „hoch“

Mit ihrem Online-Ausweis können sich deutsche Bürgerinnen und Bürger dadurch künftig im EU-Ausland online z. B. an Hochschulen ein-

schreiben, ihr Gewerbe anmelden, Steuererklärungen abgeben oder Kfz-Zulassungen beantragen.

Deutsche Behörden müssen ab September 2019 Bürgerinnen, Bürgern und Unternehmen anderer EU-Staaten die Möglichkeit geben, sich mit den von ihren Heimatstaaten bereitgestellten und notifizierten elektronischen Identifizierungsmitteln einfach und sicher gegenüber deutschen Verwaltungsdienstleistungen identifizieren zu können.

Detaillierte Informationen über die eIDAS-Verordnung und die erforderlichen Schritte zu deren Umsetzung finden Sie auf <https://www.personalausweisportal.de/eIDAS-Verordnung>.

Dort ist u. a. ein Leitfaden für Behörden veröffentlicht. Er enthält Informationen über die Anbindung an die eIDAS-Infrastruktur sowie über erforderliche Anpassungen für Online-Dienste.

Checkliste zur Überprüfung einer Anwendung

	Aufgabe	erledigt
1	Klärung: Ab wann steht der eID-Server/-Service mit erweitertem eIDAS-Funktionsumfang zur Verfügung.	<input type="checkbox"/>
2	Anwendung mehrsprachig zur Verfügung stellen (empfohlen: mindestens Deutsch und Englisch).	<input type="checkbox"/>
3	Festlegung Vertrauensniveau	<input type="checkbox"/>
4	Klärung: Umgang mit fehlenden Daten.	<input type="checkbox"/>
5	Klärung: Umgang mit zusätzlichen Daten.	<input type="checkbox"/>
6	Klärung: Länderauswahl (serverseitig oder in der Anwendung).	<input type="checkbox"/>
7	Test und Wirksystem beschaffen/beauftragen.	<input type="checkbox"/>
8	Zeichensatz für Übermittlungen der Daten klären (UTF-8)-	<input type="checkbox"/>

Diese eIDAS-Checkliste finden Sie auf https://www.personalausweisportal.de/Leitfaden_eIDAS_Verordnung.

VII. Nutzerkonten mit Online-Ausweis für Bürger und Unternehmen

Viele Kommunen, Länder und Bundesbehörden bieten ihre Verwaltungsleistungen online auf Serviceportalen an. Diese Angebote werden auf der Grundlage des im Sommer 2017 in Kraft getretenen „Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen“ (Onlinezugangsgesetz – OZG, <https://www.gesetze-im-internet.de/ozg/OZG.pdf>) flächendeckend in Deutschland ausgebaut. Das OZG verpflichtet Bund und Länder, alle rechtlich und tatsächlich geeigneten Verwaltungsleistungen bis 2022 auch online auf ihren Verwaltungsportalen anzubieten und ihre Portale zu einem Portalverbund zu verknüpfen.

Bürgerinnen, Bürger und Unternehmen können künftig die von ihnen gewünschte Verwaltungsleistung einfach online finden – unabhängig von Kenntnissen der föderalen Verwaltungsstruktur Deutschlands und des Verwaltungsportals, auf dem sie „einsteigen“. Sie erhalten die benötigten Informationen schnell und haben die Möglichkeit, die Leistung direkt und sicher zu nutzen. Da hierfür in der Regel eine Identifizierung notwendig ist,

sieht das OZG das Angebot persönlicher Nutzerkonten auf den Verwaltungsportalen vor, die den Nutzerkonten im Online-Handel ähneln.

Als Identifizierungsmittel bei Verwaltungsleistungen, die ein besonders hohes Maß an Sicherheit und Vertrauenswürdigkeit erfordern, ist der Online-Ausweis vorgeschrieben. Ein Beispiel ist die internetbasierte Fahrzeugzulassung (i-Kfz) auf den Portalen der Zulassungsbehörden. Die Identifizierung des Halters erfolgt hierbei stets mit dem Online-Ausweis. Seit 1. Oktober 2019 ist es möglich, den Online-Ausweis für alle Standardzulassungsvorgänge von Kfz im Internet zu nutzen.

Für die Identifizierung auf einem weniger hohen Sicherheitsniveau ist die Einführung eines aus dem Online-Ausweis abgeleiteten und mit Sicherheitselementen geschützten Identifizierungsmittels für das Smartphone geplant.

VIII. Die Online-Signatur

Elektronische Signaturen dienen dazu, Dokumente elektronisch rechtsverbindlich zu unterzeichnen. Zusätzlich lassen sie erkennen, ob Dokumente nach dem Signieren verändert wurden. Die Unterzeichnenden nutzen die elektronische Signatur also zur Abgabe einer rechtsverbindlichen Willenserklärung.

Der Personalausweis ist für die Nutzung der digitalen Unterschrift vorbereitet. Mit der qualifizierten elektronischen Signatur (QES) kommt eine sehr sichere Form zum Einsatz, die zudem der persönlichen, eigenhändigen Unterschrift rechtlich gleichgestellt ist (Schriftformersatz).



Unterschied zwischen qualifizierter elektronischer Signatur und Online-Ausweis

Die **qualifizierte elektronische Signatur (QES)** dient dazu, ein Dokument rechtsverbindlich zu unterzeichnen – im Sinne von „Das habe ich geschrieben“ bzw. „Das **will** ich“.

Der **Online-Ausweis (eID)** ermöglicht den sicheren und eindeutigen Identitätsnachweis im Internet – im Sinne von „Das **bin** ich“.

Mit der Umsetzung der eIDAS-Verordnung entfaltet eine qualifizierte elektronische Signatur, die von der Bürgerin bzw. dem Bürger eines EU-Mitgliedstaats erstellt wird, in allen Mitgliedstaaten die gleiche Rechtswirkung wie eine handschriftliche Unterschrift in dem betreffenden Staat. Erstmals ist daher eine europaweite, grenzüberschreitende elektronische Kommunikation in rechtsverbindlicher Form möglich.

A. Kartenbasierte Signaturen

Bisher basiert die technische Umsetzung der QES auf dem Einsatz von Signaturkarten. Hierbei wird die Sicherheit durch die Signaturkarte sowie eine Zwei-Faktor-Authentifizierung bei der Signaturerstellung realisiert. Der private Schlüssel auf der Signaturkarte ist vor unbefugten Zugriffen geschützt und seine Verwendung ist nur in Verbindung mit den Authentifizierungsfaktoren Wissen (PIN) und Besitz (Signaturkarte) möglich. Diese QES mit dem Personalausweis hat sich jedoch nicht durchgesetzt.

B. eIDAS-konforme Fernsignaturen

Im Sommer 2017 wurde das deutsche Signaturgesetz vom Vertrauensdienstegesetz (VDG, <http://www.gesetze-im-internet.de/vdg/VDG.pdf>) abgelöst. Das VDG ist das deutsche Durchführungsgesetz zur europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910>). Mit dem VDG ist erstmals die qualifizierte elektronische Fernsignatur (QES) in Deutschland möglich.

Bei der Fernsignatur wird eine qualifizierte elektronische Signatur von einem staatlich zugelassenen Vertrauensdiensteanbieter im Auftrag der unterzeichnenden Person über einen zugelassenen Signatur-Serverdienst erstellt. Das neue Verfahren erfordert keine zusätzliche technische Ausstattung (Signaturkarte, Lesegerät). Die unterzeichnende Person muss dafür zuvor ihre Identität gegenüber dem Vertrauensdiensteanbieter sicher nachgewiesen haben. Dafür ist der Online-Ausweis am besten geeignet.

C. Die „On-the-Fly“-Signatur mit dem Online-Ausweis

Bisherige Signaturverfahren trennen die Vorgänge der ‚Identifizierung‘ (zum Erhalt des Signaturzertifikates) und der ‚Authentisierung‘ (Auslösung der Signatur) in separate Schritte.

Mit dem Online-Ausweis können **beide Vorgänge** künftig **in einem Schritt** zusammengefasst werden. Mit dieser „On-The-Fly“-Signatur kann die unterzeichnende Person ohne vorherige Registrierung bei einem Vertrauensdiensteanbieter anlassbezogen und ad hoc eine qualifizierte elektronische Signatur erstellen. Dieses „1-Schritt-Verfahren“ ist vor allem für Personen attraktiv, die nur gelegentlich elektronische Signaturen erstellen möchten.

Das Verfahren erfüllt alle Anforderungen an qualifizierte elektronische Signaturen gemäß eIDAS-Verordnung sowie alle Anforderungen an den Vertrauensdiensteanbieter gemäß Vertrauensdienstegesetz.

Informationen über die eIDAS-konforme Fernsignatur finden Sie auf https://www.personalausweisportal.de/Wirtschaft_eidas_konforme_fernsignatur.

Auch für die Fernsignatur mit dem Online-Ausweis kann ein geeignetes Smartphone oder Tablet verwendet werden (siehe Kapitel IV.). Dadurch wird die rechtsgültige elektronische Unterschrift erstmals mit dem Mobiltelefon möglich (mobile Signatur).

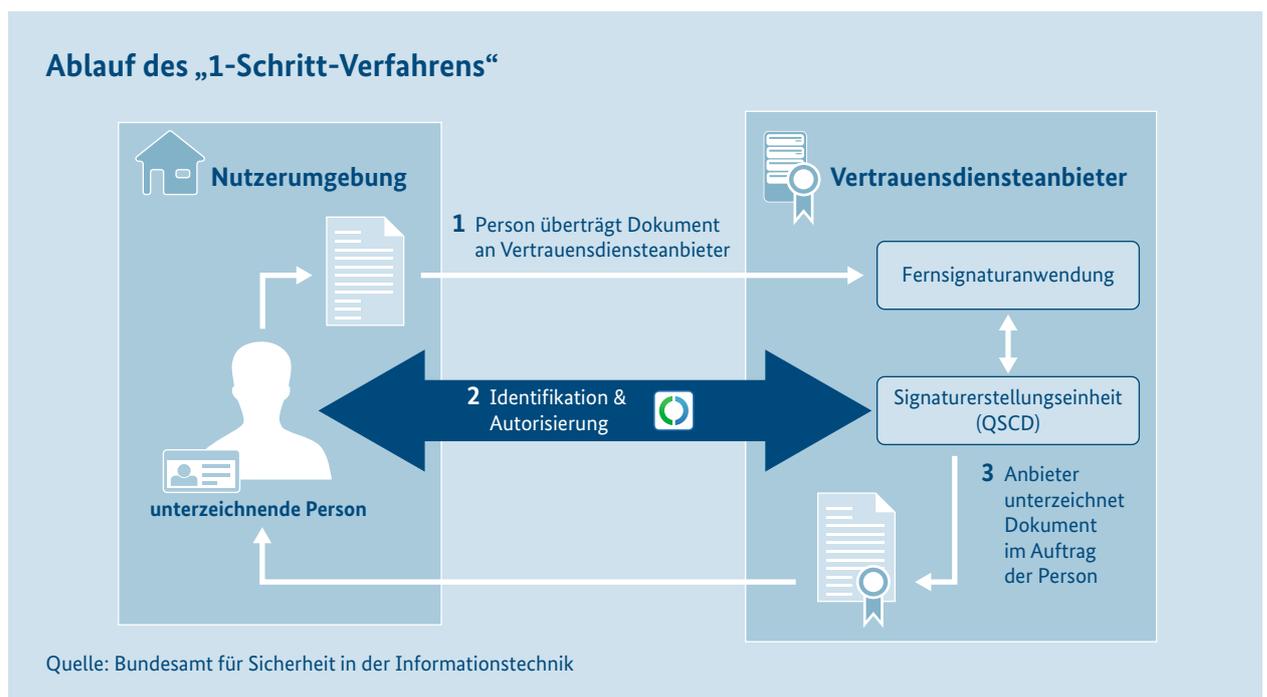


Abbildung: Ablauf des „1-Schritt-Verfahrens“

IX. Informationsquellen und Ansprechstellen

A. Im Internet

- <https://www.personalausweisportal.de>
Die Internetseite des Bundesinnenministeriums bietet umfassende Informationen für Bürgerinnen und Bürger sowie für Diensteanbieter aus Wirtschaft und Verwaltung.
- <https://www.ausweisapp.bund.de>
Hier finden Sie die AusweisApp2 des Bundes zum Herunterladen, Informationen über geeignete mobile Endgeräte sowie eine Rubrik für Diensteanbieter. Zudem werden kurze Video-Tutorials angeboten, die erklären, wie einfach der Online-Ausweis mit der AusweisApp2 genutzt werden kann und was dazu nötig ist.
Diensteanbieter können die Videos unter der Lizenz Common Creatives 3.0 BY und ND kostenfrei auf ihren Internetseiten einbinden.
- <https://www.apple.com/de/ios/app-store/>
<https://play.google.com/store/apps?hl=de>
Hier finden Sie kostenlose Apps für das Online-Ausweisen mit mobilen Geräten, darunter die AusweisApp2 und die Apps von AUTHADA.
- <https://www.bsi.bund.de/eID>
Das Bundesamt für Sicherheit in der Informationstechnik ist für die technischen Spezifikationen des Personalausweises verantwortlich, erstellt Spezifikationen, Schutzprofile und Konformitätstests für die einzelnen Komponenten und führt Zertifizierungen durch.

B. Broschüren und Leitfäden

- **Leitfaden eIDAS-Verordnung**
https://www.personalausweisportal.de/Leitfaden_eIDAS_Verordnung
Der von der Governikus KG im Auftrag des Bundesinnenministeriums erstellte Leitfaden für die öffentliche Verwaltung gibt Auskunft über Möglichkeiten und Verpflichtungen der eIDAS-Verordnung für die Anerkennung elektronischer Identitäten aus anderen EU-Mitgliedstaaten.

- **Der ideale Diensteanbieter**
<https://www.ausweisapp.bund.de/fuer-diensteanbieter/leitfaden/>
Der Leitfaden enthält Handlungsempfehlungen zur Gestaltung von Online-Angeboten mit der eID-Funktion und wurde 2017 im Auftrag des Bundesministeriums des Innern, für Bau und Heimat von der Governikus KG in Kooperation mit der AG Identity Management der Freien Universität Berlin erstellt.
- **Ein-Schritt-Fernsignaturen mit eID**
https://www.personalausweisportal.de/Info_Fernsignaturen
Die Publikation des Bundesamtes für Sicherheit in der Informationstechnik informiert über die Ein-Schritt-Fernsignatur mit Online-Ausweis.
- **Broschüre „Der Personalausweis mit Online-Ausweisfunktion“**
https://www.personalausweisportal.de/Broschuere_Online_Ausweisfunktion
In dieser Broschüre des Bundesministeriums des Innern, für Bau und Heimat erfahren die Bürgerinnen und Bürger, wie sie ihren Ausweis in der digitalen Welt nutzen und mit welchen Sicherheitsmechanismen er ihre persönlichen Daten schützt. Außerdem wird erklärt, wie die biometrischen Daten im Personalausweis verwendet werden, wie wichtig der Brief ist, den Antragstellende nach Herstellung ihres Personalausweises erhalten, und welche Sicherheitshinweise sie beachten sollten. Die Broschüre muss Bürgerinnen und Bürgern bei der Antragstellung in der Personalausweisbehörde angeboten werden.
Diensteanbieter können das PDF zur Information ihrer Kundinnen und Kunden auf ihren Internetseiten anbieten oder darauf verlinken.

C. Beantragung von Berechtigungszertifikaten

Informationen über die Beantragung von Berechtigungszertifikaten als Diensteanbieter, Identifizierungsdiensteanbieter oder Anbieter für das Vor-Ort-Auslesen sowie die notwendigen Formulare erhalten Sie auf <https://www.personalausweisportal.de> und bei der Vergabestelle für Berechtigungszertifikate (VfB).

Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt

Telefon: 022899 358-3300

E-Mail: nPA@bva.bund.de

Homepage: <https://www.bva.bund.de/vfb>

D. Testkonzept für die eID-Infrastruktur

Das Testkonzept beschreibt die einzelnen Komponenten der eID-Infrastruktur und informiert über die Testmöglichkeiten sowie die verfügbaren Testwerkzeuge. Das Testkonzept richtet sich an die Hersteller und Anwender der einzelnen Komponenten und wird gemeinsam mit den Herstellern kontinuierlich fortgeschrieben.

Das Testkonzept finden Sie auf https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/Online-Ausweisfunktion/Testkonzept/testkonzept_node.html

E. Pilotprojekt Fernsignaturverfahren

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt ein Pilotprojekt durch, mit dem die prototypische Umsetzung eines Fernsignaturverfahrens anhand des Online-Ausweises realisiert werden soll.

Bei Interesse an der weiteren Entwicklung des Verfahrens wenden Sie sich bitte an eid@bsi.bund.de.

