"On the Internet, nobody knows you're a dog."

©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

150729, Miene, Lea, Nutzungszahlen des neuen Personalausweises

30.07.2015 10:55

Von noreply@bmi.bund.de <noreply@bmi.bund.de>

An leamiene@t-online.de <leamiene@t-online.de>

Az: O3-12007/1#1 - Miene, Lea

Sehr geehrte Frau Miene,

vielen Dank für Ihre Anfrage vom 30. Juli 2015 an das Bundesministerium des Innern (BMI), mit der Sie um statistische Angaben zur bundesweiten Ausgabe des elektronischen Personalausweises zur Verwendung für Ihre Bachelorarbeit bitten.

Ihre Anfrage kann ich nur im Allgemeinen beantworten, da dem Bundesministerium des Innern keine genauen Zahlenangaben hierüber vorliegen.

Hinsichtlich des Personalausweises mit Online-Ausweisfunktion kann ich Ihnen mitteilen, wie viele Ausweise seit der Einführung am 1. November 2010 von der Bundesdruckerei ausgeliefert wurden.

Da hierbei auch Neuausstellungen wegen Diebstahls, Verlusts und Namensänderungen etc. mitgerechnet werden, entspricht die Zahl von ca. 31.000.000 produzierten Ausweisen nicht der Zahl, der tatsächlich im Umlauf befindlichen Ausweise mit Online-Ausweisfunktion.

Leider können wir auch nur eine Hochrechnung der Einschaltquote anbieten, da nicht alle der bundesweit 5.500 Personalausweisbehörden, entsprechende Zahlen übermitteln. Das BMI geht derzeit davon aus, dass die Einschaltquote bei ca. 28 Prozent liegt, was wiederum bedeutet, dass ca. 8.600.000 Online-Ausweisfunktionen eingeschaltet sind.

Ich hoffe, dass ich Ihnen mit meinen Ausführungen weiter helfen konnte.

Mit freundlichen Grüßen
Im Auftrag

Angelika Zimmermann

Bundesministerium des Innern
- Bürgerservice -
E-Mail: Buergerservice@bmi.bund.de
www.bmi.bund.de
www.115.de

Achtung!
Telefonische Sperrung der Online-Ausweisfunktion beim Personalausweis und beim elektronischen Aufenthaltstitel ab dem 01.01.2014 nur noch über die Rufnummer 116 116.

Die 116 116 ist 7 Tage in der Woche 24 Stunden erreichbar. Deutschlandweit kann diese Sperrhotline kostenfrei genutzt werden. Aus dem Ausland ist die Sperrhotline gebührenpflichtig über die deutsche
Ländervorwahl +49 116 116 und alternativ über die Rufnummer +49 30 40 50 40 50 zu erreichen.
****

Bundesministerium des Innern

IT-Planungsrat

Leitfaden Online-Ausweisfunktion in Behörden

Ergebnis der Maßnahme M4: Handreichungen des IT-Planungsrats

der Strategie für eID und andere Vertrauensdienste im E-Government
- eID-Strategie -

Stand: März 2015

Inhalt

1 Zielsetzung und Aufbau des Leitfadens ... 4
2 Grundlagen zur Online-Ausweisfunktion ... 5
2.1 Nutzen und Bedarf ... 5
2.2 Funktionsweise ... 6
2.3 Rechtliche Rahmenbedingungen ... 7
2.3.1 Rechtsgrundlagen und Technische Richtlinien ... 8
2.3.2 Schriftformersatz ... 9
2.4 Organisatorische Rahmenbedingungen ... 12
2.5 Technische Rahmenbedingungen ... 12
3 Integration der Online-Ausweisfunktion in einer Behörde ... 17
3.1 Vorgehensmodell ... 17
3.2 Schritt 1: Geeignete Verwaltungsprozesse identifizieren ... 18
3.3 Schritt 2: Soll-Prozess definieren ... 19
3.4 Schritt 3: Wirtschaftlichkeitsbetrachtung durchführen ... 22
3.5 Schritt 4: Berechtigung beantragen ... 27
3.6 Schritt 5: Technische Umsetzung ... 30
3.7 Schritt 6: Test und Aufnahme Live-Betrieb ... 32
3.8 Schritt 7: Kommunikation ... 33
3.9 Schritt 8: Evaluierung/ Erfolgsmessung des eID-Prozesses ... 37
4 Einsatzszenarien für die Online-Ausweisfunktion ... 38
4.1 Einsatzszenario: Erstregistrierung und Login an einem Bürgerkonto ... 38
4.2 Einsatzszenario: Antragsverfahren ... 39
4.3 Einsatzszenario: E-Partizipation ... 39
4.4 Einsatzszenario: Zugang zu einem internen Portal ... 41
4.5 Einsatzszenario: Beantragung von Fördermitteln ... 42
4.6 Einsatzszenario: Bürgerterminal ... 43
5 Glossar ... 45
6 Begleitdokumente ... 47
6.1 Rechtliche Grundlagen ... 47
6.1.1 Bundesgesetze und Verordnungen ... 47

6.1.2 Verwaltungsverfahrensgesetze des Bundes und der Länder ... 47
6.1.3 Technische Richtlinien ... 48
6.2 Steckbriefe - Zentrale eID-Strukturen in den Ländern ... 49
6.2.1 Baden-Württemberg ... 49
6.2.2 Bayern ... 50
6.2.3 Berlin ... 51
6.2.4 Brandenburg ... 52
6.2.5 Bremen ... 53
6.2.6 Hessen ... 53
6.2.7 Niedersachsen ... 54
6.2.8 Nordrhein-Westfalen ... 55
6.2.9 Rheinland-Pfalz ... 56
6.2.10 Saarland ... 57
6.2.11 Sachsen ... 58
6.2.12 Schleswig-Holstein ... 59
6.2.13 Thüringen ... 60
6.3 Checkliste ... 61

Abbildungsverzeichnis

Abbildung 1: Schema der gegenseitigen Authentifizierung ... 7
Abbildung 2: Praxisbeispiel Landeshauptstadt München ... 11
Abbildung 3: Authentisieren mit der Online-Ausweisfunktion ... 15
Abbildung 4: Vorgehensmodell Integration der Online-Ausweisfunktion in einer Behörde ... 17
Abbildung 5: Praxisbeispiel Stadt Düren ... 21
Abbildung 6: Praxisbeispiel Stadt Dresden - eID-Nutzung ... 24
Abbildung 7: Praxisbeispiel Stadt Dresden - Einsparung/ Nutzen ... 24
Abbildung 8: Deutscher Bundestag ePetition - Bewertung der Kriterien der WiBe-Q ... 26
Abbildung 9: Praxisbeispiel Stadt Bielefeld ... 31
Abbildung 10: Praxisbeispiel – Informationskarte Online-Ausweisfunktion ... 36

1 Zielsetzung und Aufbau des Leitfadens

Im Rahmen der vom IT-Planungsrat beschlossenen Strategie für eID und andere Vertrauensdienste im E-Government (eID-Strategie) wurde in Maßnahme M4 die Erarbeitung von Handreichungen vereinbart, mit denen die Anwendung der vom IT-Planungsrat empfohlenen Vertrauensdienste für Verwaltungen, Bürgerinnen, Bürger und Unternehmen vereinfacht wird. Dies beinhaltete auch Empfehlungen zur Integration der Vertrauensdienste in die IT-Verfahren der einsetzenden Behörden sowie die Beschreibung langfristiger Modelle für den Betrieb der benötigten Infrastrukturkomponenten. Als ein Ergebnis dieser Maßnahme wurde der hier vorliegende Leitfaden zur Integration der Online-Ausweisfunktion erstellt.

Der Leitfaden richtet sich an Behörden in Bund, Ländern und Kommunen, die Anwendungen mit der Online-Ausweisfunktion des Personalausweises in ihre Verwaltungsprozesse integrieren möchten. Das Dokument adressiert Mitarbeiterinnen und Mitarbeiter aus den Bereichen Recht, Technik und Organisation. Ziel des Leitfadens sind Empfehlungen zur Integration der Online-Ausweisfunktion in die IT-Verfahren der Behörden sowie die Beschreibung von Modellen für den Aufbau und Betrieb der benötigten Infrastrukturkomponenten.

Zu Beginn des Leitfadens werden der konkrete Nutzen und die Funktionsweise der Online-Ausweisfunktion des Personalausweises und des elektronischen Aufenthaltstitels für Ausländerinnen und Ausländer beschrieben (Kapitel 2). Anschließend werden die bestehenden rechtlichen, technischen und organisatorischen Rahmenbedingungen dargestellt, um die Leserin und den Leser in die Lage zu versetzen, das relevante Umfeld und die Beteiligten an einem Vorhaben zur Integration der Online-Ausweisfunktion besser einschätzen zu können. Dabei werden die neuen Möglichkeiten des Einsatzes durch die Anpassungen der Verwaltungsverfahrensgesetze und des E-Government-Gesetzes des Bundes zum Schriftformersatz einbezogen sowie zentrale Infrastrukturen im Bund und in den Ländern berücksichtigt.

Im Fokus dieses Leitfadens steht mit Kapitel 3 die schrittweise Beschreibung der Identifikation von Anwendungsmöglichkeiten für einen gewinnbringenden Einsatz der Online-Ausweisfunktion sowie die sich hierauf aufbauende Konzeption und Einführung in die Prozesse einer Behörde. Anhand beispielhafter Einsatzszenarien werden in Kapitel 4 die Einsatzmöglichkeiten und der Nutzen der Online-Ausweisfunktion nochmals anschaulich dargestellt, um aufzuzeigen, wie diese in den unterschiedlichen Prozessen der Verwaltung umgesetzt werden können. Unter Berücksichtigung der Vorgehensweisen, Erfahrungen und Ergebnisse bestehender Angebote, werden alle für eine Integration der Online-Ausweisfunktion erforderlichen Schritte praxisbezogen erläutert. Weiterhin soll der Leitfaden Hilfestellungen liefern, die Behörden bei der Konzeption und Umsetzung eigener Anwendungen nutzen können.

Abgerundet wird der Leitfaden im Anhang mit einer Checkliste, die eine Übersicht und Zusammenfassung aller notwendigen Schritte zur Implementierung der Online-Ausweisfunktion für Behörden bietet und zur Fortschrittskontrolle in der Umsetzung genutzt werden kann.

2 Grundlagen zur Online-Ausweisfunktion

Kapitel 2 bietet einen Überblick über Nutzen und Bedarf, Funktionsweisen sowie die rechtlichen, technischen und organisatorischen Rahmenbedingungen der Online-Ausweisfunktion.

2.1 Nutzen und Bedarf

Immer mehr Aktivitäten werden ins Internet verlagert. So ist es für eine Vielzahl von Bürgerinnen und Bürger häufig schon zur Gewohnheit geworden, sich nicht nur Informationen im Netz einzuholen, sondern Dienstleistungen vollständig über das Internet abzuwickeln.

Gleichzeitig steigt die Gefahr durch Identitätsdiebstahl im Internet rasant, das Vertrauen in Online-Dienste schwindet, unabhängig davon, ob diese von einem Unternehmen oder eine Behörde angeboten werden.[1] Somit steigt das Bedürfnis, diese Aktivitäten im Netz sicher durchführen zu können. Dies gilt auch für die Zusammenarbeit mit Behörden. Diesem Bedarf an sicheren und durch den Nutzer verifizierbaren Informations-, Kommunikations- und Transaktionswegen wird über den Einsatz sicherer Identitäten entsprochen. Eine einfache und sichere Identifizierung wird mit dem Personalausweis mit Online-Ausweisfunktion, auch elektronische Identität (eID) genannt, seit dem Jahr 2010 und des elektronischen Aufenthaltstitels seit 2011 bereitgestellt.[2]

Für Bürgerinnen und Bürger sowie Unternehmen gewinnt E-Government immer mehr an Bedeutung, Leistungen der Verwaltung werden zunehmend über das Internet in Anspruch genommen und abgewickelt.[3] Für den Einsatz der Online-Ausweisfunktion wurden mit dem E-Government-Gesetz des Bundes weitere Möglichkeiten für die Nutzung der Online-Ausweisfunktion eröffnet. Das Gesetz hat das Ziel, die elektronische Kommunikation mit der Verwaltung zu erleichtern und Bund, Ländern und Kommunen einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste zu ermöglichen (siehe dazu auch Kapitel 2.3.2). Darüber hinaus wird die elektronische Abwicklung von Verwaltungsprozessen zunehmend auch in Fachgesetzen verankert. So sieht beispielsweise die Fahrzeug-Zulassungsverordnung die internetbasierte Fahrzeugzulassung (i-Kfz) mit der Online-Ausweisfunktion vor.

Die Nutzung der Online-Ausweisfunktion leistet in Behörden einen Beitrag zu schlanken, automatisierten Prozessen. Verwaltungsprozesse, die bisher noch in Teilen in Papierform abgewickelt wurden, können auf diese Weise vollständig medienbruchfrei abgewickelt werden. Die Integration der Online-Ausweisfunktion ermöglicht bei der Beantragung von Verwaltungsdienstleistungen einerseits eine Erhöhung der Verfahrenseffizienz und andererseits eine Verbesserung der Datenqualität, da sich Behörden auf die Richtigkeit der übermittelten Daten verlassen können.[4]

---

[1] Der GfK-Studie „Daten & Schutz“ zufolge sorgen sich knapp 70 Prozent der Deutschen um den Schutz ihrer Daten im Internet und befürchten den Missbrauch ihrer Identität. Die Studie steht unter www.gfk.com zur Verfügung.

[2] In den folgenden Ausführungen wird der Begriff Online-Ausweisfunktion verwendet. Dies beinhaltet auch die elektronische Funktion des Aufenthaltstitels.

[3] Derzeit nehmen 45 Prozent der Personen, die das Internet nutzen, E-Government-Angebote der Verwaltung in Anspruch. Insgesamt wird die Hälfte aller Behördenkontakte in Deutschland online erledigt. eGovernment Monitor 2014, S. 10-11.

[4] Im Hinblick auf die weitere elektronische Prozessgestaltung ist hierauf aufbauend entscheidend, dass die Daten nach dem Eingang weiter elektronisch verarbeitet werden, z. B. durch den Einsatz einer elektronischen Akte.

Da sich die Bürgerinnen und Bürger einfache, bequeme und sichere Behördengänge unabhängig von Öffnungszeiten - ohne Anfahrtskosten und Wartezeiten - wünschen, kommt ihnen die Nutzung der Online-Ausweisfunktion in Verfahren entgegen, die ein hohes Vertrauensniveau erfordern (vgl. Kapitel 3.2). Das zeit- und ressourcenintensive Prüfen einer Identität durch die Behörde, z. B. durch das persönliche Vorstellen einer Bürgerin oder eines Bürgers, entfällt hierbei. Durch diese eingesparten personellen Kapazitäten können sich Mitarbeiterinnen und Mitarbeiter auf ihre fachlichen Aufgaben konzentrieren und es kann eine Umverteilung personeller Ressourcen vorgenommen werden. Diese ökonomische Arbeitsweise trägt u.a. zur Verbesserung des Images der Behörde bei.

2.2 Funktionsweise

Der Chip des Personalausweises verfügt über verschiedene technische Funktionen. Dazu gehören die Online-Ausweisfunktion, die Unterschriftsfunktion und die Biometriefunktion. Im Rahmen des Leitfadens wird nachfolgend im Detail auf die Online-Ausweisfunktion eingegangen. Der Personalausweis enthält einen kontaktlos lesbaren Chip, mit dem je nach Erforderlichkeit Daten übermittelt werden (§ 18 Abs. 3 PAuswG). Dabei ist zu beachten, dass die Übermittlung der Datenfelder auf einer formellen Genehmigung durch die Vergabestelle für Berechtigungszertifikate beruht (vgl. Kapitel 3.5). Zu den Daten gehören:

- Familienname, Geburtsname (seit November 2013) und Vorname(n)
- Geburtsdatum und -ort
- Anschrift und Postleitzahl
- wenn angegeben: Ordens- bzw. Künstlername
- wenn angegeben: Doktorgrad
- das dienste- und kartenspezifische Kennzeichen
- Abkürzung „D“ für Bundesrepublik Deutschland
- Angabe, ob ein bestimmtes Alter über- oder unterschritten wird,
- Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht.

Der elektronische Aufenthaltstitel enthält noch folgende Daten (§ 78 Abs. 3 Aufenthaltsgesetz):

- Staatsangehörigkeit
- Nebenbestimmungen zum Aufenthalt

Für Bürgerinnen und Bürger besteht die Möglichkeit, sich mit dem dienste- und kartenspezifischen Kennzeichen an einem Dienst anzumelden. Dies ist für Anwendungsfälle relevant, die keine personenbezogenen Daten benötigen. So ist beispielsweise bei der Wiederanmeldung an einem Bürgerkonto ein erneutes Übermitteln von Daten nicht erforderlich, wenn die Nutzerin oder der Nutzer bei einer Erstregistrierung dort bereits die erforderlichen Daten hinterlegt hat. Die Anmeldung kann in diesem Fall mit einem Pseudonym erfolgen, ohne dass Personendaten wie beispielsweise Vorname, Nachname oder Anschrift übermittelt werden.

Bei dem dienste- und kartenspezifischen Kennzeichen handelt es sich um eine Zeichenfolge, die im Chip des Personalausweises für den entsprechenden Dienst anhand des Berechtigungszertifikats berechnet

wird. Es dient der eindeutigen elektronischen Wiedererkennung eines bestimmten Personalausweises durch die Behörde, für die es errechnet wurde. Das Kennzeichen wird für jeden Personalausweis und für jeden Dienst neu berechnet. Eine Verbindung zwischen den unterschiedlichen in Anspruch genommen Diensten ist daher nicht möglich.

Der Nachweis der Identität erfolgt nach dem Prinzip der Gegenseitigkeit. Bürgerinnen und Bürger identifizieren sich auf der einen Seite mit der Online-Ausweisfunktion ihres Personalausweises und auf der anderen Seite weist die Behörde den Bürgerinnen und Bürgern ihre Identität mit ihrem Berechtigungszertifikat nach. Bürgerinnen und Bürger können mit der Online-Ausweisfunktion demnach ihre Identität nachweisen, ohne persönlich anwesend zu sein. Anbieter von Online-Dienstleistungen in der Verwaltung können die Online-Ausweisfunktion in ihre Prozesse einbinden, um sicherzustellen, wer ihr Gegenüber in einem Verwaltungsprozess ist.

Folgende Abbildung soll das Prinzip der gegenseitigen Authentifizierung verdeutlichen:

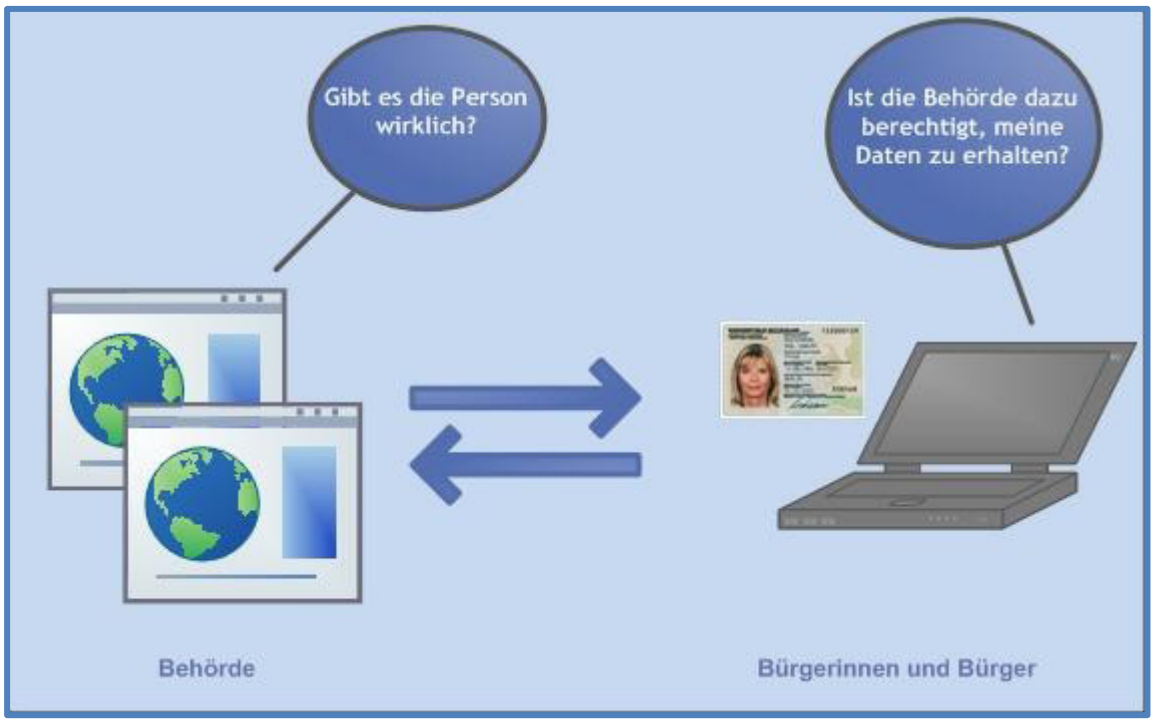


Abbildung 1: Schema der gegenseitigen Authentifizierung

Um Missbrauch mit gestohlenen Personalausweisen mit eingeschalteter Online-Ausweisfunktion zu verhindern, ist eine Sperrung möglich. Das zentrale Sperrregister wird beim Bundesverwaltungsamt geführt. Die Sperrlisten werden bei jeder Prüfung eines Ausweises abgeglichen.

2.3 Rechtliche Rahmenbedingungen

Nachfolgend werden die Rechtsgrundlagen zur Nutzung der Online-Ausweisfunktion erläutert. Dabei wird insbesondere auf die Regelungen zum Schriftformersatz eingegangen.

2.3.1 Rechtsgrundlagen und Technische Richtlinien

Behörden, die Angebote mit der Online-Ausweisfunktion bereitstellen, haben einige Vorgaben und Vorschriften zu berücksichtigen. Die nachfolgende Tabelle gibt einen Überblick über Vorgaben und Vorschriften.

Regelung	Beschreibung
Personalausweisgesetz PAuswG	Regelungen zum Umgang mit personenbezogenen Daten, Voraussetzungen für die Nutzung der Online-Ausweisfunktion insbesondere § 10 - 22
Personalausweisverordnung PAuswV	Voraussetzungen für die Nutzung der Online-Ausweisfunktion und Konkretisierungen zu den im Personalausweisgesetz enthaltenen Regelungen.
Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften	Änderung § 3a Verwaltungsverfahrensgesetz des Bundes: die Online-Ausweisfunktion kann in Verbindung mit einem elektronischen Formular im Bundesrecht die Schriftform ersetzen. Verpflichtung zum elektronischen Identitätsnachweis für Bundesbehörden, in Verwaltungsverfahren, in denen sie die Identität einer Person aufgrund einer Rechtsvorschrift festzustellen haben oder aus anderen Gründen eine Identifizierung für notwendig erachten
Verwaltungsverfahrensgesetze des Bundes und der Länder[5]	Regelungen zum Schriftformersatz in Bund und Ländern, u.a. durch Nutzung der Online-Ausweisfunktion. Viele Bundesländer haben §3a VwVfG des Bundes in die eigene Gesetzgebung bereits übernommen oder planen dieses.
Leitlinie für die Vergabe von Berechtigungen für Diensteanbieter	Die Leitlinien beschreiben das Prüfungsverfahren zur Erlangung einer Berechtigung bei der Vergabestelle für Berechtigungszertifikate unter Berücksichtigung der Erforderlichkeit der zu übermittelnden Daten nach dem Personalausweisgesetz.
Technische Richtlinien Bundesamt für Sicherheit in der Informationstechnik (BSI)	Die technischen Richtlinien liefern alle relevanten Vorgaben und Informationen zu technischen Umsetzungen und den damit verbundenen Sicherheitsbestimmungen. Folgende Richtlinien sind relevant: [6] ▪ BSI TR-03130 eID-Server ▪ BSI TR-03107 Elektronische Identitäten und Vertrauensdienste im E-Government ▪ BSI TR-03127 Architektur Elektronischer Personalausweis

Tabelle 1: Übersicht rechtlicher Rahmen zur Online-Ausweisfunktion

Den Begleitdokumenten des Leitfadens sind alle Verweise auf die gesetzlichen Regelungen sowie der genannten Vorschriften und Vorgaben zu entnehmen. Eine Auflistung der Dokumente ist dem Kapitel 6 zu entnehmen.

[5] Einen Überblick über die Verwaltungsverfahrensgesetze des Bundes und der Länder findet sich in Kapitel 6.1.2.

[6] Technische Richtlinien stehen unter www.bsi.bund.de, Bereich Publikationen zur Verfügung.

Darüber hinaus sind die europäischen Regelungen der Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt der Europäischen Kommission, eIDAS-Verordnung, zu berücksichtigen. Die eIDAS-Verordnung sieht keine eigenständige europäische Identität vor, sondern sich gegenseitig anzuerkennende nationale Identifizierungssysteme. Die Verpflichtung zur Anerkennung gilt ab dem 18.09.2018. Voraussetzung hierfür ist, dass das elektronische Identifizierungsmittel des jeweiligen Mitgliedstaates notifiziert ist. Behörden, die den Zugang zu einer E-Government-Dienstleistung nach nationalem Recht oder aufgrund der Verwaltungspraxis eine elektronische Identifizierung erfordern, müssen dabei alle notifizierten Identifizierungssysteme akzeptieren, die mindestens das Vertrauensniveau haben, das die deutsche Online-Ausweisfunktion hat.

2.3.2 Schriftformersatz

Mit dem Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften des Bundes wurde § 3a Verwaltungsverfahrensgesetz des Bundes geändert. Dort wurde u. a. die Online-Ausweisfunktion des Personalausweises in Verbindung mit einem elektronischen Formular als Ersatz zur Schriftform im Bundesrecht zugelassen. Damit können nun deutlich mehr Antragsprozesse als bisher medienbruchfrei abgewickelt werden.

Einige Länder arbeiten derzeit an vergleichbaren Rechtsvorschriften. Alle Verfahren, die sich auf das Verwaltungsverfahrensgesetz des Bundes beziehen, können den Ersatz der Schriftform durch die Online-Ausweisfunktion des Personalausweises in ihre Verwaltungsverfahren integrieren.

Die Regelung zum Einsatz des Schriftformersatzes gilt auch für Behörden, die Landesrecht umsetzen, wenn die länderspezifischen Verwaltungsverfahrensgesetze dies ebenfalls vorsehen. Zum aktuellen Zeitpunkt ist dies bei den Verwaltungsverfahrensgesetzen der Länder Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Thüringen der Fall. In die Begleitdokumente zu diesem Leitfaden wurden auch die Verwaltungsverfahrensgesetze der Länder aufgenommen. Eine Auflistung ist Kapitel 6 zu entnehmen.

Bei der Identifikation eines eID-fähigen Prozesses sollte die Behörde zunächst prüfen, ob im Verwaltungsprozess Formerfordernisse einzuhalten sind. In der Regel erfolgt die Überprüfung durch die jeweils fachkundigen Juristen. In die Prüfung sind auch Satzungen, Verfahrensanweisungen oder Richtlinien einzubeziehen, da auch hier Formerfordernisse verankert sein können. Dabei empfiehlt es sich, ein Normenscreening durchzuführen, um eine mögliche Verzichtbarkeit bestehender Schriftformerfordernisse zu identifizieren.

In der Praxis zeigt sich, dass in einem Verwaltungsverfahren häufig von einer sog. „gefühlten Schriftform“ ausgegangen wird, die sich nicht aus einer Rechtsgrundlage ableiten lässt. Der Bund hat mit dem E-Government-Gesetz in § 13 auch festgelegt, dass alleine aus der Vorschrift eines bestimmten Formulars kein Schriftformerfordernis entsteht.

Liegt ein Schriftformerfordernis vor, ist im E-Government-Gesetz des Bundes festgelegt, dass diese im Bundesrecht mit einem Formular in Verbindung mit der Online-Ausweisfunktion ersetzt werden kann. Diese Regelung erfordert eine direkte Abgabe der Erklärung über ein elektronisches Formular oder auch

Formularserver genannt. Ein Hochladen eines lokal auf dem Computer ausgefüllten Dokuments ist nicht zulässig.

Die konkrete technische und organisatorische Ausgestaltung wird durch den Gesetzgeber nicht vorgegeben, die Behörde kann selbst über die Ausgestaltung entscheiden. Maßgebend für die Behörde ist die Sicherstellung einer „sicheren und nachvollziehbaren Verknüpfung von Erklärung mit [dem] elektronischen Identitätsnachweis des Erklärenden“.[7]

Die technische Richtlinie des BSI TR-03107-2 konkretisiert den Schriftformersatz mit der Online-Ausweisfunktion zur Abgabe von Erklärungen über ein Formular.[8] Dieses wird in der Regel über eine Internetseite bereitgestellt, welche die Bürgerin oder der Bürger aufrufen kann. Diese Internetseite kann direkt in den Internetauftritt der Behörde integriert oder ein alleinstehendes Formularsystem sein. Auch der Zugang zu einem Formular mithilfe einer von der Behörde bereitgestellten Applikation ist unter bestimmten Voraussetzungen möglich. Das Format (z.B. HTML) des angebotenen Formulars sollte nach Möglichkeit ohne aktive Inhalte auskommen. Entscheidend ist, dass das Formular innerhalb der gleichen Websession im Browser des Bürgers befüllt und abgeschickt wird, in der auch die Authentisierung mithilfe des elektronischen Identitätsnachweises stattfindet.

Darüber hinaus gibt die technische Richtlinie des BSI TR-03107-2 zwei Varianten vor, die beim Befüllen und Abschicken des Formulars zu berücksichtigen sind:

Variante 1: Identitätsnachweis nach Formularbefüllung

Die Nutzung der Online-Ausweisfunktion findet nach Ausfüllen des Formulars statt. Die Bürgerin oder der Bürger ist bei Verwendung dieser Variante eindeutig auf die erhöhte rechtliche Verbindlichkeit und persönliche Zurechnung bei der Nutzung des Identitätsnachweises hinzuweisen. Der Prozessablauf dieser Variante gestaltet sich wie folgt:

a. Die Bürgerin oder der Bürger ruft mit dem Browser das Formular auf der Internetseite des Formularservers auf.
b. Die Bürgerin oder der Bürger füllt die einzelnen Felder des Formulars aus.
c. Das ausgefüllte Formular wird anschließend unter Nutzung der Online-Ausweisfunktion abgeschickt.

[7] Vgl. Bundesministerium des Innern: Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften, S. 52.

[8] Eine ausführliche Darstellung zum Schriftformersatz mit elektronischem Identitätsnachweis findet sich in der technischen Richtlinie, TR-03107-2 des Bundesamts für Sicherheit in der Informationstechnik. Diese steht unter www.bsi.bund.de, Bereich Themen, Elektronische Ausweise zur Verfügung.

Variante 2: Identitätsnachweis vor Formularbefüllung

Die Nutzung der Online-Ausweisfunktion findet vor Ausfüllen des Formulars statt. Bei dieser Variante werden die Formulardaten erst nach der Betätigung eines „Warn-Buttons“ durch die Bürgerin oder den Bürger von dem Formularserver entgegengenommen. Dieser „Warn-Button“ muss die Bürgerin oder den Bürger eindeutig auf die erhöhte rechtliche Verbindlichkeit und die persönliche Zurechnung des zu versendenden Formulars hinweisen. Der Prozessablauf dieser Variante gestaltet sich wie folgt:

a) Die Bürgerin oder der Bürger ruft mit dem Browser das Formular auf dem Formularserver auf.
b) Die Bürgerin oder der Bürger nutzt den elektronischen Identitätsnachweis, um sich gegenüber dem Formularserver zu authentisieren.
c) Die Bürgerin oder der Bürger füllt die einzelnen Felder des Formulars aus.
d) Das ausgefüllte Formular mit den darin enthaltenen Angaben des Bürgers oder der Bürgerin wird durch Betätigung eines „Warn-Buttons“ abgeschickt.

Unabhängig von der gewählten Variante sollte der Bürgerin oder dem Bürger die Möglichkeit gegeben werden, das von ihr oder ihm ausgefüllte Formular einschließlich der von ihr oder ihm gemachten Angaben als Beleg vom Formularserver herunterzuladen oder auszudrucken. Auf diese Weise erhält die Bürgerin oder der Bürger eine Kontroll- und Archivierungsmöglichkeit für die abgegebene Erklärung.

Praxisbeispiel: Landeshauptstadt München

Die Stadt München hat ein Prüfschema „Schriftformerfordernis“ entwickelt, um für verschiedene Verwaltungsprozesse zu prüfen, ob diese dem Schriftformerfordernis unterliegen und ob die Schriftform durch die elektronische Form ersetzbar ist.

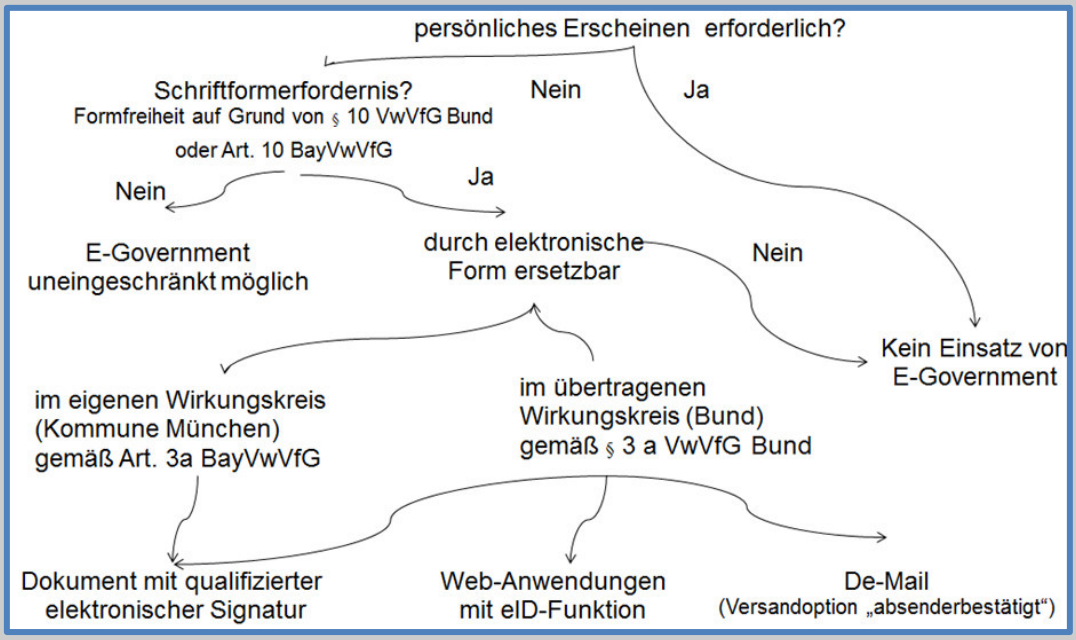


Abbildung 2: Praxisbeispiel Landeshauptstadt München

Quelle: Konzept der Landeshauptstadt München, Ergebnis der E-Government-Initiative, www.personalausweisportal.de, Bereich Downloads.

2.4 Organisatorische Rahmenbedingungen

Im Rahmen der Einführung der Online-Ausweisfunktion wirken viele verschiedene Bereiche und Akteure innerhalb der Behörde zusammen:

- Jeweils zuständige Fachabteilung(en)
- Bereich Recht
- Bereich Technik sowie der relevanten IT-Dienstleister
- Bereich Organisation
- Bereich Öffentlichkeitsarbeit

Zudem empfiehlt sich eine frühzeitige Abstimmung mit dem Datenschutzbeauftragten. Aufgrund der Vielzahl an Akteuren bietet sich eine zentrale Steuerung an, z. B. durch einen E-Government-Beauftragten.

Bezogen auf die eID-Infrastruktur sind folgende weitere Behörden und Unternehmen zu beteiligen:

- das Bundesverwaltungsamt (BVA) mit der Vergabestelle für Berechtigungszertifikate (VfB) und dem Sperrdienst; hier sind Genehmigungen zum Auslesen der Datenfelder zu beantragen
- die Berechtigungszertifikate-Anbieter (BerCA), die die technische Ausstellung der Berechtigungszertifikate übernehmen; sie stellen darüber hinaus auch aktuelle Listen aller gesperrten Personalausweisweise zur Prüfung durch den eID-Service zur Verfügung
- die Anbieter von Hardware, Software und Diensten für die Anwendung des Personalausweises mit Online-Ausweisfunktion, insbesondere eID-Service-Anbieter, sofern die Behörde keinen eigenen eID-Server betreibt.[9]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist verantwortlich für technische Sicherheitsspezifikationen, Zertifizierungen, z. B. für Kartenlesegeräte.

2.5 Technische Rahmenbedingungen

Für die Nutzung der Online-Ausweisfunktion des Personalausweises müssen sowohl Bürgerinnen und Bürger als auch die Behörden verschiedene technische Rahmenbedingungen berücksichtigen.

Infrastruktur in der Behörde

Um die Online-Ausweisfunktion in Verwaltungsprozesse einzubinden, benötigt eine Behörde ein technisches Berechtigungszertifikat. In diesem ist festgelegt, welche personen- und ausweisbezogenen Daten vom Dienst aus dem Personalausweis abgefragt werden dürfen. Die Erteilung einer rechtlichen Genehmigung erfolgt auf Antragstellung bei der Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt (vgl. Kapitel 3.5). Erst nach Erhalt eines positiven Bescheids können bei einem Berechtigungszertifikate-Anbieter die technischen Berechtigungszertifikate erworben werden.

[9] Sowohl die Berechtigungszertifikate-Anbieter als auch eID-Service-Anbieter sind unter www.personalausweisportal.de, Bereich Verwaltung, Technik aufgeführt.

Darüber hinaus ist eine Verbindung des Fachverfahrens oder einer Webanwendung zu einem eID-Server oder eID-Service erforderlich, der die sichere Kommunikation mit dem Personalausweis übernimmt. Diese steuern die elektronische Kommunikation zwischen dem Online-Angebot der Behörde und der Authentifizierungskomponente der Bürgerin oder des Bürgers. Durch technisch geprüfte Protokolle[10] und Verfahren werden Datenschutz und Datensicherheit sowie Zugriffsschutz und Authentizität gewährleistet.[11]

Für die Anbindung stehen der Behörde zwei Varianten zur Verfügung: Es besteht die Möglichkeit, selbst einen eID-Server einzurichten [1] oder diesen als Service [2] zu beziehen. Unabhängig von der Auswahl der gewählten Variante ist die Behörde Inhaberin der Berechtigung, die die Vergabestelle für Berechtigungszertifikate ausgestellt hat und damit für die Einhaltung sämtlicher Vorgaben und Anforderungen verantwortlich. Hierzu muss die Behörde, unter anderem ein Sicherheitskonzept erstellen, welches den IT-Sicherheitsanforderungen des BSI (BSI TR-03130-2) entspricht.

[1] Einrichtung eines eigenen eID-Servers

Entscheidet sich die Behörde für den Betrieb eines eigenen eID-Servers, ist diese selbst für die Einhaltung der organisatorischen, technischen und sicherheitstechnischen Maßnahmen zur Durchführung der Online-Authentisierung verantwortlich.

[2] Nutzung eines eID-Services

Übernimmt ein IT-Dienstleister für eine Behörde die Aufgabe der elektronischen Identifizierung, wird diese Dienstleistung „eID-Service“ und der Dienstleister „eID-Service-Anbieter“ genannt. In diesem Fall betreiben eID-Service-Anbieter für mehrere Dienste einen mandantenfähigen eID-Service. Es handelt sich bei diesem Betreibermodell um eine Datenverarbeitung im Auftrag gemäß §11 des Datenschutzgesetzes. Bei dieser Variante werden alle wesentlichen Maßnahmen zur Durchführung der Online-Authentisierung beim Betreiber des eID-Servers durchgeführt, worauf die Bürgerinnen und Bürger bei Nutzung der Dienstleistung hingewiesen werden müssen. Die Nutzung eines eID-Servers ermöglicht Behörden somit eine einfache Integration der Online-Ausweisfunktion in ihre bereits existierenden IT-Systeme. Bei der Anbindung kann auf zusätzliche Ausstattung (z. B. in Form Hard- und Software) weitgehend verzichtet werden.

Zentrale eID-Services des Bundes und der Länder

Der Bund plant, Rahmenbedingungen für die Nutzung zentraler eID-Serviceleistungen zu schaffen. Auch einige Länder stellen ihren Behörden zentrale eID-Infrastrukturen zur Verfügung. Die Bereitstellung kann auch durch übergreifende Verbände, z. B. kommunale Zweckverbände erfolgen. Über zentrale Lösungen können Aufwands- und Kosteneinsparungen erzielt werden, da der Aufbau und Betrieb einer eigenen

[10] Z. B. PACE (Password Authenticated Connection Establishment): Das zur Eingabe der PIN verwendete Protokoll dient dem Aufbau eines verschlüsselten und integritätsgesicherten Kanals zwischen dem lokalen Kartenlesegerät und dem kontaktlosen Chip. Siehe dazu auch die technische Richtlinie TR-03110-2 des BSI. Diese steht unter www.bsi.bund.de, Bereich Publikationen zur Verfügung.

[11] Eine ausführliche Beschreibung zu Architektur und Schnittstellen des eID-Servers findet sich in der technischen Richtlinie, TR-03130 des BSI. Diese steht unter www.bsi.bund.de, Bereich Publikationen zur Verfügung.

eID-Infrastruktur in jeder einzelnen Kommune entfällt. Sowohl das rechtliche als auch das technische Berechtigungszertifikat können dann gemeinsam genutzt werden.

Steht eine solche zentrale Infrastruktur nicht zur Verfügung, ist ein Aufbau in Eigenregie erforderlich. In der Regel kann die Online-Ausweisfunktion einfach in das bestehende Webangebot der Kommune integriert werden. Die Umsetzung erfolgt über ein standardisiertes Vorgehen. In den Begleitdokumenten des Leitfadens sind die bestehenden zentralen eID-Services in den Bundesländern aufgeführt (vgl. Kapitel 6).

Infrastruktur bei Bürgerinnen und Bürger

Damit sich Bürgerinnen und Bürger mit dem Personalausweis im Internet authentifizieren können, muss die Online-Ausweisfunktion des Personalausweises eingeschaltet sein. Für die Nutzung am eigenen Computer benötigen Bürgerinnen und Bürger folgende Komponenten:

- den Personalausweis mit eingeschalteter Online-Ausweisfunktion,
- das Kartenlesegerät: es gibt drei Arten von Kartenlesern mit unterschiedlicher Ausstattung. Diese sind in der technischen Richtlinie TR-03119 spezifiziert.[12]
- die sechsstellige PIN für die Online-Ausweisfunktion.

Darüber hinaus wird eine Software benötigt, mit deren Hilfe eine sichere Verbindung zwischen dem Kartenlesegerät, dem Personalausweis und dem Diensteanbieter hergestellt werden kann und den verschlüsselten Datenaustausch ermöglicht. Seit November 2014 wird durch den Bund mit der AusweisApp2 eine neue, verbesserte Version bereitgestellt. Diese funktioniert unabhängig vom Browser und ist damit unabhängig von Update-Zyklen der Browser-Hersteller. Die AusweisApp2 zeigt die Daten an, die auf dem Chip des Personalausweises gespeichert sind und gibt eine Übersicht, welche eID-Dienste konkret genutzt werden können und welche bereits genutzt wurden. Die Software kann kostenfrei unter www.ausweisapp.bund.de heruntergeladen werden. Über die AusweisApp2 hinaus wird mit dem Projekt PersoApp durch eine Open-Source-Community die Softwareentwicklung der Online-Ausweisfunktion vorangetrieben.

[12] Eine Übersicht ausgewählter Kartenleser, die für die Anwendung des Personalausweises mit Online-Ausweisfunktion geeignet sind, ist unter www.ausweisapp.bund.de veröffentlicht.

Technischer Ablauf der Online-Ausweisfunktion

Der technische Ablauf der Online-Ausweisfunktion und die beteiligten Systeme sind in der folgenden Abbildung dargestellt.[13]

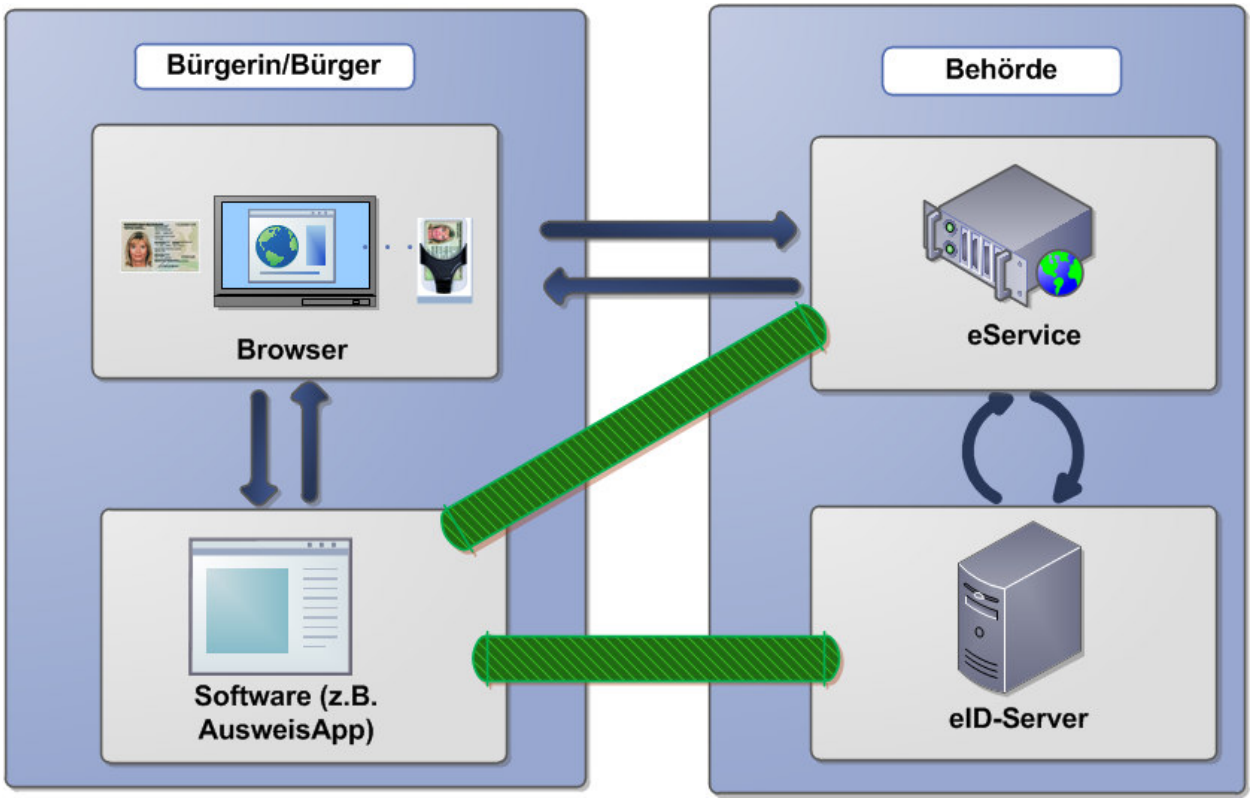


Abbildung 3: Authentisieren mit der Online-Ausweisfunktion

Die Authentisierung wird schrittweise am Beispiel eines Webangebots beschrieben:

1. Der/Die Bürger/in ruft über einen Browser den Webdienst der Behörde auf, die eine Online-Authentisierung mit Hilfe des Personalausweises mit Online-Ausweisfunktion ermöglicht.
2. Die Anwendung leitet eine Authentisierungsanfrage über den eService der Behörde an den eID-Server weiter.
3. Zwischen dem eID-Server, der Software z. B. der AusweisApp, dem Lesegerät und dem Ausweis-Chip wird ein sicherer Kanal aufgebaut und die Authentizität der Behörde sowie die Authentizität und Integrität (Fälschungssicherheit) des Ausweises geprüft.
4. Die Software zeigt dem/der Bürger/in das Berechtigungszertifikat der Behörde und die angefragten Ausweisdatenkategorien an.
5. Der/Die Bürger/in entscheidet, ob sie/er mit der Übermittlung der angefragten Daten einverstanden ist. Dies bestätigt der/die Bürger/in durch die Eingabe der PIN. Im Zuge dessen ist es für den / die Bürger/in möglich, einzelne Datenfelder abzuwählen. Werden

[13] Siehe dazu auch Technical Guideline eID-Server, Part 1: Functional Specification des BSI. Diese steht unter www.bsi.bund.de, Bereich Themen, Elektronische Ausweise zur Verfügung.

dabei Datenfelder abgewählt, bei denen es sich um vom Diensteanbieter definierte Pflichtfelder handelt, kann der Verwaltungsprozess in der Folge nicht weiter fortgesetzt werden.

6. Die Ausweisdaten werden an den eID-Server übermittelt. Der Server prüft, ob der Personalausweis gesperrt ist, indem das Sperrmerkmal mit einer diensteanbieterspezifischen Sperrliste abgeglichen wird.
7. Der eID-Server überträgt eine Authentisierungsantwort und die Ausweisdaten an den Dienst. Ist der Ausweis gesperrt, erscheint ein entsprechender Hinweis.
8. Der Dienst prüft die Authentisierungsergebnisse und entscheidet, ob die Authentisierung als erfolgreich anzusehen ist. Abschließend erfolgt eine Ergebnisantwort an die Nutzerinnen und Nutzer bzw. die Ausführung des Dienstes.

3 Integration der Online-Ausweisfunktion in einer Behörde

Im nachfolgenden Kapitel werden die einzelnen Schritte zur Integration der Online-Ausweisfunktion in einer Behörde beschrieben. Dabei wird explizit auf die spezifischen rechtlichen, technischen und organisatorischen Rahmenbedingungen verwiesen, die bei der Umsetzung der einzelnen Schritte zu berücksichtigen sind.

3.1 Vorgehensmodell

Der Leitfaden sieht eine schrittweise Integration der Online-Ausweisfunktion anhand eines Vorgehensmodells mit den Phasen Vorbereitung, Durchführung und Nachbereitung vor. In das Vorgehensmodell sind die Erfahrungen der E-Government-Initiative des Bundesinnenministeriums eingeflossen. Hier wurden gemeinsam mit über 40 Kooperationspartnern der öffentlichen Verwaltung eID-Integrationen konzipiert und umgesetzt.[14]

Die drei Phasen des Vorgehensmodells wurden in acht einzelne Schritte unterteilt. Dabei ist zu beachten, dass es sich bei dem Vorgehensmodell nicht um ein statisches Schema handelt. So kann es für die einzelne Behörde sinnvoll sein, die Reihenfolge der Schritte zu ändern oder auf die Umsetzung einzelner Schritte zu verzichten. Dies bedarf einer Prüfung zu Beginn des Vorhabens. Generell empfiehlt es sich, das Projekt zentral zu steuern und in eine zentrale E-Government-Strategie einzubinden.

Die Phasen des Vorgehensmodells werden detailliert in den jeweiligen Unterkapiteln erläutert:

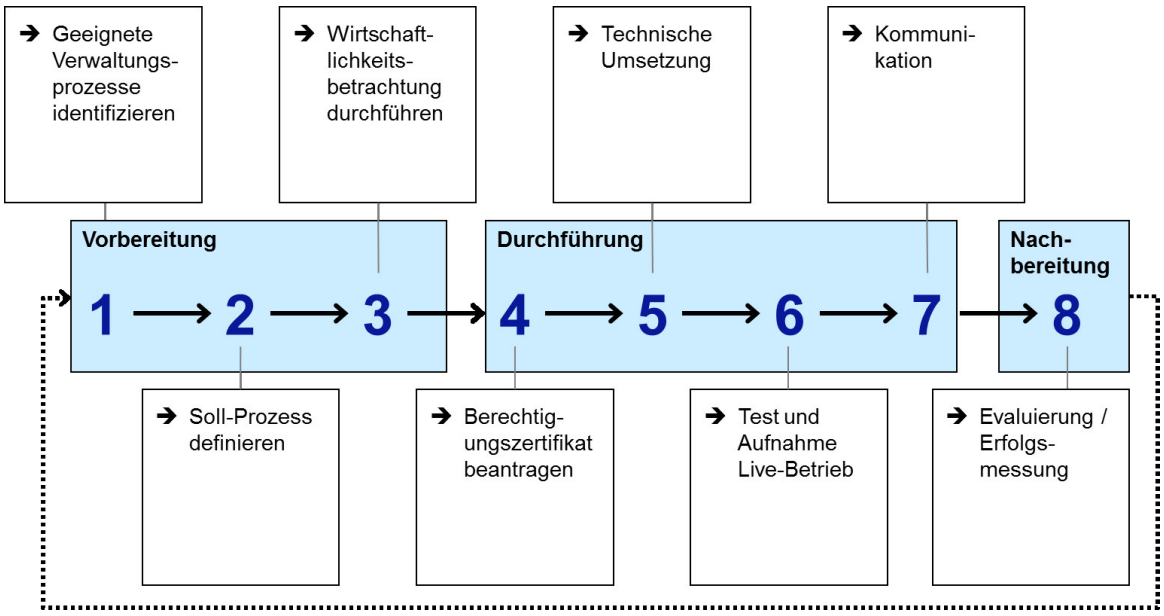


Abbildung 4: Vorgehensmodell Integration der Online-Ausweisfunktion in einer Behörde

Zu Beginn empfiehlt es sich, das Vorgehensmodell in eine Projektplanung zu überführen. Diese sollte verbindliche Meilensteine enthalten, um allen Beteiligten einen Überblick über den Projektfortschritt zu ermöglichen. Da an der Konzeption, Umsetzung und Bereitstellung von Anwendungen mehrere Akteure aus den Bereichen Recht, Technik, Organisation sowie der Fachabteilungen beteiligt sind, hat es sich in

[14] Die Ergebnisse stehen auf www.personalausweisportal.de, Bereich Downloads zur Verfügung.

der Praxis bewährt, die Ergebnisse der einzelnen Schritte als verbindliche Grundlage für den weiteren Projektverlauf zu dokumentieren.

Ist die eID erfolgreich eingeführt, kann die Umsetzung weiterer Vorhaben mit der Online-Ausweisfunktion erfolgen. In diesem Fall ist nach Abschluss der Phase „Nachbereitung“, ein erneutes Durchlaufen der Schritte möglich.

3.2 Schritt 1: Geeignete Verwaltungsprozesse identifizieren

Für die Identifikation geeigneter Verwaltungsprozesse hat es sich in der Vergangenheit bewährt, dass die Pilotierung anhand eines ausgewählten (Teil-)Prozesses erfolgt und im Anschluss auf weitere Prozesse ausgerollt wird. So ist in einem ersten Schritt zu identifizieren, in welche Verwaltungsprozesse die Online-Ausweisfunktion integriert werden kann.

Der Einsatz der Online-Ausweisfunktion richtet sich nach dem Vertrauensniveau der jeweiligen Verwaltungsdienstleistung. Das Bundesamt für Sicherheit in der Informationstechnik legt in der TR 03107-1 („Elektronische Identitäten und Vertrauensdienste im E-Government“) den Einsatz der Online-Ausweisfunktion für Verwaltungsdienstleistungen mit Vertrauensniveaus „hoch“ und „hoch+“ fest. Für Verwaltungsverfahren, die einem niedrigeren Vertrauensniveau unterliegen, ist der Einsatz alternativer Identifizierungslösungen möglich. Der IT-Planungsrat wird im Rahmen der Umsetzung der eID-Strategie Empfehlungen aussprechen, für welche Verwaltungsdienstleistungen der Einsatz der Online-Ausweisfunktion erfolgt.

Zudem bieten sich Verwaltungsprozesse an, bei denen ein gesetzliches Schriftformerfordernis besteht und für die ein Schriftformersatz durch die Online-Ausweisfunktion möglich ist. Bei der Prüfung sind ebenfalls Satzungen, Verfahrensanweisungen oder Richtlinien einzubeziehen, da auch hier Formerfordernisse verankert sein können. Dies kann auch in Regelungen von Zweckverbänden, Regiebetrieben und öffentlichen Betrieben verankert sein.

Mit dem E-Government-Gesetz des Bundes wurde § 3a Verwaltungsverfahrensgesetz des Bundes geändert. Dort wurde u. a. die Online-Ausweisfunktion des Personalausweises in Verbindung mit einem elektronischen Formular als Ersatz zur Schriftform im Bundesrecht zugelassen. Die Länder arbeiten derzeit an der Anpassung ihrer Rechtsvorschriften. Nur wenn eine rechtliche Verankerung besteht, ist ein Formerfordernis einzuhalten (siehe dazu auch Kapitel 2.3.2). Zudem hat der Bund mit dem E-Government-Gesetz in § 13 festgelegt, dass alleine aus der Vorschrift eines bestimmten Formulars kein Schriftformerfordernis entsteht.

Bestehen bereits elektronische Verfahren in der Verwaltung, sollte geprüft werden, ob die Online-Ausweisfunktion in diese integriert werden kann. Darüber hinaus lohnt es sich, Verwaltungsprozesse zu prüfen, die bisher noch in Papierform abgewickelt werden und erstmalig elektronisch bereitgestellt werden sollen. Letzteres hat den Vorteil, dass die Integration der Online-Ausweisfunktion gleich zu Beginn der elektronischen Ausgestaltung des Prozesses optimal berücksichtigt werden kann.

Weitere Anknüpfungspunkte zur Identifikation von Prozessen bietet auch die Nationale Prozessbibliothek. Dort werden in einem Register alle Prozesse (Kern-, Führungs- und

Unterstützungsprozesse) aus allen Ebenen der öffentlichen Verwaltung eingestellt.[15] Zudem hat die Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V., VITAKO, in einer Positivliste exemplarisch 20 kommunale Prozesse hinsichtlich ihrer durchgängigen elektronischen Abwicklungsmöglichkeit untersucht.[16]

Bei der Auswahl des konkreten Prozesses sollten auch Fallzahlen erhoben werden. So ermöglichen Prozesse mit hohen Fallzahlen einen breiten Einsatz der Online-Ausweisfunktion und wirken sich begünstigend auf die Wirtschaftlichkeit aus (vgl. Kapitel 3.4).

3.3 Schritt 2: Soll-Prozess definieren

Nach der Identifikation des geeigneten Verwaltungsprozesses wird im Anschluss der inhaltliche Soll-Prozess unter Integration der Online-Ausweisfunktion definiert. Dabei empfiehlt es sich, den Soll-Prozess nicht nur im Hinblick auf die Online-Ausweisfunktion zu modellieren, sondern auch zu untersuchen, ob darüber hinausgehende Optimierungspotenziale erschlossen werden können. Das E-Government-Gesetz des Bundes hat in diesen Fällen in § 9 eine Prozessoptimierung gesetzlich verankert. Demnach sind Verwaltungsabläufe, die erstmals zu wesentlichen Teilen elektronisch unterstützt werden, zu dokumentieren, zu analysieren und zu optimieren.

Für die Darstellung des Soll-Prozesses empfehlen sich Flussdiagramme oder tabellarische Übersichten mit textlichen Erläuterungen.[17] Die Beauftragte der Bundesregierung für Informationstechnik bietet hierzu Vorgehensweisen an.[18] Neben der Darstellung der einzelnen Prozessschritte sollten darüber hinaus folgende Inhalte Berücksichtigung finden:

- Am Kommunikationsprozess beteiligte Akteure und Fachverfahren: Häufig sind an einem Prozess mehrere Akteure beteiligt. Darüber hinaus können mehrere Fachverfahren zum Einsatz kommen, für die eine Weiterleitung und Speicherung der Daten erforderlich ist.
- Festlegung des Geschäftszwecks und der erforderlichen Daten des Personalausweises: Es ist zu prüfen, welche Daten des Personalausweises für die Abwicklung des Verwaltungsprozesses benötigt werden. Diese Informationen werden im weiteren Verlauf der eID-Integration auch für die Beantragung des Berechtigungszertifikats benötigt (vgl. Kapitel 3.4).
- Erforderlichkeit begleitender Anlagen: Verwaltungsprozesse sehen häufig die Übermittlung von begleitenden Anlagen in Papierform vor. Bei der Definition des Sollprozesses sollte deren Erforderlichkeit überprüft werden. Das E-Government-Gesetz des Bundes sieht in § 7 hierfür das ersetzende Scannen vor.[19] Alternativ ist zu prüfen, ob auf das Einreichen von Anlagen verzichtet

[15] Weitere Informationen stehen unter www.prozessbibliothek.de zur Verfügung.

[16] Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V., VITAKO: Positivliste elektronische Prozesse, Umsetzungsmöglichkeiten von E-Governmentprozessen, Stand: Juni 2012.

[17] Dabei bestehen verschiedene Standards für Notationen. Häufig wird hierfür Business Process Model and Notation oder die ereignisgesteuerte Prozesskette eingesetzt.

[18] Die Inhalte stehen unter http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/Daten-und-Prozessmodellierung/Prozessmodellierung/prozessmodellierung_node.html zur Verfügung.

[19] Siehe auch: Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie TR-03138 Ersetzendes Scannen (RESISCAN), verfügbar unter www.bsi.bund.de, Bereich Publikationen

werden kann oder die Nutzerinnen und Nutzer der Verwaltung eine Erlaubnis erteilen können, die Unterlagen selbständig bei einer anderen Behörde einzuholen.

- Nutzung einer E-Akte-Lösung: Das Potenzial elektronischer Verwaltungsdienstleistungen kann nur durch die elektronische Aktenführung vollständig erschlossen werden. Es ist zu prüfen, welche technischen Voraussetzungen in der jeweiligen Verwaltung existieren und wie diese in den eID-gestützten Verwaltungsprozess integriert werden können. Das E-Government-Gesetz des Bundes sieht in § 6 eine verpflichtende Einführung der E-Akte für Bundesbehörden bis zum 1. Januar 2020 vor.
- Vergleich mit ähnlichen Verfahren in der Verwaltung: Es ist ratsam, Best-Practice-Lösungen anderer Behörden bei der Definition des Soll-Prozesses einzubeziehen. Hier bieten sich Vergleiche mit anderen Kommunen, Ländern sowie dem Bund an. Im Rahmen der E-Government-Initiative des Bundesinnenministeriums wurden vielfältige Lösungen entwickelt und auf www.personalausweisportal.de frei zugänglich veröffentlicht.

Praxisbeispiel: Stadt Düren

Die Stadt Düren hat im Rahmen der E-Government-Initiative die Online-Ausweisfunktion in ihr Bürgerportal integriert. Nach Einrichtung eines Bürgerkontos kann die Online-Ausweisfunktion für das Login genutzt werden. Der dargestellte Soll-Prozess zeigt den schematischen Ablauf beim Login mit der Online-Ausweisfunktion. Nach erfolgreichem Login an das Bürgerportal können verschiedene Online-Dienste genutzt werden. Dazu gehören u.a. die Beantragung von Bewohnerparkausweisen, die Anmeldung zur Hundesteuer oder die Beantragung einer Meldebescheinigung.

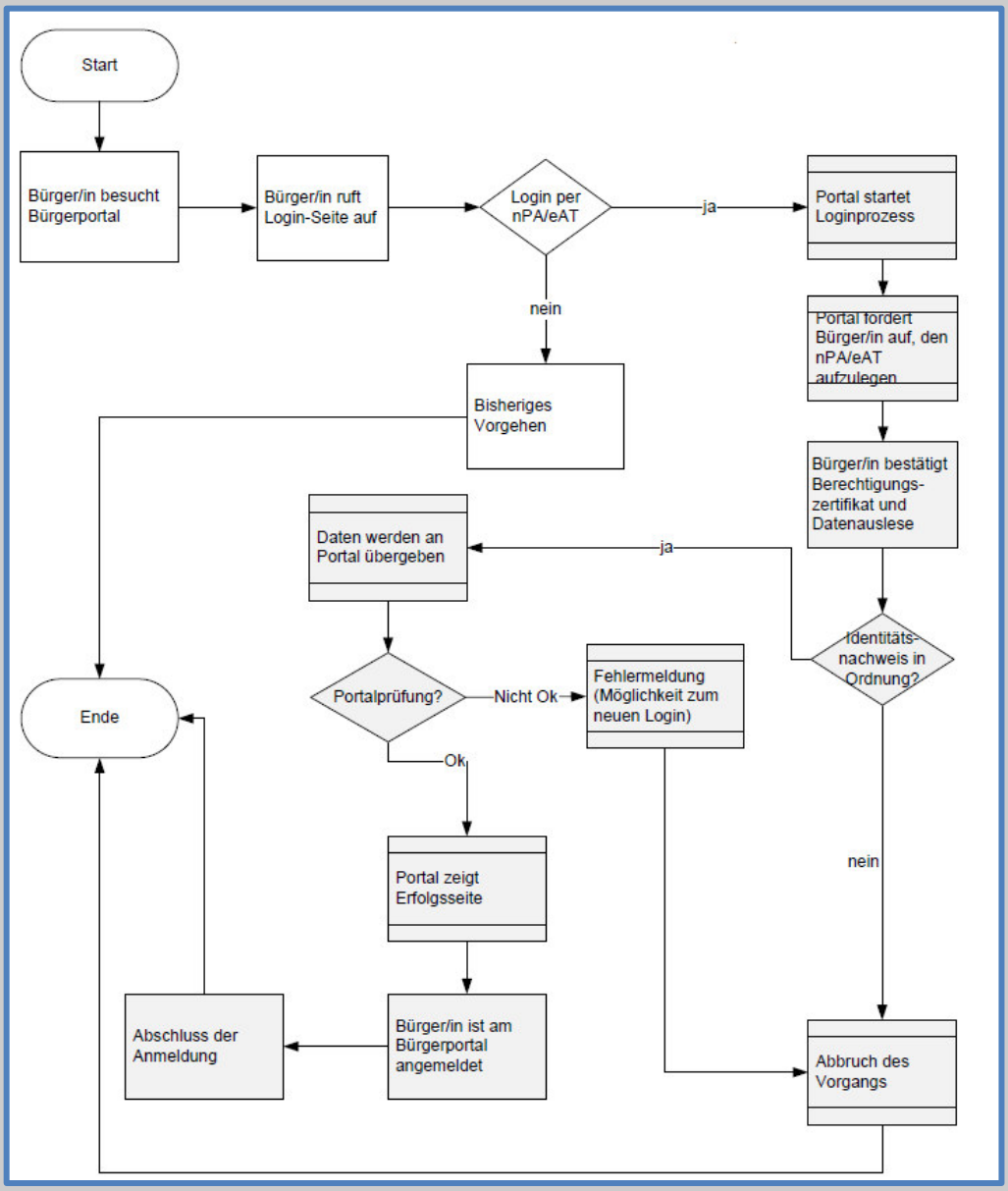


Abbildung 5: Praxisbeispiel Stadt Düren

Quelle: Fachkonzept der Stadt Düren, Ergebnis der E-Government-Initiative, www.personalausweisportal.de, Bereich Downloads.

3.4 Schritt 3: Wirtschaftlichkeitsbetrachtung durchführen

Unterschiedliche Nutzenaspekte und Kostenkategorien sind in einer Wirtschaftlichkeitsbetrachtung (WiBe) zu analysieren. Das Verfahren der WiBe dient der Untersuchung von monetären Auswirkungen sowie der Bewertung nicht monetärer Faktoren und ist ein standardisiertes Instrument für die Einführung IT-gestützter Vorhaben des Bundes. Grundsätzlich ist es möglich, Wirtschaftlichkeitsbetrachtungen zu verschiedenen Zeitpunkten durchzuführen. Der hier vorliegende Leitfaden empfiehlt die Durchführung während der Planungsphase. Gleichwohl kann eine solche Wirtschaftlichkeitsbetrachtung auch während der Durchführung (im Rahmen einer begleitenden Erfolgskontrolle) sowie nach Abschluss der Einführung der Online-Ausweisfunktion (im Rahmen einer abschließenden Erfolgskontrolle) durchgeführt werden (vgl. Kapitel 3.9).

Über die hier dargestellte Wirtschaftlichkeitsbetrachtung hinaus besteht die Möglichkeit eine Berechnung von Bürokratiekosten nach dem Standardkostenmodell, SKM, durchzuführen. Bei diesem Modell handelt es sich um einen methodischen Ansatz für die systematische Ermittlung bestehender bürokratischer Belastungen. Dabei werden die Lasten gemessen, die durch gesetzlich veranlasste Informationspflichten und Berichtspflichten entstehen. Ziel einer Ex-ante-Einschätzung nach dem Standardkostenmodell ist es, die Kostenbelastung – sofern realisierbar und sachgerecht – von Anfang an so gering wie möglich zu halten.[20] Analog der Wirtschaftlichkeitsbetrachtung ist es auch möglich, die Berechnung zu einem späteren Zeitpunkt durchzuführen.

Quantitative Faktoren einer Wirtschaftlichkeitsbetrachtung

Es gibt verschiedene quantitative Faktoren, die in der WiBe analysiert werden können. Für die Einführung der Online-Ausweisfunktion empfiehlt sich beispielsweise die Betrachtung der [1] Kosten der Systemeinführung und der [2] Systemkosten im laufenden Betrieb.[21] Bei der Durchführung von eID-Integrationsprojekten ist zu berücksichtigen, dass die Kosten abhängig von der Preisgestaltung der eID-Service-Anbieter am Markt sind. Aus diesem Grund sollten im Rahmen einer Marktanalyse Angebote verschiedener eID-Service-Anbieter eingeholt und diese unter Berücksichtigung bestehender Rahmenverträge geprüft werden. Neben der Angebotseinholung von verschiedenen eID-Services sollte auch der Eigenbetrieb des eID-Servers geprüft werden.

Im Vorfeld einer Marktanalyse ist zu prüfen, ob auf eine bestehende zentrale eID-Infrastruktur zurückgegriffen werden kann (vgl. Kapitel 2.5). Einen Überblick über die bestehende Infrastruktur in Bund und Ländern wird in den Begleitdokumenten des Leitfadens in Kapitel 6 aufgelistet. Über die

[20] Die Bundesregierung hat einen Leitfaden zur Durchführung einer Ex-Ante-Einschätzung nach dem Standardkostenmodell herausgegeben. Dieser kann abgerufen werden unter http://www.bundesregierung.de/Content/DE/StatischeSeiten/Breg/Anlagen/2007-05-25-ex-ante-leitfaden.html

[21] Die Durchführung einer WiBe mit quantitativen und qualitativen Faktoren kann auf Grundlage eines standardisierten Kriterienkatalogs einschließlich eines entsprechenden Berechnungstools durchgeführt werden. Dieser differenziert die monetären Faktoren in Projektkosten, Technikkosten, Betriebskosten und Nutzenpotentiale. Der Kriterienkatalog sowie der WiBe-Kalkulator steht über die Homepage der IT-Beauftragten der Bundesregierung www.cio.bund.de im Bereich Architekturen und Standards zur Verfügung.

Nutzung zentraler Lösungen können Kosteneinsparungen erzielt werden, da der Aufbau und Betrieb einer eID-Infrastruktur in der einzelnen Kommune entfällt. Die Online-Ausweisfunktion kann meist in das bestehende Webangebot der Behörde integriert werden.

Die [1] Kosten der Systemeinführung bilden den Investitionsbedarf ab, der für die Einführung der Online-Ausweisfunktion notwendig ist. Diese lassen sich grob in Personalbedarfe (-kosten) sowie Software- und Hardwarekosten unterscheiden:

- Bei der Berechnung der Personalbedarfe ist der interne Aufwand für die Einbindung der Online-Ausweisfunktion zu berücksichtigen. Dazu gehören:
    - Aufwände für die Analyse und Neugestaltung der Geschäftsprozesse,
    - Konzeption,
    - Kommunikations-/ Informationsmanagement und Marketing,
    - die Durchführung der technischen Integration,
    - Abstimmungen mit den Bereichen Recht, Technik und Organisation sowie dem Datenschutzbeauftragen und der Vergabestelle für Berechtigungszertifikate.
- Die Ermittlung der Software- und Hardwarekosten ist abhängig vom:
    - Umfang des Vorhabens,
    - den Software-Lizenzen für eID-Server / eID-Services,
    - den Software-Zertifizierungen,
    - Anzahl und Kosten der erforderlichen Berechtigungszertifikate,
    - der Anpassung von Fachverfahren,
    - der Beschaffung spezieller Hardware (z. B. Einbau von Kartenlesern, spezielle Eingabetatstaturen etc.)
    - Aufbau der Systeme.

Bei der Ermittlung der [2] Systemkosten im laufenden Betrieb sind die Kosten zu berücksichtigen, die für den Betrieb der Online-Ausweisfunktion anfallen.

Neben der Ermittlung der entstehenden Kosten wird in der WiBe auch der monetäre Nutzen der Einführung der Online-Ausweisfunktion betrachtet. Dazu gehören in erster Linie Einsparungen von Personal- und Standortkosten, die zum Beispiel durch die Verlagerung von Geschäftsprozessen in das Internet und die Erhöhung der Qualität von Stammdaten erzielt werden können. Darüber hinaus kann auch die Ablösung eines Altsystems bzw. Fachverfahrens Kosten einsparen.

Praxisbeispiel: Stadt Dresden

Die Stadt Dresden hat die Online-Ausweisfunktion bei der Beantragung von Baumfällgenehmigungen eingeführt. Die durchgeführte strategische Kostenbetrachtung bezieht sich auf zehn Prozesse/ Antragsverfahren, die zukünftig mit der Online-Ausweisfunktion umgesetzt werden sollen. Dabei wird die Tendenz der Nutzung (optimistisch, realistisch, pessimistisch) von Angeboten mit Online-Ausweisfunktion in die Kostenbetrachtung integriert. Es wird davon ausgegangen, dass in der Landeshauptstadt Dresden jährlich durchschnittlich 10 Online-Formulare umgesetzt werden. Darüber hinaus wird angenommen, dass die Hälfte der 10 Formulare in diesem Zuge mit der Online Ausweisfunktion ausgestattet wird. Pro Formular wird von einer Nutzerzahl von 500 Anträgen pro Jahr ausgegangen. Damit steigt die Anzahl an Anträgen jährlich um 2.500. Dem werden die Fixkosten und die variablen Kosten der Einführung der Online-Ausweisfunktion bei der Antragsbearbeitung gegenübergestellt. Die Einsparung / Nutzen bemisst sich über die Verkürzung der Bearbeitungszeit.

Jahr	eID-Nutzung			Gesamtanzahl der Anträge	Fixkosten	variable Kosten	Summe der Kosten	kumulierte Kosten
	optimistisch	realistisch	pessimistisch					
2013	2%	1%	1%	650	2.600,00€	3.000,00€	5.600,00€	5.600,00€
2014	5%	3%	1%	3150	0,00€	3.000,00€	3.000,00€	8.600,00€
2015	8%	5%	2%	5650	0,00€	3.000,00€	3.000,00€	11.600,00€
2016	12%	7%	2%	8150	0,00€	3.000,00€	3.000,00€	14.600,00€
2017	15%	10%	3%	10650	0,00€	3.000,00€	3.000,00€	17.600,00€
2018	18%	13%	4%	13150	0,00€	3.000,00€	3.000,00€	20.600,00€
2019	22%	16%	5%	15650	0,00€	3.000,00€	3.000,00€	23.600,00€
2020	26%	19%	6%	18150	0,00€	3.000,00€	3.000,00€	26.600,00€
2021	30%	23%	7%	20650	0,00€	3.000,00€	3.000,00€	29.600,00€
2022	35%	26%	8%	23150	0,00€	3.000,00€	3.000,00€	32.600,00€

Abbildung 6: Praxisbeispiel Stadt Dresden - eID-Nutzung

Jahr	Einsparung / Nutzen					
	optimistisch	kumuliert	realistisch	kumuliert	pessimistisch	kumuliert
2013	47,78 €	47,78 €	23,89 €	23,89 €	23,89 €	23,89 €
2014	578,81 €	626,59 €	347,29 €	371,18 €	115,76 €	139,65 €
2015	1.661,10 €	2.287,69 €	1.038,19 €	1.409,36 €	415,28 €	554,93 €
2016	3.594,15 €	5.881,84 €	2.096,59 €	3.505,95 €	599,03 €	1.153,95 €
2017	5.870,81 €	11.752,65 €	3.913,88 €	7.419,83 €	1.174,16 €	2.328,11 €
2018	8.698,73 €	20.451,38 €	6.282,41 €	13.702,24 €	1.933,05 €	4.261,16 €
2019	12.653,03 €	33.104,40 €	9.202,20 €	22.904,44 €	2.875,69 €	7.136,85 €
2020	17.342,33 €	50.446,73 €	12.673,24 €	35.577,68 €	4.002,08 €	11.138,93 €
2021	22.766,63 €	73.213,35 €	17.454,41 €	53.032,09 €	5.312,21 €	16.451,14 €
2022	29.776,69 €	102.990,04 €	22.119,83 €	75.151,91 €	6.806,10 €	23.257,24 €

Abbildung 7: Praxisbeispiel Stadt Dresden - Einsparung/ Nutzen

Quelle: Konzept der Stadt Dresden, Ergebnis der E-Government-Initiative, www.personalausweisportal.de, Bereich Downloads.

Qualitative Faktoren einer Wirtschaftlichkeitsbetrachtung

Damit Vorteile, die sich aus der Umsetzung der geplanten IT-Vorhaben ergeben, nicht nur monetär betrachtet werden, können in der WiBe auch qualitative Aspekte im Rahmen einer Nutzwertanalyse Berücksichtigung finden. Für die Betrachtung qualitativer Aspekte bei Einführung der Online-Ausweisfunktion empfiehlt es sich zum Beispiel die Kategorien externe Effekte und Faktoren mit qualitativ-strategischer Bedeutung zu berücksichtigen.[22]

Zum Bereich der externen Effekte zählen beispielsweise Qualitäts- und Leistungssteigerungen (Vergrößerung des Dienstleistungsangebots, Qualitäts- und Leistungssteigerungen), Ablösedringlichkeit (Nachfrage der Bürgerin oder des Bürgers) sowie Benutzerfreundlichkeit (Realisierung eines einheitlichen Zugangs, Erhöhung der Nachvollziehbarkeit). Zu den Faktoren von qualitativ-strategischer Bedeutung gehören zum Beispiel der Qualitätszuwachs bei der Erledigung von Fachaufgaben (einheitliches Verwaltungshandeln, Imageverbesserung), mitarbeiterbezogene Effekte (Attraktivität der Arbeitsbedingungen, Qualifikationserweiterung) sowie die Priorität der IT-Maßnahme (Pilot-Projekt-Charakter, Bedeutung innerhalb des IT-Rahmenkonzepts). Jeder Aspekt wird anschließend auf Grundlage eines standardisierten Punktesystems gewertet und gewichtet. So ist es möglich, den Nutzen bei der Einführung der Online-Ausweisfunktion darzustellen.

Darüber hinaus ist die Sicht der Bürgerinnen und Bürger einzubeziehen. So ist es für diese ein Vorteil, wenn ihnen der Weg in die Behörde erspart bleibt und sie ihre Anliegen vom eigenen Computer zu Hause medienbruchfrei und jederzeit abwickeln können. Auch direkte monetäre Faktoren können sich durch die Einführung der Online-Ausweisfunktion für die Bürgerinnen und Bürger ergeben. Diese sparen zum Beispiel bei der Online-Abwicklung eines Antrages u. a. Papier- und Druck sowie Portokosten. Zudem ergibt sich bei digitaler Abwicklung der Vorteil einer schnelleren Entscheidung bzw. Genehmigung, durch den Wegfall von Transportzeiten und kürzeren Liegezeiten.

Eine umfassende qualitative Wirtschaftlichkeitsbetrachtung hat der Bundestag für die Integration der Online-Ausweisfunktion in sein Portal für das Einreichen von Petitionen durchgeführt.

[22] Die Betrachtung qualitativer Aspekte in der WiBe ist ebenfalls über den standardisierten Kriterienkatalog des IT-Beauftragten der Bundesregierung im Bereich Architekturen und Standards abzurufen.

Praxisbeispiel: Deutscher Bundestag - ePetition

Der Deutsche Bundestag hat bei der Einführung der Online-Ausweisfunktion in das Petitionsportal eine quantitative und qualitative Wirtschaftlichkeitsbetrachtung im Rahmen einer Nutzwertanalyse durchgeführt. Dabei wurden externe Effekte (die sog. WiBe-E) und die qualitativ-strategische Bedeutung (sog. WiBe-Q) betrachtet. In der WiBe-E wurden u.a. folgende Kriterien beleuchtet: Realisierung eines einheitlichen Zugangs, Unmittelbarer wirtschaftlicher Nutzen für den Kunden, Vergrößerung des Dienstleistungsangebotes oder Nachnutzung von Projektergebnissen für vergleichbare Projekte.
In der nachfolgenden Tabelle findet sich die Bewertung der Kriterien der WiBe-Q.

Kriterium	Gewichtung	Punkte	Produkt
Bedeutung innerhalb IT- Rahmenkonzept	5	10	50
Einpassung in den IT-Ausbau der BV insgesamt	5	10	50
Pilot-Projekt-Charakter	5	8	40
Nachnutzung bereits vorhandener Technologien	5	6	30
Plattform-/Herstellerunabhängigkeit	10	8	80
Qualitätsverbesserung bei der Aufgabenabwicklung	15	6	90
Beschleunigung von Arbeitsabläufen und -prozessen	10	2	20
Einheitliches Verwaltungshandeln	10	10	100
Imageverbesserung	5	8	40
Informationsbereitstellung für Entscheidungsträger und Controlling	10	4	40
Unterstützung des Entscheidungsprozesses/ Führungsvorganges	10	8	80
Attraktivität der Arbeitsbedingungen	5	4	20
Qualifikationssicherung/-erweiterung	5	0	0
Summe	**100**	**84**	**640**
Mittelwert			**49,23**
Kriterium Q			**64**

Abbildung 8: Deutscher Bundestag ePetition - Bewertung der Kriterien der WiBe-Q

Quelle: Konzept des Deutschen Bundestages, Ergebnis der E-Government-Initiative, www.personalausweisportal.de, Bereich Downloads.

3.5 Schritt 4: Berechtigung beantragen

Im Vorfeld der eID-Integration ist zu prüfen, ob bereits ein zentrales Berechtigungszertifikat vorliegt, das für den Soll-Prozess genutzt werden kann. Ist das der Fall, entfällt der hier dargestellte Schritt 4, Berechtigung beantragen. Liegt hingegen noch kein zentrales Berechtigungszertifikat vor, sollte geprüft werden, ob die Online-Ausweisfunktion über den identifizierten Soll-Prozess perspektivisch auch in weitere Fachprozesse integriert werden soll. Dies ist bei der Begründung des Geschäftszwecks zu berücksichtigen.

Wer stellt den Antrag

Trägern öffentlicher Verwaltung, d. h. insbesondere Behörden des Bundes, der Länder und der Kommunen ist es selbst möglich, ein Berechtigungszertifikat bei der Vergabestelle für Berechtigungszertifikate beantragen. Sie haben die datenschutzrechtliche Verantwortlichkeit i.S.d. § 3 Abs. 7 BDSG aufgrund der öffentlich-rechtlichen Aufgabe für die erhobenen Daten und sind deshalb Diensteanbieter i.S.d. § 2 Abs. 3 PAuswG.[23]

In vielen Fällen ist die Aufgabe der Identifikation von den einzelnen Trägern auf eine zentrale Stelle übertragen worden. Beispielsweise erlaubt das Gesetz über kommunale Gemeinschaftsarbeit (GkG) in Nordrhein-Westfalen den dortigen Zweckverbänden, Aufgaben beteiligter Gemeinden zu übernehmen und für diese auszuführen. In diesem Fall kann die Beantragung eines Berechtigungszertifikats für die beteiligten Städte und Gemeinden entfallen.

Bei der Nutzung des Berechtigungszertifikats ist zu berücksichtigen, dass diese an eine konkrete URL geknüpft ist. Die URL muss zu der Webseite gehören, auf der die Authentisierung durchführt wird.[24] Dies ist insbesondere bei der Integration der Online-Ausweisfunktion in Bürgerportalen relevant, da dort häufig ein Berechtigungszertifikat für mehrere Verwaltungsdienstleistungen genutzt wird (vgl. Kapitel 4.1). Die im Berechtigungszertifikat angegebene URL wird dann als Rücksprungadresse nach erfolgreicher Authentisierung genutzt.

Die Vergabestelle für Berechtigungszertifikate prüft im Einzelfall, ob die rechtliche Grundlage ausreicht, ein Berechtigungszertifikat durch eine zentrale Stelle zu beantragen. Einen Überblick über die Angebote der einzelnen Länder bieten die Begleitdokumente zu diesem Leitfaden (vgl. Kapitel 6).

Die Nutzung eines zentralen Berechtigungszertifikats erfolgt über ein standardisiertes Vorgehen, bei welchem die Verwaltungsdienstleistungen in eine zentrale Verfahrensliste des Landes oder des Zweckverbandes aufgenommen werden. Diese Verfahrensliste wird der Vergabestelle für Berechtigungszertifikate in der jeweils aktuellen Fassung vorgelegt.

[23] Die Formulare, Voraussetzungen und Musteranträge zur Einreichung des Antrags für ein Berechtigungszertifikat stehen unter www.personalausweisportal.de, Bereich Downloads zur Verfügung.

[24] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie TR-03127, Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel

Was wird beantragt

Dem Diensteanbieter ist es aufgrund der Berechtigung möglich, seine Verwaltungsdienstleistungen mit der Online-Ausweisfunktion des Personalausweises anzubieten. Dies geschieht in der Regel entweder mit dem Geschäftszweck

1. „Temporäres Bürgerkonto“ und / oder
2. „Permanentes Bürgerkonto“.

In beiden Szenarien legt die Bürgerin oder der Bürger ein sogenanntes „Bürgerkonto“ an. Es werden die für Verwaltungsdienstleistungen mit Identifikationsbedarf mindestens benötigten Daten des Ausweises angefragt.

Der Unterschied der beiden Arten von Bürgerkonten besteht darin, dass bei dem „Temporären Bürgerkonto“ die Daten aus dem Bürgerkonto für eine bestimmte Verwaltungsdienstleistung benutzt werden und nach erfolgreicher Übergabe an das sachbearbeitende Verwaltungsverfahren bei der zentralen Stelle wieder gelöscht werden. Die freigegeben Daten werden bei der zentralen Stelle nicht gespeichert und nur temporär zur Abwicklung von Verwaltungsdienstleistungen verwendet.

Beim „Permanenten Bürgerkonto“ kann die Bürgerin oder der Bürger nach der Registrierung jederzeit auf die Daten im angelegten Bürgerkonto für entsprechende Verwaltungsdienstleistungen mit Identifikationsbedarf zugreifen und diese für entsprechende Verwaltungsdienstleistungen zur Verfügung stellen.

Im Übrigen ist es dem Diensteanbieter möglich, auch für Verwaltungsdienstleistungen, die mehr als die beschriebenen Daten zur Identifikation aus dem Ausweis des Ausweisinhabers benötigen (z. B. Geburtsort, Geburtsname), die Online-Ausweisfunktion einzusetzen. Hierfür ist für jeden Anwendungsfall eine weitere Berechtigung mit dem speziellen Geschäftszweck zu beantragen

Die Vorgehensweise, um für einen oder mehrere Geschäftszwecke berechtigt zu werden, Datenfelder aus dem Ausweis anzufragen, teilt sich in zwei Bereiche auf:

1. Vorbereitung des Diensteanbieters, um die Online-Ausweisfunktion in seiner Infrastruktur anwenden zu können und
2. Antrags- und Erteilungsvoraussetzungen der Vergabestelle für Berechtigungszertifkate (§ 21 Abs. 2 Nr. 1-5 PAuswG)

Zu 1:

- Analyse der eigenen Geschäftsprozesse; es empfiehlt sich, dass vor Beantragung des Berechtigungszertifikats eine Beschreibung der fachlichen Dienste vorliegt, denn eine intensive Analyse und Anpassung von Geschäftsprozessen kann unnötige Berechtigungszertifikate und damit verbundene Kosten vermeiden (vgl. Kapitel 3.3)

- Nutzung der Daten innerhalb der definierten Geschäftsprozesse darlegen
- Zeitliche Komponente der Nutzung (erheben, speichern, weiterverarbeiten, löschen)
- Technische Dienstleistung (Auftragsdatenverarbeitung) erläutern
- Rechtliche Selbstständigkeit von Behördenteilen beachten
- Datensparsamkeit **„So viel wie nötig, so wenig wie möglich“**

Zu 2: Im Einzelnen wird geprüft, ob

- der angegebene Zweck nicht rechtswidrig ist
- der Zweck nicht in der geschäftsmäßigen Übermittlung der Daten besteht und keine Anhaltspunkte für die geschäftsmäßige oder unberechtigte Übermittlung der Daten vorliegen
- eine Übermittlung an bestimmte Dritte zur Erfüllung eines Geschäftszwecks erforderlich ist, der nicht in der geschäftsmäßigen Übermittlung der Daten besteht und keine Anhaltspunkte für eine geschäftsmäßige oder unberechtigte Übermittlung der Daten vorliegen
- der antragstellende Diensteanbieter die Erforderlichkeit der zu übermittelnden Angaben für den beschriebenen Zweck nachgewiesen hat
- die Anforderungen, insbesondere an Datenschutz und Datensicherheit erfüllt sind (siehe Personalausweisverordnung §§ 28, 29); zusätzlich muss die Behörde bei der Beantragung bestätigen, dass ein Sicherheitskonzept vorliegt, welches sich an den Standards des IT-Grundschutzes orientieren muss[25]
- keine Anhaltspunkte für eine missbräuchliche Verwendung der Berechtigung vorliegen

In der Regel wird die Berechtigung für die Datenfelder

- **Name, Geburtsname, Vorname, Tag der Geburt und Anschrift, Abkürzung „D“ für Bundesrepublik Deutschland, Dokumentenart** beim „Temporären Bürgerkonto“ erteilt

und zusätzlich

- beim „Permanenten Bürgerkonto“ das Datenfeld **Dienste- und kartenspezifisches Kennzeichen (DKK)**[26]

[25] Die IT-Grundschutz-Standards (insbesondere BSI 100-2 und BSI 100-3) des Bundeministeriums für Sicherheit in der Informationstechnik stehen unter www.bsi.bund.de, Bereich IT-Grundschutz zur Verfügung. Eine Vorlage für das Sicherheitskonzept findet sich in der technischen Richtlinie TR-03130. Dies steht ebenfalls über die Homepage des BSI zur Verfügung.

[26] VITAKO: Neuer Personalausweis, Aus der Praxis für die Praxis, Beantragung von Zertifikaten für das Auslesen von Daten aus dem neuen Personalausweis, Stand: April 2011.

Damit ist für die Behörde eine Vielzahl von Verwaltungsdienstleistungen mit Identifikationsbedarf abgedeckt und dem Grundsatz der Datensparsamkeit wird aufgrund des kleinsten gemeinsamen Nenners bei der Erhebung der Daten entsprochen. Die Vergabestelle für Berechtigungszertifikate stellt eine Berechtigung für maximal drei Jahre aus. Anschließend ist eine Verlängerung zu beantragen.

3.6 Schritt 5: Technische Umsetzung

Mit der Integration der Online-Ausweisfunktion geht eine Anpassung der bestehenden Systemarchitektur der Behörde einher. Diese erfolgt in Abhängigkeit der technischen Infrastruktur der Behörde vor Ort.

Für die technische Integration bestehen folgende Möglichkeiten: [27]

- Es kann eine Anbindung über eine SAML-Schnittstelle erfolgen.
- Alternativ ist eine Anbindung über einen Web-Service möglich.

Die konkrete technische Ausgestaltung der Anbindung des eID-Servers ist mit dem eID-Server-Betreiber abzustimmen. Dazu stellen die Betreiber eines eID-Services den Behörden Informationen zur Verfügung, wie die eID-Anbindung technisch erfolgt und welche Softwareunterstützung für welche Plattformen bereitgestellt wird. Diese beinhalten auch technische Dokumentation für die Anbindung an den Service sowie Informationen über das Einrichten und den Austausch der technischen Zertifikate.

[27] Weitergehende Informationen werden in der Technischen Richtlinie TR-03130 aufgeführt.

Praxisbeispiel: Stadt Bielefeld

Die Stadt Bielefeld hat die Online-Ausweisfunktion für die Online-Beantragung von Wahlscheinen eingeführt. Im Rahmen der Einführung wurden zwei Betreibermodelle diskutiert (eigener eID-Server oder eID-Service-Anbieter). Die hier dargestellte Variante ist ein Betreibermodell, bei dem der Anwendungsserver durch einen eID-Service-Anbieter betrieben wird. Bei dieser Variante werden Schnittstellen zum eigentlichen Fachverfahren (VoteManager), d.h. die Schnittstellen zwischen dem Anwendungsserver (Webformular) und dem Server auf Seiten der Stadt Bielefeld realisiert. Dazu ist die Implementierung eines Vorverfahrens notwendig, welches bei der Stadt Bielefeld betrieben wird. Das eigentliche Fachverfahren VoteManager kommuniziert mit dem Vorverfahren.

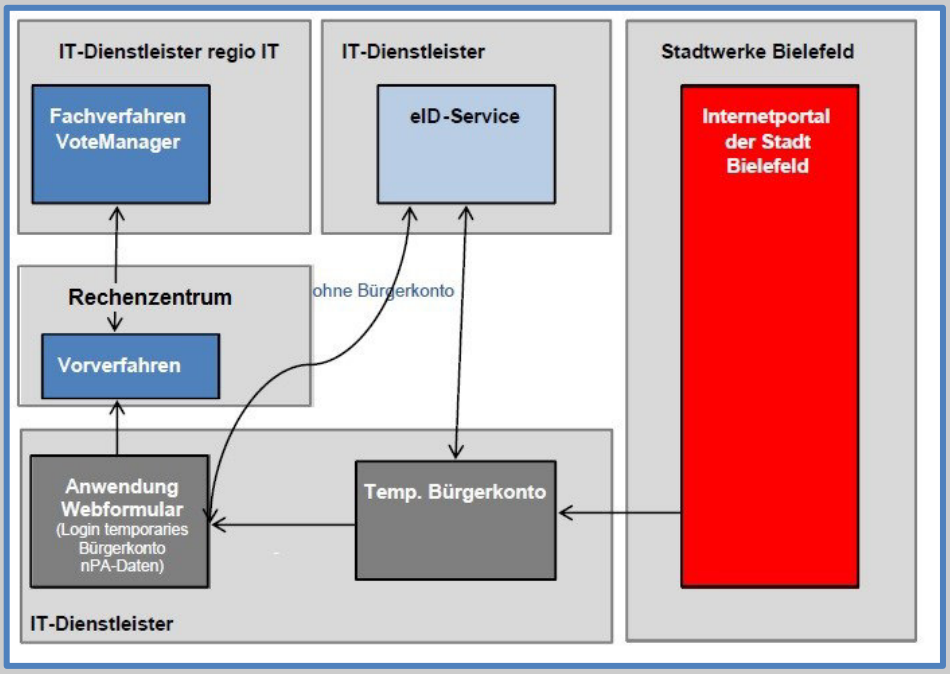


Abbildung 9: Praxisbeispiel Stadt Bielefeld

Quelle: Konzept der Stadt Bielefeld, Ergebnis der E-Government-Initiative, www.personalausweisportal.de, Bereich Downloads.

Die bei der Authentifizierung erzeugten und übermittelten Daten sollten in geeigneter Form dokumentiert und abgelegt werden. Dies ist insbesondere von Relevanz, wenn die Online-Ausweisfunktion im Rahmen des Schriftformersatzes genutzt wird. Dazu werden die Formulardaten vom Formularserver an das Fachverfahren übermittelt.

An dieser Stelle gibt es für die Behörde zwei Varianten, die zur Weiterverarbeitung und Archivierung der Daten in Frage kommen. Für beide Varianten gilt, dass nicht nur die von den Bürgerinnen und Bürger gemachten Angaben Teil der Archivierung sind, sondern auch der Bezug zu dem befüllten Formular mit seinen einzelnen Formularfeldern gewährleistet sein muss.[28]

[28] Siehe dazu auch technische Richtlinie, TR-03107-2, des BSI, www.bsi.bund.de, Bereich Themen – Elektronische Ausweise.

Variante 1: Organisatorische Sicherungsmaßnahmen

Die Behörde speichert die Identitäts-und Formulardaten als zusammengehörigen Datenbankeintrag im Fachverfahren. Die Integrität des Fachverfahrens wird über die Umsetzung des Sicherheitskonzepts der Behörde gesichert und sorgt so dafür, dass die logische Zusammengehörigkeit der Daten erhalten bleibt. Die Integrität der Erklärung lässt sich Dritten (auch Gerichten) gegenüber nur durch den Nachweis der Integrität der Behördenprozesse und des Fachverfahrens belegen. Es ist kein unabhängiger Nachweis durch Dritte möglich. Dies schränkt die Behörde zwar in Bezug auf eine einfache Nachvollziehbarkeit der Identitäts- und Formulardaten ein, senkt aber den Aufwand für die Integration.

Variante 2: Kryptographische Sicherungsmaßnahmen

Der Formularserver fasst die Identitäts- und Formulardaten in einem Datensatz zusammen und sichert diesen mit einem qualifizierten elektronischen Siegel. Alternativ hierzu kann auch eine fortgeschrittene Signatur eingesetzt werden. Diese muss, um ein angemessenes Sicherheitsniveau zu erreichen, mit einem Hardwaretoken erstellt werden. Durch die Nutzung eines Hardwaretoken wird sichergestellt, dass die Signatur unter Verwendung von zwei Faktoren (Besitz und Wissen) erzeugt wurde.
Darüber hinaus besteht die Möglichkeit, die während der Transaktion zwischen eID-Server und dem beteiligten Fachverfahren entstehenden Daten sowie die ausgelesenen Informationen mit einem „Laufzettel“ zu dokumentieren.[29] Mit Hilfe des Laufzettels kann der Nachweis erbracht werden, dass Daten aus dem Personalausweis unverändert übernommen wurden. Des Weiteren kann die Herkunft der Daten nachvollzogen werden. Der Laufzettel kann zusätzlich zur Bestätigung der Eingangszeit und zum Integritätsnachweis mit einem qualifizierten Zeitstempel versehen werden (z. B. ein PDF-Dokument).

3.7 Schritt 6: Test und Aufnahme Live-Betrieb

Nach Realisierung der vorherigen Schritte, erfolgen der Test sowie die Aufnahme des Live-Betriebs. Im Folgenden wird dargestellt, welche Test-Infrastrukturen und Anwendungsfälle zum Test der eID-Anwendung genutzt werden können und wie die Aufnahme des Live-Betriebs gestaltet werden kann.

Hat die Behörde einen eID-Service-Anbieter beauftragt, stellt dieser eine Test-Infrastruktur bereit. Dazu wendet sich die Behörde direkt an den beauftragten eID-Service-Anbieter. Betreibt die Behörde einen eigenen eID-Server, muss sie eine eigene Test-Infrastruktur aufbauen.

Für die Test-Infrastruktur wurden von der Vergabestelle für Berechtigungszertifikate beim Bundesverwaltungsamt verschiedene Berechtigungen für unterschiedliche Zwecke vordefiniert. Dazu gehören z. B. Altersverifikation, Anmeldung an ein Internetportal und Pseudonym. Die notwendigen rechtlichen Musterzertifikate werden von der Vergabestelle zur Verfügung gestellt. Entsprechend ist für die Nutzung der Test-Infrastruktur kein eigenes Berechtigungszertifikat der Behörde notwendig, sodass zunächst die technische Verbindung zwischen eID-Service-Anbieter und Infrastruktur der Behörde getestet werden kann. Besitzt eine Behörde bereits die Genehmigung der Vergabestelle für Berechtigungszertifikate für die Ausstellung eines Berechtigungszertifikats, kann sie sich auch für die

[29] Eine solche Lösung bietet z. B. die Governikus GmbH & Co. KG.

Test-Infrastruktur ein entsprechendes Zertifikat mit den genehmigten Datengruppen und Funktionen ausstellen lassen.

Das Bundesamt für Sicherheit in der Informationstechnik stellt für die Durchführung Testausweise (sogenannte Musterkarten) mit unterschiedlichen Datensätzen zur Verfügung. Die Testausweise können von den Behörden über die eID-Service-Anbieter beantragt werden. Die Übermittlung von Daten aus echten Personalausweisen ist aus rechtlichen Gründen ausgeschlossen.

Abhängig von der Art des Berechtigungszertifikats (z. B. temporäres oder permanentes Bürgerkonto) sowie des Einsatzszenarios sind verschiedene Anwendungsfälle in der Testumgebung zu testen. Unabhängig von der Art des Berechtigungszertifikats sollte immer getestet werden, ob das Übermitteln und die Übernahme der Daten aus dem Personalausweis möglich ist. Dazu empfiehlt es sich z. B. die beiden Testfälle [1] Beantragung einer Dienstleistung mit der Online-Ausweisfunktion und [2] Beantragung einer Dienstleistung mit der Online-Ausweisfunktion und Widerspruch zum Auslesen der Daten (Standardablauf) bzw. die Abwahl einzelner Datenfelder auszuführen.[30] Wenn die definierten Testfälle erfolgreich beendet wurden, erfolgt ein Abschlusstest unter Verwendung der produktiven Teilsysteme (z. B. eID-Server, Formularserver etc.).

3.8 Schritt 7: Kommunikation

Bei der Integration der Online-Ausweisfunktion in Verwaltungsdienstleistungen empfiehlt es sich, über das neue E-Government-Angebot zu informieren und dessen Nutzung durch geeignete Maßnahmen zu fördern. Durch erfolgreiche Kommunikations- und Werbemaßnahmen können die Nutzerzahlen deutlich erhöht und die Nachhaltigkeit der Einführungsinvestitionen gesichert werden.

Vor der Auswahl geeigneter Maßnahmen sind drei Zielgruppen zu unterscheiden:

1. Beschäftigte der die eID-Funktion integrierenden Fachämter oder Fachabteilungen,
2. Beschäftigte der Personalausweisbehörden, die Personalausweise ausgeben und Bürgerfragen zur Online-Ausweisfunktion beantworten,
3. Bürgerinnen und Bürger, Unternehmen bzw. die Öffentlichkeit

Die zielgruppenspezifische Ansprache sollte alle weiteren Überlegungen während der Konzeption von Kommunikations- und Werbemaßnahmen leiten. Denn die internen Adressaten – die Beschäftigten des Fachamtes oder der Fachabteilung sowie der Personalausweisbehörde – benötigen andere Informationen als die externen Adressaten – die potenziellen Nutzerinnen und Nutzer des Dienstes:

1. Den Mitarbeiterinnen und Mitarbeitern des Fachamtes oder der Fachabteilung sollten die ungewohnten Prozesse erläutert werden. Hier sollte deutlich werden, worin für sie die Vorteile des Dienstes liegen.

[30] Die Landeshauptstadt Dresden hat im Rahmen der E-Government-Initiative ein Konzept zur Umsetzung und Bereitstellung von Online-Diensten unter Nutzung der Online-Ausweisfunktion entwickelt. In diesem sind verschiedene Testfälle ausführlich beschrieben. Abzurufen unter www.personalausweisportal.de im Bereich Downloads.

2. Die Beschäftigten der Meldebehörden sollten über die Vorteile des Dienstes für die Bürgerinnen und Bürger informiert werden, damit sie die Nutzung der Online-Ausweisfunktion anhand konkreter lokaler bzw. regionaler Anwendungsmöglichkeiten vertreten und empfehlen können.
3. Bei den Bürgerinnen und Bürgern sollte der neue Dienst bekannt gemacht werden, ebenso bei der Wirtschaft. Seine Funktionsweise sollte erklärt werden und die Vorteile des Dienstes für die Nutzerinnen und Nutzer sollten überzeugend vermittelt werden.

Sind die Botschaften und Inhalte der Kommunikationsmaßnahmen für die drei Zielgruppen festgelegt, gilt es, die Anlässe zu definieren, die für die Kommunikation genutzt werden sollen. Feste Termine, wie z. B. Schulungen und Workshops, können für die Information der beiden internen Adressatengruppen genutzt werden. Die Öffentlichkeit kann z. B. bei Stadtfesten und Tagen der offenen Tür erreicht werden. Unternehmen können zudem in Kooperation z. B. mit der Handwerkskammer und der Industrie- und Handelskammer erreicht werden. Grundsätzlich ist hier zu beachten, dass nicht nur anlässlich der Bereitstellung des neuen Dienstes kommuniziert werden sollte. Mit Blick auf die nachhaltige Akzeptanz des Dienstes sollten die Maßnahmen für einen längeren Zeitraum geplant werden. Im Idealfall werden die „Bürgerdienste mit Online-Ausweisfunktion“ zu einem festen Bestandteil der behördlichen Öffentlichkeitsarbeit.

Anschließend werden die Kommunikationsmittel festgelegt, die eingesetzt werden sollen. Hierbei kann auch auf vorhandene Mittel zurückgegriffen werden. Z. B. stellt das Bundesministerium des Innern umfangreiches Material zur freien Verfügung bereit: Faltblätter, Broschüren, Plakate, Informationskarten, Filme und eigens für Anbieter von elektronischen Verwaltungsdiensten erstellte Schulungsunterlagen erläutern die Funktionsweise sowie die Vorteile der Online-Ausweisfunktion, geben anschauliche Anwendungsbeispiele aus der Praxis und vermitteln Fachwissen.[31]

Mit Blick auf die interne Zielgruppe der Mitarbeiterinnen und Mitarbeiter der Behörde können diese Informationsmaterialien z. B. verwendet werden für Leitfäden, interne Schulungen und Informationsveranstaltungen sowie Beschäftigten-Sprechstunden. Etwaigen Berührungsängsten in Bezug auf neue Technologien und Prozesse kann dadurch wirksam vorgebeugt werden.

Die Beschäftigten der Personalausweisbehörden haben den ersten und häufig einzigen direkten Kontakt mit den potenziellen Nutzerinnen und Nutzern. Von ihrer Beratungskompetenz hängt daher oft die Entscheidung der Bürgerinnen und Bürger für oder gegen die Aktivierung der Online-Ausweisfunktion maßgeblich ab. Deshalb sollte der Kommunikation mit dieser Zielgruppe besondere Aufmerksamkeit geschenkt werden. So sollten die Beschäftigen in Fragen der Unterstützung bei der Nutzung der Online-Ausweisfunktion auskunftsfähig sein. Es empfiehlt sich, Informationen bzw. Kontaktmöglichkeiten über Unterstützungsangebote für Nutzerinnen und Nutzer auszulegen. Das Informationsmaterial des Bundesinnenministeriums kann auch bei dieser Zielgruppe eingesetzt werden. Ziel sollte dabei sein, die Qualität der Beratung zu steigern und die Vorteile der Online-Ausweisfunktion so anschaulich zu erläutern, dass die Beschäftigten sie bei der Bürgerberatung überzeugend wiedergeben können. Dass

[31] Die Informationsmaterialien des Bundesinnenministeriums stehen auf www.personalausweisportal.de im Bereich Downloads zur Verfügung.

die Kommune eigene Online-Bürgerdienste mit eID-Funktion anbietet, ist ein hierbei wesentliches Argument.

Zur Erreichung der potenziellen Nutzerinnen und Nutzer des neuen Dienstes können die Informationsmaterialien des Bundesinnenministeriums z. B. verwendet werden für Pressemitteilungen, Aushänge in Personalausweisbehörden und Hinweistexte auf der Homepage. Darüber hinaus können sie für einmalige oder regelmäßige Aktionen verwendet werden, z. B. für Vorführungen des neuen Dienstes am Besucher-Terminal im Bürgerbüro, in E-Government-Sprechstunden für die Bürgerinnen und Bürger, und bei Informationsveranstaltungen für Bürgerinnen und Bürger oder Unternehmen.

Die Informationsbroschüre, die allen Bürgerinnen und Bürgern bei Beantragung eines Personalausweises ausgehändigt werden muss, kann zudem mit geringem Aufwand um ein Einlegeblatt ergänzt werden, das über die eID-fähigen Online-Bürgerdienste der örtlichen Behörden informiert. Sinnvoll sind auch Hinweise auf das neue E-Government-Angebot in den E-Mail-Signaturen des Fachamtes und der Meldebehörde.

Im Zuge dessen lohnt es sich, für Bürgerinnen und Bürger einen Rahmen zu schaffen, der sie bei der Nutzung der Online-Ausweisfunktion unterstützt. Sinnvoll ist z. B. eine Schritt-für-Schritt-Anleitung für die Verwendung der eID-Funktion mit dem entsprechenden Bürgerdienst.[32] Ebenfalls hilfreich ist die Information zu den technischen Voraussetzungen der eID-Nutzung und/oder der Hinweis auf www.personalausweisportal.de. Dort sind alle Komponenten - Software, Kartelesegeräte etc. - erläutert. Zudem werden dort E-Mail-Adresse und Telefonnummer des Bürgerservice genannt, der Fragen zur eID-Funktion beantwortet. Des Weiteren sollte auf die Unterstützungsangebote bei der Nutzung der AusweisApp2 hingewiesen werden. Auf www.ausweisapp.bund.de finden Interessierte Antworten auf häufig gestellte Fragen sowie Kontaktdaten für direkte Unterstützung per Telefon oder E-Mail.

Zusammenfassend werden folgende Schritte bei der Erstellung eines Kommunikationskonzeptes empfohlen:

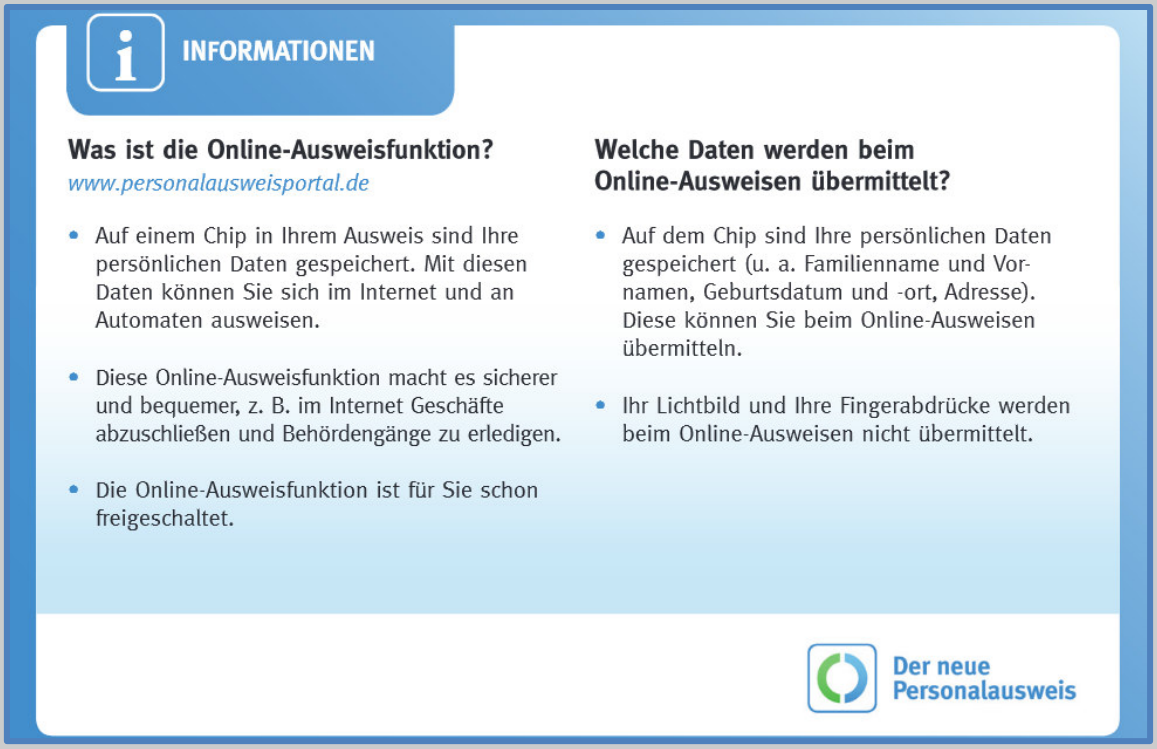
I. Festlegung der Ziele,
II. Identifizierung der Zielgruppen (intern, extern),
III. Sammlung von zielgruppenspezifischen Botschaften und Inhalte, die die konkreten Vorteile der Online-Ausweisfunktion herausarbeiten und deren praktische Anwendbarkeit in der Kommune/Behörde,
IV. Definition von zielgruppenspezifischen Kommunikationsmaßnahmen zu bestimmten Anlässen mit vorhandenen oder zu erstellenden Mitteln,
V. Kalkulation der für die Umsetzung der Maßnahmen erforderlichen finanziellen und personellen Ressourcen,
VI. Erstellung eines Plans für die zeitliche Abfolge der Kommunikationsmaßnahmen (hier sollten öffentlichkeitswirksame Termine, wie z. B. Stadtfeste, Volkshochschulkurse, Tage der offenen Tür etc. berücksichtigt werden).

[32] Das Kraftfahrt-Bundesamt hat eine solche Schritt-für-Schritt-Anleitung realisiert. Siehe dazu www.kba-online.de/faeronline/faeranfrage.do.

Praxisbeispiele für die Umsetzung von Kommunikationsmaßnahmen finden sich im Marketingkonzept der Stadt Wiesbaden sowie in dem Akzeptanzkonzept der Kreisstadt Kitzingen.[33]

Praxisbeispiel: Informationskarten des Bundesministerium des Innern

Das Bundesministerium des Innern stellt Informationskarten zum kostenlosen Download bereit. Diese beantworten die wichtigsten Fragen zur Online-Ausweisfunktion und stellen zahlreiche Anwendungen aus der Praxis vor. Das nachfolgende Beispiel gibt Auskunft über die Funktionalität der Online-Ausweisfunktion. Beschäftigte in Personalausweisbehörden können mit Hilfe dieser Antworten wesentliche Fragen der Bürgerinnen und Bürger kurz und einfach verständlich beantworten.


INFORMATIONEN

Was ist die Online-Ausweisfunktion?
www.personalausweisportal.de

- Auf einem Chip in Ihrem Ausweis sind Ihre persönlichen Daten gespeichert. Mit diesen Daten können Sie sich im Internet und an Automaten ausweisen.
- Diese Online-Ausweisfunktion macht es sicherer und bequemer, z. B. im Internet Geschäfte abzuschließen und Behördengänge zu erledigen.
- Die Online-Ausweisfunktion ist für Sie schon freigeschaltet.

Welche Daten werden beim Online-Ausweisen übermittelt?

- Auf dem Chip sind Ihre persönlichen Daten gespeichert (u. a. Familienname und Vornamen, Geburtsdatum und -ort, Adresse). Diese können Sie beim Online-Ausweisen übermitteln.
- Ihr Lichtbild und Ihre Fingerabdrücke werden beim Online-Ausweisen nicht übermittelt.

Der neue Personalausweis

Abbildung 10: Praxisbeispiel – Informationskarte Online-Ausweisfunktion

Quelle: BMI - Informationskarten zur Online-Ausweisfunktion, www.personalausweisportal.de, Bereich Downloads.

[33] Beide Konzepte stehen auf www.personalausweisportal.de im Bereich Download zur Verfügung.

3.9 Schritt 8: Evaluierung/ Erfolgsmessung des eID-Prozesses

Der Mehrwert der Integration der Online-Ausweisfunktion in einen Verwaltungsprozess sollte nach einem bestimmten Zeitpunkt, z. B. ein Jahr nach der Bereitstellung des Dienstes, evaluiert werden. Dazu sind verschiedene Vorgehensweisen möglich.

Wie bereits in Kapitel 3.4 ausgeführt, können die Optimierungen und Einsparungen sowohl vor der Integration der Online-Ausweisfunktion gemessen werden, als auch im Rahmen einer abschließenden Erfolgskontrolle. Dies ist beispielsweise mit einer Wirtschaftlichkeitsbetrachtung oder einer Messung nach dem Standardkostenmodell, SKM, möglich.

Ein weiterer Indikator für den Erfolg der Online-Ausweisfunktion ist die eID-Einschaltquote in der Kommune, in der die eID-Anwendung eingeführt wurde. Die eID-Einschaltquote sollte durch kontinuierliches Monitoring ermittelt und bewertet werden. So können auf Grundlage der Quote u.a. Rückschlüsse auf den Erfolg öffentlichkeitswirksamer Aktivitäten gezogen werden.

Ein weiterer Erfolgsindikator sind Fallzahlen zur Nutzung des neuen eID-Dienstes. Es empfiehlt sich, nicht nur schlaglichtartig, sondern kontinuierlich über einen längeren Zeitraum zu beobachten, wie viele Vorgänge mit der Online-Ausweisfunktion abgewickelt werden.

Gezielte Umfragen (online und offline) können die Evaluierung sinnvoll unterstützen. Der Informationsbedarf bestimmt hier sowohl die Auswahl der zu Befragenden, als auch die Formulierung und die Platzierung der Fragen sowie den Zeitpunkt der Umfrage. Wünschenswert sind z. B. Erkenntnisse

- zum Bekanntheitsgrad der neuen Anwendung in der Kommune,
- zu den Erfahrungen der Nutzerinnen und Nutzer des Dienstes hinsichtlich der Nutzerfreundlichkeit,
- zu den Erwartungen der Nutzerinnen und Nutzer hinsichtlich weiterer eID-Einsatzmöglichkeiten,
- zu den Erfahrungen der Mitarbeiterinnen und Mitarbeiter mit den Prozessen und
- zu den Beratungserfahrungen der Mitarbeiterinnen und Mitarbeiter in den Personalausweisbehörden.

Aus diesen Erkenntnissen können Rückschlüsse für die Weiterentwicklung der Anwendung und der Kommunikationsmaßnahmen sowie für den weiteren Ausbau der E-Government-Angebote mit Online-Ausweisfunktion gezogen werden.

4 Einsatzszenarien für die Online-Ausweisfunktion

Die Online-Ausweisfunktion ist für eine Vielzahl unterschiedlichster Einsatzszenarien in der Verwaltung geeignet, so u.a. für die Abwicklung einzelner Verwaltungsverfahren (z. B. einzelne Antragsprozesse zwischen Bürgerinnen und Bürger sowie Verwaltung) oder die Förderung der Bürger- und Mitarbeiterbeteiligung. Die hier vorgestellten Praxisbeispiele sowie viele weitere können über www.personalausweisportal.de abgerufen werden.

4.1 Einsatzszenario: Erstregistrierung und Login an einem Bürgerkonto

In immer mehr Ländern und Kommunen bestehen zentrale Bürgerkonten, bei denen die Online-Ausweisfunktion für unterschiedliche Verwaltungsdienstleistungen für Erstregistrierung und Login an einem Bürgerkonto eingesetzt wird.

So bietet beispielsweise der Freistaat Bayern mit dem Bürgerservice-Portal eine E-Government-Plattform für Kommunen. Online-Bürgerdienste können mit dem Personalausweis mit Online-Ausweisfunktion abgewickelt werden. Zurzeit haben rund 150 Kommunen und Verwaltungen das Bürgerservice-Portal in ihre Website integriert. Das Portal basiert auf einer Portalrahmen-Technologie, so können sowohl fachliche Dienste als auch Basisdienste eingebunden werden. Das Portal übernimmt mit der Online-Ausweisfunktion die Registrierungs- und Authentifizierungsfunktion des Bürgers oder der Bürgerin. Das zentrale Angebot ermöglicht auch ein Single-Sign-On zwischen den verschiedenen Bürgerservice-Portalen. So müssen sich Bürgerinnen und Bürger nur einmal für die Nutzung der verschiedenen Diensteangebote registrieren und können z. B. die Online-Angebote ihrer Heimatgemeinde, des Landkreises und des Freistaats Bayern ohne erneute Registrierung nutzen. Dieses ist aufgrund der Nutzung des gleichen Berechtigungszertifikats möglich.

Darüber hinaus bietet Rheinland-Pfalz 85 Prozent der Kommunen Bürgerdienste mit der Online-Ausweisfunktion über das landesweite Kommunal-Portal „rlpDirekt“ an. „rlpDirekt“ ist ein Portalsystem, die angeschlossenen Kommunen benötigen kein eigenes Berechtigungszertifikat. Die Bürgerinnen und Bürger können ein Bürgerkonto mit der Online-Ausweisfunktion einrichten. Zahlreiche Verwaltungsprozesse können dadurch vollständig medienbruchfrei in den kommunalen Fachverfahren bearbeitet werden. Hierbei handelt es sich um Vorgänge aus dem Bereichen Melde- und Personenstandswesen, wie z. B. das Ausstellen einer Meldebescheinigung oder Personenstandsurkunden.

In Bürgerkonten kommt häufig das dienste- und kartenspezifische Kennzeichen zum Einsatz. Dieses wird nach einer erstmaligen Registrierung an einem Dienst gespeichert (sogenanntes permanentes Bürgerkonto, vgl. Kapitel 3.5). Im Anschluss kann die Bürgerin oder der Bürger bei zukünftigen Anmeldeprozessen wiedererkannt werden. Da eine erneute Übermittlung personenbezogener Daten nicht mehr erforderlich ist, trägt das dienste- und kartenspezifische Kennzeichen in hohem Maße zur Sparsamkeit von Daten bei.

4.2 Einsatzszenario: Antragsverfahren

Der Einsatz der Online-Ausweisfunktion empfiehlt sich generell bei der elektronischen Abwicklung von Antragsverfahren. Diese wird nachfolgend an den Beispielen Beantragung von Führungszeugnissen und Auskünften aus dem Gewerbezentralregister und Gewerbeanmeldung vorgestellt.

Über das Online-Portal des Bundesamts für Justiz können mit der Online-Ausweisfunktion Führungszeugnisse beantragt werden. Neben Führungszeugnissen können auch Auskünfte aus dem Gewerbezentralregister beantragt werden. Solche Auskünfte benötigen häufig Unternehmen, die sich in Ausschreibungsverfahren um öffentliche Aufträge bewerben. Das Online-Portal wird am Computer gestartet und die Daten des Personalausweises oder des elektronischen Aufenthaltstitels werden über die Online-Ausweisfunktion übermittelt. Auf diese Weise kann eindeutig identifiziert werden, wer den Antrag stellt.

Das Bundesamt für Justiz bietet die Bezahlung mit Kreditkarte oder durch Überweisung an. Das Online-Portal ist an allen Wochentagen rund um die Uhr verfügbar. Hierdurch entstehen keine Warteschlangen oder keine Beschränkungen durch Öffnungszeiten. Der Gang zur Behörde kann damit entfallen.

Die Stadt Bonn bietet als Online-Dienstleistung den Prozess der Gewerbean-, ab- und ummeldung mit Online-Ausweisfunktion an. Vor der Integration der eID-Funktion in das Fachverfahren wurde eine Machbarkeitsstudie erstellt. Die Projektverantwortlichen stellten sicher, dass alle zur Auswahl angebotenen Rechtsformen verarbeitet werden und insbesondere die Plausibilitäts- und Abhängigkeitsprüfungen der Formularfelder den fachlichen Anforderungen entsprechen. Gemäß Gewerbeordnung besteht für Gewerbemeldungen kein Schriftformerfordernis.

Die Stadt Bonn besitzt ein Berechtigungszertifikat für ein temporäres Bürgerkonto, sodass Ausweisdaten für Gewerbemeldungen auch ohne dauerhafte Registrierung übermittelt werden können. Diese übermittelten Daten werden gelöscht, sobald die Gewerbedaten an das Fachverfahren übergeben werden.

4.3 Einsatzszenario: E-Partizipation

E-Partizipation umfasst internetgestützte Verfahren, die eine Beteiligung von Bürgerinnen und Bürgern an politischen Entscheidungsprozessen ermöglichen. Durch den Einsatz dieser Verfahren werden politische Entscheidungen verständlicher und damit besser akzeptiert. Die Online-Ausweisfunktion kann für eine elektronische Überprüfung genutzt werden, die sicherstellt, dass die Person nur einmal an einem Entscheidungsprozess teilnimmt. Dadurch entfällt der aufwändige papierbasierte Abgleich mit Wählerlisten. Nachfolgend werden drei Praxisbeispiele für E-Partizipation mit Online-Ausweisfunktion vorgestellt.

Der Deutsche Bundestag betreibt seit 2008 ein elektronisches Petitionsportal (ePetition-Portal). Mit diesem Portal ermöglicht es der Deutsche Bundestag den Bürgerinnen und Bürgern, Bitten und Beschwerden online einzureichen und zu diskutieren. Seit Mai 2014 besteht hier die Möglichkeit der Identifizierung mit der Online-Ausweisfunktion. Die Integration der eID-Funktion unterstützt die Petentinnen und Petenten beim Einreichungs- und Mitzeichnungsprozess. Zudem wird die Eingabe und Aktualisierung von Registrierungsdaten und die Anmeldung erleichtert.

Das Projekt wurde in mehrere Schritte unterteilt. Dazu gehörten eine Planungsphase, eine technische Konzeptionsphase, eine Realisierungsphase sowie eine Testphase. Im Rahmen der Planungsphase wurde die Eignung der Online-Authentisierung für zwei Anwendungsfallgruppen ausgewählt. Dies waren zum einen Anwendungsfälle, die keine Speicherung der personenbezogenen Daten erfordern und zum anderen Anwendungsfälle, die einer dauerhaften Speicherung der personenbezogenen Daten auf dem ePetition-Portal bedürfen. So gibt es Anwendungsfälle, für die kein Benutzerkonto notwendig ist, da die Daten, die während der Online-Authentisierung ausgelesen werden, direkt im Prozess genutzt und anschließend sofort gelöscht werden. Für die anderen Anwendungsfallgruppen wird ein Benutzerkonto benötigt, da die ausgelesenen Daten der Petentin bzw. des Petenten gespeichert werden müssen. Auf Grundlage dieser Unterscheidung wurden vier Funktionalitäten in das Portal integriert, die die Nutzung der Online-Ausweisfunktion unterstützen:

- Einreichen einer Einzelpetition am ePetition-Portal (ohne Benutzerkonto)
- Einreichen einer Petition zur Veröffentlichung (mit Benutzerkonto),
- Mitzeichnen einer Petition (mit Benutzerkonto),
- Diskussion einer Petition (mit Benutzerkonto).

Durch die Nutzung der Online-Ausweisfunktion erwartet der Deutsche Bundestag vor allem einen politischen Mehrwert, da die Bürgerinnen und Bürger Einzelpetitionen leichter einreichen können und Petitionen einfacher mitzeichnen oder diskutieren können. Die Mitarbeiterinnen und Mitarbeiter im Sekretariat des Petitionsausschusses profitieren durch die Integration der Online-Ausweisfunktion bei der internen Petitions- und Forenbearbeitung.

Im Land Berlin hat das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) die Nutzung der Online-Ausweisfunktion im Rahmen von Volksbefragungen geprüft. Dafür analysierte das LABO im Rahmen einer Machbarkeitsstudie, welche Wahl- und Abstimmungsprozesse mit Hilfe der Online-Ausweisfunktion optimiert werden können. Damit verbunden war die Grobkonzeption einer begrenzten Auswahl von Prozessen, die den größten Nutzen für Verwaltung sowie Bürgerinnen und Bürger versprechen. Der Einsatz der Online-Ausweisfunktion wurde anhand von zehn Wahl- bzw. Abstimmungsprozessen untersucht. Dabei stellte sich heraus, dass vor allem fünf Prozesse zur Unterschriftensammlung von der Integration der Online-Ausweisfunktion profitieren können. Dazu gehörten die Unterschriftensammlung bei Volksinitiativen, Volksbegehren, Einwohnerantrag, Bürgerbegehren und Kandidaten. Die Anwendung soll den Bürgerinnen und Bürgern die Partizipation an Entscheidungsprozessen erleichtern, da sie Zeit und Aufwände sparen. Zudem können die Daten medienbruchfrei bearbeitet und somit Ressourcen des Landes Berlin gespart werden.

In der Stadt Wiesbaden haben Bürgerinnen und Bürger die Möglichkeit, ihre Briefwahlunterlagen online mit ihrer Online-Ausweisfunktion zu bestellen. Das Bürgeramt Wiesbaden erwartet einen hohen Nutzen von der Einführung dieser Online-Dienstleistung, da die Bestellung von Briefwahlunterlagen dadurch deutlich schneller und effizienter abgewickelt werden kann.

4.4 Einsatzszenario: Zugang zu einem internen Portal

Der Einsatz der Online-Ausweisfunktion erlaubt eine sichere Authentifizierung zur Anmeldung an internen Portalen von Behörden. Im nachfolgenden Praxisbeispiel wird das Mitarbeiterportal der Senatsverwaltung für Finanzen des Landes Berlin vorgestellt, das die Online-Ausweisfunktion für einen sicheren externen Anmeldeprozess integriert hat.

Im Rahmen ihres behördeninternen Programms „ audit berufundfamilie“ verfolgt die Senatsverwaltung für Finanzen des Landes Berlin das Vorhaben, einen gesicherten Zugang zum personifizierten Beschäftigtenportal der Senatsverwaltung im Berliner Landesnetz über das Internet bereitzustellen. Der sichere Zugang soll dabei mit der Online-Ausweisfunktion erfolgen.

Den Beschäftigten der Senatsverwaltung für Finanzen soll ein externer Zugang mit höchster IT-Sicherheit zu den Inhalten im Intranet (Beschäftigtenportal) angeboten werden. Die IT-Sicherheit soll in der Pilotphase mit einem zweifachen Authentifizierungsverfahren gewährleistet werden. Die erste Stufe beinhaltet die Online-Ausweis-Funktionalität. Durch Anmeldung mit dem Personalausweis und Eingabe der dazugehörigen PIN-Nummer wird die erste Authentifizierungsstufe durchgeführt. In der zweiten Stufe erfolgt die benutzerspezifische Portalanmeldung durch Eingabe von Benutzername und Kennwort. Bisher existieren keine webbasierten Lösungen, die einen Zugang in das Landesnetz erlauben. Eine direkte einstufige Anmeldung am Portal nach Authentifizierung mit der Online-Ausweis-Funktion wird grundsätzlich nicht ausgeschlossen, soll in einem ersten Schritt während der Pilotphase jedoch noch nicht realisiert werden.

Zur Integration der Online-Ausweisfunktion in den neuen Zugangskanal des Beschäftigtenportals wurden die inhaltlichen Prozesse und technischen Erfordernisse erhoben, bewertet und in die neue Lösung zu überführt. Dabei waren auch auf Seiten der Portalsoftware entsprechende technische und fachliche Anpassungen durchzuführen.

Von der neuen Anwendung erwartet die Senatsverwaltung für ihre Mitarbeiterinnen und Mitarbeiter einen verbesserten Zugang zu Informationen und eine effizientere Kommunikation. Der Zugang zum Beschäftigtenportal von zu Hause aus soll die Vereinbarkeit von Beruf und Familie stärken. Mit dem erweiterten Zugang zur Wissensplattform „Beschäftigtenportal“ sollen zudem die Prozesse innerhalb der Verwaltung beschleunigt werden und zu verbesserten Ergebnissen durch schnelle und direkte Beteiligung aller Kompetenzträger führen.

Bürgerinnen und Bürger sowie Unternehmen profitieren dabei von einer Verbesserung der Leistungsfähigkeit der Verwaltung, indem die internen Abläufe in der Verwaltung optimiert werden und eine breite Wissensbasis die bestmögliche Bearbeitung eines Anliegens ermöglicht.

Im Rahmen der Umsetzung des Vorhabens wurden zunächst die notwendigen Prozesse inhaltlich unter Berücksichtigung der Online-Ausweisfunktion konzipiert. Auf dieser Basis erfolgte die technische Konzeption und Erstellung des IT-Sicherheitskonzeptes. Im Anschluss an die Konzeptionsphase wurde die neue Anwendung einem Testverfahren unterzogen und in den Echtbetrieb überführt.

Über geeignete kommunikative Maßnahmen wird sichergestellt, dass den Mitarbeitern diese Möglichkeit des Zugangs per Online-Ausweisfunktion bekannt gemacht wird. Folgende Maßnahmen sind zur Bekanntmachung und Nutzung des Verfahrens vorgesehen bzw. in Prüfung:

- Innerhalb der Senatsverwaltung für Mitarbeiterinnen und Mitarbeiter: Newsletter, Mitarbeiterversammlung, Rundmail an alle Mitarbeiterinnen und Mitarbeiter, Aufstellen eines Terminals zum "Ausprobieren" inkl. Angebot des eID-Szenarios "Selbstauskunft" zum Lesen der eigenen Daten auf dem Personalausweis.
- Angebot der Behörde, die Kosten zur Beantragung eines neuen Personalausweises mit freigeschalteter eID-Funktion bzw. zur nachträglichen Freischaltung behördenseitig für die Mitarbeiterinnen und Mitarbeiter zu übernehmen.
- Für Externe (Medien, Mitarbeiterinnen und Mitarbeiter der gesamten Berliner Landesverwaltung): Pressemitteilung/ Pressekonferenz, Fachartikel in E-Government-Medien, Fachartikel in Hauszeitungen der Berliner Verwaltung, Landesweiter Newsletter, Informationen in den sozialen Medien

Im Rahmen der Kommunikation wird u.a. ein Leitfaden erstellt, verteilt und im Beschäftigtenportal veröffentlicht, mit dem die Beschäftigten erfahren, was sie bei der Nutzung ihrer Online-Ausweisfunktion beachten sollten, wie das Verfahren abläuft und an wen sie ggf. ihre Fragen richten können.

4.5 Einsatzszenario: Beantragung von Fördermitteln

Die Online-Ausweisfunktion bietet sich auch für die Beantragung von Fördermitteln an. Auf diese Weise kann eine sichere Authentifizierung der Antragstellenden erfolgen. Häufig erfolgen diese Prozesse noch papierbasiert. Der Einsatz der Online-Ausweisfunktion erlaubt hier eine vollständige medienbruchfreie elektronische Abwicklung des Antragsprozesses. Dabei ist zu berücksichtigen, dass die Europäische Kommission unter dem Vorhaben e-Cohesion bis zum 31.12.2015 die elektronische Abwicklung von Fördermitteln des Europäischen Strukturfonds vorsieht. Im Nachfolgenden wird die Beantragung von Fördermitteln mit der Online-Ausweisfunktion bei der Berliner Investitionsbank (IBB) vorgestellt.

Die IBB plant die Einführung eines Kundenportals zur elektronischen Beantragung von Förderungen, Krediten und anderen Produkten. Das Kundenportal soll über eine Postbox-Funktion verfügen und den elektronischen Daten- und Dokumentenaustausch ermöglichen. Die IBB strebt an, alle Prozesse elektronisch mit der eID-Funktion zu unterstützen. Dadurch sollen die Nutzerinnen und Nutzer sich sicher registrieren, anmelden und Produkte beantragen können. Zugleich wird der IBB eine durchgehend elektronische Bearbeitung der Anträge ermöglicht.

Die IBB erwartet durch die Einbindung der Online-Ausweisfunktion medienbruchfreie und schlankere Prozesse sowie verkürzte Bearbeitungszeiten. Die Kundinnen und Kunden werden unabhängig von den Öffnungszeiten und können sich die Anfahrtswege in die Bank ersparen.

Die IBB strebt an, ihren Kunden eine möglichst einfache und komfortable Erstellung von Förderanträgen auch auf elektronischem Weg zu ermöglichen. Nachdem die IBB-internen Verfahren bereits auf elektronische Aktenführung umgestellt wurden, soll die elektronische Antragsbearbeitung jetzt auch zu

den Kunden hin erweitert werden. Dazu wird ein Kundenportal eingerichtet, das perspektivisch der Antragstellung, der Kundenkommunikation und der Abwicklung von Fördermaßnahmen dienen soll. In diesem Zusammenhang soll Kunden die Möglichkeit geboten werden, sich auch auf elektronischem Wege mit Hilfe der Online-Ausweisfunktion zu legitimieren. Hierzu ist die Einbindung der Ausweisfunktion in das neue Kundenportal erforderlich.

Zielsetzung ist ein Verfahren, das sowohl eine elektronische Antragstellung wie auch einen authentifizierten elektronischen Daten- und Dokumentenaustausch ermöglicht. Dabei soll die Online-Ausweisfunktion zur Legitimation genutzt werden können. Die bisherigen Möglichkeiten zur Legitimation (persönliches Erscheinen und PostIdent) werden weiterhin unterstützt.

Zunächst ist ein Pilotverfahren umzusetzen, das sich auf folgende Kernthemen beschränkt:

- Unterstützung jeweils eines Förderprogrammes aus der Wirtschafts- und Immobilienförderung
- Elektronische Legitimation des Kunden mit Hilfe der Online-Ausweisfunktion des Personalausweises (neben den bisherigen Legitimationsformen)
- Unterstützung von Kunden mit bis zu zehn persönlichen Mitantragstellern

Im weiteren Verlauf wird das elektronische Antragsverfahren auf die neue Förderperiode der Europäischen Union ausgeweitet und soll für alle Förderungen im Europäischen Fonds für regionale Entwicklung zum Einsatz kommen. Abschließende Zielsetzung ist die elektronische Antragsstellung für alle Produkte, die die IBB im Rahmen ihres Geschäftsauftrages anbietet.

Das Fachverfahren zur Antragstellung und zur elektronischen Kommunikation präsentiert sich dem Kunden in Form eines Internet-Portals („IBB-Kunden-Portal“). Der Zugang zum Portal erfolgt über Verweise („Links“) im Internet-Auftritt der IBB. Die elektronische Antragstellung erfolgt mit Hilfe der bisher in der IBB genutzten PDF-Formulare sowie durch Upload von Anlagen zum Antrag.

4.6 Einsatzszenario: Bürgerterminal

Terminallösungen bieten den Bürgerinnen und Bürgern die Möglichkeit, Verwaltungsdienstleistungen als Self Service zu nutzen. Hierüber können verschiedene Dienstleistungen angeboten werden. Es empfiehlt sich, den Bürgerterminal mit einem geeigneten Kartenlesegerät (z. B. Lesegeräte mit PIN Pad) auszustatten und die Online-Ausweisfunktion zu integrieren, um die Identität der Antragstellerin bzw. des Antragstellers anhand der eID-Funktion sicher prüfen zu können. Nachfolgend werden vier Bürgerterminals aus verschiedenen Bundesländern vorgestellt.

Das Land Bremen nutzt Bürgerterminals zur Abwicklung häufig anfallender Behördenvorgänge. Durch die Selbstbedienung werden die Mitarbeiterinnen und Mitarbeiter entlastet. Denn mit Hilfe der Bürgerterminals können Behördengänge via Terminal angeboten werden. Auch vorbereitende Arbeiten können von den Bürgerinnen und Bürgern erledigt werden. Beides führt zu einer erheblichen Entlastung der Behörden. Zudem werden Wartezeiten, gerade zu Stoßzeiten, gesenkt. In Bremen wurden ein Datenschutzkonzept für das Bürgerterminal sowie ein Personalkonzept mit Schulungsunterlagen und Anleitungsmaterial für die Betreuerinnen und Betreuer der Terminals erstellt.

Im Freistaat Sachsen wird im Projekt „Mobile Bürgerservices und Bürgerterminals als Bestandteil moderner Bürgerdienste im ländlichen Raum“ mit elf kommunalen Vertretern aus Städten, Gemeinden und Landkreisen der Nutzen mobiler Bürgerservices mit verschiedenen Anwendungsszenarien in der Praxis erprobt. Eine Umsetzungsvariante ist das Bürgerterminal, das an verschiedenen, publikumsnahen Orten innerhalb einer Region aufgestellt wird. Es ermöglicht Bürgerinnen und Bürgern, über eine Videokonferenz mit Sachbearbeiterinnen und Sachbearbeitern der zuständigen Verwaltung in Kontakt zu treten. Das Bürgerterminal ist mit einem Drucker, einem Scanner und einem Komfort-Kartenlesegerät ausgestattet. Dieses Kartenlesegerät soll zur eindeutigen Identifizierung per Online-Ausweisfunktion eingesetzt werden. Den Verwaltungsmitarbeiterinnen und -mitarbeitern wird es dadurch möglich, die Bürgerin bzw. den Bürger auch im Rahmen der Videokonferenz eindeutig zu identifizieren. Die Behörde kann somit ihren Bürgerservice erweitern und Bürgeranliegen medienbruchfrei bearbeiten. Die Bürgerinnen und Bürger können einen neuen orts- und zeitunabhängigen Zugangskanal zur Verwaltung nutzen – ohne lange Anfahrtswege und Wartezeiten.

In der Landeshauptstadt München sollen zukünftig Bürgerterminals aufgestellt werden. Die Bürgerinnen und Bürger können an den Terminals die Online-Angebote der Stadt München nutzen, insbesondere das Bürgerservice-Portal mit zahlreichen E-Government-Dienstleistungen. Integrierte Kartenlesegeräte ermöglichen den Einsatz der Online-Ausweisfunktion.

5 Glossar

AusweisApp2

Die AusweisApp2 ist eine Software, die die Kommunikation zwischen dem Personalausweis und dem Diensteanbieter (bzw. dessen eID-Service) übernimmt. Die AusweisApp wird kostenfrei zur Verfügung gestellt.

Authentisierung

Eine Authentisierung ist das Versehen einer Identität oder anderer übermittelter Daten mit Metadaten, die es einer vertrauenden Person oder Organisation (z.B. Bürgerinnen/Bürger, Diensteanbieter oder Websiten) ermöglichen, die Herkunft, Echtheit und Gültigkeit der Identität oder der Daten zu überprüfen.

Authentifizierung

Eine Authentisierung mit der Online-Ausweisfunktion ermöglicht es, die Herkunft, Echtheit und Gültigkeit der Identität oder der Daten zu überprüfen. Der Überprüfungsvorgang wird als Authentifizierung der Identität bezeichnet.

Berechtigungszertifikat

Ein Berechtigungszertifikat stellt sicher, dass ein Diensteanbieter die Erlaubnis hat, auf die Daten des Personalausweises zuzugreifen. Dort wird genau festgelegt, um welche Datenfelder es sich handelt. Der Diensteanbieter weist über das Berechtigungszertifikat dem Nutzer seine Identität nach. Ein rechtliches Berechtigungszertifikat kann bei der Vergabestelle für Berechtigungszertifikate beantragt werden. Die Zertifikate sind in ihrer Gültigkeit beschränkt. Die technischen Berechtigungszertifikate haben eine Gültigkeit von bis zu 30 Tagen. Diese werden über den eID-Server automatisiert erneuert.

Bürgerkonto

Bei einer eID-Integration wird unter dem Begriff „Bürgerkonto“ ein Geschäftszweck für die Beantragung eines Berechtigungszertifikats verstanden. Es besteht ein „temporäres Bürgerkonto“, die Daten werden hier für eine bestimmte Verwaltungsdienstleistung verwendet und danach gelöscht. Das „permanente Bürgerkonto“ sieht eine Speicherung der Daten vor, die für weitere Verwaltungsdienstleistungen genutzt werden können.

eCard-API-Framework

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 die des neuen Personalausweises.

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

Der so genannte eID-Service eines beauftragten externen Dienstleisters (siehe dazu auch **eID-Serviceanbieter**), der für mehrere Dienste einen mandantenfähigen eID-Server betreibt, ist eine Möglichkeit sich als Diensteanbieter an die Infrastruktur anzubinden. Auch in diesem Fall ist der Diensteanbieter der Inhaber des Berechtigungszertifikats und damit für die Einhaltung sämtlicher Vorgaben und Anforderungen im eigenen Haus sowie im Falle der Aufgabenübertragung an einen Dritten vollständig verantwortlich.

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.

PACE

PACE (Password Authenticated Connection Establishment): Das zur Eingabe der PIN verwendete Protokoll dient dem Aufbau eines verschlüsselten und integritätsgesicherten Kanals zwischen dem lokalen Kartenlesegerät und dem kontaktlosen Chip.

Dienste- und kartenspezifisches Kennzeichen (DKK)

Das Dienste- und kartenspezifische Kennzeichen (DKK) stellt als einen Anwendungsfall das Wiedererkennen eines Benutzers nach erfolgreicher Erstregistrierung sicher. Das DKK 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.

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.

6 Begleitdokumente

6.1 Rechtliche Grundlagen

6.1.1 Bundesgesetze und Verordnungen

E-Government-Gesetz	http://www.gesetze-im-internet.de/bundesrecht/egovg/gesamt.pdf
Personalausweisgesetz (PAuswG)	http://www.gesetze-im-internet.de/pauswg/BJNR134610009.html
Personalausweisverordnung	http://www.gesetze-im-internet.de/bundesrecht/pauswv/gesamt.pdf
Personalausweisgebührenverordnung	http://www.gesetze-im-internet.de/pauswgebv/

6.1.2 Verwaltungsverfahrensgesetze des Bundes und der Länder

Verwaltungsverfahrensgesetz des Bundes	http://www.gesetze-im-internet.de/bundesrecht/vwvfg/gesamt.pdf
Verwaltungsverfahrensgesetz Baden-Württemberg	http://www.landesrecht-bw.de/jportal/?quelle=jlink&query=VwVfG+BW&max=true&aiz=true
Verwaltungsverfahrensgesetz Bayern	http://www.gesetze-bayern.de/jportal/portal/page/bsbayprod.psml?showdoccase=1&doc.id=jlr-VwVfGBYrahmen&doc.part=X
Verwaltungsverfahrensgesetz Berlin	http://www.berlin.de/imperia/md/content/balichtenberghohenschoenhausen/gesetze-vorschriften/vwvfg.pdf?start&ts=1252316464&file=vwvfg.pdf
Verwaltungsverfahrensgesetz Brandenburg	http://www.bravors.brandenburg.de/sixcms/detail.php?gsid=land_bb_bravors_01.c.48287.de
Verwaltungsverfahrensgesetz Bremen	https://bremen.beck.de/?bcid=Y-100-G-brvwvfg-name-inh
Verwaltungsverfahrensgesetz Hamburg	http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&doc.id=jlr-VwVfGHArahmen
Verwaltungsverfahrensgesetz Hessen	http://www.datenschutz.hessen.de/hvwvfg.htm
Verwaltungsverfahrensgesetz Mecklenburg-Vorpommern	http://www.landesrecht-mv.de/jportal/portal/page/bsmvprod.psml?showdoccase=1&st=lr&doc.id=jlr-VwVfGMV2014rahmen&doc.part=X&doc.origin=bs
Verwaltungsverfahrensgesetz Niedersachsen	http://www.lexsoft.de/cgi-bin/lexsoft/niedersachsen_recht.cgi?chosenIndex=Dummy_nv_6&xid=147043,2
Verwaltungsverfahrensgesetz Nordrhein-Westfalen	https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=2&gld_nr=2&ugl_nr=2010&bes_id=4844&aufgehoben=N&menu=1&sg=0
Verwaltungsverfahrensgesetz Rheinland-Pfalz	http://landesrecht.rlp.de/jportal/?quelle=jlink&query=VwVfG+RP+%C2%A7+1&psml=bsrlpprod.psml
Verwaltungsverfahrensgesetz Saarland	http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/VwVfG_SL_rahmen.htm
Verwaltungsverfahrensgesetz Sachsen	https://beck-online.beck.de/?bcid=Y-100-G-SaVwVfG

Verwaltungsverfahrensgesetz Sachsen-Anhalt	http://www.landesrecht.sachsen-anhalt.de/jportal/?quelle=jlink&query=VwVfG+ST&psml=bssahprod.psml&max=true&aiz=true
Verwaltungsverfahrensgesetz Schleswig-Holstein	http://www.gesetze-rechtsprechung.sh.juris.de/jportal/portal/t/39g/page/bsshoprod.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=448&fromdoctodoc=yes&doc.id=jlr-VwGSHrahmen%3Ajuris-lr00&doc.part=X&doc.price=0.0&doc.hl=1
Verwaltungsverfahrensgesetz Thüringen	http://landesrecht.thueringen.de/jportal/?quelle=jlink&query=VwVfG+TH&psml=bsthueprod.psml&max=true&aiz=true

6.1.3 Technische Richtlinien

BSI TR-03112 Das eCard-API-Framework	https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03112/index_htm.html
BSI TR-03130 eID-Server	https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03130/tr-03130.html
BSI TR-03107 Elektronische Identitäten und Vertrauensdienste im E-Government	https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html
BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen	https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
BSI TR-03104 Produktionsdatenerfassung, -qualitätsprüfung und Übermittlung für hoheitliche Dokumente	https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03104/index_htm.html
BSI TR-03107-2 Elektronische Identitäten und Vertrauensdienste im E-Government	https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html
BSI TR-03127 Architektur Elektronischer Personalausweis	https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03127/tr-03127.html

6.2 Steckbriefe - Zentrale eID-Strukturen in den Ländern

6.2.1 Baden-Württemberg

1. Land	Baden-Württemberg
2. Zuständige Stelle	Innenministerium
3. Bezeichnung des Angebots	www.service-bw.de, dort „mein service-bw“
4. Beschreibung des Angebots	Permanentes Bürgerkonto mit Kernfunktionalitäten: • Dokumentensafe • Sichere Behördenkommunikation • Passwortsafe • Online-Verfahren zur Umsetzung der EU-DLR (Selbständigkeit Online) • Zentrales Identitätsmanagement für Fachverfahren des Landes • Temporäre Identifikationsabwicklung für Fachverfahren im Land
5. Beschreibung technische Infrastruktur	Zentrale Datenbankanwendung mit hoher, individueller Verschlüsselung der Bürgerdaten. Bereitstellung des Zertifikats über mtG/noris und T-TeleSec
6. Services bei Nutzung der Infrastruktur	Entwicklung und Betrieb in Generalunternehmerschaft für service-bw durch T-Systems.
7. Berechtigungszertifikate	Registrierung / Login "mein service-bw" Die Berechtigung ist erteilt für: Innenministerium Baden-Württemberg Postfach 103465 70029 Stuttgart poststelle@im.bwl.de
8. Nutzen	Behörden und Bürger profitieren von der sicheren und verschlüsselten serverbasierte Kommunikation sowie der Abwicklung von durchgängig elektronischen Verfahren mit der Möglichkeit der Anbindung von Fachverfahren. Behörden profitieren davon, dass Sie nicht in eigene e-ID-Lösungen investieren müssen, sondern eine zentral bereitgestellte Komponente nutzen können.
9. Bsp. für angebundene Verfahren/Systeme	Als Fachverfahren sind der Service „Selbständigkeit online“ und die Landesoberkasse für sichere Bescheid-Verteilung unter Nutzung des Dokumentensafes angebunden.
10. Besonderheit des Ansatzes	Im Rahmen des Projektes „Trusted Link“ wurde im Jahr 2013 ein erfolgreiches Projekt zwischen den Portalen service-bw.de und help.gv.at durchgeführt. Inhaber der österreichischen eID (Anmeldekomponente mit

	Handysignatur) konnten sich damit in „mein service-bw“ automatisch identifizieren und im Bürgerkonto Baden-Württemberg verfügbare Online-Dienste nutzen
11. Beschreibung der geplanten Erweiterungen / Ausbaustufen	Nach der Neuentwicklung von service-bw mit Produktionsbeginn Anfang 2016 soll die eID-Komponente als Basis-Service-Komponente zur Einbindung in Fachverfahren und Anwendungen des Landes und der Kommunen standardmäßig bereitgestellt werden.
12. Ansprechpartner	Stephan Jaud / Frank Schiele, (0711) 231-3520 / (0711) 231-3516, Stephan.Jaud@im.bwl.de / Frank.Schiele@im.bwl.de

6.2.2 Bayern

1. Land	Bayern
2. Zuständige Stelle	Bayerisches Staatsministerium der Finanzen, für Landesentwicklung und Heimat
3. Bezeichnung des Angebots	Zentrales Bürgerkonto
4. Beschreibung des Angebots	Registrierung und Identifizierung von Bürgerinnen und Bürgern über Username/Password oder die eID-Funktion des neuen Personalausweises
5. Beschreibung technische Infrastruktur	Das Bürgerkonto basiert auf dem Bürger-Serviceportal der AKDB.
6. Services bei Nutzung der Infrastruktur	Betrieb, Unterstützung der User
7. Berechtigungszertifikate	Je ein zentrales Zertifikat für ein permanentes und ein temporäres Bürgerkonto
8. Nutzen	Elektronisch identifizierter Zugang zu allen Online-Verwaltungsleistungen aller staatlicher Stellen und aller Kommunen über ein Bürgerkonto.
9. Bsp. für angebundene Verfahren/Systeme	Aktuell an das Bürgerkonto angebunden sind die kommunalen Online-Verfahren der AKDB.
10. Besonderheit des Ansatzes	Zugang zu allen Verwaltungsleistungen in Bayern über ein Bürgerkonto.
11. Beschreibung der geplanten Erweiterungen / Ausbaustufen	k.A.
12. Ansprechpartner	MR Dr. Andreas Mück, andreas.mueck@stmflh.bayern.de, 089 2306-3011

6.2.3 Berlin

1. Land	Berlin
2. Zuständige Stelle	Senatsverwaltung für Inneres und Sport
3. Bezeichnung des Angebots	Service-Konto Berlin (Aktueller Stand: Konzeptphase)
4. Beschreibung des Angebots	Einmalige zentrale Einrichtung eines personalisierten Online-Accounts zur Identifizierung bei allen Fachverfahren (als s.g. permanentes Bürgerkonto); Das Berliner Service-Konto wird bereits als interoperables Identitätsmanagement konzipiert, welches auch in anderen Kommunen, Ländern und beim Bund genutzt werden soll.
5. Beschreibung technische Infrastruktur	Im Planung - Wird derzeit entworfen
6. Services bei Nutzung der Infrastruktur	Im Planung - Betrieb; fachliche oder inhaltliche Beratungsunterstützung; Offenlegung der Schnittstelle;
7. Berechtigungszertifikate	Es werden zentrale und landesweit nutzbare Berechtigungszertifikate für ein temporäres Bürgerkonto und ein permanentes Bürgerkonto bereitgestellt (gemäß VITAKO-Konzept). Weitere Berechtigungszertifikate werden zentral beschafft und landesweit bereitgestellt, wenn der „Geschäftszweck“ dies erfordert
8. Nutzen	Die Behörden profitieren mit dem Bürgerkonto von einer zentralen Einrichtung eines personalisierten Online-Accounts mit offen gelegter Schnittstelle zur Anbindung aller Fachverfahren. Die Bürgerinnen und Bürger sowie Unternehmen profitieren von der Möglichkeit eines Single-Sign-On für alle Online-Dienste der Stadt Berlin
9. Bsp. für angebundene Verfahren/Systeme	Fachverfahren, die an das Bürgerkonto angebunden werden sollen, sind z. B. die „KFZ-Halterauskunft“ und „Feinstaubplakette“, die bereits mit den s.g. Temporären Bürgerkonto die eID-Funktion nutzen.. Beihilfe-Online, E-Partizipation oder Sozialhilfeportal planen bei der derzeitigen Neuerstellung die Nutzung von Beginn an ein. Weitere konkrete Fachverfahren sind derzeit noch nicht bekannt.
10. Besonderheit des Ansatzes	Juristische Personen sind neben natürlichen Personen wesentlicher Bestandteil der eingeplanten Nutzer, so dass diese Nutzergruppe von Beginn an eingeplant wird. Es wird davon ausgegangen, dass s.g. Bürgerkonten als sonstige sichere Verfahren gem. § 3a Abs. 2 Satz 4 Nr. 4 VwVfG zugelassen

	werden und somit als Formersatz Anwendung finden können.
11. Beschreibung der geplanten Erweiterungen / Ausbaustufen	Bestätigung einer juristischen Person aus externen Registern, Erweiterung der Anwendungsfälle im „Unternehmerprofil“ in Richtung Unternehmenskonto; Postfach zur Zustellung
12. Ansprechpartner	Herr Dirk Meyer-Claassen, 030-902232110 Dirk.Meyer-Claassen@seninnsport.berlin.de

6.2.4 Brandenburg

1. Land	Brandenburg
2. Zuständige Stelle	Ministerium des Innern und für Kommunales Brandenburg
3. Bezeichnung des Angebots	Temporäres Bürgerkonto Governikus/Formularserver
4. Beschreibung des Angebots	Derzeit ist das technische Berechtigungszertifikat „temporäres Bürgerkonto“ in der Pilotphase. Es ist geplant, dass ab Wirkbetrieb jede Landesbehörde und Kommune (vorausgesetzt der rechtlichen Befugnisse, Ausweisdaten auslesen zu dürfen) ein verfahrensspezifisches Berechtigungszertifikat beantragen kann, um das eID-Produkt „temporäres Bürgerkonto“ zu nutzen.
5. Beschreibung technische Infrastruktur	eID-Service Governikus/temporäres Bürgerkonto bzw. Formularserver
6. Services bei Nutzung der Infrastruktur	eID-Service Governikus, Betrieb Formularserver/Governikus Intermediär und Support
7. Berechtigungszertifikate	Temporäres Bürgerkonto/Formularserver
8. Nutzen	Formularserver als Basiskomponente des Portals „service.brandenburg.de“
9. Bsp. für angebundene Verfahren/Systeme	Derzeit wird der Prozess Beantragung nach dem Schwerbehindertenrecht pilotiert (schweb.net)
10. Besonderheit des Ansatzes	Komplett digitaler Workflow des Antrages
11. Beschreibung der geplanten Erweiterungen / Ausbaustufen	In Überlegung: Service auch für Kommunen, Einbindung De-Mail
12. Ansprechpartner	Sascha Proch,0331 866 2111, sascha.proch@mik.brandenburg.de

6.2.5 Bremen

1. Land	Bremen
2. Zuständige Stelle	Senatorin für Finanzen
3. Bezeichnung des Angebots	eBürgerSafe
4. Beschreibung des Angebots	Bürgerkonto
5. Beschreibung technische Infrastruktur	Governikus eBürgerSafe
6. Services bei Nutzung der Infrastruktur	Betrieb der Anwendung und des eID-Services
7. Berechtigungszertifikate	Bürgerkonto
8. Nutzen	Erhöhter Service für die Nutzerinnen und Nutzer
9. Bsp. für angebundene Verfahren/Systeme	Gesamte Fachverfahrenslandschaft über Governikus-Infrastruktur anbindbar
10. Besonderheit des Ansatzes	(Wahrscheinlich) der am längsten bestehende Bürgerkontoansatz, sehr geringe Einführungskosten, niedrigschwelliger Ansatz
11. Beschreibung der geplanten Erweiterungen / Ausbaustufen	Auf Nachfrage
12. Ansprechpartner	Dr. Martin Hagen, Zentrales IT-Management und E-Government, office-ref02@finanzen.bremen.de

6.2.6 Hessen

1. Land	Hessen
2. Zuständige Stelle	HMdIS VII/3
3. Bezeichnung des Angebots	Die Umsetzung des Angebots befindet sich in Vorbereitung. Eine Konkretisierung der Angaben ist derzeit noch nicht möglich.
4. Beschreibung des Angebots	Eine Konkretisierung ist derzeit noch nicht möglich.
5. Beschreibung technische Infrastruktur	Eine Konkretisierung ist derzeit noch nicht möglich.
6. Services bei Nutzung der Infrastruktur	Eine Konkretisierung ist derzeit noch nicht möglich.
7. Berechtigungszertifikate	Eine Konkretisierung ist derzeit noch nicht möglich.

8. Nutzen	Für die Behörden soll die eID-Infrastruktur den manuellen Aufwand in der Verwaltung reduzieren und Abläufe beschleunigen. Zudem entsteht ein Nutzen durch die Verbesserung in der Dokumentation der Prozesse und Geschäftsvorfälle. Bürgerinnen und Bürger profitieren von der Beschleunigung der Abläufe, der durchgängigen Erreichbarkeit der Verwaltung. Weiterhin besteht eine Wiedernutzung elektronischer Bescheide bei Folge-Anträgen.
9. Bsp. für angebundene Verfahren/Systeme	Eine Konkretisierung ist derzeit noch nicht möglich.
10. Besonderheit des Ansatzes	Eine Konkretisierung ist derzeit noch nicht möglich.
11. Beschreibung der geplanten Erweiterungen / Ausbaustufen	Eine Konkretisierung ist derzeit noch nicht möglich.
12. Ansprechpartner	Jens W. Wieltsch, 0611 353 1989, Jens.wieltsch@hmdis.hessen.de

6.2.7 Niedersachsen

1. Land	Niedersachsen
2. Zuständige Stelle	Niedersächsisches Ministerium für Inneres und Sport
3. Bezeichnung des Angebots	Bürgerkonto Niedersachsen
4. Beschreibung des Angebots	Zentraler Registrierungsdienst inklusive eID-Service zur Nachnutzung in div. Portalen und Fachverfahren, der neben dem Registrierungsverfahren über den nPA auch Registrierungen mittels Angabe der Emailadresse sowie einen eID-Service ohne Registrierung unterstützt.
5. Beschreibung technische Infrastruktur	Hinter dem Bürgerkonto verbirgt sich ein hochkomplexes zentrales Identitymanagement-system (IDM) betrieben im Rechenzentrum des Landesbetriebs IT.Niedersachsen, Basissoftware ist Quest. Das IDM tauscht über SAML Nutzerdaten mit dem eID-Service Governikus-Authent aus. Portale können das Bürgerkonto über eine Webserviceschnittstelle anschließen. Die Nutzeroberflächen können dabei nach Bedarf angepasst werden. Basisprotokoll ist SAML. Verzeichnisdienste (LDAP oder AD) können an das

	IDM angeschlossen und Identitäten übernommen werden.
6. Services bei Nutzung der Infrastruktur	Neben dem Betrieb wird ein First bis Third-Level Support bereitgestellt. Es erfolgt eine Beratung und Anbindungsunterstützung für Anbindungswillige.
7. Berechtigungszertifikate	Es können sowohl temporäre als auch permanente Berechtigungszertifikate genutzt werden.
8. Nutzen	Kommunen müssen nicht selbst einen eID-Service betreiben, sondern können auf zentrale eID-Infrastrukturen zurückgreifen. Bürgerinnen und Bürger sowie Unternehmen profitieren von der rechtssicheren Online-Abwicklung von Anträgen.
9. Bsp. für angebundene Verfahren/Systeme	Als Fach- und Antragsverfahren sind das Hunderegister, das Betreuungsgeld, das Elterngeld, iKFZ, Beurkundungen (in Planung), Bauen online sowie der kommunale Finanzausgleich an das Bürgerkonto angebunden. Des Weiteren wird auch das Dienstleisterportal Niedersachsen mit ca. 260 Antragsverfahren aus dem Bereich GewerbeO vom Bürgerkonto als Registrierungsdienst unterstützt.
10. Besonderheit des Ansatzes	Das Bürgerkonto ist hochflexibel aufgestellt, so dass es unterschiedlichen Bedarfen gerecht wird. Es ist einfach skalierbar, jede Identität zählt als eine Lizenz. Lizenzen können beliebig ergänzt werden.
11. Beschreibung der geplanten Erweiterungen / Ausbaustufen	Anschluss an einen Federationservice: Zukünftig soll es möglich sein Identitäten resp. Berechtigungen mit anderen / ähnlichen Verfahren auszutauschen.
12. Ansprechpartner	Kirsten Nax, 0511 120 4865, Kirsten.nax@mi.niedersachsen.de

6.2.8 Nordrhein-Westfalen

1. Land	Nordrhein-Westfalen
2. Zuständige Stelle	In Nordrhein-Westfalen besteht auf Ebene der Landesverwaltung aktuell noch kein übergreifendes Bürgerkonto. Auf kommunaler Ebene können die als Zweckverbände organisierten kommunalen Gebietsrechenzentren eID-Leistungen anbieten. Dadurch können sie kommunale Bürgerkonten mit integrierter eID-Funktion für ihre Mitgliedskommunen einrichten und betreiben, sodass die Bürgerkonten mit der eID-Funktion genutzt werden können. Die Kommunen selbst benötigen keine eigenen Zertifikate mehr.
3. Bezeichnung des Angebots	Zu den ersten Gebietsrechenzentren, die ihren

	Mitgliedskommunen diese Lösung anbieten, zählen die citeq in Münster (www.citeq.de) sowie das Kommunale Rechenzentrum Minden-Ravensberg / Lippe (www.krz.de).
4. Beschreibung des Angebots	Beispielsweise bietet die citeq in Münster Bürgerinnen und Bürgern verschiedene Verwaltungsleistungen mit der eID-Funktion an, z. B. Personenstandsurkunden bestellen, Wunschkennzeichen beantragen und Erklärungen zum Elterneinkommen abgeben. Ein weiteres Beispiel ist der Kreis Lippe, der in Zusammenarbeit mit dem Kommunalen Rechenzentrum Minden-Ravensberg/Lippe (krz) ein Bürgerportal anbietet, über das Eltern online ihre Einschätzung zum Elternbeitrag einreichen können
5. Beschreibung technische Infrastruktur	Informationen auf Anfrage bei den kommunalen Gebietsrechenzentren erhältlich
6. Services bei Nutzung der Infrastruktur	Informationen auf Anfrage bei den kommunalen Gebietsrechenzentren erhältlich
7. Berechtigungszertifikate	Informationen auf Anfrage bei den kommunalen Gebietsrechenzentren erhältlich
8. Nutzen	Informationen auf Anfrage bei den kommunalen Gebietsrechenzentren erhältlich
9. Bsp. für angebundene Verfahren/Systeme	Informationen auf Anfrage bei den kommunalen Gebietsrechenzentren erhältlich
10. Besonderheit des Ansatzes	Informationen auf Anfrage bei den kommunalen Gebietsrechenzentren erhältlich
11. Beschreibung der geplanten Erweiterungen / Ausbaustufen	Informationen auf Anfrage bei den kommunalen Gebietsrechenzentren erhältlich
12. Ansprechpartner	Informationen auf Anfrage bei den kommunalen Gebietsrechenzentren erhältlich

6.2.9 Rheinland-Pfalz

1. Land	Rheinland-Pfalz
2. Zuständige Stelle	KommWis für die kommunalen Spitzenverbände in RLP, sowie für das Personenstandswesen der Betriebszweckverband ZIDKOR.
3. Bezeichnung des Angebots	Online Bürgerdienste Rheinland-Pfalz Ausbaustufe 1: temporäres Bürgerkonto
4. Beschreibung des Angebots	Online Vorgänge aus den Bereichen Melde-, Personenstandswesen, Kfz-Zulassung und diverse

	Formulare (mit eID-Authentifikation).
5. Beschreibung technische Infrastruktur	RZ-Betrieb im KGRZ Koblenz. Betrieb der Komponenten für die Fachanwendungen auf virtualisierten Umgebungen. Für den Betrieb der Komponenten existieren entsprechende Sicherheitskonzepte.
6. Services bei Nutzung der Infrastruktur	Hinweistexte in den Verfahrensabläufen informieren die Anwender. Daneben steht eine Kontaktmöglichkeiten per E-Mail und Telefon zur Verfügung.
7. Berechtigungszertifikate	Es wird ein Berechtigungszertifikat von D-Trust verwendet. Der Geschäftszweck lautet: Anlegen und Nutzung eines Bürgerkontos zur Abwicklung von Online-Services im Sinne der GemO Rheinland-Pfalz.
8. Nutzen	Die Kommunen nutzen landesweit eine einheitliche eID-Infrastruktur. Diese zentrale Lösung schafft erhebliche wirtschaftliche Vorteile. Die Dienste können als Web-Service für eigene Fachverfahren eingebunden werden. Der Online-Prozess mittels Bürgerkonto erspart den Bürgerinnen und Bürgern die Vorsprache in der Kommune. Das persönliche Erscheinen des Antragsstellers kann entfallen.
9. Bsp. für angebundene Verfahren/Systeme	Fachverfahren für das Meldewesen (OLAV) Fachverfahren für das Personenstandswesen (xSta) Fachverfahren für die Kfz-Zulassung (iKfz) Formulare mit eID-Authentifikation (Formular-Server)
10. Besonderheit des Ansatzes	Da die Nutzung der eID-Funktion in einem Verwaltungsprozess nur beschränkt nachweisbar ist, wurde die Funktion eines elektronisch signierten Laufzettels implementiert, mit dem die Nutzung dokumentiert und protokolliert wird. Der Laufzettel wird an die Fachverfahren übergeben. In der nächsten Ausbaustufe werden zusätzliche Services implementiert, die die schriftformersetzende Verwendung (§ 3 a Abs. 2 Ziffer 1 VwVfG) des neuen Personalausweises in elektronischen Formularen belegen.
11. Beschreibung der geplanten Erweiterungen / Ausbaustufen	Konzeptionsphase zur Implementierung eines permanenten Bürgerkontos (Bürgerdesktop Rheinland-Pfalz) = Ausbaustufe 2.
12. Ansprechpartner	Achim Fürst, Herbert Benz, 06131/6277-268, afuerst@kommwis.de, hbenz@kommwis.de

6.2.10 Saarland

Die zentrale eID-Infrastruktur für das Land und die Kommunen im Saarland befindet sich derzeit im Aufbau. Eine Konkretisierung im Rahmen eines Steckbriefs ist derzeit noch nicht möglich.

6.2.11 Sachsen

1. Land	Freistaat Sachsen
2. Zuständige Stelle	Sächsisches Staatsministerium des Innern
3. Bezeichnung des Angebots	Zentrale Bereitstellung eines temporären Bürgerkontos und eines eID-Services.
4. Beschreibung des Angebots	Das temporäre Bürgerkonto wird technisch als Serverkomponente „Governikus Temporäres Bürgerkonto“ der Governikus KG zur Verfügung gestellt. Derzeit wird noch der der eID-Service der der Governikus KG genutzt. Später ist der Aufbau eines landeseigenen eID-Services geplant
5. Beschreibung technische Infrastruktur	Bisher steht bei Staatsbetrieb Sächsische Informatikdienste (SID) ein Testsystem des temporären Bürgerkontos zur Verfügung.
6. Services bei Nutzung der Infrastruktur	SID leistet die Anwendungsbetreuung (Betrieb, Testmanagement, Beratungsleistungen und Projektunterstützung) im Rahmen der Basiskomponente „Elektronische Signatur und Verschlüsselung“ (BAK ESV) auch für das temporäre Bürgerkonto und den eID-Service.
7. Berechtigungszertifikate	Die Landeshauptstadt Dresden nutzt das zentral bereitgestellte temporäre Bürgerkonto mit einem eigenen Berechtigungszertifikat. Mit Inkrafttreten des Sächsischen E-Government-Gesetzes gibt es ein gemeinsames Verfahren (Art. 1 § 6 Abs.2 SächsEGovG). Auf dieser Basis wird die Beantragung eines gemeinsamen Zertifikats für alle Träger der öffentlichen Verwaltung angestrebt.
8. Nutzen	Es wird erwartet, dass Behörden und Kommunen Verwaltungsprozesse schnell und vollständig, rechtssicher und elektronisch abbilden können. Bürgerinnen und Bürger profitieren von einem einfacheren und rechtssicheren elektronischer Zugang zu Verwaltungsdienstleistungen, sowie einem Zeit- und Kostenersparnis.
9. Bsp. für angebundene Verfahren/Systeme	Als Fachverfahren ist der Formularservice der Landeshauptstadt Dresden angebunden (Antragsverfahren Baumfällgenehmigung), den Bürgerinnen und Bürger nutzen können.
10. Besonderheit des Ansatzes	Serviceleistungen siehe Punkt 6. Rechtliche Rahmenbedingungen werden z. B. durch das SächsEGovG bestimmt.
11. Beschreibung der geplanten Erweiterungen / Ausbaustufen	Mittelfristig ist die Bereitstellung eines permanenten Bürgrkontos vorgesehen.
12. Ansprechpartner	Herr Karl-Heinz Walther, 0351 564 3613, karl-heinz.walther@smi.sachsen.de

6.2.12 Schleswig-Holstein

1. Land	Schleswig-Holstein
2. Zuständige Stelle	Staatskanzlei des Landes Schleswig-Holstein - Zentrales IT-Management
3. Bezeichnung des Angebots	eID-in-SH
4. Beschreibung des Angebots	Das Schleswig-Holstein-Gateway (SHGW) realisiert als Portallösung und elektronischer Basisdienst einen gleichartigen Zugang zu Online-Diensten der Landesverwaltung Schleswig-Holstein. Services, die von den nutzenden Fachverfahren benötigt werden, sind zentral für diese Fachverfahren umgesetzt und gegen unbefugte Zugriffe aus dem Internet gesichert. Dies sind z. Z.: • die Verwaltung, Identifikation (Bürger, Firmen, Behörden) und Authentifizierung der Kunden (Benutzerverwaltung) • Rollenkonzept • sichere Kommunikation zwischen Kunden und Verwaltung • die Bezahlung mit Hilfe eines Payment-Providers • die Ablage der Ergebnisse, ggf. auch der Antragsunterlagen, in einem Kunden-Postfach (Bürgerkonto) • die Zwischenspeicherung der Aufträge bei Ausfall des Fachverfahrens im Backend (asynchrone Verarbeitung).
5. Beschreibung technische Infrastruktur	Das Schleswig-Holstein-Gateway (SHGW) wurde so gestaltet, dass die Architektur wieder verwendbar und vor allem erweiterbar ist. Basierend auf Microsoft.NET, wurde das "GovernmentGateway" als zentrale Infrastruktur für Fachverfahren und andere Dienste der Behörden und Ämter des Schleswig-Holstein (Landesverwaltung und Kommunen), die webbasiert angeboten werden sollen, konzipiert. Um diese Fachverfahren und Dienste kostengünstig entwickeln zu können, werden ein einheitliches Programmiermodell, eine konsequente Ausrichtung an den Funktionalitäten des .NET Framework, die Verwendung offener Standards (HTML, XML, SOAP), Standardprodukte sowie die leistungsfähige Visual Studio.NET Entwicklungsumgebung eingesetzt
6. Services bei Nutzung der Infrastruktur	Die Infrastruktur wird von Dataport in einem BSI zertifizierten Rechenzentrum betrieben. Für den Bereich Benutzerverwaltung und E-Payment ist ein Second Level Support vorhanden. Das Portal wird mit automatisierter

	und proaktiver Überwachung.7*24 betrieben.
7. Berechtigungszertifikate	Es gibt Berechtigungszertifikate für permanente und temporäre Nutzungen.
8. Nutzen	Bürgerinnen und Bürger sowie Unternehmen profitieren von asynchronen Rückantworten der Verwaltung.
9. Bsp. für angebundene Verfahren/Systeme	Das Fachverfahren der Außerbetriebsetzung von Kraftfahrzeugen und die Anforderung von Urkunden im Standesamtswesen sind an das Bürgerkonto angebunden. Die Einbindung von Bürgerterminals ist in Planung. Daneben gibt es weitere Dienste die mit „niedrigeren“ Vertrauensniveaus genutzt werden können (z. B. Bewerberverfahren für den Schuldienst in SH, landesweite Melderisterauskunft; Fischereidokument, Geoserver; Gewerbeanzeigen; Meldeservice Heimaufsicht).
10. Besonderheit des Ansatzes	Das Schleswig-Holstein-Gateway (SHGW) ist eine komponentenbasierte skalierbare Transaktionsinfrastruktur, die einen zentralen Zugang (Single Point of Entry) für die Bereitstellung verschiedener OnlineFachverfahren und div. Services (siehe Pt. 4) bietet.
11. Beschreibung der geplanten Erweiterungen / Ausbaustufen	Das Schleswig-Holstein-Gateway (SHGW) wird jährlich über entsprechende CR’s im technischen Bereich bzw. aufgrund gesetzlicher und durch die Dienste erforderlichen Änderungen bzw. Anforderungen weiterentwickelt und angepasst.
12. Ansprechpartner	Michael Schmidtke,0431/988-2920, Michael.Schmidtke@stk.landsh.de

6.2.13 Thüringen

In Thüringen besteht aktuell kein Bürgerkonto, eine Entscheidung wurde noch nicht getroffen.

6.3 Checkliste

Schritte zur Implementierung der Online-Ausweisfunktion	Fragen	Erläuterungen zum Umsetzungsstand	Status *z. B. nicht umgesetzt, in Arbeit, umgesetzt*	Verantwortlich
1. Geeignete Verwaltungsprozesse identifizieren				
1.1 Auswahl Verwaltungsprozess(e)	Welche potenziellen Verwaltungsprozesse, in die die Online-Ausweisfunktion integriert werden kann, werden ausgewählt und bewertet?			
1.2 Rechtsgrundlagen	Sind die zugrundeliegenden Rechtsgrundlagen (z. B. Fachgesetze, Verfahrensanweisungen, Satzungen, Ermessensbereiche) geprüft?			
1.3 Formerfordernisse	Sind die bestehenden Formerfordernisse (z. B. Schriftform, Identitätsüberprüfung, „gefühlte“ Schriftform) bewertet?			
1.4 Technisches Verfahren	Sind die technischen Umsetzungsmöglichkeiten bewertet? (erfolgt z. B. bereits eine elektronische Umsetzung des Prozesses?)			
2. Soll-Prozess definieren				
2.1 Analyse beteiligter Akteure	Sind alle relevanten Akteure innerhalb und außerhalb der Behörde berücksichtigt?			
2.2 Analyse beteiligter Fachverfahren	Sind die beteiligten Fachverfahren hinreichend berücksichtigt? Bestehen Schnittstellen für den Datenaustausch?			
2.3 Festlegung benötigter Personalausweisdaten	Was sind die erforderlichen Datenfelder für den jeweiligen Geschäftsprozess? Wie lautet der Geschäftszweck?			
2.4 Erforderlichkeit begleitender Anlagen	Ist eine Überprüfung der Erforderlichkeit der Übermittlung von begleitenden Anlagen in			

Schritte zur Implementierung der Online-Ausweisfunktion	Fragen	Erläuterungen zum Umsetzungsstand	Status *z. B. nicht umgesetzt, in Arbeit, umgesetzt*	Verantwortlich
	Papierform bei der Definition des Sollprozesses erfolgt?			
2.5 Nutzung elektronischer Aktenführung	Was sind die technischen Voraussetzungen für die Nutzung elektronischer Aktenführung in der Verwaltung? Was sind die technischen Voraussetzungen für die Integration der elektronischen Aktenführung in die mit Online-Ausweisfunktion gestützten Verwaltungsprozesse?			
2.6 Nutzung von Best-Practice Lösungen	Kann bei der Definition des Soll-Prozesses ein Vergleich mit ähnlichen Verfahren in der Verwaltung und der Einbezug von Best-Practice-Lösungen anderer Behörden berücksichtigt werden? (Eine Übersicht bietet www.personalausweisportal.de)			
2.7 Optimierung von Geschäftsprozessen	Welche Optimierungspotentiale bestehen bei der Entwicklung des Soll-Prozesses?			
3. Wirtschaftlichkeitsbetrachtung durchführen				
3.1 Quantitative Faktoren	Welche monetäre Faktoren (Kosten und Nutzen) bei der Einführung/Integration der Online-Ausweisfunktion werden betrachtet?			
3.1.1 Kosten der Systemeinführung	Sind Investitionsbedarfe, die für die Einführung der Online-Ausweisfunktion notwendig sind, berücksichtigt? Erfolgt eine Betrachtung von Personalbedarfen (-kosten) sowie Software- und Hardwarekosten?			

Schritte zur Implementierung der Online-Ausweisfunktion	Fragen	Erläuterungen zum Umsetzungsstand	Status *z. B. nicht umgesetzt, in Arbeit, umgesetzt*	Verantwortlich
3.1.2 Systemkosten im laufenden Betrieb	Sind Kosten, die für den Betrieb und die Wartung der Online-Ausweisfunktion anfallen, ermittelt?			
3.2 Qualitative Faktoren	Welche externen Effekte und Faktoren mit qualitativ-strategischer Bedeutung (z. B. Qualitäts- und Leistungssteigerungen, Benutzerfreundlichkeit, Qualitätszuwachs bei der Erledigung von Fachaufgaben) sind zu berücksichtigen?			
4. Berechtigungszertifikat beantragen				
4.1 Ermittlung Anforderungen	Ist eine Analyse der Anforderungen bei der Abwicklung elektronischer Bürgerdienste (z. B. Permanentes Bürgerkonto oder Temporäres Bürgerkonto) erfolgt? Gegebenenfalls sind mehrere Berechtigungszertifikate für unterschiedliche Dienste zu beantragen. Können zentrale Berechtigungszertifikate genutzt werden, bzw. kommt die Beantragung eines neuen zentralen Berechtigungszertifikats in Frage?			
4.2 Berechtigung beantragen	Ist ein Berechtigungszertifikat bei der Vergabestelle für Berechtigungszertifikate (VfB) beantragt? Die Beantragung einer Berechtigung muss folgende Informationen für den Nachweis der Erforderlichkeit für den Geschäftszweck			

Schritte zur Implementierung der Online-Ausweisfunktion	Fragen	Erläuterungen zum Umsetzungsstand	Status *z. B. nicht umgesetzt, in Arbeit, umgesetzt*	Verantwortlich
	enthalten: ▪ Behördendaten ▪ Zweck des Berechtigungszertifikats ▪ Beschreibung des Dienstangebots ▪ Gewünschte Datenfelder ▪ Verantwortliche Datenschutzaufsichtsbehörde ▪ Begründung, ob bzw. warum die ausgelesenen Daten gespeichert werden sollen ▪ Bestätigung über Vorhandensein eines IT-Sicherheitskonzeptes			
4.3 Berechtigungszertifikate-Anbieter auswählen	Welcher Berechtigungszertifikateanbieter wird ausgewählt? Hierzu muss ein Vertragsverhältnis mit einem durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Anbieter geschlossen werden.			
5. Technische Umsetzung				
5.1 Umsetzung eines eigenen eID-Servers	Wird eine Bewertung durchgeführt, ob und wie ein eigener eID-Server in Anspruch genommen werden kann? Die Behörde sollte prüfen, ob eventuell mit bestehenden Anbietern von eID-Servern bereits eigene Vertragsverhältnisse bestehen oder auf			

Schritte zur Implementierung der Online-Ausweisfunktion	Fragen	Erläuterungen zum Umsetzungsstand	Status *z. B. nicht umgesetzt, in Arbeit, umgesetzt*	Verantwortlich
	Rahmenverträge zurückgegriffen werden kann.			
5.2 Beauftragung eID-Service Provider	Wird eine Bewertung durchgeführt, ob die Nutzung eines bereits vorhandenen eID-Service-Anbieters sinnvoll ist? Dies ist mit unterschiedlichem Aufwand und Kosten verbunden, daher sollten verschiedene Angebote der Anbieter miteinander verglichen werden.			
6. Test und Aufnahme Live-Betrieb				
6.1 Testszenarien und Testinfrastruktur	Welche Testszenarien sind entwickelt und ist eine Test-Infrastruktur (ggf. durch den eID-Service Anbieter) eingerichtet? Nach erfolgreichem Abschluss der Testphase kann der Übergang in den Live-Betrieb vorbereitet werden.			
6.2 Aufnahme Live-Betrieb	Zu welchem Datum ist die Aufnahme des Live-Betriebs geplant?			

7. Kommunikation an die Zielgruppen				
7.1 Ermittlung von Zielgruppen und Definition von Maßnahmen	Welche Aktivitäten im Bereich der Kommunikation für interne (z. B. Verwaltungsbeschäftigte) als auch externe Zielgruppen (z. B. Bürgerinnen und Bürger) sind geplant?			
8. Evaluierung / Erfolgsmessung des eID-Prozesses				
8.1 Auswertungen	Soll eine Evaluation oder Monitoring erfolgen, um den konkreten Nutzen der Online-Ausweisfunktion in einem Verwaltungsprozess zu bewerten? Dazu können verschiedene Auswertungen vorgenommen werden (z. B. Wirtschaftlichkeitsbetrachtungen, Standardkosten-Modell, Betrachtung der eID-Einschaltquote in der Kommune, Befragungen).			

Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften

(erstellt durch BMI, Referat O2)

Allgemeines

Stand und Perspektiven des E-Governments in Deutschland

E-Government ist die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien.

E-Government ist kein Selbstzweck, sondern ein Mittel, um die Verwaltung effektiver, bürgerfreundlicher und effizienter zu gestalten.

Elektronische Verwaltungsdienste können einen bedeutenden Beitrag zur Verwaltungsmodernisierung und zum Bürokratieabbau leisten. Anders als in herkömmlichen Verwaltungsabläufen ist es möglich, dass räumlich voneinander entfernte Beteiligte ohne bedeutende Zeitverzögerung zusammenarbeiten. Während Bürgerinnen und Bürger sowie Unternehmen ihre Anliegen im herkömmlichen Verwaltungsverfahren meist noch nach den sachlichen und örtlichen Zuständigkeiten der Behörden und den von diesen vorgegebenen Abläufen aufgliedern müssen, können elektronische Verwaltungsdienste viel einfacher entlang der Lebenslagen von Bürgerinnen und Bürgern sowie der Bedarfslagen von Unternehmen strukturiert werden. Ungeachtet bestehender Zuständigkeiten ist es möglich, nutzerfreundliche, ebenenübergreifende Verwaltungsdienstleistungen auf einer gemeinsamen Oberfläche anzubieten. Hierbei kann auch die Verwaltung Redundanzen abbauen und zu schlankeren und effizienteren Verfahren gelangen. Voraussetzung ist allerdings, dass vor einer Digitalisierung die Prozesse analysiert und gegebenenfalls neu strukturiert werden und nicht lediglich eine elektronische Abbildung der Papierwelt stattfindet.

Elektronische Verwaltungsdienste können bei der Bewältigung der Herausforderungen helfen, die der demographische Wandel mit sich bringt. Perspektivisch ist ein spürbarer Rückgang der Bevölkerung, vor allem in ländlichen Räumen zu erwarten. Dies kann nicht ohne Auswirkungen auf die Dichte des Netzes an Verwaltungsinfrastruktur bleiben. Elektronische Verwaltungsdienste sind ein bedeutender Beitrag, auch künftig in ländlichen Räumen eine für alle Bürgerinnen und Bürger leicht zugängliche Verwaltungsinfrastruktur anbieten zu können, sei es in Form von unmittelbar über öffentlich zugängliche Netze (das Internet oder mobile Anwendungen) erreichbaren Diensten, sei es durch mobile Bürgerbüros, in denen Verwaltungsmitarbeiter zeitweise vor Ort anwesend sind. Die durch elektronische Verwaltungsdienste gestiegene Ortsunabhängigkeit kommt schließlich auch den Beschäftigten in der öffentlichen Verwaltung zugute, indem sie die Telearbeit erleichtert und mobiles Arbeiten unterstützt. Dies dient damit auch der Vereinbarkeit von Familie und Beruf. Mit der elektronischen Publikation von behördlichen Informationen, z. B. der Einstellung von Planungsunterlagen ins Internet, kann sehr schnell ein großes Publikum unterrichtet werden. Offen zugängliche behördliche Datenbestände dienen neben persönlicher Information auch Wissenschaft und Forschung und ermöglichen die Entwicklung neuer Produkte.

Mit der Verabschiedung des Signaturgesetzes (SigG), der Einführung des elektronischen Identitätsnachweises des neuen Personalausweises (nPA) durch das Personalausweisgesetz (PAuswG) und mit dem De-Mail-Gesetz wurden grundlegende Infrastrukturen geschaffen. Durch die Einfügung des Artikels 91c in das Grundgesetz (GG) und die Schaffung des IT-Planungsrates wurden die Voraussetzungen für eine enge Zusammenarbeit von Bund und Ländern bei der Planung, der Errichtung und dem Betrieb ihrer informationstechnischen Infrastruktur erheblich verbessert.

Im internationalen Vergleich zeigt das kürzlich veröffentlichte EU-E-Government Benchmark 2012[1)] der Europäischen Kommission Verbesserungspotenziale im Bereich der Nutzerzufriedenheit und bei der Aufnahme der angebotenen E-Government Dienste (sog. "Take-up"). Die zum ersten Mal unter 32 europäischen Staaten entlang einer neuausgerichteten Methodologie durchgeführte Studie hat Deutschland als besonders stark im Bereich der grenzübergreifenden Dienste ausgezeichnet. Dabei hat die eng an den EU-E-Government Aktionsplan 2011-2015 orientierte Studie weitgehend ihren bisherigen Rankingcharakter verloren und fokussiert sich auf die Identifizierung der Stärken und Schwächen der angebotenen E-Government-Dienstleistungen im Sinne eines sog. Benchlearning-Ansatzes.

Die Internetseiten der Verwaltungen bieten heute vor allem reine Information. Oft fehlt es noch an einem Rückkanal. Es können häufig Formulare heruntergeladen werden. Meist ist es jedoch nötig, sie auszudrucken, zu unterschreiben und per herkömmlicher (also nicht elektronischer) Post zur Behörde zu schicken. Aus den per Post eingehenden Antragsunterlagen müssen die Beschäftigten der Verwaltung Daten wieder manuell in die elektronischen Fachanwendungen der Verwaltung übernehmen. Nach Erstellung des Bescheids muss dieser ausgedruckt werden und die Unterlagen – meist wieder in Papierform – zu den Akten verfügt werden. Diese Medienbrüche sind für Bürgerinnen und Bürger, Unternehmen und Beschäftigte der Verwaltung aufwändig und teuer. Medienbruchfreie, elektronische Verwaltungsprozesse sind noch die Ausnahme. Auch eine Neustrukturierung der Prozesse unterbleibt häufig. Statt die spezifischen Vorteile einer elektronischen Abwicklung auszuschöpfen, wird noch zu oft nur die Papierwelt digital abgebildet.

Rechtliche Rahmenbedingungen beeinflussen die Nutzbarkeit von E-Government-Angeboten. Derzeit kommt es insbesondere in den zahlreichen Verfahren, in denen Schriftformerfordernisse bestehen, Nachweise in Papierform eingereicht werden müssen oder die behördlichen Akten noch in Papierform geführt werden, zu Medienbrüchen. Den überwiegenden Teil ihrer Verwaltungskontakte haben Bürgerinnen und Bürger sowie Unternehmen nicht mit Bundes-, sondern mit Länder- und Kommunalbehörden. Soweit Bundesrecht Hindernisse für elektronische Verwaltungsdienstleistungen enthält, können die für den Vollzug zuständigen Länder diese nicht selbst beseitigen. Ferner gibt es in vielen Fragen noch Rechtsunsicherheit, da es etwa bei der elektronischen Aktenführung an Erfahrungen fehlt.

Ziel und Gegenstand des Gesetzes

Ziel des Gesetzes ist es, durch den Abbau bundesrechtlicher Hindernisse die elektronische Kommunikation mit der Verwaltung zu erleichtern. Das Gesetz soll dadurch über die föderalen Ebenen hinweg Wirkung entfalten und Bund, Ländern und Kommunen ermöglichen, einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten.

Medienbruchfreie Prozesse vom Antrag bis zur Archivierung sollen möglich werden. Dabei sollen Anreize geschaffen werden, Prozesse entlang der Lebenslagen von Bürgerinnen und Bürgern sowie der Bedarfslagen von Unternehmen zu strukturieren und nutzerfreundliche, ebenenübergreifende Verwaltungsdienstleistungen „aus einer Hand“ anzubieten. Ebenso sollen Rechtsunsicherheiten beseitigt werden.

Ein Gesetz schafft noch keine Anwendungen. Hierfür bedarf es auf allen föderalen Ebenen in den nächsten Jahren erheblicher Anstrengungen. Neben finanziellen Ressourcen ist der Wille zur Zusammenarbeit nötig und die Bereitschaft, bestehende Prozesse zu überdenken.

[1)] Siehe eGovernment Benchmark 2012 report (lediglich in englischer Sprache verfügbar) unter https://ec.europa.eu/digital-agenda/en/ict-enabled-benefits-eu-society-analysis-and-data

Regulatorisches Umfeld

Der Auftrag zur Erarbeitung eines E-Government-Gesetzes ergibt sich aus dem Koalitionsvertrag der 17. Legislaturperiode. Dort ist festgehalten: „In der Informationsgesellschaft liegen große Chancen auch für die öffentliche Verwaltung. Wir werden daher E-Government weiter fördern und dazu wo und soweit rechtlich notwendig, rechtliche Regelungen anpassen (EGovG).“

Der Bund richtet sein Handeln im E-Government zudem an den Leitgedanken und an den Zielen der nationalen E-Government-Strategie des IT-Planungsrats aus: „Das Zusammenwirken betrifft auch die Gesetzgebung in Fragen des E-Governments. Bund und Länder prüfen hier gemeinsam den Handlungsbedarf für eine weitere elektronische Abbildung von Prozessen des Regierens und Verwaltens. Dabei werden die Erfahrungen der Kommunen aus dem Verwaltungsvollzug und ihre Anregungen zu gesetzgeberischem Handlungsbedarf eingebracht. Bund und Länder nutzen den IT-Planungsrat, um die Förderung des E-Government auch in Gesetzesinitiativen fachlich abzustimmen und zu begleiten.“[2)]

Damit folgt die Nationale E-Government-Strategie der Malmöer Erklärung[3)] der Europäischen Union vom 18. November 2009. Die von den Vertretern der EU-Mitgliedstaaten, Beitritts- und Kandidatenländern sowie EFTA-Staaten auf der E-Government-Ministerkonferenz in Malmö verabschiedete Ministererklärung sieht vor, dass bis 2015 Bürgerinnen und Bürger sowie Unternehmen E-Government-Services erhalten, die nutzerzentriert sind, die Transparenz staatlichen Handelns erhöhen sowie den Zugang zu öffentlichen Informationen und die Partizipation am staatlichen Handeln erleichtern. Zudem soll die Mobilität im Binnenmarkt erhöht, grenzüberschreitend Unternehmensgründungen und -niederlassungen, Studieren, Arbeiten und die Wahl des Alterswohnsitzes vereinfacht werden.

Im internationalen Kontext sind im Sinne eines kohärenten und interoperablen Rahmens von E-Government auf EU-Ebene neben der Ministererklärung von Malmö insbesondere die Mitteilung der Kommission „Eine Digitale Agenda für Europa“[4)] sowie der E-Government-Aktionsplan zu berücksichtigen.

Die digitale Agenda schlägt eine bessere Nutzung der Informations- und Kommunikationstechnologien (IT) vor, um Innovation, Wirtschaftswachstum und Fortschritt für Bürgerinnen und Bürger sowie Unternehmen zu fördern.[5)]

Der Ende 2010 von der EU vorgestellte E-Government-Aktionsplan ist ein wesentlicher Bestandteil der Digitalen Agenda für Europa. Er soll den Übergang zu einer neuen Generation offener, flexibler und medienbruchfrei funktionierender elektronischer Behördendienste auf örtlicher, regionaler, nationaler und europäischer Ebene fördern und insbesondere dafür sorgen, dass die Online-Services in allen EU-Mitgliedstaaten verfügbar sind.

Die wesentlichen Änderungen im Überblick

1. E-Government-Gesetz des Bundes

   Mit Artikel 1 wird ein E-Government-Gesetz (EGovG) vorgeschlagen. Die wesentlichen Regelungen sind:

---

2) Nationale E-Government-Strategie, S. 6.
3) Ministererklärung von Malmö zum E-Government vom 18. November 2009
4) KOM (2010) 245.
5) KOM (2010) 245.

– Verpflichtung der Verwaltung zur Eröffnung eines elektronischen Zugangs und zusätzlich Verpflichtung der Bundesverwaltung eines De-Mail-Zugangs und der Identifikationsmöglichkeiten mit dem nPA,

– Erleichterung bei der Erbringung von elektronischen Nachweisen und der elektronischen Bezahlung in Verwaltungsverfahren,

– Erfüllung von Publikationspflichten durch elektronische Amts- und Verkündungsblätter,

– Grundsätze der elektronischen Aktenführung und des ersetzenden Scannens,

– Verpflichtung zur Dokumentation und Analyse von Prozessen,

– Regelung zur Bereitstellung von maschinenlesbaren Datenbeständen durch die Verwaltung („open data“).

2. Regelungen betreffend die Ersetzung der Schriftform durch andere technische Verfahren als die qualifizierte elektronische Signatur (qeS) (Artikel 2 – Artikel 4 sowie Artikel 7).

Ein wesentliches Hindernis für E-Government-Angebote der öffentlichen Verwaltung besteht darin, dass als elektronisches Äquivalent der Schriftform allein die qeS zugelassen ist. Im Gegensatz zum Zivilrecht gibt es in öffentlich-rechtlichen Normen eine große Anzahl (mehrere Tausend) von gesetzlichen Schriftformerfordernissen. Die öffentlich-rechtliche Anordnung der Schriftlichkeit wird traditionell weniger formenstreng gehandhabt als im Zivilrecht – so ist z. B. nicht stets eine handschriftliche Unterschrift erforderlich, es werden teilweise auch Kopien oder Computerfaxe anerkannt. Andererseits wird als elektronisches Äquivalent der Schriftform wie im Zivilrecht bisher allein die qeS zugelassen (vgl. des § 3a Verwaltungsverfahrensgesetzes (VwVfG), § 36a Erstes Buch Sozialgesetzbuch (SGB I), § 87a der Abgabenordnung (AO) und § 55b der Verwaltungsgerichtsordnung (VwGO)). Ausnahmen hiervon sind zwar in einigen Rechtsbereichen grundsätzlich möglich (vgl. § 36a Absatz 2 SGB I, § 87a Absatz 6 und § 150 Absatz 6 AO, § 55a Absatz 1 Satz 4 VwGO, § 52a Absatz 1 Satz 4 der Finanzgerichtsordnung und § 65a Absatz 1 Satz 4 des Sozialgerichtsgesetzes), jedoch bisher mit Ausnahme des Verfahrens ATLAS im Zollbereich und des ELSTER-Verfahrens im Steuerbereich nicht konkret zugelassen. Die qeS hat sich jedoch entgegen ursprünglichen Erwartungen in der Breite der Bevölkerung nicht durchgesetzt und wird nur in wenigen Verfahren für professionelle Anwender in der Praxis genutzt. Die Vielzahl der verwaltungsrechtlichen Schriftformerfordernisse und die Tatsache, dass diese in der elektronischen Welt allein durch die sehr wenig verbreitete qeS ersetzt werden können, führt dazu, dass in schriftformbedürftigen Verwaltungsverfahren letztlich derzeit keine ausreichend praktikable Alternative zur Papierform existiert. Mit dem Gesetz sollen daher neben der qualifizierten elektronischen Signatur weitere sichere Technologien zur elektronischen Ersetzung der Schriftform zugelassen werden, wie etwa in § 87a Absatz 6 AO für den Steuerbereich bereits geschehen. Hierfür wurden zwei Verfahren identifiziert, mit denen alle Funktionen der Schriftform abgebildet werden können.

Das erste dieser Verfahren ist De-Mail mit der Versandoption „absenderbestätigt“, welche eine „sichere Anmeldung“ voraussetzt. Der Sender der Nachricht ist dabei durch ein sicheres Anmeldeverfahren identifiziert, die Nachricht einschließlich aller Metadaten durch eine vom De-Mail-Provider aufgebrachte qeS (des De-Mail-Providers) gegen Veränderungen geschützt. Im Umgang mit dem so versandten elektronischen Dokument bleibt diese Form der Signierung erhalten, solange dieses mit der jeweiligen De-Mail-Nachricht verbunden bleibt.

Das zweite Verfahren sind elektronische Anwendungen der Verwaltung durch Bereitstellung elektronischer Formulare in Verbindung mit sicherer elektronischer Identifizierung, insbesondere durch die eID-Funktion des nPA. Bei diesem Verfahren können nicht alle Schriftformfunktionen allein durch den Einsatz des nPA oder ein vergleichbares Identifizierungsverfahren erfüllt werden, es bedarf immer zusätzlich der seitens der Behörde bereitgestellten Anwendung. Dieses Verfahren ist also angebotsgesteuert und lässt sich nicht ohne weiteres auf den privatrechtlichen Bereich übertragen.

Außerdem erlaubt eine Rechtsverordnungsermächtigung der Bundesregierung mit Zustimmung des Bundesrates die rasche Anpassung an die deutschland- wie europaweite technologische Weiterentwicklung. Mit der Rechtsverordnung können weitere ausreichend sichere Verfahren als Schriftformersatz festgelegt werden.

Auf diesen Regelungen aufbauend soll in einem nächsten Schritt eine Überprüfung des gesamten Normenbestandes dahingehend erfolgen, welche der zahlreichen öffentlich-rechtlichen Schriftformerfordernisse aus heutiger Sicht entbehrlich sind. Hier-zu wurde in Artikel 30 eine Berichtspflicht an den Deutschen Bundestag aufgenommen. Auf der Grundlage des Berichts soll ein entsprechender Gesetzentwurf erstellt werden.

3. Weitere Regelungen des Gesetzes

Das Gesetz enthält ferner Regelungen in verschiedenen Rechtsgebieten, in denen die Praxis gezeigt hat, dass zur Verbesserung und Erweiterung von E-Government-Angeboten Änderungen angezeigt sind. Hierunter fallen z. B. die Ergebnisse einer Abfrage des IT-Planungsrates nach bundesrechtlichen Hindernissen für die elektronische Verfahrensabwicklung, die überwiegend die Abschaffung von Schriftformerfordernissen oder Erfordernissen zur persönlichen Vorsprache in Fachgesetzen betrifft. Ebenso fallen hierunter Vorschriften zur Georeferenzierung von statistischen Daten und Registerdaten.

4. Zuletzt enthält das Gesetz in Artikel 30 Vorschriften zur Evaluierung und Weiterentwicklung.

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

Inhaltsübersicht

Artikel 1 Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz – EGovG)

Artikel 2 Änderung des De-Mail-Gesetzes

Artikel 3 Änderung des Verwaltungsverfahrensgesetzes

Artikel 4 Änderung des Ersten Buches Sozialgesetzbuch

Artikel 5 Änderung des Vierten Buches Sozialgesetzbuch

Artikel 6 Änderung des Zehnten Buches Sozialgesetzbuch

Artikel 7 Änderung der Abgabenordnung

Artikel 8 Änderung des Passgesetzes

Artikel 9 Änderung des Personalausweisgesetzes

Artikel 10 Änderung des Gesetzes über die Umweltverträglichkeitsprüfung

Artikel 11 Änderung des Umweltschutzprotokoll-Ausführungsgesetzes

Artikel 12 Änderung des Aufenthaltsgesetzes

Artikel 13 Änderung des Bundesstatistikgesetzes

Artikel 14 Änderung des Rechtsdienstleistungsgesetzes

Artikel 15 Änderung der Rechtsdienstleistungsverordnung

Artikel 16 Änderung des Satellitendatensicherheitsgesetzes

Artikel 17 Änderung des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern

Artikel 18 Änderung der Gewerbeordnung

Artikel 19 Änderung der Handwerksordnung

Artikel 20 Änderung der Ersten Verordnung zum Sprengstoffgesetz

Artikel 21 Änderung der Dritten Verordnung zum Sprengstoffgesetz

Artikel 22 Änderung des Berufsbildungsgesetzes

Artikel 23 Änderung des Berufsqualifikationsfeststellungsgesetzes

Artikel 24 Änderung des Straßenverkehrsgesetzes

Artikel 25 Änderung der Fahrzeug-Zulassungsverordnung

Artikel 26 Änderung des Bundeswasserstraßengesetzes

Artikel 27 Änderung des Luftverkehrsgesetzes

Artikel 28 Änderung der Luftverkehrs-Zulassungs-Ordnung

Artikel 29 Änderung schifffahrtrechtlicher Vorschriften

Artikel 30 Evaluierung

Artikel 31 Inkrafttreten

Artikel 1

Gesetz zur Förderung der elektronischen Verwaltung

(E-Government-Gesetz – EGovG)

Inhaltsübersicht

§ 1 Geltungsbereich

§ 2 Elektronischer Zugang zur Verwaltung

§ 3 Information zu Behörden und über ihre Verfahren in öffentlich zugänglichen Netzen

§ 4 Elektronische Bezahlmöglichkeiten

§ 5 Nachweise

§ 6 Elektronische Aktenführung

§ 7 Übertragen und Vernichten des Papieroriginals

§ 8 Akteneinsicht

§ 9 Optimierung von Verwaltungsabläufen und Information zum Verfahrensstand

§ 10 Umsetzung von Standardisierungsbeschlüssen des IT-Planungsrates

§ 11 Gemeinsame Verfahren

§ 12 Anforderungen an das Bereitstellen von Daten, Verordnungsermächtigung

§ 13 Elektronische Formulare

§ 14 Georeferenzierung

§ 15 Amtliche Mitteilungs- und Verkündungsblätter

§ 16 Barrierefreiheit

§ 1

Geltungsbereich

(1) Dieses Gesetz gilt für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden des Bundes einschließlich der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts.

(2) Dieses Gesetz gilt auch für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, wenn sie Bundesrecht ausführen.

(3) Für die Tätigkeit der Gerichtsverwaltungen und der Behörden der Justizverwaltung einschließlich der ihrer Aufsicht unterliegenden Körperschaften des öffentlichen Rechts gilt dieses Gesetz nur, soweit die Tätigkeit der Nachprüfung durch die Gerichte der Verwaltungsgerichtsbarkeit oder der Nachprüfung durch die in verwaltungsrechtlichen Anwalts-, Patentanwalts- und Notarsachen zuständigen Gerichte unterliegt.

(4) Dieses Gesetz gilt, soweit nicht Rechtsvorschriften des Bundes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten.

(5) Dieses Gesetz gilt nicht für

1. **die Strafverfolgung, die Verfolgung und Ahndung von Ordnungswidrigkeiten, die Rechtshilfe für das Ausland in Straf- und Zivilsachen, die Steuer- und Zollfahndung (§ 208 der Abgabenordnung) und für Maßnahmen des Richterdienstrechts,**

2. **Verfahren vor dem Deutschen Patent- und Markenamt und den bei diesem errichteten Schiedsstellen,**

3. **die Verwaltungstätigkeit nach dem Zweiten Buch Sozialgesetzbuch.**

Erläuterungen

1. Bundesbehörden (Absatz 1)

Absatz 1 regelt den Geltungsbereich dieses Gesetzes für Behörden des Bundes einschließlich der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts. Diese werden im weiteren Gesetzestext zusammengefasst als „Behörden des Bundes“ bezeichnet. Der Begriff der Behörde lehnt sich an die weite Definition des § 1 Absatz 4 VwVfG, des § 1 Absatz 2 SGB X und des § 6 Absatz 1 AO an und umfasst damit jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt.

Dieses Gesetz gilt für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden. Der Begriff wird ebenso verwendet wie im VwVfG und im SGB X. Fiskalisches Handeln, wie es insbesondere im Vergaberecht bei der Beschaffung von Gütern und Leistungen durch bürgerlich-rechtliche Verträge der Verwaltung vorkommt, ist damit vom Anwendungsbereich dieses Gesetzes nicht erfasst.

Öffentlich-rechtliche Verwaltungstätigkeit im Sinne dieses Gesetzes ist – ebenso wie im VwVfG und im SGB X – nicht auf Handeln mit Außenwirkung beschränkt. Der Begriff wird z. B. in § 1 VwVfG und § 1 Absatz 1 Satz 1 SGB X verwendet und ist nicht zu verwech-

seln mit dem Begriff des Verwaltungsverfahrens, der in § 9 VwVfG und § 8 SGB X definiert ist und als ein Kriterium die Außenwirkung der Tätigkeit der Behörde festlegt. Verwaltungsverfahren ist insoweit eine Teilmenge der öffentlich-rechtlichen Verwaltungstätigkeit. Im Einzelfall kann öffentlich-rechtliche Verwaltungstätigkeit auch behördeninterne Verwaltungstätigkeit erfassen, vgl. z. B. die §§ 6, 7 oder 9 dieses Gesetzes. Solche Regelungen werden in diesem Gesetz getroffen, weil sie dazu beitragen, Medienbrüche abzubauen und damit letztlich die elektronische Kommunikation zwischen Verwaltung und Bürgerinnen und Bürgern oder der Wirtschaft verbessern. Dieses Gesetz gilt auch für den Bundesrechnungshof und seine nachgeordneten Prüfungsämter, soweit diese als Verwaltungsbehörde tätig werden. Wird der Bundesrechnungshof als Organ der externen Finanzkontrolle tätig, übt er keine Verwaltungstätigkeit aus (vgl. BT-Drs. 10/3323, S. 10). Insoweit obliegt es ihm, sein Verfahren in seiner Geschäftsordnung selbst zu regeln (§ 20 Absatz 1 Satz 3 Gesetz über den Bundesrechnungshof).

2. Landesbehörden (Absatz 2)

Absatz 2 regelt den Geltungsbereich dieses Gesetzes für Behörden der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, wenn sie Bundesrecht ausführen. Die Regelung orientiert sich an § 1 Absatz 1 Nr. 2 VwVfG, wodurch betont wird, dass die verwaltungsverfahrensrechtliche Ausgestaltung in Bezug genommen wird.

Ausführen von Bundesrecht im Sinne dieser Vorschrift meint entweder Ausführen als eigene Angelegenheit des Landes (Artikel 84 GG) oder Ausführen im Auftrag des Bundes (Artikel 85, Artikel 108 Absatz 3 GG).

Soweit das E-Government-Gesetz Aufgaben im Sinne der Artikel 84 und 85 des Grundgesetzes enthält, kann die Übertragung dieser Aufgaben nur durch Landesrecht erfolgen. Als solche Aufgabe, die der Übertragung durch Landesrecht bedarf, ist § 3 EGovG zu sehen, da dort eine Verpflichtung zur Bereitstellung von Informationen unabhängig von einem konkreten Verwaltungsverfahren angeordnet wird.

Von einer – unter den Vorbehalt der landesrechtlichen Übertragung gestellten – Aufgabe zu unterscheiden ist eine Regelung des Verwaltungsverfahrens. Bei diesen Regelungen werden keine Aufgaben übertragen und es erfolgt kein Eingriff in die behördliche Einrichtung, was eine weitere Abgrenzungsschwelle darstellt.

Regelungen des Verwaltungsverfahrens betreffen die Ausgestaltung des Verwaltungsverfahrens, wie sie auch im EGovG enthalten sind.

Soweit das Gesetz den Anwendungsbereich einzelner Regelungen nicht explizit auf Behörden des Bundes beschränkt (vgl. z. B. § 2 Absatz 2 und 3, § 6 oder § 9 EGovG), gelten sie für alle Behörden, mithin auch für Behörden der Länder und der Gemeinden und Gemeindeverbände, wenn sie Bundesrecht ausführen. Mit Ausnahme von § 3 EGovG werden dabei keine Aufgaben übertragen, sondern Regelungen zur Ausgestaltung des Verwaltungsverfahrens getroffen.

So enthalten § 2 Absatz 1 EGovG (Ermöglichung auch eines elektronischen Zugangs) und § 4 EGovG (Ermöglichung auch der bargeldlosen Bezahlung von Gebühren) nur Regelungen zur Ausgestaltung der jeweiligen Verwaltungsverfahren. Auch die in § 14 EGovG vorgesehene Georeferenzierung von Ortsangaben in Registern ist nicht anders zu beurteilen als beispielsweise eine Verpflichtung zur Angabe von Postleitzahlen und daher als eine Regelung zur Ausgestaltung des betroffenen Verwaltungsverfahrens anzusehen.

3. Gerichts- und Justizverwaltung (Absatz 3)

Die Regelung orientiert sich an § 2 Absatz 3 Nummer 1 VwVfG. Sie hat zum Inhalt, dass dieses Gesetz genauso für den Bereich der Justizverwaltung gelten soll wie das VwVfG. Die Einschränkung des Anwendungsbereiches erfolgt damit nach denselben Kriterien wie im VwVfG. Aus dieser Regelung ergibt sich also, dass dieses Gesetz grundsätzlich auch für die Tätigkeit der Gerichtsverwaltungen und die Behörden der Justizverwaltung gilt, soweit die jeweilige Tätigkeit der Nachprüfung durch die im Gesetzestext erwähnten Gerichte unterliegt. Die Regelung ist im Zusammenhang mit den §§ 23 ff. des Einführungsgesetzes zum Gerichtsverfassungsgesetz zu sehen.

4. „Soweit nicht Rechtsvorschriften des Bundes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten“ (Absatz 4)

Diese Kollisionsregelung stellt klar, dass dieses Gesetz dann gilt, soweit nicht Rechtsvorschriften des Bundes inhaltsgleiche oder entgegenstehende Regelungen enthalten. Solche Regelungen gehen diesem Gesetz vor. Soweit also die entsprechende Rechtsvorschrift etwa eine Bestimmung zur elektronischen Verwaltung enthält, hat diese Vorrang. Damit soll sichergestellt werden, dass die aufgrund der jeweiligen Besonderheiten für bestimmte Rechtsgebiete getroffenen Regelungen zur elektronischen Verwaltung (z. B. in den Sozialgesetzbüchern oder in den Steuergesetzen) Gültigkeit behalten. Soweit Rechtsvorschriften des Bundes für einen Bereich des besonderen Verwaltungsrechts (einschließlich des Steuerrechts und des Sozialrechts) keine Regelungen zur elektronischen Verwaltung enthalten, gilt dieses Gesetz ergänzend. Gegenüber dem VwVfG gehen die Regelungen dieses Gesetzes vor. Regelungen des SGB I und des SGB X zum Sozialdatenschutz sind gegenüber diesem Gesetz vorrangig.

Die Regelung orientiert sich an § 1 Absatz 1 letzter Teilsatz und Absatz 2 Satz 1 letzter Teilsatz VwVfG.

5. Ausnahmen vom Geltungsbereich (Absatz 5)

Die Regelung sieht Ausnahmen vom Geltungsbereich dieses Gesetzes vor.

a) Strafverfahren u.a. (Nummer 1)

Nummer 1 orientiert sich an § 2 Absatz 2 Nummer 2 VwVfG mit der Ausnahme, dass hier auch die Steuerfahndung (Zollfahndung) nach § 208 AO aufgenommen wurde. Dies ist erforderlich, weil die Tätigkeit der Steuer- und Zollfahndung in rechtlicher und organisatorischer Hinsicht dem Straf- und Ordnungswidrigkeitenverfahren sehr ähnelt. In § 2 Absatz 2 Nummer 2 VwVfG ist § 208 AO nicht explizit erwähnt, da in § 2 Absatz 2 Nummer 1 VwVfG die AO insgesamt vom Anwendungsbereich des VwVfG ausgenommen ist. Hinsichtlich Nummer 1 ist anzumerken, dass mit der Formulierung „Rechtshilfe für das Ausland in Strafsachen“ alle Bereiche der Rechtshilfe (Aus- und Durchlieferungsverkehr, Vollstreckungshilfeverkehr sowie sonstige Rechtshilfe) sowohl auf Grundlage der Instrumente der Rechtshilfe in Strafsachen als auch auf Grundlage der Instrumente der gegenseitigen Anerkennung in Strafsachen vom Anwendungsbereich des EGovG ausgeschlossen sind.

b) Verfahren vor dem Deutschen Patent- und Markenamt (Nummer 2)

Nummer 2 orientiert sich an § 2 Absatz 2 Nummer 3 VwVfG. Aufgrund der spezifischen Anforderungen bei Verfahren vor dem Deutschen Patent- und Markenamt, die sich u. a. in der Einführung der Elektronischen Schutzrechtsakte (ElSA) für Patent- und Gebrauchsmusterverfahren manifestiert haben, soll das vorliegende Gesetz keine Anwendung finden. Der Anwendungsausschluss erstreckt sich auch auf Verfahren nach dem Urheberrechtswahrnehmungsgesetz.

c) Verwaltungstätigkeit nach SGB II (Nummer 3)

Nummer 3 regelt, dass die gesamte Verwaltungstätigkeit nach dem Zweiten Buch Sozialgesetzbuch (SGB II) nicht vom Anwendungsbereich dieses Gesetzes umfasst ist. Dies gilt auch für die mit der Grundsicherung für Arbeitsuchende verbundenen Aufgaben der Sozialversicherung, die als Annex zur Leistungserbringung wahrgenommen werden. Damit wird sichergestellt, dass der besonderen Form der Mischverwaltung nach Artikel 91e Absatz 1 GG Rechnung getragen wird. Zugleich wird durch die einheitliche Regelung für das gesamte SGB II der gebotene Gleichklang zwischen gemeinsamen Einrichtungen und zugelassenen kommunalen Trägern gewährleistet.

Zu berücksichtigen ist, dass einige Regelungen des EGovG jedoch mittelbar auch im SGB II gelten. So betreffen die in Artikel 4 vorgenommenen Änderungen des SGB I die elektronischen Formulare und die in Artikel 6 aufgeführten Änderungen des SGB X behandeln die Akteneinsicht. Diese Regelungen korrespondieren mit den §§ 8, 13 EGovG. Da es sich beim SGB I um den allgemeinen Teil und beim SGB X um allgemeine Vorschriften zum Sozialverwaltungsverfahren handelt (vgl. auch § 1 Absatz 1 Satz 1 SGB X), wirken Änderungen hier grundsätzlich auch in den übrigen Büchern.

Sonstige Änderungen in den Artikeln 4 und 6 wirken ohnehin auch für das SGB II, da die hier angesprochene Bereichsausnahme sich nur auf das EGovG, also auf Artikel 1 bezieht.

§ 2

Elektronischer Zugang zur Verwaltung

(1) Jede Behörde ist verpflichtet, auch einen Zugang für die Übermittlung elektronischer Dokumente, auch soweit sie mit einer qualifizierten elektronischen Signatur versehen sind, zu eröffnen.

(2) Jede Behörde des Bundes ist verpflichtet, den elektronischen Zugang zusätzlich durch eine De-Mail-Adresse im Sinne des De-Mail-Gesetzes zu eröffnen, es sei denn, die Behörde des Bundes hat keinen Zugang zu dem zentral für die Bundesverwaltung angebotenen IT-Verfahren, über das De-Mail-Dienste für Bundesbehörden angeboten werden.

(3) Jede Behörde des Bundes ist verpflichtet, in Verwaltungsverfahren, in denen sie die Identität einer Person auf Grund einer Rechtsvorschrift festzustellen hat oder aus anderen Gründen eine Identifizierung für notwendig erachtet, einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes anzubieten.

Erläuterungen

1. Allgemeine Zugangseröffnungspflicht für elektronische Dokumente (Absatz 1)

Mit dieser Vorschrift wird das Ziel A.1 der Nationalen E-Government-Strategie umgesetzt, wonach der Zugang allen potenziellen Nutzern eines Dienstes ermöglicht wird.

Absatz 1 verpflichtet alle Behörden, neben den allgemein üblichen Zugängen zur Verwaltung (z. B. Posteingang für papierbasierte Eingänge, persönliche Vorsprache), auch einen Zugang für die elektronische Kommunikation zu eröffnen. In vielen Fällen wird dies bereits geschehen sein. Es soll jedoch umfassend die Möglichkeit eröffnet werden, mit jeder Be-

hörde elektronisch in Kontakt treten zu können, und zwar grundsätzlich in jeder Angelegenheit.

Der Wortlaut der Regelung orientiert sich an § 3a Absatz 1 VwVfG sowie den wortgleichen § 36a Absatz 1 SGB I und § 87a Absatz 1 Satz 1 AO und ergänzt diese.

Nach § 3a Absatz 1 VwVfG, § 36a SGB I und § 87a AO ist Voraussetzung für die Übermittlung elektronischer Dokumente, dass der Empfänger hierfür einen Zugang eröffnet hat. Eine Verpflichtung von Behörden zur Eröffnung des Zugangs ergibt sich aus diesen Regelungen noch nicht, sondern es bedarf eines ausdrücklichen oder konkludenten Akts. Bei Behörden wird insbesondere in der öffentlichen Angabe einer E-Mail-Adresse z. B. in Briefköpfen oder auf der Internetseite, eine konkludente Eröffnung des Zugangs gesehen. Satz 1 sieht nunmehr diese Verpflichtung zur Eröffnung eines Zugangs vor.

Im einfachsten Fall erfolgt die Eröffnung des Zuganges durch die Bereitstellung eines E-Mail-Postfaches der Behörde. Hat eine Behörde ein E-Mail-Postfach, so erfüllt sie die Verpflichtung im Sinne des Satzes 1. Darüber sollte jede Behörde verfügen, um eine insbesondere für Bürgerinnen und Bürger einfach handhabbare elektronische Kommunikation zu gewährleisten. Mit jedem einfachen E-Mail-Postfach können in technischer Hinsicht elektronische Dokumente, die mit einer qeS nach SigG versehen sind – sofern sie unverschlüsselt sind -, als E-Mail-Anhang empfangen, gesichtet und gespeichert werden. Soweit eine Behörde also ein E-Mail-Postfach hat, kann sie unverschlüsselte, qualifiziert elektronische signierte Dokumente empfangen.

Eine Verpflichtung der Behörden zur Überprüfung einer Signatur oder zur Annahme von verschlüsselten Dokumenten wird durch das EGovG nicht begründet. Dennoch sei auf Folgendes hingewiesen: Damit eine Behörde die Integrität eines Dokumentes und die Gültigkeit der Signatur überprüfen kann, benötigt sie eine entsprechende Software. Eine Standardsoftware dazu ist beispielsweise mit dem Governikus Signer in 15 Ländern (außer Baden-Württemberg) kostenfrei verfügbar, da entsprechende Lizenz- und Pflegeverträge bereits bestehen.

Die Verpflichtung zur Eröffnung eines Zuganges z. B. ist auch dann erfüllt, wenn eine Behörde ein elektronisches Gerichts- und Verwaltungspostfach (EGVP) oder ein anderes Verfahren (z. B. das Verfahren im Sinne von § 87a Absatz 6 Satz 1 AO, sog. „ Elsterverfahren“) oder andere spezielle Verfahren oder Portallösungen einrichtet, über das ihr elektronische Dokumente übermittelt werden können. Wichtig ist, dass auch solche Dokumente an die Behörde übermittelt werden können, die mit einer qeS nach SigG versehen sind. Die meisten Behörden des Bundes dürften nach diesen Maßstäben bereits heute über einen elektronischen Zugang im Sinne der genannten Vorschriften verfügen, da sie zumindest über ein E-Mail-Postfach verfügen. In den Verwaltungen der Länder und Kommunen ist dies jedoch noch nicht flächendeckend der Fall. Insoweit soll die Norm – soweit sie nicht direkt anwendbar ist - auch ein Beispiel geben und zur Nachahmung anregen.

Absatz 1 legt lediglich fest, dass ein Zugang für die Übermittlung elektronischer Dokumente eröffnet werden muss. Es erfolgt keine Festlegung auf ein bestimmtes Verfahren. Die Regelung ist also technikoffen gestaltet.

Neben dem einfachen E-Mail-Zugang ist beispielsweise auch ein elektronischer Zugang über Verwaltungspostfächer oder über Online-Formulare und Web-Anwendungen möglich und teilweise auch bereits verbreitet.

Durch das Wort „auch“ wird das sogenannte „Multikanalprinzip“ abgesichert. Das heißt, dass eine Behörde nicht ausschließlich elektronisch erreichbar sein darf, sondern den Zugang für die papierbasierte Eingänge nach wie vor offen halten muss. Denn nicht alle Personen wollen E-Government-Angebote nutzen oder sind hierzu in der Lage. Grund-

sätzlich sollen Bürgerinnen und Bürger wählen können, auf welche Weise sie mit der Verwaltung in Kontakt treten. Elektronische Informations-, Kommunikations- und Transaktionsangebote der Verwaltung treten als zusätzlicher Service neben die etablierten Zugänge (insbesondere persönliche Vorsprache, Telefon, Telefax oder Schreiben).

Für Unternehmen kann dagegen in einigen Bereichen die Nutzung von E-Government gesetzlich vorgeschrieben sein. So besteht z.B. für die Umsatzsteuervoranmeldung, vgl. § 18 UStG, bzw. die Lohnsteuer-Anmeldung durch den Arbeitgeber, vgl. § 41a EStG, eine steuerrechtliche Pflicht, die entsprechenden Angaben elektronisch an die Finanzämter zu übermitteln. Die Verfassungskonformität dieser Regelungen im Hinblick auf die Artikel 12 und 14 GG wird hierbei durch den Einsatz von Ausnahmeregelungen für „unbillige Härte“ gewährleistet, vgl. dazu auch die Urteile FG Hamburg 2. Senat, 9. November 2009, Az: 2 K 65/08 und BFH 11. Senat, 14. März 2012, Az: XI R 33/09.

Es gilt, dass elektronische Eingänge gegenüber solchen in Papierform weder bevorzugt noch benachteiligt werden dürfen. Vorzüge, die sich durch die elektronische Bearbeitung ergeben, können jedoch berücksichtigt werden. Die Gleichstellung elektronischer und papiergebundener Kommunikation dient der Umsetzung des Ziels A.4 der Nationalen E-Government-Strategie: („Alle geeigneten Verwaltungsangelegenheiten lassen sich über das Internet abschließend elektronisch erledigen“).

2. De-Mail-Zugangseröffnungspflicht für Bundesbehörden (Absatz 2)

Absatz 2 konkretisiert die Zugangseröffnung insoweit, als alle Behörden des Bundes verpflichtet werden, ein De-Mail-Konto zu eröffnen. Insoweit wird auf die Begründung zum De-Mail-Gesetz verwiesen (BT-Drucksache 17/3630 vom 8. November 2010, Begründung AT I. 1., S. 18), wonach „hinsichtlich der Kommunikation insbesondere zwischen dem Bürger/der Bürgerin und Behörden gilt, dass auch diese darum bemüht sein sollten, für die Kommunikation mit dem Bürger/der Bürgerin De-Mail zu verwenden, wenn dieser es fordert. Eine Kommunikation zwischen Bürgerinnen und Bürgern und öffentlicher Stelle mittels De-Mail setzt voraus, dass auch die Behörde sich entschieden hat, De-Mail zu nutzen, denn anderenfalls könnte der Bürger/die Bürgerin der Behörde keine De-Mail senden. Die Behörde soll also den Bürger/die Bürgerin nicht ohne Grund auf andere Kommunikationswege als auf den über De-Mail verweisen können. Sollte ein Bürger oder eine Bürgerin gegenüber der Behörde den Zugang allein mittels seines De-Mail-Kontos eröffnet haben und die öffentliche Stelle ebenfalls an De-Mail angeschlossen sein, wird sie in diesen Fällen verpflichtet sein, per De-Mail mit dem Bürger oder der Bürgerin zu kommunizieren.“ Diese Pflicht wird die Behörde jedenfalls in der Regel treffen. Die Pflicht wird nunmehr insoweit verstärkt, als die Behörden des Bundes verpflichtet werden, den Zugang über eine De-Mail-Adresse im Sinne von § 5 des De-Mail-Gesetzes zu eröffnen. Hierzu muss die Behörde Inhaberin eines De-Mail-Kontos nach § 3 des De-Mail-Gesetzes sein. Es ist geplant, dass De-Mail-Dienste für die Bundesverwaltung als IT-Verfahren zentral durch ein Dienstleistungszentrum IT (DLZ-IT) angeboten werden („De-Mail-Gateway“). Diese zentrale Anbindung mittels De-Mail-Gateway soll über ein Netz realisiert werden, über das die Bundesbehörden sicher und hochverfügbar miteinander verbunden sind (zukünftig „Netze des Bundes“, z.Zt. IVBB, IVBV/BVN sowie das Verbindungsnetz gemäß IT-NetzG). Insoweit regelt der letzte Halbsatz, dass die Pflicht solche Behörden nicht trifft, die keinen Zugang zu dem zentral im internen Verbindungsnetz des Bundes angebotenen „De-Mail-Gateway“ haben.

De-Mail-Nachrichten an Bundesbehörden gelten als eingegangen, sobald sie sich im De-Mail-Postfach der jeweiligen Behörde beim zugehörigen De-Mail-Provider befinden. Im Rahmen des IT-Verfahren De-Mail ist zu gewährleisten, dass die eingegangenen De-Mail-Nachrichten schnellstens an Infrastrukturkomponenten der Behörden des Bundes ausgeliefert werden. Auf die Machbarkeitsstudie De-Mail vom 6. Januar 2012, die im Rat der IT-Beauftragten der Bundesregierung (IT-Rat) durch Beschluss vom 24. Januar 2012 zur Kenntnis genommen wurde, wird Bezug genommen.

Die Einrichtung des De-Mail-Postfachs über Netze des Bundes ist für die Behörden kostenfrei. Der bloße Empfang von De-Mails ist kostenneutral und lediglich das Versenden von De-Mails ist mit Kosten verbunden. Eine Verpflichtung der Behörden, dem Bürger auf dem De-Mail-Wege zu antworten, besteht nicht, wenn der Bürger mehrere Zugänge gegenüber der Behörde eröffnet hat. Außerdem ist die Behörde nicht verpflichtet, per De-Mail zu antworten, wenn sie wegen der Versendung von Daten, z. B. Sozialdaten, mit sehr hohem Schutzbedarf verpflichtet ist, weitere Sicherungsmaßnahmen, z. B. eine Ende-zu-Ende-Verschlüsselung, einzusetzen.

Die insoweit mögliche Nutzung des De-Mail-Verfahrens durch den Bürger/die Bürgerin in seiner/ihrer Kommunikation mit jeder Behörde des Bundes ist sinnvoll und insbesondere für sog. unstrukturierte Kommunikation (z. B. Word-, pdf-Dokumente) geeignet, weil er/sie auf diese Weise ein wesentlich sichereres Kommunikationsverfahren nutzen kann als bei sonstigen Verfahren, die heute im öffentlichen Internet üblicherweise zur Verfügung gestellt werden. Die besondere Sicherheit u. a. hinsichtlich Datensicherheit und Datenschutz ergibt sich dadurch, dass ein De-Mail-Konto erst dann von einem De-Mail-Provider angeboten werden darf, wenn er sich zuvor durch das BSI nach De-Mail-Gesetz hat akkreditieren lassen. Um die Akkreditierung zu erhalten, muss er ein aufwändiges Verfahren durchlaufen, in welchem er unter anderem Nachweise des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) auf ausreichenden Datenschutz und von seitens des BSI zertifizierten IT-Sicherheitsdienstleistern auf ausreichende Datensicherheit vorlegen muss.

Die Verpflichtung der Bundesbehörden zur Einrichtung einer De-Mail-Adresse macht die bisher gefundenen IT-Lösungen für elektronische Kommunikation in speziellen Verfahren nicht überflüssig, sondern ergänzt diese.

Die Einrichtung einer De-Mail-Adresse zwingt die Behörde nicht, ausschließlich die De-Mail-Infrastruktur zu nutzen: Wenn etwa der Empfänger (z. B. ein Rechtsanwalt) die Kommunikation mittels EGVP bevorzugt, dann kann die Behörde mit ihm mittels EGVP kommunizieren. Darüber hinaus kann sie auch andere Verfahren zur sicheren elektronischen Übermittlung eröffnen, bei denen die Authentizität und Integrität der Daten gewährleistet werden und bei Nutzung allgemein zugänglicher Netze ein Verschlüsselungsverfahren angewendet wird, das die Vertraulichkeit der übermittelten Daten sicherstellt.

Die Verpflichtung der Behörden des Bundes zur Zugangseröffnung mittels De-Mail und zum Angebot der Nutzung des elektronischen Identitätsnachweises nach PAuswG in geeigneten Verfahren (vgl. Absatz 3) ist sinnvoll, weil so mehr Sicherheit in der Fläche für die elektronische Kommunikation erreicht werden kann, die grundsätzlich jeden Bürger und jede Bürgerin erreichen kann. Denn jede Bürgerin und jeder Bürger kann einen nPA mit allen seinen Funktionen erhalten und nutzen. Ebenso kann sich jede Bürgerin und jeder Bürger und auch jedes (kleine, mittlere oder große) Unternehmen ein De-Mail-Konto einrichten und untereinander sicher kommunizieren. Außerdem kann jedes dieser beiden Verfahren für sich genommen unter bestimmten Voraussetzungen die Schriftform im Bereich des öffentlichen Rechtes erfüllen, vgl. Artikel 3 (Änderung des § 3a VwVfG), Artikel 4 (Änderung des § 36a SGB I) und 7 (Änderung des § 87a AO) dieses Gesetzes. Andere sichere Übermittlungswege wie z. B. das EGVP haben dagegen eine andere, zumeist spezialisierte Zielgruppe.

3. Angebotspflicht für elektronischen Identitätsnachweis für Bundesbehörden (Absatz 3)

Die Vorschrift verpflichtet die Behörden des Bundes, Identitätsfeststellungen auch durch einen elektronischen Identitätsnachweis nach § 18 PAuswG oder § 78 Absatz 5 AufenthG zu ermöglichen und die dazu notwendige Infrastruktur bereitzustellen. § 2 Absatz 3 gilt nicht, sofern die Feststellung einer Identität unter Anwesenden erfolgt.

Verwaltungsverfahren können damit effektiver und bürgerfreundlicher gestaltet werden. Insbesondere könnte dem Personalausweisinhaber oder Inhaber eines elektronischen Aufenthaltstitels in vielen Fällen der Weg in die Behörde erspart werden.

§ 3

Information zu Behörden und über ihre Verfahren in öffentlich zugänglichen Netzen

(1) Jede Behörde stellt über öffentlich zugängliche Netze in allgemein verständlicher Sprache Informationen über ihre Aufgaben, ihre Anschrift, ihre Geschäftszeiten sowie postalische, telefonische und elektronische Erreichbarkeiten zur Verfügung.

(2) Jede Behörde soll über öffentlich zugängliche Netze in allgemein verständlicher Sprache über ihre nach außen wirkende öffentlich-rechtliche Tätigkeit, damit verbundene Gebühren, beizubringende Unterlagen und die zuständige Ansprechstelle und ihre Erreichbarkeit informieren sowie erforderliche Formulare bereitstellen.

(3) Für Gemeinden und Gemeindeverbände gelten die Absätze 1 und 2 nur dann, wenn dies nach Landesrecht angeordnet ist.

Erläuterungen

1. Bereitstellung von allgemeinen Informationen über die Behörde (Absatz 1)

Absatz 1 enthält einen Mindestkatalog von Informationen, die jede Behörde, unabhängig von konkreten Verfahren, über öffentlich zugängliche Netze (das Internet oder mobile Anwendungen) veröffentlichen muss. Dabei ist es nicht erforderlich, dass sie eine eigene Internetseite unterhält, sondern diese kann z. B. auch von dem übergeordneten Verwaltungsträger zur Verfügung gestellt werden oder es können entsprechende Portale (Zuständigkeitsfinder) eingerichtet werden. Nach derzeitigem Kenntnisstand sind diese Basisinformationen bereits weitgehend im Internet elektronisch abrufbar. Auch die Informationsfreiheitsgesetze des Bundes und der Länder enthalten Vorschriften über die Bereitstellung amtlicher Informationen. § 11 des Informationsfreiheitsgesetzes (IFG) des Bundes regelt dabei, anders als die übrigen Vorschriften des IFG, die Bereitstellung von Informationen ohne vorherigen Antrag. Danach sollen insbesondere Verzeichnisse über Informationssammlungen, Organisations- und Aktenpläne ohne personenbezogene Daten im Internet veröffentlicht werden. Allerdings steht § 11 IFG im Kontext des antragsgebundenen Auskunftsverfahrens nach den Vorschriften des IFG und dient diesem. Durch die zu veröffentlichenden Sammlungen soll den potenziellen Antragstellern die Informationssuche erleichtert, die Stellung präziserer Anfragen ermöglicht und durch die aktive Verbreitung behördlicher Information die individuelle Bearbeitung von Informationsanträgen reduziert werden.

Die in diesem Gesetz vorgesehene Regelung dient dem gegenüber vorrangig dem Ziel eines bürger- und unternehmensfreundlichen Verfahrens. Die Information über Zuständigkeiten und Verfahren sollen verbessert werden, Ansprechstelle und Kontaktmöglichkeiten sollen benannt werden. Grundsätzlich eröffnet die Vorschrift die Möglichkeit, sich besser auf einen Kontakt mit der Behörde vorzubereiten. Wenn dadurch Antragsteller besser über die einzuhaltenden Verfahrensschritte und die erforderlichen Nachweise informiert sind, trägt dies auch zur Beschleunigung der Verfahren und zur Entlastung der Verwal-

tung bei. § 3 ist keine Regelung im Sinne von § 1 Absatz 3 IFG. Die Verpflichtung des § 11 IFG besteht somit weiterhin.

Die Vorgabe an die Behörden, sich bei der Information an Bürgerinnen und Bürger einer allgemein verständlichen Sprache zu bedienen, soll sicherstellen, dass klare, einfache und dem allgemeinen Sprachgebrauch entnommene Formulierungen verwendet werden, um die Adressaten auch tatsächlich zu erreichen und nicht durch eine zu stark juristisch geprägte oder mit fachspezifischer Terminologie gespickte Sprache zu verunsichern.

Um ihre problemlose elektronische Erreichbarkeit im Bereich des Binnenmarktes gemäß den unionsrechtlichen Anforderungen sicherzustellen, weisen die Behörden, die über De-Mail-Dienste erreichbar sind, nicht ausschließlich auf akkreditierte De-Mail-Dienste, sondern auch auf im Sinne des § 19 des De-Mail-Gesetzes gleichgestellte ausländische Dienste hin. Hier genügt es, einen elektronischen Verweis auf die im Internet durch das BSI veröffentlichte Liste solcher Anbieter in ihrer jeweils aktuellen Fassung einzufügen.

2. Bereitstellung verfahrensbezogener Informationen über die Behörde (Absatz 2)

Absatz 2 enthält einen Katalog von Informationen, die jede Behörde über sich und insbesondere in Bezug auf ihre nach außen wirkende öffentlich-rechtliche Tätigkeit in öffentlich zugänglichen Netzen veröffentlichen soll.

Die nach außen wirkende öffentlich-rechtliche Tätigkeit umfasst sämtliche Leistungen und Verfahren der Behörde, die über eine rein verwaltungsinterne Tätigkeit der Behörde hinausgehen.

Ist eine Bundesbehörde für den Vollzug eines Verfahrens zuständig, so stellt sie alle verfahrensrelevanten Informationen über öffentlich zugängliche Netze zur Verfügung. Ist eine Landesbehörde in Ausführung von Bundesrecht (vgl. § 1 Absatz 2) für den Vollzug eines Verfahrens zuständig, so trifft sie diese Pflicht. Dies gilt auch für die Träger von Sozialleistungen, die Bundesrecht ausführen, mit Ausnahme der Gemeinden und Gemeindeverbände. Allerdings bleiben die spezifischen und detaillierten Regelungen des Beitrags- und Melderechts im Bereich der sozialen Sicherung von dieser Regelung unberührt.

Bei der Art der Veröffentlichung und dem Umfang von Informationen über Verfahren durch die Landesbehörden sollte berücksichtigt werden, dass die Länder in der überwiegenden Anzahl der von ihnen verantworteten Verfahren Bundesrecht ausführen. In diesem Fall haben sie auch die durch die bundesgesetzliche Regelung geltenden Bestandteile einer Verfahrensinformation bereitzustellen. Hierbei sollte die Landesbehörde idealerweise auf Informationen der für die dem Verfahren zugrunde liegenden bundesgesetzlichen Regelungen zuständigen Bundesbehörde zurückgreifen können. Um diesem Bedürfnis Rechnung zu tragen, haben sich Bund und Länder auf den Aufbau und die Pflege eines Leistungskatalogs der öffentlichen Verwaltung (LeiKa) verständigt. Dieser (verwaltungsintern geführte, also nicht über öffentlich zugängliche Netze erreichbare) Katalog soll als Teil der föderalen Infrastruktur die Anbieter von Informationen zu Verfahren auf allen föderalen Ebenen redaktionell unterstützen. Bundesbehörden stellen für den LeiKa so genannte Stammtexte zu den Verfahren bereit, deren Ausführung den Ländern übertragen wurde. Die Länder stellen die ggf. ihrerseits über Ausführungsvorschriften ergänzten Stammtexte den vollziehenden Behörden auf Landes- oder kommunaler Ebene zur Verfügung. Die das Verfahren ausführende Stelle muss in der Regel lediglich die ortspezifischen Informationen zu einer finalen Beschreibung des Verfahrens ergänzen.

Das so genannte „Föderale Stammtexte-Management“ über den LeiKa trägt wesentlich zur Konsolidierung der Redaktionsaufwände zu Verfahrensinformationen in der öffentlichen Verwaltung bei. Auskünfte zu Verfahren in allgemein verständlicher Sprache müssen nicht mehr durch jede vollziehende Landes- oder Kommunalbehörde vollständig selbst erstellt und gepflegt werden. Über den LeiKa kann auf validierte und aktuelle Ver-

fahrensinformationen zugegriffen werden. Dadurch werden deutschlandweit einheitliche und sachlich richtige Auskünfte zu Verwaltungsverfahren unterstützt. Um der Verpflichtung, die mit § 3 geschaffen wird, nachzukommen, bietet es sich also an, dass die Behörden der Länder die im LeiKa zusammengestellten Informationen nutzen und betreffend das jeweilige Verfahren vollständig über öffentlich zugängliche Netze veröffentlichen.

Verwaltungsintern sollten die Informationen in einer maschinenlesbaren Form zur Weiterverarbeitung durch internetbasierte Endkundenanwendungen der öffentlichen Verwaltung auf allen staatlichen Ebenen zur Verfügung gestellt werden. Die Bereitstellung der Informationen sollte sich in Struktur und Format an den zwischen Bund und Ländern festgelegten Standards des LeiKa richten. Die Bereitstellung der Informationen sollte möglichst im Vorfeld des Inkrafttretens einer regulatorischen Änderung oder innerhalb einer kurzen Frist bei ungeplanten Ereignissen, wie beispielsweise ad hoc eintretenden Informationslagen, erfolgen.

Die Regelung dient den Zielen 3 und 18 der nationalen E-Government-Strategie („Die Nutzer haben einfachen Zugang zur Verwaltung“ und „Inhalte, Basisdienste, Anwendungen und Infrastrukturen lassen sich bündeln und wiederverwenden“). Dabei vereinfacht die Bereitstellung von Informationen zu Verfahren nicht nur den elektronischen, sondern auch alle anderen Zugangswege zur Behörde. Es wurde eine Soll-Vorschrift gewählt, weil bei der Anwendung nach den Aufgaben der Behörden zu differenzieren ist. Sie richtet sich in erster Linie an Behörden mit Publikumsverkehr und ist nicht in vollem Umfang anwendbar auf Behörden, die keine Verfahren mit Beteiligung von Bürgerinnen, Bürgern oder Unternehmen abwickeln.

Zweck der Vorschrift ist, dass Bürgerinnen, Bürger oder Unternehmen über öffentlich zugängliche Netze (das Internet oder mobile Anwendungen) und alle weiteren Zugangskanäle gleichlautende Informationen erhalten können dahingehend, wie ein bestimmtes Verfahren abläuft, welche Nachweise gefordert werden, welche Kosten entstehen und wer ihre zuständige Ansprechstelle in der Behörde ist. Eine funktionale Beschreibung der Ansprechstelle ist ausreichend, jedoch ist auch eine namentliche Nennung des zuständigen Ansprechpartners zulässig (vgl. Beschluss des BVerwG vom 12. März 2008 - 2B 131.07).

3. Anordnungsvorbehalt für Gemeinden und Gemeindeverbände (Absatz 3)

Absatz 3 stellt klar, dass es sich hierbei um die einzige Norm des EGovG handelt, mit der eine Aufgabenübertragung erfolgt und nicht lediglich ein Verwaltungsverfahren ausgestaltet wird. Die Bereitstellung von Informationen zu Behörden und über ihre Verfahren in öffentlich zugänglichen Netzen erfolgt unabhängig von einem konkreten Verwaltungsverfahren und wird den Behörden als neue Aufgabe übertragen.

Vor dem Hintergrund Unzulässigkeit der Aufgabenübertragung durch Bundesrecht an die Gemeinden und Gemeindeverbände, vgl. Artikel 84 Absatz 1 Satz 7, 85 Absatz 1 Satz 2 GG, ist die Geltung der Verpflichtung in § 3 EGovG unter den Vorbehalt einer Anordnung nach Landesrecht gestellt.

Erst wenn eine landesrechtliche Regelung diese Aufgabe Gemeinden undGemeindeverbänden überträgt, tritt die Rechtsfolge der Absätze 1 und 2 mit der entsprechenden Verpflichtung ein.

§ 4

Elektronische Bezahlmöglichkeiten

Fallen im Rahmen eines elektronisch durchgeführten Verwaltungsverfahrens Gebühren oder sonstige Forderungen an, muss die Behörde die Einzahlung dieser Gebühren oder die Begleichung dieser sonstigen Forderungen durch Teilnahme an mindestens einem im elektronischen Geschäftsverkehr üblichen und hinreichend sicheren Zahlungsverfahren ermöglichen.

Erläuterungen

Die Regelung dient der Umsetzung des Ziels A.4 der Nationalen E-Government-Strategie („Alle geeigneten Verwaltungsangelegenheiten lassen sich über das Internet abschließend elektronisch erledigen"). Sehr häufig fallen in einem Verwaltungsverfahren Gebühren oder sonstige Forderungen (öffentlich-rechtlicher, gegebenenfalls auch privatrechtlicher Natur) an. Diese sollen mittels üblicher Zahlungsverfahren wie z. B. mittels Überweisung, Lastschrift, EC-Karte, Kreditkarte oder elektronische Bezahlsysteme (über Payment-Service-Provider), die sich bereits im elektronischen Geschäftsverkehr als unbare Zahlungsmethoden bewährt haben, beglichen werden können. Da die Möglichkeit besteht, eine Überweisung online abzuwickeln, ist die gesetzliche Vorgabe also bereits dann erfüllt, wenn für die Zahlung von Gebühren oder sonstiger Forderungen eine Bankverbindung angegeben wird. Beim Einsatz dieser Systeme ist den Anforderungen der Datensicherheit und des Datenschutzes hinreichend Rechnung zu tragen.

Mit der Regelung werden die Behörden verpflichtet, mindestens eines dieser üblichen Zahlverfahren anzubieten, damit die an dem Verwaltungsverfahren Beteiligten die Gebühren oder sonstigen Forderungen öffentlich-rechtlicher, gegebenenfalls auch privatrechtlicher Art, auf einfache Weise begleichen können. Dies gilt auch für die Träger von Sozialleistungen, die Bundesrecht ausführen, mit Ausnahme der Gemeinden und Gemeindeverbände. Der Zahlungspflichtige soll nicht etwa aus diesem Grunde doch eine Behörde persönlich aufsuchen müssen. Das Angebot ist bei Verwaltungsverfahren zu eröffnen, die ganz oder teilweise elektronisch durchgeführt werden und bei denen Bürgerinnen und Bürger für das gesamte Verfahren keine Behörde persönlich aufsuchen müssen. Zu den öffentlich-rechtlichen Forderungen zählen neben den Gebühren auch Steuern und steuerliche Nebenleistungen sowie alle sonstigen Abgaben wie Beiträge, Zinsen, Geldstrafen oder Geldbußen. Für die Behörden des Bundes steht als E-Payment-Lösung die „Zahlungsverkehrsplattform des Bundes ZVP BundOnline 2005" zur Verfügung. Andere vorhandene Zahlungsplattformen der Länder können ebenso genutzt werden. Weitere Möglichkeiten wären eine Anbindung an das jeweilige Kassensystem der Kommune oder die Anbindung des Fachverfahrens.

Die Regelung beruht auf einem Vorschlag seitens der Länder.

§ 5

Nachweise

(1) Wird ein Verwaltungsverfahren elektronisch durchgeführt, können die vorzulegenden Nachweise elektronisch eingereicht werden, es sei denn, dass durch Rechtsvorschrift etwas anderes bestimmt ist oder die Behörde für bestimmte Verfahren oder im Einzelfall die Vorlage eines Originals verlangt. Die Behörde ent-

scheidet nach pflichtgemäßem Ermessen, welche Art der elektronischen Einreichung zur Ermittlung des Sachverhalts zulässig ist.

(2) Die zuständige Behörde kann erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, mit der Einwilligung des Verfahrensbeteiligten direkt bei der ausstellenden öffentlichen Stelle elektronisch einholen. Zu diesem Zweck dürfen die anfordernde Behörde und die abgebende öffentliche Stelle die erforderlichen personenbezogenen Daten erheben, verarbeiten und nutzen.

(3) Sofern gesetzlich nichts anderes bestimmt ist, kann die Einwilligung nach Absatz 2 elektronisch erklärt werden. Dabei ist durch die Behörde sicherzustellen, dass der Betroffene

1. seine Einwilligung bewusst und eindeutig erteilt hat,

2. den Inhalt der Einwilligung jederzeit abrufen kann und

3. die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

Die Einwilligung ist zu protokollieren.

Erläuterungen

1. Vorbemerkungen

Ein bedeutendes Hindernis für die Etablierung durchgehend elektronischer Verfahrensabwicklung ist das Erfordernis der Vorlage von Nachweisen und Bescheiden im Original. Wenn die zur Begründung eines Antrags erforderlichen Nachweise im (Papier-)Original vorgelegt werden müssen, entfällt für den Antragsteller die mit der elektronischen Antragstellung verbundene Verfahrenserleichterung. Infolgedessen wird in diesen Fällen auch der Antrag häufig in Papierform gestellt werden. Für die Verwaltung bedeutet dies einen Medienbruch, der z. B. bewirkt, dass Daten aufwändig manuell in Fachanwendungen übernommen und – bei elektronischer Aktenführung – die Papieranträge eingescannt werden müssen. Die Vorschrift trägt dazu bei, hier zu durchgehend elektronischen Lösungen zu kommen, und dient damit der Umsetzung des Ziels B.6 der Nationalen E-Government-Strategie („Prozessketten sind ebenenübergreifend und kundenorientiert optimiert sowie durchgängig digitalisiert“). Die Vorschrift gilt auch für das Sozialverwaltungsverfahren mit Ausnahme des vom Anwendungsbereich dieses Gesetzes nicht umfassten Verfahrens nach dem SGB II. Für die Form der Einwilligung gilt jedoch der insoweit speziellere § 67b Absatz 2 SGB X.

2. Elektronische Nachweise (Absatz 1)

Die elektronische Durchführung eines Verwaltungsverfahrens erfasst sowohl die durchgängige wie auch die lediglich teilweise elektronische Durchführung mittels elektronischer Kommunikation (vgl. § 2).

Die Verwaltungspraxis lässt bereits derzeit häufig die Vorlage von Kopien genügen. Dies soll zur Regel werden, wenn die Vorlage eines Originals nicht durch Rechtsvorschrift angeordnet ist oder die Behörde in Ausübung ihres Verfahrensermessens (§ 26 VwVfG) für bestimmte Verfahren (z. B. Visumverfahren) oder im Einzelfall die Vorlage eines Originals verlangt, da selbst eine beglaubigte elektronische Kopie ausnahmsweise keine hinreichende Sicherheit gewährt. Letzteres kommt insbesondere bei Verfahren in Betracht, bei denen ein besonderes Täuschungsrisiko besteht. Auch für den Fall, dass Umstände zu der Annahme berechtigen, dass die eingereichte elektronische Kopie mit dem Original

nicht übereinstimmt, kann die Behörde die Vorlage im Original verlangen. Solche Umstände können z. B. Bearbeitungsspuren an der Kopie oder Inkonsistenzen im Vorbringen sein, die anderweitig in dem Verfahren zutage getreten sind oder in einem späteren Stadium zutage treten. Als Originale sind sowohl papiergebundene Formate wie auch elektronische Originale zu verstehen. Die von der Behörde zu bestimmende Art der Einreichung umfasst neben der Frage der Zulassung einer Kopie oder der Forderung des Originals auch die bewusst technikoffen gestaltete und an § 3a VwVfG angelehnte Frage, in welchem Format ein elektronisches Dokument einzureichen ist.

3. Elektronische Übermittlung von Nachweisen zwischen verschiedenen Behörden (Absatz 2)

Der Grundsatz, dass personenbezogene Daten regelmäßig beim Betroffenen zu erheben sind, führt häufig dazu, dass dieser die Daten auch dann noch einmal erneut bei einer Behörde angeben muss, wenn die Daten bereits in einem anderen Verwaltungsverfahren bei einer anderen Behörde angegeben wurden. Dies ist nicht nur eine unnötige Erschwernis für Bürgerinnen und Bürger sowie Unternehmen, sondern auch für die elektronische Abwicklung von Verwaltungsverfahren. Denn wenn in einem Verwaltungsverfahren als Nachweise z. B. Bescheide oder Bescheinigungen einer anderen Behörde benötigt werden, könnte die Behörde auf die Vorlage der Originale durch Bürgerinnen und Bürger oder das Unternehmen verzichten und stattdessen diese Nachweise elektronisch bei der ausstellenden Behörde einholen. Auch andere öffentliche Stellen im Sinne des Bundesdatenschutzgesetzes (BDSG) wie z. B. Organe der Rechtspflege, Handwerkskammern stellen häufig Bescheinigungen aus, die in Verwaltungsverfahren benötigt werden. Sie sollten daher diesbezüglich gleichgestellt werden. Elektronische Bescheinigungen der Handwerkskammern entsprechen bereits der Praxis im Rahmen der Anwendung der Dienstleistungsrichtlinie.

Dieser Weg ist insbesondere dann von Interesse, wenn wegen eines besonderen Bedürfnisses nach Verlässlichkeit der Nachweise die Vorlage einfacher elektronischer Kopien durch den Antragsteller nicht ausreicht. Im Interesse der Bürgerfreundlichkeit sollte die Devise „die Daten sollen laufen, nicht die Bürgerin/der Bürger“ den Verwaltungsverfahren zugrunde gelegt werden. § 5 Absatz 2 ist eine Kann-Bestimmung. Der Antragsteller hat die Möglichkeit der Entscheidung, ob er der Behörde die Daten selbst übermittelt, z. B. durch Vorlage der Originalbescheide, oder ob er die Behörde ermächtigt, die Daten bei der Stelle abzurufen, bei der sie vorliegen. Dabei darf die Mitwirkungspflicht, die sich auch auf das Beibringen von Unterlagen erstreckt, nicht auf die Behörde abgewälzt werden. Es bedarf weiterhin einer aktiven Beteiligung des Antragstellers. § 26 VwVfG bleibt als Grundsatz von der Regelung des § 5 EGovG unberührt.

Als bereichsspezifische Ausnahme zum in § 4 Absatz 2 Satz 1 BDSG normierten Grundsatz der Direkterhebung regelt Absatz 2 daher als weitere Verfahrenserleichterung, dass eine für ein Verwaltungsverfahren zuständige Behörde erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, direkt bei der ausstellenden Behörde elektronisch einholen kann. Die Erforderlichkeit der Datenübermittlung ergibt sich auch aus dem datenschutzrechtlichen Rahmen, der für die anfordernde und die abgebende Behörde gilt.

Dabei muss die Einwilligung des betroffenen Verfahrensbeteiligten vorliegen. Gegebenenfalls notwendige Schwärzungen personenbezogener oder schutzwürdiger Daten Dritter, auf die sich die Einwilligung naturgemäß nicht beziehen kann, sind dabei auch in elektronischen Dokumenten vorzunehmen. Die Einwilligung des Verfahrensbeteiligten ist entbehrlich, sofern Rechtsvorschriften die Erhebung bei der ausstellenden Behörde bzw. die Übermittlung zwischen den beteiligten Stellen erlauben. Der Grundsatz der Direkterhebung gilt dann nicht, sofern es spezialgesetzliche Sondervorschriften gibt.

Im Zusammenhang mit der Datenübermittlung ist auch die Frage nach einem sicheren Übermittlungsweg zwischen den Behörden relevant. Die Software Governikus kann in 15 Bundesländern im Rahmen bestehender Lizenz- und Pflegeverträge genutzt werden und gewährleistet eine sichere Kommunikation nach dem OSCI-Standard. Melde- und Justizbehörden nutzen dieses System bereits.

4. Ausgestaltung des Einwilligungsvorbehalts (Absatz 3)

Die Einwilligung kann nach Absatz 3 auch elektronisch erteilt werden. Für die elektronische Einwilligung, die bislang für den Bereich des Datenschutzes nicht normiert ist, wurde an die Anforderungen des § 13 Absatz 2 des Telemediengesetzes angeknüpft. Die Ausgestaltung dieser Anforderungen soll einfach und bürgerfreundlich erfolgen, ohne unnötigen zusätzlichen Verwaltungsaufwand zu produzieren. So kann – ähnlich wie zu AGB bei Internet-Verkäufen – die bewusste Aktivierung eines Einwilligungsfeldes ausreichend sein.

§ 6

Elektronische Aktenführung

Die Behörden des Bundes sollen ihre Akten elektronisch führen. Satz 1 gilt nicht für solche Behörden, bei denen das Führen elektronischer Akten bei langfristiger Betrachtung unwirtschaftlich ist. Wird eine Akte elektronisch geführt, ist durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik sicherzustellen, dass die Grundsätze ordnungsgemäßer Aktenführung eingehalten werden.

Erläuterungen

1. Begriff und Vorteile der elektronischen Aktenführung

Eine elektronische Akte ist eine logische Zusammenfassung sachlich zusammengehöriger oder verfahrensgleicher Vorgänge und/oder Dokumente, die alle bearbeitungs- und aktenrelevanten E-Mails, sonstigen elektronisch erstellten Unterlagen sowie gescannten Papierdokumente umfasst und so eine vollständige Information über die Geschäftsvorfälle eines Sachverhalts ermöglicht. Die elektronische Akte ersetzt auf diese Weise die Aktenführung auf Papierbasis. Die Vorteile der elektronischen Akte liegen vor allem im schnelleren Auffinden bearbeitungsrelevanter Informationen, im ortsunabhängigen, kontinuierlichen Zugriff auf Informationen, im Wegfall von Medienbrüchen und in der Verbesserung von Transparenz. Daher sollen die Behörden des Bundes die Akten möglichst elektronisch führen.

2. Regelungstechnik (Soll-Vorschrift)

Um die mit der Umstellung auf eine elektronische Aktenführung erforderliche Bewältigung der komplexen technisch-organisatorischen Aufgaben zu ermöglichen, wurde eine „Soll-Regelung“ gewählt, die mit zeitlicher Verzögerung in Kraft tritt. Bis zu diesem Zeitpunkt ist der Übergang zur elektronischen Aktenführung in das Ermessen der Behörde gestellt. Dies trägt insbesondere dem Umstand Rechnung, dass die Behörden je nach Haushaltslage einer Übergangszeit bedürfen, um die technischen, organisatorischen und finanziellen Voraussetzungen für die Einführung der elektronischen Aktenführung zu schaffen. Neben einer stufenweisen, zeitlich gestreckten Einführung können dabei auch Teilbereiche, die besondere Schwierigkeiten in der Umsetzung erwarten lassen (z. B. Personalak-

ten oder Verschlusssachen), einer späteren, nicht oder weniger verbindlich gestalteten Stufe vorbehalten sein. Die Regelung bietet hier den notwendigen Spielraum, um notwendigen individuellen Bedarfslagen einzelner Behörden angemessen Rechnung zu tragen.

3. Vorbehalt der Wirtschaftlichkeit

Ist die Einführung der elektronischen Akte in Einzelfällen auf einen langfristigen Zeitraum betrachtet unwirtschaftlich (z. B. bei kleinen und Kleinst-Behörden oder Behörden mit geringen Aktenbeständen), ist eine notwendige Abweichung von dem gesetzlichen Gebot denkbar. Eine Abweichung von der Soll-Vorschrift ist auch gerechtfertigt, soweit bei den Nachrichtendiensten des Bundes überwiegende nachrichtendienstliche Belange einer elektronischen Aktenführung entgegenstehen oder Gründe der besonderen Geheimhaltung im Sinne der Verschlusssachenanweisung diese unwirtschaftlich machen. Eine Abweichung von der Soll-Vorschrift kann ferner gerechtfertigt sein, soweit die Vergabekammern im Sinne des Vierten Teils des Gesetzes gegen Wettbewerbsbeschränkungen als europarechtlich vorgeschriebene, unabhängige Kontrollinstanz in einem gerichtsähnlichen Verfahren entscheiden.

4. Gewährleistung ordnungsgemäßer Aktenführung

Der nicht gesetzlich normierte Grundsatz ordnungsgemäßer Aktenführung umfasst die Pflicht der Behörde zur objektiven Dokumentation des bisherigen wesentlichen sachbezogenen Geschehensablaufs und folgt aus dem Rechtsstaatsprinzip, da nur eine geordnete Aktenführung einen rechtsstaatlichen Verwaltungsvollzug mit der Möglichkeit einer Rechtskontrolle durch Gerichte und Aufsichtsbehörden ermöglicht. Hieraus ergibt sich die Verpflichtung der öffentlichen Verwaltung, Akten zu führen (Gebot der Aktenmäßigkeit), alle wesentlichen Verfahrenshandlungen vollständig und nachvollziehbar abzubilden (Gebot der Vollständigkeit und Nachvollziehbarkeit) und diese wahrheitsgemäß aktenkundig zu machen (Gebot wahrheitsgetreuer Aktenführung). Umgekehrt folgt aus dieser Pflicht das grundsätzliche Verbot der nachträglichen Entfernung und Verfälschung von rechtmäßig erlangten Erkenntnissen und Unterlagen aus den Akten (Sicherung von Authentizität und Integrität) sowie das Gebot, den Aktenbestand langfristig zu sichern. Diese Grundsätze gelten auch für die auf IT gestützte elektronische Aktenführung. Die elektronische Akte ist daher auf Datenträgern zu führen, die ermöglichen, dass ihr Inhalt wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand unbefugt geändert oder gelöscht werden kann. Die Daten müssen zudem bis zum Ablauf der Aufbewahrungsfrist gespeichert werden können. Daneben ist unter Datenschutzaspekten die Vertraulichkeit (und ggf. Löschbarkeit) der Daten zu gewährleisten. Nicht zuletzt ist die Verkehrsfähigkeit sicherzustellen und dass die Inhalte in vertretbarer Zeit verfügbar sind und lesbar gemacht werden können. Dies kann die sichere Portierung und Konvertierung aufgrund der begrenzten Haltbarkeit der Trägermedien oder Datenformate auf aktuelle Datenträger oder Datenformate beinhalten.

Die Art und Weise der Aktenführung steht weitestgehend im Organisationsermessen der Behörden. Eine gesetzliche Klarstellung erscheint jedoch geboten, um den (Rechts-)Unsicherheiten zu begegnen, die in der Verwaltungspraxis derzeit noch hinsichtlich der Zulässigkeit der elektronischen Aktenführung und der einzuhaltenden Anforderungen bestehen. Daneben ermöglicht nur eine umfassende Nutzung der elektronischen Aktenführung ein durchgängig medienbruchfreies elektronisches Verwaltungshandeln.

Die Behörde hat durch geeignete technisch-organisatorische Maßnahmen nach dem – jeweils geltenden – Stand der Technik sicherzustellen, dass die zuvor beschriebenen Grundsätze der ordnungsgemäßen Aktenführung eingehalten werden.

Die zur Umsetzung dieser Vorgaben erforderlichen konkreten technisch-organisatorischen Maßnahmen werden aufgrund der rasant voranschreitenden technischen Entwicklung nicht explizit gesetzlich vorgegeben. Die Behörde kann hierzu konkretisierende organisa-

torische Regelungen treffen oder vorhandene technische Richtlinien nutzen. Für den Erhalt des Beweiswerts qualifiziert elektronisch signierter Dokumente kann z. B. die Technische Richtlinie des BSI (TR-03125 (TR-ESOR)) als Stand der Technik herangezogen werden. Diese ist abrufbar unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_V1.1.pdf?__blob=publicationFile.

§ 7

Übertragen und Vernichten des Papieroriginals

(1) Die Behörden des Bundes sollen, soweit sie Akten elektronisch führen, an Stelle von Papierdokumenten deren elektronische Wiedergabe in der elektronischen Akte aufbewahren. Bei der Übertragung in elektronische Dokumente ist nach dem Stand der Technik sicherzustellen, dass die elektronischen Dokumente mit den Papierdokumenten bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. Von der Übertragung der Papierdokumente in elektronische Dokumente kann abgesehen werden, wenn die Übertragung unverhältnismäßigen technischen Aufwand erfordert.

(2) Papierdokumente nach Absatz 1 sollen nach der Übertragung in elektronische Dokumente vernichtet oder zurückgegeben werden, sobald eine weitere Aufbewahrung nicht mehr aus rechtlichen Gründen oder zur Qualitätssicherung des Übertragungsvorgangs erforderlich ist.

Erläuterungen

1. Übertragung in elektronische Dokumente (Absatz 1)

Diese Norm gilt für die Behörden des Bundes, soweit nicht spezielle Gesetze vorgehen, z. B. die §§ 110a bis 110d SGB IV.

Die Behörden sollen anstelle der Papierdokumente diese als elektronische Wiedergabe in der elektronischen Akte aufbewahren.

Satz 2 konkretisiert die Anforderungen an die Übertragung von Papierdokumenten in die elektronische Form. Zugleich werden damit auch Anforderungen an das Scanergebnis festgelegt. Das Scannen von Papierdokumenten ist Voraussetzung für ein im Weiteren medienbruchfreies Verwaltungsverfahren und stellt künftig den Regelfall dar, was durch die „Soll"-Regelung zum Ausdruck gebracht wird. Zur Sicherstellung auf Übereinstimmung mit dem Papieroriginal ist eine vollständige Sichtprüfung aller Digitalisate dabei nicht erforderlich. Die Behörde kann konkretisierende organisatorische Regelungen in einer internen Organisationsverfügung (Scan-Anweisung) treffen.

Nach Satz 2 hat die Behörde für die Umwandlung in ein digitales Dokument nach dem Stand der Technik die Übereinstimmung zwischen Papierdokument und Digitalisat sicherzustellen. Als Beispiel für den Stand der Technik kann die Technische Richtlinie „Rechtssicheres ersetzendes Scannen" (TR-RESISCAN) des BSI herangezogen werden. Diese ist inklusive Anlagen abrufbar unter:
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html.
Hiernach werden Anforderungen technisch-organisatorischer Art an Scanprozesse entwickelt, deren Einhaltung das Erstellen und die Anwendung möglichst rechtssicherer Scanlösungen ermöglicht. Gegenstand der Richtlinie sind Papieroriginale, die in einem siche-

ren Scanprozess so eingescannt werden können, dass trotz Vernichtung des Originals die damit einhergehende Minderung des Beweiswerts so gering wie möglich ist.

Satz 3 beinhaltet eine Generalklausel für Ausnahmen vom Scannen. Soweit der Aufwand technisch unvertretbar hoch ist, kann die Behörde von dem Grundsatz des Satzes 1 abweichen. Dies kann z. B. bei großen Formaten der Fall sein, die mit herkömmlichen Scan-Geräten nur unter erhöhtem Aufwand eingelesen werden können.

Die Bestimmungen des § 7 beziehen sich nicht auf „Altbestände“ von Papierakten. Ob eine Umwandlung von bereits vorhandenen Papierunterlagen in die E-Akte erfolgt, ist unter Berücksichtigung des Wirtschaftlichkeitsgebots in das Ermessen der jeweiligen Behörde gestellt.

2. Vernichten des Papieroriginals (Absatz 2)

Nach Einführung der elektronischen Akte soll diese grundsätzlich die einzige bzw. die „führende“ Akte sein. Bereits aus Gründen der erforderlichen Ressourcen soll eine doppelte Aktenführung nach Möglichkeit vermieden werden.

Das ersetzende Scannen ist in vielen Bereichen bereits Praxis. Regelungen dazu gibt es bisher kaum. Auch § 298a Absatz 2 der Zivilprozessordnung (ZPO) trifft lediglich generelle Aussagen. Allein untergesetzlich ist bislang die Richtlinie für das Bearbeiten und Verwalten von Schriftgut (Akten und Dokumenten) in Bundesministerien (Registraturrichtlinie) einschlägig. In der Praxis bestehen beträchtliche Rechtsunsicherheiten hinsichtlich der Zulässigkeit und der Grenzen des ersetzenden Scannens, die die Ausbreitung der elektronischen Aktenführung hemmen und nach einer gesetzlichen Klarstellung verlangen.

Absatz 2 beinhaltet die Ermächtigungsgrundlage für die Vernichtung der eingescannten Papierunterlagen nach ihrer Digitalisierung, so dass das Scanprodukt zur Grundlage der weiteren Bearbeitung gemacht werden kann. Dabei soll das ersetzende Scannen zum Regelfall des Umgangs mit Papierdokumenten werden.

Eine vorübergehende Aufbewahrung (in der Praxis dürften bis zu 6 Monate ausreichend sein) der Originaldokumente nach dem Scanvorgang in einer Zwischenablage der Behörde kann zum Zweck der "Qualitätsprüfung" des Digitalisats zweckmäßig sein. Hierdurch können nachträgliche Korrekturen vorgenommen werden, falls trotz der technischen und organisatorischen Vorkehrungen für den Scanvorgang einmal ein Dokument fehlerhaft oder unvollständig eingescannt worden sein sollte. Auch können Dokumente doch noch erhalten werden, wenn sich erst im Verlauf der Sachbearbeitung herausstellt, dass es auf die Originaleigenschaft ankommen könnte.

Eine ausnahmslose Vernichtung des Papieroriginals ist aufgrund des Rechts auf effektiven Rechtsschutz nach Artikel 19 Absatz 4 GG sowie aufgrund des im Rechtsstaatsprinzip verbürgten Justizgewährungsanspruchs nicht möglich. Hierzu zählt das Recht auf faires Verfahren, zu dem auch eine faire Handhabung des Beweisrechts gehört. Mit der ausnahmslosen Vernichtung der Originalurkunden würde in einzelnen Fällen dem Betroffenen die Möglichkeit genommen, den Urkundsbeweis führen zu können. Durch den Scanvorgang entsteht nur ein zweidimensionales Abbild des Originals. Die forensischen Prüfungsmöglichkeiten, etwa im Hinblick auf die Echtheit einer handschriftlichen Unterschrift, sind gegenüber einem Originaldokument eingeschränkt. Zudem sind Privaturkunden grundsätzlich im Original vorzulegen, wenn der Urkundsbeweis greifen soll.

Ausnahmen von der grundsätzlichen Vernichtung des Papierdokuments greifen, wenn es für das Verfahren auf die Originaleigenschaft des Dokumentes ankommt bzw. eine Vernichtung aus anderen Gründen ausgeschlossen ist.

Als solche Ausnahmetatbestände können in Betracht kommen:

– Ausschluss der Vernichtung durch eine (spezialgesetzliche) Vorschrift,

– eine nur für die Dauer der Bearbeitung vorübergehende Überlassung der Dokumente, die dann nicht in das Eigentum der Behörde übergehen und dem Absender entweder nach expliziter Erklärung oder aus den Umständen des Falles erkennbar zurückzugeben sind (z. B. bei Ausweispapieren, Originalverträgen),

– Urkunden, an denen die Verfahrensbeteiligten ein Beweisführungsrecht haben und bei denen es im Verfahren auf die Gewährung der Möglichkeit des Urkundsbeweises ankommen kann.

Eine Abweichung von der Soll-Vorschrift ist auch gerechtfertigt z. B.:

– bei kulturhistorisch wertvollen archivwürdigen Papierunterlagen,

– wenn die Abgabe des Verfahrens an eine Behörde notwendig ist, die ihre Akten nicht elektronisch führt, oder

– soweit bei den Nachrichtendiensten des Bundes überwiegende nachrichtendienstliche Belange entgegenstehen.

Einzelheiten sollten von der Behörde in einer Organisationsverfügung (Scan-Anweisung) klargestellt werden, um für die betroffenen Mitarbeiter Klarheit und Rechtssicherheit zu schaffen.

Die eingescannten Papierdokumente können vernichtet werden. Die Anbietungspflicht gegenüber dem Bundesarchiv nach § 2 des Bundesarchivgesetzes wird durch die spätere Anbietung der elektronischen Dokumente erfüllt. Insoweit handelt es sich lediglich um einen Wechsel des Mediums.

§ 8

Akteneinsicht

Soweit ein Recht auf Akteneinsicht besteht, können die Behörden des Bundes, die Akten elektronisch führen, Akteneinsicht dadurch gewähren, dass sie

1. einen Aktenausdruck zur Verfügung stellen,

2. die elektronischen Dokumente auf einem Bildschirm wiedergeben,

3. elektronische Dokumente übermitteln oder

4. den elektronischen Zugriff auf den Inhalt der Akten gestatten.

Erläuterungen

Die Vorschrift regelt Art und Weise der Akteneinsicht und schafft kein eigenes Akteneinsichtsrecht. § 1 IFG wird durch sie weder modifiziert, noch eingeschränkt. Während § 1 Absatz 2 IFG dem Bürger ein Bestimmungsrecht bezüglich der Wahl einer bestimmten Art des Informationszugangs (Auskunftserteilung, Akteneinsicht, Informationszugang in sonstiger Weise) gewährt, betrifft die Regelung in § 8 EGovG lediglich die konkrete Durchführung der Akteneinsicht. Zu dieser Durchführung enthält § 1 Absatz 2 IFG aber

keine Vorgaben, vgl. Schoch, Kommentar zum IFG, 2009, § 1 Rn. 141. Das Recht auf Akteneinsicht ist Bestandteil des rechtsstaatlichen fairen Verwaltungsverfahrens und ergibt sich aus dem grundrechtlich verbürgten Anspruch auf rechtliches Gehör. Der Umfang des Akteneinsichtsrechts darf nicht vom Medium abhängig gemacht werden, dessen sich die Behörde zur Führung der Akte bedient. Soweit die allgemeinen Voraussetzungen an die Gewährung der Akteneinsicht gegeben sind bzw. eine solche überhaupt vorgesehen ist, muss also die Einsicht in die elektronische Akte im gleichen Umfang ermöglicht werden wie bei der Papierakte. Es gelten aber auch die gleichen Grenzen (z. B. sind geheimhaltungsbedürftige Informationen auszuklammern).

Über die Art und Weise der Erteilung der Akteneinsicht hat die Behörde nach pflichtgemäßem Ermessen zu entscheiden. Dabei muss die Behörde darauf achten, auch weniger technikaffine Bevölkerungsgruppen nicht auszuschließen. In diesem Fall können z. B. Papierausdrucke gefertigt werden. Auch kann die Behörde dem Begehrenden einen elektronischen Zugriff auf dem Bildschirm in den Behördenräumen ermöglichen. Hierbei sind im pflichtgemäßen Ermessen der Behörde liegende Vorkehrungen zu treffen, die sicherstellen, dass der Begehrende nur von den für ihn bestimmten Informationen Kenntnis erlangen kann und Manipulationen ausgeschlossen sind. Erforderlichenfalls sind die ihn betreffenden Teile zu extrahieren. Daneben ist auch die Zurverfügungstellung des Inhalts der elektronischen Akte mittels Datenträger oder über E-Mail-Versand zulässig.

Bei der elektronischen Übermittlung ist den Erfordernissen des § 9 BDSG Rechnung zu tragen, insbesondere ist zu gewährleisten, dass die Integrität und Authentizität der Daten sichergestellt und deren Inhalte nicht unbefugt zur Kenntnis genommen und nicht missbräuchlich verwendet werden können.

Der elektronische Zugriff auf den Akteninhalt stellt eine zukunftsträchtige, wenngleich technisch derzeit aufwendige Form der Aktenübermittlung dar. Sie ist in der Rechtsordnung bereits in § 299 Absatz 3 ZPO sowie § 100 Absatz 2 VwGO eröffnet und soll auch außerhalb gerichtlicher (Verwaltungs-)Verfahren genutzt werden können.

§ 9

Optimierung von Verwaltungsabläufen und Information zum Verfahrensstand

(1) Behörden des Bundes sollen Verwaltungsabläufe, die erstmals zu wesentlichen Teilen elektronisch unterstützt werden, vor Einführung der informationstechnischen Systeme unter Nutzung gängiger Methoden dokumentieren, analysieren und optimieren. Dabei sollen sie im Interesse der Verfahrensbeteiligten die Abläufe so gestalten, dass Informationen zum Verfahrensstand und zum weiteren Verfahren sowie die Kontaktinformationen der zum Zeitpunkt der Anfrage zuständigen Ansprechstelle auf elektronischem Wege abgerufen werden können.

(2) Von den Maßnahmen nach Absatz 1 kann abgesehen werden, soweit diese einen nicht vertretbaren wirtschaftlichen Mehraufwand bedeuten würden oder sonstige zwingende Gründe entgegenstehen. Von den Maßnahmen nach Absatz 1 Satz 2 kann zudem abgesehen werden, wenn diese dem Zweck des Verfahrens entgegenstehen oder eine gesetzliche Schutznorm verletzen. Die Gründe nach den Sätzen 1 und 2 sind zu dokumentieren.

(3) Die Absätze 1 und 2 gelten entsprechend bei allen wesentlichen Änderungen der Verwaltungsabläufe oder der eingesetzten informationstechnischen Systeme.

Erläuterungen

1. Optimierung von Verwaltungsabläufen und Information zum Verfahrensstand (Absatz 1)

a) Prozessoptimierung (Satz 1)

Die fortschreitende Vernetzung der öffentlichen Verwaltung erfordert eine konsequente Ausrichtung auf die Optimierung von Verwaltungsabläufen. Verwaltungsabläufe im Sinne dieser Vorschrift sind Prozesse, die von bestimmten Personen(gruppen) in einer sich wiederholenden Reihenfolge unter bestimmten Vorgaben (z. B. Gesetze, Verwaltungsvorschriften etc.) und unter Nutzung von Hilfsmitteln (z. B. IT-Unterstützung, Formulare etc.) bearbeitet werden. Damit wird eine bestimmte Aufgabe erfüllt – das Ergebnis ist ein Produkt, eine Leistung oder allgemeiner ein Arbeitsergebnis („output“) der Organisation. In Betracht kommen sowohl verwaltungsinterne Prozesse als auch solche mit Beteiligung von Bürgerinnen und Bürgern oder Unternehmen. Der Begriff des Verwaltungsablaufs ist im übergeordneten, verwaltungswissenschaftlichen Sinn zu verstehen. Er umfasst zugleich auch Verwaltungsverfahren gemäß § 9 VwVfG.

Die Optimierung von Verwaltungsabläufen bezieht sich auf sämtliche Methoden, mit denen die beschriebenen Prozesse in Organisationen verbessert werden. Die Optimierung dient primär dem Ziel, die einzuführenden oder vorhandenen Prozesse mit Blick auf das zu erstellende Arbeitsergebnis zu verbessern. Optimierung ist im Sinne einer Steigerung der Effizienz und der Qualität bei der Erstellung des Arbeitsergebnisses zu verstehen. Entlastungs- und Einsparpotenziale können mit der Durchführung von Prozessoptimierungen generiert werden. Ebenso soll die „Kundenorientierung“ im weiten Sinne der Orientierung an den Bedürfnissen der (verwaltungsinternen oder externen) Abnehmer des jeweiligen Arbeitsergebnisses gesteigert werden. Bei der Optimierung von Verwaltungsabläufen mit Außenwirkung hat daher auch eine Orientierung an den Bedürfnissen der beteiligten Bürgerinnen und Bürger bzw. Unternehmen zu erfolgen.

Eine prozessorientierte elektronische Verwaltungsarbeit im Sinne dieser Vorschrift setzt die systematische und ganzheitliche Untersuchung und Dokumentation von Prozessen voraus. Gängige Methoden zur Prozessmodellierung sind insbesondere solche Vorgehensweisen, die die Bundesbeauftragte für Informationstechnik für die Erfassung und Erstellung von IT-Zustandsanalysen empfiehlt.[6)]

Auf Basis der zur Dokumentation geeigneten Methoden erfolgt die Auswahl der zu verwendenden Werkzeuge, wobei deren Nutzung einheitlich erfolgen sollte. Ziel ist die einheitliche Darstellung der Prozess- und Datenmodelle durch Werkzeuge, welche die geeigneten Standards und Technologien unterstützen. Hierdurch wird zugleich dem übergreifenden Wirtschaftlichkeitsgedanken Rechnung getragen.

Auf Basis der Prozessdokumentation wird eine Analyse der Prozesse durchgeführt, die auch eine Aufgabenkritik umfasst. Die Analyse hat zum Ziel, die Wirtschaftlichkeit der Aufgabenerledigung sowie die Kommunikation und Kooperation zwischen den Prozessbeteiligten, die Funktionsfähigkeit verwaltungsübergreifender Prozesse, ihre Ausrichtung auf den Stand der Technik und ihre Sicherheit zu verbessern. Übergreifendes Ziel der Prozessanalyse ist es, Schwachstellen in den bestehenden Abläufen aufzuzeigen und Optimierungspotenziale zu erkennen. Potenzielle Synergien aus der IT-gestützten Prozessabwicklung sind vollumfänglich zu heben und die Interoperabilität der neuen Prozesse mit

---

6) vgl. http://www.cio.bund.de/DE/Architekturen-und-Standards/Daten-und-Prozessmodellierung/Prozessmodellierung/prozessmodellierung_node.html

vor- und nachgelagerten Prozessen ist sicherzustellen, wobei insbesondere die Schnittstellen dieser Prozesse zu externen Prozessbeteiligten zu berücksichtigen sind.

Die Prozessanalyse ist zu dokumentieren, um eine verlässliche Grundlage für die informationstechnische Umsetzung zu schaffen.

Insbesondere bei verwaltungsträgerübergreifenden Prozessen ist für den Erfolg der Prozessanalyse wichtig, dass soweit wie möglich durchgängige, trägerübergreifende Standardmethoden eingesetzt werden. Es empfiehlt sich daher, dass der IT-Rat der Bundesregierung und der IT-Planungsrat entsprechende Standards etablieren.

b) Abruf von Informationen (Satz 2)

Die Regelung dient der Umsetzung des Ziels A.4 der Nationalen E-Government-Strategie („Alle geeigneten Verwaltungsangelegenheiten lassen sich über das Internet abschließend elektronisch erledigen“). Werden Verwaltungsabläufe elektronisch angeboten, ist es möglich, den Verfahrensbeteiligten medienbruchfrei und automatisiert Informationen zum Verfahrensstand bereitzustellen. Dadurch lässt sich für Bürgerinnen und Bürger sowie Unternehmen nutzerfreundlich und zeitsparend Verfahrenstransparenz herstellen. Hiervon erfasst werden nur Verfahren, die eine Außenwirkung haben; für rein verwaltungsinterne Verfahren greift die Verpflichtung nicht. Die Verwaltung kann durch das elektronische Bereitstellen der Informationen eine Entlastung erfahren, da eine bislang häufig telefonisch erfolgte Information auf Nachfragen der Beteiligten in vielen Fällen unterbleibt. Die Angabe des Verfahrensstandes soll dabei so konkret wie möglich erfolgen, um dem Auskunftsinteresse des Verfahrensbeteiligten nachzukommen, aber auch so abstrakt wie nötig, um das Verfahren nicht zu gefährden bzw. den Handlungsspielraum der Behörde einzuengen (vgl. hierzu auch Ausnahmetatbestände in Absatz 2).

2. Ausnahmen (Absatz 2)

Die Vorschrift beschreibt abschließend die Ausnahmen zu den Anordnungen nach Absatz 1. Mit ihr wird dem Umstand Rechnung getragen, dass es Fälle geben kann, in denen die nach Absatz 1 zu treffenden Maßnahmen den Grundsätzen der Wirtschaftlichkeit und Sparsamkeit widersprechen (§ 7 der Bundeshaushaltsordnung). Dies ist z. B. der Fall, wenn von vornherein kein Optimierungspotenzial absehbar ist, so dass Kosten und Aufwand, welche für die Durchführung der Dokumentation und Analyse nach Absatz 1 Satz 1 aufgebracht werden müssten, in keinem Verhältnis zu dem möglichen Optimierungsziel stehen würden. Daneben können Fälle in Betracht kommen, bei denen die Kenntnis des Verfahrensstandes den Verfahrenszweck gefährden oder den Erfolg der Entscheidung vereiteln würde (etwa bei laufenden Ermittlungsverfahren oder bei beabsichtigten Vollzugmaßnahmen). Letztlich sind auch gesetzliche Offenbarungsverbote zu beachten. Nach Satz 2 sind die Gründe einer Abweichung von Absatz 1 zu dokumentieren. Diese sind für alle Fälle des Absatzes 1 gesondert zu prüfen.

3. Erweiterung auf laufende Verwaltungsabläufe (Absatz 3)

Mit dieser Vorschrift wird der Auftrag der Absätze 1 und 2 für laufende IT-gestützte Verwaltungsabläufe erweitert. Unter Wirtschaftlichkeitsgesichtspunkten sollen aber die Prozessanalyse und die elektronische Bereitstellung von Informationen zum Verfahrensstand erst bei einer anstehenden, umfangreichen Anpassung oder Weiterentwicklung des entsprechenden IT-Verfahrens erfolgen, z. B. Versions- oder Releasewechsel. Wesentliche Änderungen der eingesetzten informationstechnischen Systeme im Sinne der Vorschrift liegen erst dann vor, wenn sich diese Änderungen wesentlich auf die Verwaltungsabläufe auswirken.

§ 10

Umsetzung von Standardisierungsbeschlüssen des IT-Planungsrates

Fasst der Planungsrat für die IT-Zusammenarbeit der öffentlichen Verwaltung zwischen Bund und Ländern (IT-Planungsrat) einen Beschluss über fachunabhängige und fachübergreifende IT-Interoperabilitäts- oder IT-Sicherheitsstandards gemäß § 1 Absatz 1 Satz 1 Nummer 2 und § 3 des Vertrages über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern - Vertrag zur Ausführung von Artikel 91c GG (BGBl. 2010 I S. 662, 663), so beschließt der Rat der IT-Beauftragten der Bundesregierung (IT-Rat) die Umsetzung dieses Beschlusses innerhalb der Bundesverwaltung. § 12 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik gilt entsprechend.

Erläuterungen

Die Vorschrift regelt die Umsetzung von Standardisierungsbeschlüssen des IT-Planungsrats innerhalb der Bundesverwaltung.

Satz 1 knüpft an die bestehende Rechtslage zur Bund-Länder-übergreifenden IT-Standardisierung an. Gemäß § 1 Absatz 1 Satz 1 Nummer 2 des Vertrages über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG vom 20. November 2009 (BGBl. 2010 I S. 662, 663) (IT-Staatsvertrag) ist der IT-Planungsrat befugt, fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards zu beschließen. Diese Beschlüsse entfalten Bindungswirkung und sind vom Bund und von den Ländern in ihren jeweiligen Verwaltungsräumen umzusetzen (§ 3 Absatz 2 Satz 2 des IT-Staatsvertrages). Nicht im IT-Staatsvertrag geregelt sind die Einzelheiten der Umsetzung. Satz 1 legt insoweit fest, dass der IT-Rat die Umsetzung innerhalb der Bundesverwaltung beschließt; die Festlegungen der IT-Steuerung des Bundes bleiben hiervon unberührt. Eine Einschränkung oder Ausweitung der Kompetenzen des IT-Planungsrats ist mit der Vorschrift nicht verbunden.

Der in Satz 2 enthaltene Verweis auf § 12 des Gesetzes über das BSI trifft Regelungen für den Fall einer Auflösung des IT-Rats und bestimmt zudem das Verhältnis des IT-Rats zu den Bundesministerien.

§ 11

Gemeinsame Verfahren

(1) Gemeinsame Verfahren sind automatisierte Verfahren, die mehreren verantwortlichen Stellen im Sinne des Bundesdatenschutzgesetzes die Verarbeitung personenbezogener Daten in oder aus einem Datenbestand ermöglichen. Soweit gemeinsame Verfahren auch Abrufe anderer Stellen ermöglichen sollen, gilt insoweit für die Abrufverfahren § 10 des Bundesdatenschutzgesetzes.

(2) Die Beteiligung öffentlicher Stellen des Bundes nach § 2 Absatz 1 des Bundesdatenschutzgesetzes an gemeinsamen Verfahren ist nur zulässig, wenn dies

unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit der Verarbeitung der Daten im Einzelfall bleiben unberührt.

(3) Vor der Einrichtung oder wesentlichen Änderung eines gemeinsamen Verfahrens ist eine Vorabkontrolle nach § 4d Absatz 5 und 6 des Bundesdatenschutzgesetzes durchzuführen und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zu hören. Ihm sind die Festlegungen nach Absatz 4 und das Ergebnis der Vorabkontrolle vorzulegen.

(4) Vor der Einrichtung oder wesentlichen Änderung eines gemeinsamen Verfahrens ist über die Angaben nach § 4e Satz 1 des Bundesdatenschutzgesetzes hinaus schriftlich insbesondere festzulegen,

1. **welche Verfahrensweise angewendet wird und welche Stelle jeweils für die Festlegung, Änderung, Fortentwicklung und Einhaltung von fachlichen und technischen Vorgaben für das gemeinsame Verfahren verantwortlich ist und**

2. **welche der beteiligten Stellen jeweils für die Rechtmäßigkeit der Datenerhebung, -verarbeitung und -nutzung verantwortlich ist.**

Die nach Satz 1 Nummer 1 verantwortlichen Stellen bestimmen eine der beteiligten Stellen, deren Beauftragter für den Datenschutz eine Kopie der von den beteiligten Stellen zu erstellenden Übersicht im Sinne von § 4g Absatz 2 Satz 1 des Bundesdatenschutzgesetzes verwahrt und diese nach § 4g Absatz 2 Satz 2 des Bundesdatenschutzgesetzes zusammen mit den Angaben nach Satz 1 Nummer 1 und 2 zur Einsicht für jedermann bereithält. Nach Satz 1 Nummer 1 können auch verantwortliche Stellen bestimmt werden, die andere Stellen mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten für das gemeinsame Verfahren beauftragen dürfen. § 11 des Bundesdatenschutzgesetzes bleibt im Übrigen unberührt.

(5) Soweit für die beteiligten Stellen unterschiedliche Datenschutzvorschriften gelten, ist vor Einrichtung eines gemeinsamen Verfahrens zu regeln, welches Datenschutzrecht angewendet wird. Weiterhin ist zu bestimmen, welche Kontrollstellen die Einhaltung der Datenschutzvorschriften prüfen.

(6) Die Betroffenen können ihre Rechte nach den §§ 19 bis 20 des Bundesdatenschutzgesetzes gegenüber jeder der beteiligten Stellen geltend machen, unabhängig davon, welche Stelle im Einzelfall für die Verarbeitung der jeweiligen Daten nach Absatz 4 Satz 1 Nummer 2 verantwortlich ist. Die Stelle, an die der Betroffene sich wendet, leitet das Anliegen an die jeweils zuständige Stelle weiter.

Erläuterungen

1. Vorbemerkungen

Die Regelung beruht auf einem Vorschlag seitens der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Eine entsprechende Vorschrift wäre zudem in die jeweiligen Datenschutzgesetze der Länder aufzunehmen. Die Vorschriften in den Datenschutzgesetzen von Bund und Ländern zu Abrufverfahren und gemeinsamen Verfahren sind sehr heterogen. Soweit es um länderübergreifende Verfahren geht, sollten die Regelungen in den Datenschutzgesetzen möglichst einheitlich sein, um die bestehenden Schwierigkeiten nicht noch zu erhöhen.

Nach einigen Landesdatenschutzgesetzen ist die Einrichtung von Abrufverfahren oder gemeinsamen Verfahren nur aufgrund einer speziellen Rechtsgrundlage zulässig. In der Praxis ist damit oft nicht viel gewonnen, da die notwendigen Regelungen zum Datenschutz dort nicht oder nur lückenhaft geschaffen werden. Deshalb enthält dieser Gesetzesvorschlag die gesetzliche Verpflichtung, wesentliche Punkte vor der Errichtung eines gemeinsamen Verfahrens zu regeln.

Ein weiteres Anliegen ist es, nur das zu regeln, was wirklich über die anderen Formen der Datenverarbeitung hinaus den Unterschied ausmacht (minimalistische Regelung).

Die vorgeschlagene Regelung versucht den im Vorfeld ermittelten unterschiedlichen Anforderungen an gemeinsame Verfahren gerecht zu werden, die bekannten Probleme mit den vorhandenen Regelungen zu vermeiden sowie die notwendigen Regelungen in solchen Verfahren festzuschreiben. Es sind dabei Konstellationen mit einbezogen, bei denen

– die beteiligten Stellen nicht bereits von vornherein feststehen und deshalb nicht gemeinsam einen Federführer bestimmen können (z. B. bei dem internetbasierten Online-Genehmigungsverfahren für Großraum- und Schwertransporte – Verfahrensmanagement Großraum- und Schwertransporte – VEMAGS),–

– öffentliche und nichtöffentliche Stellen beteiligt sind (z. B. VEMAGS, medizinische Fallakten), für die beteiligten Stellen unterschiedliches Datenschutzrecht gilt, eine Mitentscheidung über das Verfahren und Weiterentwicklungen faktisch nicht möglich ist (z. B. medizinische Fallakten).

Für den Sozialdatenschutz trifft § 79 SGB X für die näher bestimmten automatisierten Abrufverfahren andere Regelungen und geht damit als entgegenstehende Norm vor. Gleiches gilt für gemeinsame Dateien auf der Grundlage fachgesetzlicher Regelungen wie § 9a BNDG, § 22a BVerfSchG sowie dem ATDG.

2. Begriff des Gemeinsamen Verfahrens (Absatz 1)

a) Gemeinsames Verfahren i.e.S. (Satz 1)

Satz 1 definiert den Begriff des gemeinsamen Verfahrens. Ein gemeinsames Verfahren ist eine dauerhafte, zweckgerichtete Vereinbarung mehrerer datenschutzrechtlich verantwortlicher Stellen zu einer gemeinsamen Einrichtung einer technischen Anwendung/Plattform, in die Daten eingegeben werden und die den wechselseitigen Zugriff und Abruf auf bzw. aus einem so entstandenen gemeinsamen Datenbestand ermöglicht. Im Unterschied zur Auftragsdatenverarbeitung nach § 11 BDSG sind bei den gemeinsamen Verfahren alle beteiligten Stellen ihrerseits datenschutzrechtlich verantwortliche Stellen i. S. v. § 3 Absatz 7 BDSG, wobei jede der beteiligten Stellen ggf. nur für einen Teil der Datenverarbeitung jeweils verantwortlich ist. Ein gemeinsames Verfahren ist andererseits umfassender als das eindimensionale automatisierte Abrufverfahren. Während es bei letzterem lediglich um eine bestimmte technische Form der Übermittlung personenbezogener Daten von einer Stelle an eine andere Stelle (oder Person) geht, ist ein gemeinsames Verfahren durch eine einheitliche Plattform gekennzeichnet, die gemeinsam von mehreren Stellen zu einem bestimmten gemeinsamen Zweck mehrdimensional betrieben wird und bei der die Verantwortlichkeiten auf die beteiligten Stellen unterschiedlich verteilt sind. Die Datenverarbeitung zu Kontroll-, Prüf- und Aufsichtszwecken stellt deshalb selbst dann kein gemeinsames Verfahren dar, wenn die Übermittlung hierfür erforderlicher personenbezogener Daten mittels automatisierten Abrufs geschieht. Da auch öffentliche Stellen der Länder und nichtöffentliche Stellen im Sinne des BDSG an gemeinsamen Verfahren beteiligt sein können, wird für die Begriffsbestimmung ein weiter Ansatz gewählt. Der materiell-rechtliche Regelungsgehalt der Vorschrift beschränkt sich hingegen auf öffentliche Stellen des Bundes (siehe Absatz 2).

b) Abrufverfahren (Satz 2)

Satz 2 stellt klar, dass auch Abrufverfahren gemeinsame Verfahren sind. Abrufverfahren stellen prinzipiell eine Untermenge von Verfahren zur gemeinsamen Datenverarbeitung dar. Deshalb werden diese beiden Spielarten einer Datenverarbeitung durch mehrere Stellen in einer einheitlichen Vorschrift zusammengefasst. Nach den Definitionen der Datenübermittlung (vgl. z. B. § 3 Absatz 4 Nummer 3 Buchstabe b BDSG) ist der Abruf eine Form der Übermittlung und damit eine Datenverarbeitung für die aus einem „gemeinsamen“ Datenbestand zum Abruf bereitstellende und die aus diesem „gemeinsamen“ Datenbestand empfangende Stelle. Gemeinsam bezeichnet dabei nicht die „Besitzverhältnisse“, vielmehr ist damit gemeint, dass es derselbe Datenbestand ist. Für die an den gemeinsamen Verfahren beteiligten Stellen gilt für ihre interne Organisation und die Verhältnisse gegenüber Dritten mit Ausnahme des Abrufenden § 11 dieses Gesetzes. Für das Abrufverfahren selbst gilt hingegen der allgemeine § 10 BDSG. Das ist auch interessengerecht, da bei gemeinsamen Verfahren die Beteiligten die Datei gemeinsam gestalten (z. B. haben alle grundsätzlich Lese- und Schreibzugriff), wohingegen bei Abrufverfahren grundsätzlich die speichernde Stelle voll verantwortlich bleibt und der Abrufende lediglich eine begrenzte und im Einzelfall festzulegende Teilverantwortung trägt (reiner und begrenzter Lesezugriff).

3. Beteiligung öffentlicher Stellen des Bundes (Absatz 2)

Satz 1 stellt zunächst klar, dass das EGovG als Bundesgesetz die materiell-rechtlichen Voraussetzungen für die Beteiligung öffentlicher Stellen des Bundes an gemeinsamen Verfahren regeln kann. Die Beteiligung öffentlicher Stellen der Länder bedürfte einer Regelung in den Landesdatenschutzgesetzen, die Beteiligung nichtöffentlicher Stellen einer Regelung im BDSG. Wie bei § 10 BDSG setzt Satz 1 als allgemeine Zulässigkeitsvoraussetzung eine Abwägung zwischen den schutzwürdigen Belangen der Betroffenen und den Aufgaben der beteiligten Stellen voraus (Verhältnismäßigkeit). Je höher der Schutzbedarf der Daten desto eher wird sich die Einrichtung eines gemeinsamen Verfahrens verbieten. Im Hinblick auf die Beteiligung öffentlicher Stellen des Bundes ersetzt die Regelung als spezifische Regelung im Sinne von § 1 Absatz 3 BDSG deshalb die allgemeine Regelung des § 10 BDSG.

Satz 2 stellt klar, dass – auch wenn das gemeinsame Verfahren an sich zulässig ist – die konkrete Datenverarbeitung im Einzelfall zulässig sein muss.

4. Datenschutzrechtliche Vorabkontrolle (Absatz 3)

In Satz 1 werden zum Ausgleich der besonderen Risiken, die jedes gemeinsame Verfahren in sich trägt, eine obligatorische Vorabkontrolle sowie die Anhörung des BfDI vorgeschrieben. Satz 2 legt fest, welche Unterlagen schon bei der Anhörung vorzulegen sind. Die Datenschutzgesetze des Bundes und der Länder sehen verschiedene Beteiligungsformen des oder der Bundes- oder Landesdatenschutzbeauftragten vor. Hier wurde die Anhörung gewählt, weil sie in Umsetzung der Unabhängigkeit es ermöglicht, sich intensiv mit dem Verfahren zu befassen – oder wenn z. B. absehbar ist, dass die Eingriffe in das Persönlichkeitsrecht sehr gering sind, von einer Stellungnahme abzusehen. Dem BfDI ist im Zusammenhang mit seiner Anhörung ein Sicherheitskonzept vorzulegen. Unbeschadet bleibt selbstverständlich auch das Recht des BfDI, nach den sonstigen Vorschriften (z. B. § 24 Absatz 4 BDSG) weitere Unterlagen anzufordern, Einsicht zu nehmen, sich vor Ort zu informieren oder sonst die Unterstützung der verantwortlichen Stelle anzufordern. Eine Rechtsvorschrift als Voraussetzung für die Zulässigkeit eines gemeinsamen Verfahrens ist dagegen nicht gefordert.

5. Festlegung verantwortlicher Stellen und Dokumentation (Absatz 4)

Hier sind die besonderen Anforderungen hinsichtlich der erforderlichen Festlegungen und der Dokumentation zusammengefasst. Dabei ist besonders wichtig, dass die jeweiligen Akteure mit ihrem Verantwortungsbereich transparent bleiben, respektive ihnen ihr Verantwortungsbereich auch bewusst ist. Wie einleitend erläutert (minimalistische Regelung), wurde dabei auf Redundanzen mit den vorhandenen Anforderungen an Verfahren verzichtet, auch wenn sie bei gemeinsamen Verfahren eine Schlüsselrolle spielen (wie z. B. ein Rollen- und Berechtigungskonzept oder besondere Sicherheitsmaßnahmen infolge der Vernetzung). So sind z. B. bestimmte technische und organisatorische Maßnahmen von dem Betreiber des Verfahrens sicherzustellen (z. B. technische Anforderungen an das Passwort: 8 Stellen mit Sonderzeichen, Passwortwechsel regelmäßig erzwingen), während andere nur von den angeschlossenen Stellen vor Ort gewährleistet werden können (z. B. Passwort und Benutzerkennung oder Zugangskarte nicht dem Zugriff Unbefugter aussetzen). Entsprechend muss auch die datenschutzrechtliche Verantwortung aufgeteilt sein. Deshalb ist nicht der Begriff der Daten verarbeitende Stelle verwendet, sondern auf die jeweils für konkrete Sachverhalte verantwortliche Stelle abgestellt.

Satz 1 trägt der Tatsache Rechnung, dass bei gemeinsamen Verfahren mehrere Stellen beteiligt sind und deshalb die Verantwortlichkeiten aufgeteilt werden müssen. Wird das Verfahren von einer Stelle zur Verfügung gestellt und betreut, so muss das festgelegt werden und es muss geregelt sein, wer bestimmt, welche fachlichen Anforderungen umgesetzt werden bzw. wie der Einigungsprozess zu erfolgen hat. Wegen der Komplexität, zur Sicherstellung der Revisionssicherheit und weil diese Festlegungen das Verfahrensverzeichnis ergänzen, ist Schriftform erforderlich.

Satz 2 dient der Umsetzung der Transparenzanforderungen der EG-Datenschutzrichtlinie (ABl. L 281 vom 23.11.1995, S. 31) (vgl. u. a. Erwägungsgründe 38 und 41). Die einzelnen an dem gemeinsamen Verfahren beteiligten Stellen haben ein Verzeichnis zu erstellen, das naturgemäß nur ihren Ausschnitt am Verfahren abdeckt. Betroffenen ist es nahezu unmöglich, jedenfalls aber nicht zumutbar, einen Überblick über die Datenverarbeitung im gemeinsamen Verfahren nur durch Zusammentragen der einzelnen Teile zu einem gesamten Puzzle zu erhalten. Deshalb muss es eine Stelle geben, bei der der Gesamtüberblick verwahrt und zur Einsicht bereitgehalten wird. Da es nach Absatz 2 Nummer 1 mehrere verantwortliche Stellen geben kann, müssen diese sich auf eine Stelle einigen, die diese Aufgabe wahrnehmen soll. Die Angaben nach Satz 1 sind zur Ergänzung des Verfahrensverzeichnisses erforderlich, damit es seine Informationsfunktion für Betroffene erfüllen kann.

Die Sätze 3 und 4 stellen klar, dass den nach Nummer 1 verantwortlichen Stellen weitere koordinierende Funktionen zukommen können. Dazu gehört auch die Auftragsvergabe bei Auftragsdatenverarbeitung und bei Wartungs- und Fernwartungsaufträgen. Eine gesetzliche Regelung ist erforderlich, da eine Auftragsvergabe nicht notwendig nach Nummer 1 umfasst ist. Satz 3 legt fest, dass eine (nach Nummer 1) verantwortliche Stelle Aufträge zur Datenverarbeitung vergeben kann. Sie ist durch die Daten verarbeitende Stelle dazu bevollmächtigt. Es können eine oder mehrere verantwortliche Stellen in dieser Weise beauftragt werden. Verantwortlich für die Einhaltung der Datenverarbeitungsbestimmungen bleibt die Daten verarbeitende Stelle (Satz 4), denn die Vorschriften der Auftragsdatenverarbeitung bleiben im Übrigen unberührt. Gegebenenfalls ist die Aufgabe und Befugnis der verantwortlichen Stelle nach Nummer 1 und bei Auftragsvergaben tätig zu werden, gesetzlich festzulegen.

6. Festlegung des führenden Datenschutzrechts und der Kontrollstellen (Absatz 5)

Ein wesentliches praktisches Problem bei der datenschutzrechtlichen Beratung und Kontrolle von gemeinsamen Verfahren, die länderübergreifend, in Bund/Länder-Zusammenarbeit oder unter Beteiligung von nichtöffentlichen Stellen erfolgen, ist die Anwendung unterschiedlichen Datenschutzrechts und die Zuständigkeit verschiedener Datenschutzkontrollstellen. Die Abstimmungsprozesse im Vorfeld wie auch die eigentlichen Kontrollen

werden dadurch belastet, ohne dass es zu einem Qualitätsgewinn für den Datenschutz kommt.

Da die denkbaren Konstellationen zu unterschiedlich sind, ist in Absatz 5 eine allgemeine Formulierung gewählt worden, deren Ziel es ist, möglichst alles abzudecken. Deshalb gibt Absatz 5 nur vor, dass Regelungen zu treffen sind. Weder die Form der Regelung noch deren Inhalt ist vorgegeben, denn dies ist im EGovG nicht möglich. Eine solche Regelung könnte inhaltlich die Anwendung des BDSG oder eines Landesdatenschutzgesetzes und die Zuständigkeit von Kontrollstellen für das gesamte Verfahren oder für Teile beinhalten. Die vorgeschlagene Fassung der Vorschrift lässt zu, bei der Beteiligung von öffentlichen Stellen mehrerer Länder eine Regelung in einem Staatsvertrag zu treffen. Bei der Beteiligung von nichtöffentlichen Stellen kann eine gesetzliche Regelung geschaffen werden, die diese Stellen – soweit sie an diesem Verfahren teilnehmen – den Regelungen und der Kontrolle der öffentlichen Stellen unterwirft; denkbar ist aber auch eine vertragliche Regelung mit den nichtöffentlichen Stellen. Sind der Bund und die Länder beteiligt, wäre zur Schaffung einer einheitlichen Handhabung auch eine bundesrechtliche Regelung denkbar.

7. Geltendmachung der Rechte aus dem Bundesdatenschutzgesetz (Absatz 6)

Im Anschluss an die Sonderregelung in Absatz 4 Satz 2 wird mit der Regelung der Tatsache Rechnung getragen, dass in gemeinsamen Verfahren für die Betroffenen schwer durchschaubar ist, welche Stelle welche Datenverarbeitungen vornimmt, welche Stelle welche Daten speichert und deshalb auch gegenüber welcher Stelle die Rechte auf Auskunft, Löschung, Sperrung, Berichtigung und Einsicht in das Verfahrensverzeichnis geltend gemacht werden können. Um zu vermeiden, dass Betroffene bei der Geltendmachung ihrer Rechte wegen Unzuständigkeit abgewiesen werden, werden die beteiligten Stellen verpflichtet, das Anliegen an die zuständige Stelle weiterzuleiten. Ist diese nicht unmittelbar bekannt, so kann sie leicht über die von den verantwortlichen Stellen bestimmte zentrale Stelle ermittelt werden, die jeder beteiligten Stelle bekannt ist. Da diese die Verfahrensverzeichnisse aufbewahrt, woraus auch die Zuständigkeiten abzuleiten sind, kann jede anrufende Stelle bei dieser Stelle die Zuständigkeiten erfragen und die Anliegen auf Auskunft, Berichtigung, Sperrung und Löschung an die richtige Stellen weiterleiten. Über diesen Weg ist sichergestellt, dass die Rechte tatsächlich wahrgenommen werden können.

§ 12

Anforderungen an das Bereitstellen von Daten, Verordnungsermächtigung

(1) Stellen Behörden über öffentlich zugängliche Netze Daten zur Verfügung, an denen ein Nutzungsinteresse, insbesondere ein Weiterverwendungsinteresse im Sinne des Informationsweiterverwendungsgesetzes, zu erwarten ist, so sind grundsätzlich maschinenlesbare Formate zu verwenden. Ein Format ist maschinenlesbar, wenn die enthaltenen Daten durch Software automatisiert ausgelesen und verarbeitet werden können. Die Daten sollen mit Metadaten versehen werden.

(2) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates Bestimmungen für die Nutzung der Daten gemäß Absatz 1 festzulegen. Die Nutzungsbestimmungen sollen die kommerzielle und nichtkommerzielle Nutzung abdecken. Sie sollen insbesondere den Umfang der Nutzung, Nutzungsbedingungen, Gewährleistungs- und Haftungsausschlüsse regeln. Es können keine Regelungen zu Geldleistungen getroffen werden.

(3) Regelungen in anderen Rechtsvorschriften über technische Formate, in denen Daten verfügbar zu machen sind, gehen vor, soweit sie Maschinenlesbarkeit gewährleisten.

(4) Absatz 1 gilt für Daten, die vor dem ...[einsetzen: Datum der Verkündung dieses Gesetzes] erstellt wurden, nur, wenn sie in maschinenlesbaren Formaten vorliegen.

(5) Absatz 1 gilt nicht, soweit Rechte Dritter, insbesondere der Länder, entgegenstehen.

Erläuterungen

1. Open Data (Absatz 1)

Die Regelung trägt der aktuellen sog. Open-Data-Diskussion Rechnung. Unter Open (Government) Data – oder offene (Regierungs- und Verwaltungs-) Daten – wird das öffentlich verfügbare Bereitstellen von Datenbeständen der öffentlichen Hand, in der Regel in Form von Rohdaten zur Nutzung, insbesondere zur Weiterverwendung und Weiterverbreitung, verstanden. Ausgenommen hiervon sind personenbezogene Daten sowie Daten, die anderweitig schutzwürdig sind (z. B. sicherheitsrelevante Daten, Betriebs- und Geschäftsgeheimnisse).

Zentraler Begriff der Regelung ist das Wort „Daten“. Anders als in den Informationsfreiheitsgesetzen oder im Informationsweiterverwendungsgesetz (IWG) wird hier nicht der Begriff „Informationen“ verwendet. Der Begriff der „Daten“ soll reine „Fakten“ bezeichnen – unabhängig von Bedeutung, Interpretation und Kontext. Erst indem solche „Daten“ (oder „Fakten“) in einem konkreten Bedeutungskontext interpretiert werden, werden aus ihnen „Informationen“. Dies bedeutet auch, dass durch eine Weitergabe von Daten und die daraus resultierende Einbindung in andere Kontexte neue Informationen entstehen können. Die Verwendung des Begriffs „Daten“ rückt die technische Ausrichtung der Vorschrift in den Vordergrund, während der Begriff „Information“ stärker auf den Inhalt abstellt. In der Alltags- und Rechtssprache werden die beiden Begriffe weitgehend synonym gebraucht.

Die Regelung schafft keine Veröffentlichungspflicht. Sie stellt bestimmte Anforderungen an das Bereitstellen von Daten, an denen ein Nutzungsinteresse zu erwarten ist. Sie baut insoweit auf den bestehenden gesetzlichen Regelungen, wie z. B. § 11 IFG, § 10 des Umweltinformationsgesetzes (UIG), sowie auf der Praxis der Behörden, Daten unabhängig von gesetzlichen Verpflichtungen zugänglich zu machen, auf. Die allgemeinen (z. B. Schutz personenbezogener Daten) und fachspezifischen (z. B. § 10 Absatz 6 UIG) Schranken für die Veröffentlichung von Daten bleiben unberührt.

Absatz 1 Satz 1 verpflichtet die Behörden zur Datenbereitstellung in maschinenlesbaren Formaten. Die Verpflichtung gilt nur, soweit ein Nutzungsinteresse zu erwarten ist. Damit soll sichergestellt werden, dass Behörden nur für diejenigen Daten, die auch genutzt werden, den Aufwand für deren maschinenlesbare Bereitstellung betreiben müssen. Denn nur dann ist ein solcher Aufwand angemessen und vertretbar. Indikator für ein solches Nutzungsinteresse sind beispielsweise entsprechende Anfragen oder bereits bestehende Applikationen, die entsprechende Daten verwenden.

Absatz 1 Satz 2 enthält eine Definition für die Maschinenlesbarkeit. Die Definition orientiert sich an der Diskussion, die derzeit auf europäischer Ebene im Zusammenhang mit der Änderung der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-Richtline) zur Maschinenlesbarkeit geführt wird. Alle Formate, deren Daten von Software interpretiert werden können, sind maschinenlesbar. Im Zu-

sammenhang mit Open Data sind maschinenlesbar insbesondere solche Daten, die eine Weiterverarbeitung ermöglichen. Die zu Grunde liegende Datenstruktur und entsprechende Standards müssen öffentlich zugänglich sein und sollten vollständig und offen publiziert und kostenfrei erhältlich sein. Einzelne Formate erfüllen diese Voraussetzungen vollständig, andere nur gering oder gar nicht. Im Rahmen des Modernisierungsprojektes Open Government der Bundesregierung und des Steuerungsprojektes des IT-Planungsrates „Förderung des Open Government“ werden Empfehlungen für die Einordnung einzelner Formate erarbeitet. Weitere Informationen hierzu sind z. B. auf dem ebenenübergreifenden Datenportal „GovData“ (http://www.govdata.de) abrufbar.

Absatz 1 Satz 3 zielt auf einen einfachen Zugang zu den Daten ab, wozu insbesondere die leichte Auffindbarkeit der Daten zählt. Das Auffinden wird erleichtert, wenn ein Datensatz durch möglichst einheitliche und abgestimmte Metadaten erschlossen ist. Diese sollten z. B. Kontakt-Informationen, Veröffentlichungs- und Änderungsdaten, Beschreibungen, Verweise zu Nutzungsbestimmungen, geographische und zeitliche Granularitäten und Abdeckungen enthalten. Die Struktur und Beschreibung der Metadaten sollte möglichst vorhandenen Standards folgen und für Nutzer vollständig, offen und kostenfrei zugänglich sein. Im Rahmen des Modernisierungsprojektes Open Government der Bundesregierung und des Steuerungsprojektes des IT-Planungsrates „Förderung des Open Government“ wurden bereits Empfehlungen für einheitliche Metadaten erarbeitet, die die Grundlage für den Datenkatalog von „GovData“ sowie von weiteren Open-Data-Portalen bilden. Informationen zu dieser Metadatenstruktur sind unter http://www.govdata.de/metadatenschema abrufbar.

2. Rechtsverordnungsermächtigung (Absatz 2)

Absatz 2 Satz 1 ermächtigt die Bundesregierung, die Nutzungsbestimmungen (Lizenzen) festzulegen. Darunter sind die Voraussetzungen zu verstehen, unter denen die Daten weiterverwendet und weiterverbreitet werden dürfen. Nutzungsbestimmungen sind nur dort möglich, wo andere Rechtsvorschriften keine uneingeschränkte Nutzungsmöglichkeit vorgeben, wie dies z. B. für die Umweltinformationen auf Grund von Europa- und Völkerrecht der Fall ist.

Absatz 2 Satz 2 legt fest, dass insbesondere der Umfang der Nutzung (Darf der Nutzer die Daten verändern? Darf der Nutzer die Daten mit anderen Daten zusammenführen? Darf der Nutzer die Daten in private oder öffentliche Netzwerke einbinden?), die Nutzungsbedingungen (Muss die Herkunft der Daten genannt werden? Darf der Datenbereitsteller eine bestimmte Form der Namensnennung vorgeben?) sowie die Begrenzung von Haftung und Gewährleistung zu regeln sind. Die Nutzungsbedingungen sollen die kommerzielle und nicht kommerzielle Nutzung abdecken.

Absatz 2 Satz 3 stellt klar, dass die Verordnung keine Regelungen zu Geldleistungen (Gebühren und Entgelte) enthalten darf. Hierüber entscheiden die zuständigen Gebietskörperschaften bzw. die datenbereitstellenden Stellen in eigener Zuständigkeit im Rahmen des jeweils geltenden Rechts.

3. Verhältnis zu anderen gesetzlichen Anforderungen (Absatz 3)

Absatz 3 regelt das Verhältnis zu anderen gesetzlichen Anforderungen hinsichtlich des Verfügbarmachens von Daten. Sie legt die Maschinenlesbarkeit als Mindeststandard fest.

4. Übergangsregelung (Absatz 4)

Absatz 4 enthält eine Übergangsregelung für Daten, die bis zum Inkrafttreten des Gesetzes erstellt wurden und nicht maschinenlesbar vorliegen. Sie werden nicht von Absatz 1 erfasst. Sie müssen daher nicht in maschinenlesbaren Formaten bereitgestellt werden.

Die Behörden sollen nicht verpflichtet werden, ihren Datenbestand nachträglich maschinenlesbar zu machen.

5. Vorrang der Rechte Dritter (Absatz 5)

Die vorgesehene Änderung setzt den Vorschlag Nummer 11 der Stellungnahme des Bundesrates (BR Drucksache 557/12(B)) um und stellt klar, dass nur solche Daten bereitgestellt werden können, über die die jeweilige datenhaltende Stelle frei verfügen kann. Die in § 12 EGovG implizit enthaltene Beachtung der Rechte Dritter, vor allem im Verhältnis vom Bund zu den Ländern, wird damit besonders hervorgehoben. Mit der vorgesehenen Änderung wird insbesondere klargestellt, dass durch Bundesverordnung keine Nutzungsbedingungen für Daten festgelegt werden können, soweit Rechte Dritter, insbesondere Rechte der Länder, entgegenstehen.

§ 13

Elektronische Formulare

Ist durch Rechtsvorschrift die Verwendung eines bestimmten Formulars vorgeschrieben, das ein Unterschriftsfeld vorsieht, wird allein dadurch nicht die Anordnung der Schriftform bewirkt. Bei einer für die elektronische Versendung an die Behörde bestimmten Fassung des Formulars entfällt das Unterschriftsfeld.

Erläuterungen

§ 126 Absatz 1 des Bürgerlichen Gesetzbuches (BGB) bestimmt, dass eine Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden muss, wenn durch Gesetz schriftliche Form vorgeschrieben ist.

Der Umkehrschluss, dass immer dann, wenn eine Unterschrift vorgeschrieben ist, damit eine gesetzliche Schriftform angeordnet ist, kann weder aus dem Wortlaut noch aus dem Zweck der Norm hergeleitet werden. Unterschriften werden im täglichen Leben vielmehr auch außerhalb gesetzlicher Schriftformerfordernisse zu verschiedensten Zwecken geleistet und sind insbesondere als Feld für die Unterschrift des Erklärenden üblicher Bestandteil jeglicher Art von Formularen.

Dennoch gibt es eine verbreitete Rechtspraxis, die im Fall von durch Rechtsnorm vorgeschriebenen Formularen aus dem Unterschriftsfeld des Formulars ein gesetzliches Schriftformerfordernis herleitet. In der Fachliteratur und Rechtsprechung spiegelt sich diese Praxis nicht wider. Was im Fall der händischen Unterschrift unter ein Papierformular jedenfalls in der Praxis keine Probleme verursacht, wird bei der elektronischen Abbildung des Formulars zu einer erheblichen Hürde im Rechtsverkehr: Damit kann das Formular nur dann elektronisch verschickt werden, wenn es qualifiziert elektronisch signiert wird oder wenn eine durch dieses Gesetz vorgesehene andere Variante des Schriftformersatzes gewählt wird. Dies hat bisher angesichts der mangelnden Verbreitung der qeS in der Praxis dazu geführt, dass die von zahlreichen Verwaltungen im Internet schon jetzt zum Download angebotenen Formulare ausgedruckt und in Papierform versandt werden müssen, statt eine Versendung per einfacher E-Mail zu ermöglichen, wenn nicht explizit Schriftform angeordnet ist.

Mit Satz 1 wird klargestellt, dass kein Schriftformerfordernis vorliegt, wenn dieses nicht explizit in der Norm angeordnet wird.

Sofern die dem Formular zugrundeliegende Rechtsnorm für die Erklärung explizit Schriftform anordnet, kann hier in der elektronischen Welt auch künftig nur eine Unterzeichnung über die qeS sowie durch die mit diesem Gesetz neu eingeführten schriftformersetzenden Technologien abgebildet werden.

Für alle anderen durch Rechtsvorschrift angeordneten Formulare ist klargestellt, dass auch eine Übermittlung des elektronischen Formulars an die Behörde beispielsweise als ausgefülltes pdf-Dokument ohne Unterschrift möglich ist. Das Ausdrucken eines online ausgefüllten Formulars, das Unterschreiben sowie das frühere Übersenden mittels Post durch die Bürger bzw. Unternehmen entfallen. Das Interesse der Verwaltung an der durch das Formular strukturierten Abfrage von Informationen ist dadurch gleichermaßen gewahrt.

Satz 2 stellt klar, dass bei in Papierform ausgegebenen Formularen weiterhin das in der Rechtsnorm abgedruckte Format samt Unterschriftsfeld beizubehalten ist und das Unterschriftsfeld bei an die Behörde gerichteten Formularen lediglich bei der elektronischen Fassung entfällt. Dies gilt auch in den Fällen, in denen ein Schriftformerfordernis besteht, da die Schriftform gemäß § 3a VwVfG (neu), § 36a SGB I (neu), § 87a AO (neu) nicht durch eine handschriftliche Unterschrift in einem Feld, sondern durch deren elektronischen Substitute abgebildet wird.

Da das Unterschriftserfordernis häufig die Funktion hat, die moralische Hemmschwelle gegenüber Falschangaben zu erhöhen, bleibt es der Behörde unbenommen, diese Hemmschwelle auf andere Weise zu erhalten.

Hierzu kann sie z. B. das Unterschriftsfeld bei einer für die elektronische Versendung bestimmten Fassung des Formulars durch eine vorformulierte Erklärung ersetzen, mit deren Bestätigung versichert wird, dass die Person, die die Erklärung in den Rechtsverkehr gibt, mit der im Formular bezeichneten Person identisch ist, oder andere geeignete Maßnahmen ergreifen, so dass bei einem Missbrauch der Urheberschaft eine strafrechtliche Verfolgung nach § 269 des Strafgesetzbuches (StGB) erfolgen kann.

Die Regelung des § 13 findet unabhängig von der Bezeichnung als Formular, Vordruck, Formblatt oder ähnlichen Begriffen Anwendung.

§ 14

Georeferenzierung

(1) Wird ein elektronisches Register, welches Angaben mit Bezug zu inländischen Grundstücken enthält, neu aufgebaut oder überarbeitet, hat die Behörde in das Register eine bundesweit einheitlich festgelegte direkte Georeferenzierung (Koordinate) zu dem jeweiligen Flurstück, dem Gebäude oder zu einem in einer Rechtsvorschrift definierten Gebiet aufzunehmen, auf welches sich die Angaben beziehen.

(2) Register im Sinne dieses Gesetzes sind solche, für die Daten auf Grund von Rechtsvorschriften des Bundes erhoben oder gespeichert werden; dies können öffentliche und nichtöffentliche Register sein.

Erläuterungen

1. Georeferenzierung (Absatz 1)

Viele Sachdaten der öffentlichen Verwaltung (Angaben) haben einen sogenannten Raumbezug, z. B. zu einer Adresse oder zu einem Landschaftsschutzgebiet. Dennoch ist es aufgrund der Vorhaltung und Verwaltung dieser Register nicht möglich, die Informationen räumlich in Beziehung zu setzen, z. B. um Nachbarschaften oder Entfernungen, Häufigkeit von Einrichtungen o. Ä. festzustellen. Anwendungsbeispiele sind u. a.: Wo liegen die Schulen im Stadtgebiet? In welchen Entfernungen liegen Schulen zu Kindergärten? Eine Verbindung kann derzeit nur aufwändig erfolgen, z. B. indem für die Adresse oder eine geografische Angabe (Siebengebirge, Schloss Moritzburg) die Lage über Hilfsmittel ermittelt wird. Dieser Aufwand entsteht bei jeder Analyse oder Abfrage erneut. Dies kann verbessert werden, wenn sämtliche Daten, die einen Bezug zu einem Grundstück haben, mit der Koordinate des Flurstücks bzw. des Gebäudes verknüpft wird. Flurstücke sind nach dem Liegenschaftskataster definierte Eigentumsflächen. Gebiete sind z. B. ein Baugebiet oder ein Naturschutzgebiet, die wiederum häufig aus mehreren Flurstücken bestehen. Zur einheitlichen Umsetzung sind technische Regelungen zu treffen. Das Liegenschaftskataster führt bereits zu Gebäuden eine sogenannte Hauskoordinate und zu Flurstücken eine sogenannte Flurstückskoordinate. Es liegt nahe, diese Informationen zu nutzen, um Daten mit einer bundesweit einheitlich festgelegten direkten Georeferenzierung zu ergänzen. Die Speicherung der Koordinate ergänzt die Adressangabe innerhalb des Registers. Es wird keine neue Information erfasst. Zusätzlich kann zur Koordinate, die in jedem Fall innerhalb des betroffenen Gebäudes bzw. Flurstücks bzw. Gebietes liegen sollte, auch ein Flächenumring im Register gespeichert werden. Durch die Speicherung der Koordinaten ist dann eine direkte räumliche und vor allem technisch einfache Zuordnung und Verknüpfung verschiedener Informationen möglich. Damit können auch Auswertungen deutlich vereinfacht werden. Die Angaben sind für alle inländischen Grundstückbezüge zu ergänzen. Dies stellt klar, dass bei Bezügen zu ausländischen Grundstücken die Koordinaten nicht aufgenommen werden müssen. Von der Regelung sind alle Register ausgeschlossen, die ausschließlich Bezüge zu ausländischen Grundstücken haben.

Die einheitliche Festlegung für die Georeferenzierung in Registern fördert die Nutzungs- und Auswertungsmöglichkeiten aller Daten der öffentlichen Verwaltung. Einheitliche Vorgaben für die Georeferenzierung, also die Möglichkeit zur „Übersetzung“ von Raumbezugsinformationen wie Adressen in ein Koordinatenpaar, sind die grundlegende Voraussetzung für die Interoperabilität der Geodaten, auch im Sinne einer Geodateninfrastruktur Deutschland (GDI-DE). Daher ist die Festlegung gemeinsam in Bund-Länder-Gremien zu erarbeiten und im IT-Planungsrat zu beschließen. Basis für die Festlegung kann u. a. das Architekturkonzept der GDI-DE sein, dieses beinhaltet Regelungen über die einheitliche Anwendung räumlicher Bezugssysteme sowie von Metadaten. Die Metadaten zum gewählten Bezugssystem und zur Qualität der Georeferenzierung sind zwingend notwendig. Den für § 14 erforderlichen Geokodierungsdienst entwickelt derzeit das Bundesamt für Kartographie und Geodäsie (BKG).

Von der Regelung sind nur Register betroffen, die entweder neu aufgebaut oder überarbeitet werden, z. B. durch Umsetzung eines analogen Registers in ein digitales oder durch wesentliche Neustrukturierung und grundlegender Überarbeitung eines digitalen Registers. Die Ergänzung der Georeferenzierung sollte nicht den Hauptgrund und Hauptaufwand der Überarbeitung darstellen. Nicht betroffen von der Regelung ist auch das Grundbuch. Das Grundbuch dient der Dokumentation von Eigentums- und anderen Sachenrechten an Grundstücken und grundstücksgleichen Rechten und damit in erster Linie dem Grundstücksverkehr. Die Grundstücke werden im Grundbuch nach den in den Ländern eingerichteten amtlichen Verzeichnissen benannt (Liegenschaftskataster). Das Liegenschaftkataster weist die tatsächlichen Verhältnisse am Grund und Boden nach (Flurstücke) und wird auf Basis des § 2 Absatz 2 der Grundbuchordnung geführt. Eine Erstreckung des Anwendungsbereichs der Regelung auf das Grundbuch ist damit nicht erforderlich, weil eine Verbindung zum Liegenschaftskataster – und damit zu den Flurstückskoordinaten – bereits besteht.

Die Regelung legt nicht fest, ob, durch wen und wie die in den jeweiligen elektronischen Registern gespeicherten Daten genutzt werden können; dies ergibt sich aus den jeweiligen spezialgesetzlichen Vorschriften. Datenschutzrechtliche Aspekte (Abstrahierung, Löschungsfristen etc.) ergeben sich aus den jeweiligen Rechtsvorschriften für das einzelne Register. Klarstellend wird darauf hingewiesen, dass bei der Verknüpfung personenbezogener Geoinformationen die datenschutzrechtlichen Vorschriften des BDSG sowie ggf. der Datenschutzgesetze der Länder und ggf. der jeweiligen spezifischen Rechtsvorschriften des Bundes und/oder des jeweiligen Landes für das einzelne Register zu beachten sind.

2. Begriff des Registers (Absatz 2)

Die Regelung umfasst nichtöffentliche (verwaltungsinterne) sowie öffentliche (nicht lediglich für den verwaltungsinternen Gebrauch bestimmte) Register.

§ 15

Amtliche Mitteilungs- und Verkündungsblätter

(1) Eine durch Rechtsvorschrift des Bundes bestimmte Pflicht zur Publikation in einem amtlichen Mitteilungs- oder Verkündungsblatt des Bundes, eines Landes oder einer Gemeinde kann unbeschadet des Artikels 82 Absatz 1 des Grundgesetzes zusätzlich oder ausschließlich durch eine elektronische Ausgabe erfüllt werden, wenn diese über öffentlich zugängliche Netze angeboten wird.

(2) Jede Person muss einen angemessenen Zugang zu der Publikation haben, insbesondere durch die Möglichkeit, Ausdrucke zu bestellen oder in öffentlichen Einrichtungen auf die Publikation zuzugreifen. Es muss die Möglichkeit bestehen, die Publikation zu abonnieren oder elektronisch einen Hinweis auf neue Publikationen zu erhalten. Gibt es nur eine elektronische Ausgabe, ist dies in öffentlich zugänglichen Netzen auf geeignete Weise bekannt zu machen. Es ist sicherzustellen, dass die publizierten Inhalte allgemein und dauerhaft zugänglich sind und eine Veränderung des Inhalts ausgeschlossen ist. Bei gleichzeitiger Publikation in elektronischer und papiergebundener Form hat die herausgebende Stelle eine Regelung zu treffen, welche Form als die authentische anzusehen ist.

Erläuterungen

1. Elektronische Publikation (Absatz 1)

Zahlreiche Vorschriften des Bundesrechts sehen vor, dass in amtlichen Mitteilungs- oder Verkündungsblättern des Bundes, eines Landes oder einer Gemeinde bestimmte Umstände bekannt zu geben oder Unterlagen zu veröffentlichen sind. Zum Teil wird im Rechtsverkehr aus der Bezeichnung eines Publikationsorgans als „Blatt“ gefolgert, dass dieses in Papier zu führen ist. Wird die jeweilige Publikation beim Bund, in dem betroffenen Land oder der Kommune elektronisch geführt, besteht gegenwärtig Rechtsunsicherheit, ob dadurch auch diese bundesrechtlich angeordneten Publikationspflichten erfüllt werden können. Teilweise werden eigens für solche bundesrechtlich angeordneten Publikationen parallel Printausgaben geführt. Durch die Regelung in Absatz 1 wird klargestellt, dass die Publikationspflicht auch durch die elektronische Form des Publikationsorgans erfüllt wird. Die Existenz des elektronischen Publikationsorgans wird dabei vorausgesetzt.

Überdies wird in Absatz 1 klargestellt, dass es nicht ausgeschlossen ist, Mitteilungsblätter in ausschließlich elektronischer Form zu führen. Voraussetzung ist, dass die Publikation für alle Personen, auch die weniger technikaffinen, angemessen zugänglich ist. Dies wird in Absatz 2 näher konkretisiert.

Die Vorschrift findet keine Anwendung auf das Bundesgesetzblatt, für dessen Führung in ausschließlich elektronischer Form nach verbreiteter Auffassung eine Änderung des Grundgesetzes erforderlich wäre.

Mit der am 1. April 2012 in Kraft getretenen Änderung des Verkündungs- und Bekanntmachungsgesetzes (VkBkmG) vom 22. Dezember 2011 (BGBl. I S. 3044) wurde bereits die Überführung des Bundesanzeigers in die ausschließlich elektronische Ausgabe vollzogen. Als spezielle Regelungen gehen die Vorschriften des VkBkmG der Regelung des § 15 insoweit vor.

2. Gewährleistung eines angemessenen Zugangs (Absatz 2)

Dem Zweck eines amtlichen Mitteilungsblatts entsprechend ist zu gewährleisten, dass jede Person angemessenen Zugang zu der Publikation hat und diese dauerhaft unverändert bleibt.

Dies gilt nicht nur für die elektronischen Publikationsformen, sondern auch für die Papierausgabe. Bereits heute ist angesichts des hohen Verbreitungsgrades des Internets davon auszugehen, dass die elektronische Ausgabe eines amtlichen Blattes für die meisten Nutzer schneller und leichter zugänglich ist als eine Printausgabe. Manche amtlichen Blätter sind in Papierform lediglich in großen öffentlichen Bibliotheken zugänglich und damit für die meisten potenziellen Nutzer nur mit Mühe recherchierbar. Auch für Menschen mit körperlichen Einschränkungen, z. B. Sehbehinderte, kann eine elektronische Ausgabe leichter oder gar ausschließlich zugänglich sein. Dennoch wird man bis auf Weiteres davon ausgehen, dass die etablierten Verbreitungsformen auch für die Papierausgabe ausreichend im Sinne des Satzes 1 sind.

Für die elektronische Ausgabe ist zu beachten, dass auch der Teil der Bevölkerung, der zur Nutzung öffentlich zugänglicher Netze mangels der erforderlichen technischen Infrastruktur oder mangels persönlicher Fähigkeiten nicht in der Lage ist, auf die Publikation zugreifen kann. Dies kann z. B. an öffentlichen Internetterminals, etwa in Rathäusern, Bibliotheken oder anderen öffentlichen Einrichtungen, oder durch die Möglichkeit, Ausdrucke zu bestellen, geschehen. Auch andere Zugänge sind möglich, sofern sie „angemessen“ sind. Hierfür ist es nicht erforderlich, dass die Publikation wie in öffentlich zugänglichen Netzen jederzeit kostenlos verfügbar ist. Die Angemessenheit orientiert sich vielmehr an den bisher üblichen Zugangsformen und Kosten der Printausgaben. Satz 2 soll sicherstellen, dass die Nutzer sich darüber informieren lassen können, wann wieder neue Nachrichten publiziert sind. Satz 3 gewährleistet, dass der Fundort der elektronischen Publikation hinreichend bekannt gemacht wird. Satz 4 trägt dem Umstand Rechnung, dass es eine wesentliche Vorbedingung für die Authentizität der verkündeten Fassung ist, dass veröffentlichte Dokumente nachträglich nicht mehr geändert oder gar gelöscht werden können. Zugleich ist dies eine Voraussetzung dafür, dass die authentische Fassung dauerhaft zur Verfügung gehalten werden kann. Notwendige redaktionelle Korrekturen sollen von der Veränderungssperre ausgenommen sein, um den Aufwand einer erforderlichen erneuten Bekanntmachung zu minimieren. Derartige Korrekturen müssen aber als solche erkennbar gemacht werden und zudem erkennen lassen, wann die Ergänzung oder Berichtigung vorgenommen wurde. Mit der Regelung in Satz 5 wird die herausgebende Stelle verpflichtet, bei gleichzeitiger Publikation in elektronischer und papiergebundener Form eine Regelung zu treffen, welche Form als die authentische anzusehen ist. Bei einer Störung der öffentlichen Netze ist ggf. auf die Publikation in Papierform zurückzugreifen, da in diesem unwahrscheinlichen Fall die notwendige Voraussetzung eines Angebots über öffentliche Netze (Absatz 1) als nicht gegeben anzusehen ist.

Das Gebot dauerhafter Verfügbarkeit bedingt, dass von Anfang an ein zukunftssicheres Format für die elektronischen Dokumente gewählt werden muss, welches deren Interpretierbarkeit auch auf zukünftigen IT-Systemen gewährleistet.

§ 16

Barrierefreiheit

Die Behörden des Bundes sollen die barrierefreie Ausgestaltung der elektronischen Kommunikation und der Verwendung elektronischer Dokumente nach § 4 des Behindertengleichstellungsgesetzes in angemessener Form gewährleisten.

Erläuterungen

Mit § 16 wird der schon geltende Rechtsrahmen mit seiner Definition von Barrierefreiheit (§§ 1 und 4 des Behindertengleichstellungsgesetzes - BGG) hinsichtlich des barrierefreien Zugangs in der öffentlich-rechtlichen Verwaltungstätigkeit der Behörden des Bundes einschließlich der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts nach diesem Gesetz konkretisiert. Danach sollen einzelne Komponenten der elektronischen Verwaltung, z. B. der elektronische Zugang zur Verwaltung und die elektronische Aktenführung, so gestaltet werden, dass die elektronischen Kommunikationseinrichtungen und elektronischen Dokumente für Menschen mit Behinderungen in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe zugänglich und nutzbar sind.

Das ist dann der Fall, wenn ihnen der Zugang mit den hierfür vorhandenen, der jeweiligen Behinderung entsprechenden Hilfsmitteln möglich ist.

Auch die von Deutschland ratifizierte UN-Behindertenrechtskonvention verpflichtet dazu, angemessene Vorkehrungen zu treffen, um die Zugänglichkeit von Informations- und Kommunikationstechnologien und -systemen für Menschen mit Behinderungen zu gewährleisten (Artikel 9 i. V. m. Artikel 2 UN-BRK). Angemessene Vorkehrungen sind danach notwendige und geeignete Änderungen und Anpassungen, die keine unverhältnismäßige oder unbillige Belastung darstellen und die, wenn sie in einem bestimmten Fall erforderlich sind, vorgenommen werden, um zu gewährleisten, dass Menschen mit Behinderungen gleichberechtigt mit anderen alle Menschenrechte und Grundfreiheiten genießen oder ausüben können. Diese Vorgabe bildet auch den Rahmen für die nach diesem Gesetz zu gewährleistende gleichberechtigte, barrierefreie Teilnahme an der elektronischen Kommunikation.

Artikel 2

Änderung des De-Mail-Gesetzes

Das De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666), das durch Artikel 2 Absatz 3 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044) geändert worden ist, wird wie folgt geändert:

1. In § 2 werden die Wörter „und der Rechtsverordnung nach § 24“ gestrichen.

2. § 3 Absatz 3 Satz 1 Nummer 1 und 2 wird wie folgt gefasst:

„1. Bei natürlichen Personen

a) anhand eines gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, insbesondere anhand eines inländischen oder nach ausländerrechtlichen Bestimmungen anerkannten oder zugelassenen Passes, Personalausweises oder Pass- oder Ausweisersatzes,

b) anhand von Dokumenten, die bezüglich ihrer Sicherheit einem Dokument nach Buchstabe a gleichwertig sind,

c) anhand eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes,

d) anhand einer qualifizierten elektronischen Signatur nach § 2 Nummer 3 des Signaturgesetzes oder

e) anhand sonstiger geeigneter technischer Verfahren mit gleichwertiger Sicherheit zu einer Identifizierung anhand der Dokumente nach Buchstabe a;

2. bei juristischen Personen oder Personengesellschaften oder bei öffentlichen Stellen

a) anhand eines Auszugs aus dem Handels- oder Genossenschaftsregister oder aus einem vergleichbaren amtlichen Register oder Verzeichnis,

b) anhand der Gründungsdokumente,

c) anhand von Dokumenten, die bezüglich ihrer Beweiskraft den Dokumenten nach den Buchstaben a oder b gleichwertig sind, oder

d) durch Einsichtnahme in die Register- oder Verzeichnisdaten.“

3. § 5 Absatz 5 wird wie folgt geändert:

a) In Satz 2 werden die Wörter „durch eine qualifizierte elektronische Signatur“ gestrichen.

b) Die folgenden Sätze werden angefügt:

"Hierzu versieht er im Auftrag des Senders die Nachricht mit einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur; sind der Nachricht eine oder mehrere Dateien beigefügt, bezieht sich die qualifizierte elektronische Signatur auch auf diese. Die Bestätigung enthält bei natürlichen Personen den Namen und die Vornamen, bei juristischen Personen, Personengesellschaften oder öffentlichen Stellen die Firma, den Namen oder die Bezeichnung des Senders in der Form, in der diese nach § 3 Absatz 2 hinterlegt sind. Die Tatsache, dass der Absender diese Versandart genutzt hat, muss sich aus der Nachricht in der Form, wie sie beim Empfänger ankommt, ergeben. Die Bestätigung nach Satz 1 ist nicht zulässig bei Verwendung einer pseudonymen De-Mail-Adresse nach Absatz 2."

4. Dem § 7 Absatz 3 werden die folgenden Sätze angefügt:

"Auf Verlangen des Nutzers muss der akkreditierte Diensteanbieter durch einen geeigneten Zusatz die Erklärung des Nutzers im Verzeichnisdienst veröffentlichen, den Zugang im Sinne von § 3a des Verwaltungsverfahrensgesetzes, § 36a Absatz 1 des Ersten Buches Sozialgesetzbuch und des § 87a Absatz 1 Satz 1 der Abgabenordnung eröffnen zu wollen. Die Veröffentlichung der De-Mail-Adresse des Nutzers als Verbraucher mit diesem Zusatz im Verzeichnisdienst gilt als Zugangseröffnung. Satz 2 gilt entsprechend für die Entscheidung des Nutzers, die Zugangseröffnung zurückzunehmen."

Erläuterungen

1. Streichung der Wörter „und der Rechtsverordnung nach § 24“ (Nummer 1)

Die Änderung ist redaktioneller Art.

2. Erweiterte Identifizierungsmöglichkeiten bei Eröffnung eines De-Mail-Kontos – Neufassung des § 3 Absatz 3 Satz 1 Nummer 1 und 2 des De-Mail-Gesetzes (Nummer 2)

Die Ergänzung in § 3 Absatz 3 Satz 1 Nummer 1 Buchstabe e erweitert die Möglichkeiten der Identifizierung des Nutzers anlässlich der Eröffnung eines De-Mail-Kontos. Sie lehnt sich an die Regelung des § 3 Absatz 1 Nummer 4 der Signaturverordnung an. Die Möglichkeiten der Identifizierung des Nutzers werden um die Identifizierung durch „geeignete technische Verfahren“ erweitert. Hierdurch öffnet sich das De-Mail-Gesetz für alternative, insbesondere weitere medienbruchfreie Verfahren. Als Bestandteil des Sicherheitskonzepts eines akkreditierten Diensteanbieters ist die „gleichwertige Sicherheit“ der Identifizierungsmethode im Fall akkreditierter Diensteanbieter vom Bundesamt für Sicherheit in der Informationstechnik zu prüfen und zu bestätigen. Gleichwertige Sicherheit wird regelmäßig auch dann anzunehmen sein, wenn für die Identifizierung Verfahren verwendet werden, die nach dem Signaturgesetz oder dem Geldwäschegesetz für die Identifizierung einer Person zulässig sind. Des Weiteren wird in § 3 Absatz 3 Satz 1 Nummer 1 Buchstabe c der elektronische Identitätsnachweis nach § 78 Absatz 5 des Aufenthaltsgesetzes zugelassen. Die übrigen Änderungen sind lediglich redaktioneller Natur und dienen der besseren Lesbarkeit.

3. Weiterentwicklung der Versandoption „absenderbestätigt“ – Änderung des § 5 Absatz 5 De-Mail-Gesetz (Nummer 3)

a) Vorbemerkungen

Die Änderung des § 5 Absatz 5 dient dazu, die bisher in dieser Vorschrift geregelte Versandoption so zu ergänzen, dass hierdurch alle Funktionen der Schriftform des materiellen Verwaltungsverfahrensrechts sowie des gesamten Prozessrechts abgebildet werden.

Insbesondere im Zuge der Zulassung von De-Mail als Schriftformersatz im Verwaltungsrecht (vgl. Artikel 3, 4 und 7) sind die folgenden beiden Klarstellungen hinsichtlich des Verhältnisses der kurzzeitigen Entschlüsselung der De-Mail-Nachrichten bei den akkreditierten Diensteanbietern zu den Tatbestandsmerkmalen des „Übermittelns“ bzw. „Offenbarens“ notwendig, welche im Zusammenhang mit dem Steuer- bzw. Sozialgeheimnis oder sonstigen Geheimnissen, die bestimmten Berufsträgern wie z. B. Ärzten, sonstigen Angehörigen von Heilberufen, Rechtsanwälten, anvertraut wurden (hierzu vgl. z. B. § 203 StGB), eine Rolle spielen:

– Beim Versenden einer De-Mail-Nachricht liegt ein Übermitteln im Sinne des § 3 Absatz 4 Satz 2 Nummer 3 BDSG oder gleichlautender Rechtsvorschriften wie § 67 Absatz 6 Satz 2 Nummer 3 SGB X lediglich im Verhältnis zwischen Sender und Empfänger der De-Mail-Nachricht vor, nicht jedoch zwischen diesen und den in den Übermittlungsvorgang eingeschalteten akkreditierten Diensteanbietern.

– Das Versenden einer De-Mail-Nachricht mit Inhalten, die ein Geheimnis im Sinne des § 203 StGB darstellen, durch die dort bezeichneten Geheimnisträger ist kein unbefugtes Offenbaren im Sinne des § 203 StGB oder gleichlautender Rechtsvorschriften (z. B. § 30 AO), auch wenn eine kurzzeitige automatisierte Entschlüsselung durch den akkreditierten Diensteanbieter zum Zweck der Überprüfung auf Schadsoftware erfolgt.

Diese Klarstellungen sind aufgrund folgender Tatsachen gerechtfertigt: Wenn der Nutzer von seinem Endgerät eine De-Mail versendet, wird diese verschlüsselt zu dessen De-Mail-Provider geleitet, analog etwa der Nutzung von Online-Banking-Diensten. Bei dem Provider des Absenders werden die Daten in einem automatisierten Prozess entschlüsselt, auf Schadsoftware überprüft und anschließend für den Versand an den Provider des Empfängers erneut verschlüsselt. Nach Eingang beim De-Mail-Provider des Empfängers wird die Nachricht wiederum automatisiert entschlüsselt und auf Schadsoftware überprüft. Anschließend wird die Nachricht wieder verschlüsselt und in dieser Form für den Empfänger aufbewahrt. Schließlich ruft sie der Empfänger über einen verschlüsselten Kanal ab. Auf dem Weg durch das Internet sind die Daten also über bewährte Verfahren verschlüsselt, die vom BSI festgelegt wurden. Bei den De-Mail-Providern werden die Daten im Rahmen eines automatisierten Prozesses ohne menschliche Mitwirkung kurzzeitig umgeschlüsselt. Diese Umschlüsselung erfolgt in einer vom BSI zertifizierten Sicherheitsumgebung, für die die De-Mail-Provider im Rahmen des im De-Mail-Gesetz geregelten Akkreditierungsprozesses umfangreiche organisatorische und technische Sicherheitskriterien erfüllen müssen. Eine Speicherung der Inhaltsdaten beim Provider erfolgt ausschließlich in verschlüsseltem Zustand. Auf die amtliche Begründung des De-Mail-Gesetzes wird Bezug genommen (vgl. BT-Drs. 17/3630, S. 29).

Damit wird auch die durch den letzten Satz der amtlichen Begründung zu Artikel 1 § 5 Absatz 3 des Entwurfs des De-Mail-Gesetzes begünstigte Rechtsunsicherheit (BT-Drs. 17/3630, S. 29) beseitigt. Insoweit war bereits in dem Bericht des Innenausschusses zum Entwurf des De-Mail-Gesetzes vom 23. Februar 2011 (BT-Drs. 17/4893, S. 12) deutlich gemacht worden, dass die Bedeutung dieses Satzes allein darin liegt, darauf hinzuweisen, dass De-Mail ELSTER im Bereich der Steuerverwaltung nicht ablösen soll.

Ungeachtet der grundsätzlichen Zulässigkeit des Einsatzes von De-Mail im Bereich des Steuer- und Sozialgeheimnisses ohne zusätzliche Sicherheitsmaßnahmen kann es gleichwohl in bestimmten Konstellationen erforderlich werden, von der zusätzlichen Verschlüsselung nach Absatz 3 Satz 3 des De-Mail-Gesetzes Gebrauch zu machen. Insoweit sind die Empfehlungen der Beauftragten für den Datenschutz des Bundes und der Länder zu beachten.

b) Streichung der Wörter „durch eine qualifizierte elektronische Signatur (Buchstabe a)

Es handelt sich um eine Folgeänderung zu Buchstabe b.

c) Weiterentwicklung der Versandoption „absenderbestätigt“ (Buchstabe b)

Die Vorschrift entwickelt die bisherige Versandoption des § 5 Absatz 5 leicht fort, um hierdurch alle Funktionen der Schriftform des materiellen Verwaltungsverfahrensrechts sowie des gesamten Prozessrechts abbilden zu können. Es gilt, den ursprünglichen Zweck von De-Mail, lediglich „sichere Übermittlung“ von Nachrichten, um eine Funktion zu erweitern,

die auch die Schriftform im Verwaltungsverfahrensrecht sowie im Prozessrecht ersetzen können soll. Die De-Mail zugrunde liegende Technik ermöglicht diese Vorgehensweise, da sie einerseits ein hohes Maß an Sicherheit mit sich bringt, andererseits aber einfach in der Handhabung ist. Gerade Letzteres stellt einen nicht zu unterschätzenden Vorteil gegenüber der qeS dar. Konzeptionell wird so vorgegangen, dass auf der bei De-Mail bereits vorhandenen Technik aufgesetzt wird. Hierbei bietet sich die Versandoption nach § 5 Absatz 5 an, weil hier die qeS zum Einsatz kommt. Die mit dieser Versandoption versendete De-Mail-Nachricht ist mit einer qeS versehen. Allerdings muss diese nicht durch den Nutzer selbst angebracht werden; vielmehr versieht sein De-Mail-Diensteanbieter die vom Nutzer abgesendete De-Mail-Nachricht bei der gewählten Versandoption automatisch mit einer pseudonymisierten qeS des Providers und bestätigt so, dass die Nachricht des Nutzers mit diesem Inhalt versandt wurde. Dadurch wird gewährleistet, dass die Nachricht samt Anhängen nach dem Versand nicht unerkannt verändert werden kann und dies auch später jederzeit nachprüfbar ist. Um diese Nachprüfbarkeit (also die Signierfunktion) zu erhalten, dürfen auf Empfängerseite De-Mail-Nachricht und die Anhänge (z. B. pdf-Dokumente oder word-Dokumente) nicht getrennt werden, sondern müssen als Ganzes aufbewahrt werden.

Außerdem muss die qualifizierte elektronische Signatur dauerhaft überprüfbar sein. Die dauerhafte Überprüfbarkeit einer qualifizierten elektronischen Signatur soll sicherstellen, dass, soweit dies technisch möglich ist, Unterlagen mit besonderer Bedeutung über lange Zeiträume beweiskräftig bleiben. Eine Änderung des § 5 Absatz 5 des De-Mail-Gesetzes in diesem Sinne ist aus fachlichen Gründen geboten, da diese Versandart schriftformersetzend wirken soll. Bei Unterlagen, die der Schriftform bedürfen, ist generell davon auszugehen, dass sich noch nach Jahren oder Jahrzehnten die Notwendigkeit ergeben kann, auf die mit voller Beweiskraft versehene Unterlage zurückzugreifen. Die dauerhafte Überprüfbarkeit bestimmt sich dabei nach dem Stand der Technik. Derzeit heißt dies: Die qualifizierte elektronische Signatur und das ihr zugrunde liegende qualifizierte Zertifikat sind dauerhaft überprüfbar, wenn der Zertifizierungsdiensteanbieter sicherstellt, dass die von ihm ausgestellten qualifizierten Zertifikate ab dem Zeitpunkt der Bestätigung des Erhalts seiner sicheren Signaturerstellungseinheit durch den Signaturschlüssel-Inhaber für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens 30 Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikats endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Absatz 1 Satz 2 des Signaturgesetzes geführt werden. Der Zertifizierungsdiensteanbieter hat die Dokumentation im Sinne des § 10 des Signaturgesetzes und des § 8 der Signaturverordnung mindestens für diesen Zeitraum aufzubewahren. Signaturen nach § 15 Absatz 1 des Signaturgesetzes erfüllen diese Anforderungen.

Der Absender soll die Versandart nach § 5 Absatz 5 (in der Technischen Richtlinie De-Mail auch „absenderbestätigt“ genannt) bewusst wählen. Diese Wahl muss aus der gesendeten Mail in der Form, wie sie beim Empfänger angekommen ist, erkennbar sein, und zwar auch lange überprüfbar. Diesem Zweck dient der letzte Satz der Ergänzung. D.h., der übersandten Nachricht muss die Information „Benutzung der Versandart“ dauerhaft überprüfbar anhaften (Perpetuierungs- und Beweisfunktion). Die Bezeichnung des Kontoinhabers mit vollständigem Namen oder Firmen- bzw. Behördenbezeichnung muss der übersandten Nachricht ebenfalls dauerhaft überprüfbar anhaften, so dass der Empfänger den Absender eindeutig zuordnen kann. Dies wäre nicht gewährleistet, wenn in den Metadaten lediglich die De-Mail-Adresse erkennbar wäre. Insoweit werden die Technischen Richtlinien De-Mail ergänzt. Wenn z. B. Behörden über ein Gateway kommunizieren, ist die nutzende Behörde und nicht diejenige, die das Gateway betreibt, der zu bezeichnende Kontoinhaber. Weil bei der absenderbestätigten De-Mail der Absender mit Klarnamen erkennbar sein muss, ist bei dieser Versandart die Verwendung einer pseudonymen De-Mail-Adresse nicht möglich. Dies wird im letzten Satz geregelt.

Diese Informationen werden der De-Mail-Nachricht als Metadatum hinzugefügt. Dieses Metadatum wird von der vom Provider aufgesetzten qeS mit umfasst. Auch insoweit muss der Empfänger der De-Mail dafür sorgen, dass der Zusammenhang von der De-Mail-

Nachricht und deren Anhängen nicht verloren geht. Um die Verkehrsfähigkeit von De-Mail-Nachrichten nach § 5 Absatz 5 auch außerhalb des De-Mail-Verbundes zu erleichtern, werden die Technischen Richtlinien De-Mail dahingehend konkretisiert, dass die De-Mail-Diensteanbieter neben dem Export des sog. mbox-Formats (über das Archive von vielen De-Mails exportiert werden können) zusätzlich auch den Export von einzelnen De-Mails über ein Format ermöglichen, das von gängigen E-Mail-Programmen geöffnet werden kann (EML-Format).

Im Bericht der Bundesregierung nach Artikel 5 des Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften ist zur Erfüllung der Warnfunktion der Schriftform eine Schaltfläche erwähnt, (vgl. BT-Drs. 17/10720 S.7, 9 und 11). Hierzu bedarf es keiner gesetzlichen Regelung.

4. Publikationspflicht des Diensteanbieters bei Zugangseröffnung durch den Nutzer (Nummer 4)

Mit dieser Änderung soll auf die in der Praxis bestehende Unsicherheit reagiert werden, wann konkret von einer Zugangseröffnung im Sinne der Regelungen der §§ 3a Absatz 1 VwVfG, 36a Absatz 1 SGB I und 87a Absatz 1 Satz AO ausgegangen werden kann. Der Zugang kann über das De-Mail-Konto und den dort verorteten Verzeichnisdienst nach § 7 des De-Mail-Gesetzes nur allgemein für alle Verwaltungsverfahren eröffnet werden; eine Differenzierung nach VwVfG, Sozialgesetzbuch (SGB) und Abgabenordnung (AO) findet nicht statt.

Der in der De-Mail-Infrastruktur vorgesehene Verzeichnisdienst, welcher nur für De-Mail-Nutzer eingesehen werden kann, ist eine geeignete Informationsquelle, um zu erfahren, ob jemand den Zugang für den Schriftverkehr im Verwaltungsverfahren über seine De-Mail-Adresse eröffnet hat. Denn die De-Mail-Infrastruktur soll vor allem für mehr Sicherheit in der elektronischen Kommunikation des Geschäftsverkehrs (auch mit Behörden) dienen und wird voraussichtlich vor allem dann genutzt werden, wenn es auf die Identität des jeweiligen Kommunikationspartners oder die Sicherheit der Übertragung in besonderer Weise ankommt. Beides trifft für die Behördenkommunikation zu. Wer De-Mail nutzt, sich im Verzeichnisdienst eintragen lässt und dort erklärt, dass er den Zugang eröffnen will, gibt zu verstehen, dass er über De-Mail auch im Verwaltungsverfahren oder sonst mit öffentlichen Stellen kommunizieren möchte. Dies gilt für alle Kommunikationspartner (öffentliche Stellen, Bürgerinnen/Bürger oder Unternehmen) gleichermaßen.

Der Nutzer muss nach § 9 des De-Mail-Gesetzes von seinem De-Mail-Provider darüber informiert werden, dass die Veröffentlichung seiner (des Nutzers) De-Mail-Adresse und der Information, dass er den Zugang eröffnen möchte, im Verzeichnisdienst die Wirkung der Erklärung der Zugangseröffnung im Sinne der §§ 3a Absatz 1 VwVfG, 36a Absatz 1 SGB I und 87a Absatz 1 Satz AO hat.

Anders als in der Begründung zu § 7 Absatz 3 des De-Mail-Gesetzes noch ausgeführt (vgl. Bundestagsdrucksache 17/4145 vom 8. Dezember 2010, S. 6 und diese Ausführungen übernehmend Bundestagsdrucksache 17/4893 vom 23. Februar 2011, S. 20), wird von der Einschätzung, eine solche Regelung würde die Akzeptanz der De-Mail-Dienste durch die Bürgerin/den Bürger gefährden, Abstand genommen.

Allerdings wird mit Satz 3 eine Regelung eingeführt, mit welcher die Entscheidung des Nutzers als Verbraucher, die Zugangseröffnung zurückzunehmen, ebenfalls im Verzeichnisdienst zu veröffentlichen ist.

Die Regelung stellt nicht die einzige Möglichkeit der Zugangseröffnung im Sinne der Regelungen der §§ 3a Absatz 1 VwVfG, § 36a Absatz 1 SGB I und des § 87a Absatz Satz AO dar. Die Zugangseröffnung kann z. B. auch durch direkte Äußerung gegenüber der Behörde erfolgen. Erst recht stellt sie nicht die einzige Möglichkeit dar, gegen-

über nichtöffentlichen Stellen wie z. B. Unternehmen den Zugang zu eröffnen; diese Art der Zugangseröffnung wird von den §§ 3a Absatz 1 VwVfG, 36a Absatz 1 SGB I und 87a Absatz 1 Satz 1 AO gar nicht erfasst.

Die Frage, ob ein Bürger, der eine De-Mail an eine Behörde gesandt hat, sich damit auch konkludent damit einverstanden erklärt hat, dass die Behörde ihm per De-Mail antwortet, bedarf keiner Regelung. Im Einzelfall ist hier vielmehr die allgemeine Rechtslage zu § 3a Absatz 1 VwVfG bzw. § 36a Absatz 1 SGB I bzw. § 87a Absatz 1 Satz 1 AO heranzuziehen, wonach die Verkehrsanschauung maßgeblich ist, vgl. hierzu die Gesetzesbegründung zu § 3a VwVfG, BT-Drucksache 14/9000 vom 13. Mai 2002, Begründung BT zu Artikel 1 Nummer 4, S. 30f: „Der Empfänger eröffnet seinen Zugang durch entsprechende Widmung. Dies kann ausdrücklich oder konkludent erfolgen. Im Einzelfall wird hier die Verkehrsanschauung, die sich mit der Verbreitung elektronischer Kommunikationsmittel fortentwickelt, maßgebend sein [...] Beim Bürger wird hingegen die bloße Angabe einer EMail- Adresse auf seinem Briefkopf heute noch nicht dahin gehend verstanden werden können, dass er damit seine Bereitschaft zum Empfang von rechtlich verbindlichen Erklärungen kundtut. Bei ihm kann in aller Regel von der Eröffnung eines Zugangs nur ausgegangen werden, wenn er dies gegenüber der Behörde ausdrücklich erklärt hat.“

Gegenüber dieser Wertung aus dem Jahr 2002 ist davon auszugehen, dass sich die Verkehrsanschauung geändert hat. Danach kann als Verkehrsanschauung, jedenfalls bei Nutzung von De-Mail im Sinne des De-Mail-Gesetzes, nunmehr Folgendes zugrunde gelegt werden: Es ist davon auszugehen, dass die Zugangseröffnung dadurch konkludent erfolgen kann, dass sich ein Bürger oder eine Bürgerin mittels einer De-Mail-Nachricht an eine Behörde wendet, indem er oder sie z. B. einen Antrag stellt. In diesem Fall darf diese Behörde davon ausgehen, dass der Bürger oder die Bürgerin damit konkludent den Zugang für dieses Verfahren eröffnet hat mit der Folge, dass diese Behörde auch den abschließenden Bescheid per De-Mail übermitteln darf. Dies ist damit zu begründen, dass sich der Bürger oder die Bürgerin dadurch, dass er oder sie ein De-Mail-Konto eröffnet hat und sich mittels einer De-Mail-Nachricht an die Behörde wendet, bewusst für den – gegenüber der herkömmlichen E-Mail wesentlich sichereren – Weg per De-Mailentschieden hat. In einem solchen Fall muss die Behörde den Bürger oder die Bürgerin nicht mehr darum bitten, ihr gegenüber ausdrücklich den Zugang zu eröffnen. Gleiches gilt zudem für juristische Personen oder sonstige Stellen, z. B. Unternehmen.

Artikel 3

Änderung des Verwaltungsverfahrensgesetzes

Das Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), das zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 31. Mai 2013 (BGBl. I S. 1388) geändert worden ist, wird wie folgt geändert:

1. § 3a Absatz 2 wird wie folgt gefasst:

„(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht unmittelbar durch die

Behörde ermöglicht, ist nicht zulässig. Die Schriftform kann auch ersetzt werden

1. durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird;

2. bei Anträgen und Anzeigen durch Versendung eines elektronischen Dokuments an die Behörde mit der Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes;

3. bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörden durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt;

4. durch sonstige sichere Verfahren, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten; der IT-Planungsrat gibt Empfehlungen zu geeigneten Verfahren ab.

In den Fällen des Satzes 4 Nummer 1 muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen.“

2. Dem § 33 wird folgender Absatz 7 angefügt:

„(7) Jede Behörde soll von Urkunden, die sie selbst ausgestellt hat, auf Verlangen ein elektronisches Dokument nach Absatz 4 Nummer 4 Buchstabe a oder eine elektronische Abschrift fertigen und beglaubigen.“

3. Dem § 37 Absatz 3 wird folgender Satz angefügt:

„Im Fall des § 3a Absatz 2 Satz 4 Nummer 3 muss die Bestätigung nach § 5 Absatz 5 des De-Mail-Gesetzes die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lassen.“

Lesefassung § 3a Elektronische Kommunikation

(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.

(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht unmittelbar durch die Behörde ermöglicht, ist nicht zulässig. Die Schriftform kann auch ersetzt werden

1. *durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird;*

2. *bei Anträgen und Anzeigen durch Versendung eines elektronischen Dokuments an die Behörde mit der Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes;*

3. *bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörden durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt;*

4. *durch sonstige sichere Verfahren, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten; der IT-Planungsrat gibt Empfehlungen zu geeigneten Verfahren ab.*

In den Fällen des Satzes 4 Nummer 1 muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen.

(3) Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.

Erläuterungen

1. Ersetzung der Schriftform – Änderung des § 3a Absatz 2 VwVfG (Nummer 1)

Sowohl in § 3a Absatz 2 VwVfG als auch in den entsprechenden Regelungen in § 126a BGB, § 87a Absatz 3 AO und § 36a Absatz 2 SGB I ist die Bezeichnung „elektronische Form“ im Sinne einer Begriffsbestimmung als Gegenstück zur „Schriftform“ zu verstehen: „Elektronische Form“ meint danach ein elektronisches Dokument, das mit einer qeS versehen ist. Da im allgemeinen Sprachgebrauch der Begriff „elektronische Form“ in einem weiteren Sinne – etwa als Abgrenzung zu papiergebundenen Verfahren – verwendet wird, kann es zu Fehlinterpretationen dieser Formvorschrift kommen. Die Änderung von Absatz 2 Satz 2 macht die Eigenschaft der Regelung als Begriffsbestimmung deutlicher, ohne den Regelungsinhalt zu ändern. Damit ist ein Verständnis der Vorschrift ausgeschlossen, wonach die Bezeichnung „elektronische Form“ nicht als Begriffsbestimmung (elektronische Form = elektronisches Dokument + qeS), sondern als Oberbegriff zur Abgrenzung sämtlicher elektronischer Dokumente zu verkörperten (schriftlichen) Dokumenten dient und lediglich zur Ersetzung der Schriftform zusätzlich die Verknüpfung mit der qeS angeordnet wird.

Die Änderung des Satzes 3 dient der Klarstellung. Denn bei der Verwendung von Pseudonymen kann zumindest der Zertifizierungsdiensteanbieter im Sinne des § 2 Nummer 8 SigG den Signaturschlüsselinhaber identifizieren.

Eine wichtige Funktion der qeS besteht darin, die Integrität eines übermittelten elektronischen Dokuments zu gewährleisten. Im Gegensatz etwa zur einfachen E-Mail kann der Empfänger sicher sein, dass das Dokument inhaltlich unverändert ankommt. Diese wichtige Funktion kann durch unmittelbare Abgabe der Erklärung in einem elektronischen

Formular erfüllt werden. Die Formulierung „durch unmittelbare Abgabe“ in Satz 4 Nummer 1 stellt klar, dass sich die Regelung nicht auf die Verwendung elektronischer Formulare, die heruntergeladen und nach dem Ausfüllen an die Behörde gesendet werden, erstreckt. In diesen Fällen werden elektronische Dokumente versandt, so dass Satz 2 gilt. Das Verfahren darf vielmehr nur eine unmittelbare Eingabe in ein vom Verwender im Übrigen nicht veränderbares elektronisches Formular – sei es über webbasierte Anwendungen, sei es über allgemein zugängliche Eingabegeräte wie etwa Verwaltungsterminals in Bürgerämtern – ermöglichen. Denn der elektronische Identitätsnachweis erfüllt ohne diese zusätzlichen technischen Maßnahmen nicht alle Funktionen einer Schriftform, wie sie z. B. durch eine qeS erfüllt werden (z. B. Echtheitsfunktion). Ziel der Regelung ist, dass die Behörde durch technische Ausgestaltung der zur Verfügung gestellten Anwendung und die eröffneten Auswahl- oder Ausfüllfelder selbst steuert, welche Erklärungen abgegeben werden können, und so Manipulationen ausschließen kann. Daher bedarf es dieser Formulare mit „Direktausfüllung“.

Bei dem in Absatz 2 Satz 4 Nummer 1 sowie Satz 5 und 6 geregelten Verfahren wird in einem Eingabegerät bei der Behörde oder über öffentlich zugängliche Netze (z. B. das Internet oder mobile Anwendungen) eine elektronische Erklärung in der von der Behörde zur Verfügung gestellten Maske (Formular) abgegeben. Die elektronische Anwendung fungiert wie ein Formular, das aus der Ferne ausgefüllt wird. Die Behörde kann durch die technische Ausgestaltung der zur Verfügung gestellten Anwendung und die eröffneten Auswahl- oder Ausfüllfelder selbst steuern, welche Erklärungen abgegeben werden können, und Manipulationen ausschließen.

Die Authentifizierung als weitere wichtige Funktion der Schriftform kann ebenfalls von der Behörde durch entsprechende technische Ausgestaltung des Verfahrens sichergestellt werden. Die Regelung sieht dazu vor, dass zur Ersetzung der Schriftform ein sicherer Identitätsnachweis durch den Erklärenden erfolgen muss. Bei der Verwendung eines Eingabegerätes in der Behörde erfolgt die übliche Identitätsfeststellung vor Ort. Bei der Nutzung von Eingabegeräten (Terminals) in einer Behörde ist die Identität durch einen Behördenmitarbeiter zu prüfen. Für die Eingabe über öffentlich zugängliche Netze bieten die Verwendung der eID-Funktion des nPA und des elektronischen Aufenthaltstitels ein sicheres Verfahren. Die Behörde muss für eine sichere und nachvollziehbare Verknüpfung von Erklärung mit elektronischem Identitätsnachweis des Erklärenden sorgen. Die konkrete technische und organisatorische Ausgestaltung wird nicht vorgegeben, um der Verwaltung den erforderlichen Gestaltungsspielraum zu belassen.

Durch verwaltungsinterne Vorschriften kann die technische und organisatorische Ausgestaltung für sichere auf öffentlich zugänglichen Netzen basierende Dienste näher präzisiert und der erforderliche technische Sicherheitsstandard vorgegeben werden. Mit solchen Sicherheitsrichtlinien soll ein Mindeststandard für die Verwaltung etabliert werden, der ein dem jeweiligen Verwaltungsverfahren entsprechendes Sicherheitsniveau bietet. Dadurch wird der Tatsache Rechnung getragen, dass die über solche Portale angebotenen Verwaltungsdienstleistungen sehr heterogen sind. Sie sind auch angebotsgesteuert, weil die Behörde entscheidet, für welche Verfahren sie eine auf öffentlich zugänglichen Netzen basierende Abwicklung anbietet. Daher hat die Behörde es in der Hand, das für die jeweilige Anwendung erforderliche Sicherheitsniveau festzusetzen. Dafür lediglich einen Mindeststandard vorzugeben, erlaubt es zugleich, sicherheitstechnisch nach oben hin abzuweichen.

Dabei kann nach einem „Baukastenmodell“ (etwa nach dem Vorbild des IT-Grundschutzes) gearbeitet werden, bei dem anwendungsspezifisch Risiken eingeschätzt und Lösungen ausgewählt werden können. Mindeststandards in Form einer Technischen Richtlinie könnte das BSI auf Grundlage des bereits vorhandenen Materials zu „ISI-Web“ und der IT-Grundschutz-Vorgehensweise erarbeiten. Diese könnte durch entsprechende Beschlüsse (z. B. durch den IT-Rat) nicht nur für die Behörden des Bundes, sondern auch in den Ländern (z. B. durch den IT-Planungsrat) für verpflichtend erklärt werden.

In Satz 4 Nummer 2 und 3 wird zudem festgelegt, dass auch De-Mail unter bestimmten Vorgaben schriftformersetzend eingesetzt werden kann. Diese Vorgaben sind in der Vorschrift abschließend geregelt: Es muss die Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes genutzt werden und zwar in der Form, wie sie in Artikel 2 Nummer 3 dieses Gesetzes beschrieben wird. Unter diesen Voraussetzungen erfüllt diese Versandart grundsätzlich alle Schriftformfunktionen, welche für die schriftformwahrende Kommunikation mit Behörden wesentlich sind. Soweit eine behördliche Erklärung der Schriftform bedarf (z. B. bei Verwaltungsakten), muss der Empfänger zusätzlich darauf achten, dass das von der Behörde übersandte elektronische Dokument zum Erhalt der Signierfunktion nicht aus dem Zusammenhang mit der De-Mail, mit der es versandt wurde, herausgelöst wird. Diese Änderung wird durch eine Änderung von § 371a ZPO flankiert, welche in dem Gesetz zur Förderung des elektronischen Rechtsverkehrs bei den Gerichten enthalten ist. Sie soll in dieser Form mit De-Mail versandte Dokumente beweisrechtlich mit elektronischen Dokumenten gleichstellen, die vom Erklärenden selbst gemäß § 3a Absatz 2 Satz 2 VwVfG mit qeS versehen wurden. Es wird sichergestellt, dass beide Rechtsänderungen gleichzeitig in Kraft treten.

Bei Satz 2 Nummer 3 ist zu beachten: Die Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes sieht vor, dass der akkreditierte Diensteanbieter im Auftrag des Senders bestätigt, dass er – der Sender – beim Versenden der Nachricht im Sinne des § 4 des De-Mail-Gesetzes sicher angemeldet war. Die Bestätigung erfolgt nach § 5 Absatz 5 Satz 1 des De-Mail-Gesetzes in der Nachricht selbst, konkret in den sogenannten Metadaten der Nachricht. Um dem Empfänger der Nachricht diese Bestätigung nachhaltig überprüfbar zu gestalten, ist der akkreditierte Diensteanbieter nach § 5 Absatz 5 Satz 3 verpflichtet, die Nachricht mit einer, und zwar „seiner“ qualifizierten elektronischen Signatur zu versehen. Diese qualifizierte Signatur selbst enthält nicht die erlassende Behörde als Senderin. Dies ist nicht notwendig, weil sich die erlassende Behörde aus den Metadaten der Nachricht ergibt.

Außerdem wird mit Satz 2 Nummer 4, der die Vorschläge Nummer 17 und 19 der Stellungnahme des Bundesrates aufgreift, eine Regelung über den Ersatz der Schriftform in § 3a Absatz 2 VwVfG eingeführt, die technologie- und binnenmarktoffen gestaltet ist. Denn neben den gesetzlich als Schriftformersatz zugelassenen Technologien nach den Nummern 1 bis 3 werden zukünftig durch Rechtsverordnung auch andere sichere Verfahren zugelassen. Die Festlegung dieser Verfahren wird für den Bund durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates erfolgen. Dabei wird sichergestellt, dass die Zulassung anderer sicherer Verfahren im Vorfeld zwischen Bund und Ländern im IT-Planungsrat abgestimmt wird. Aufgrund der Empfehlungskompetenz des IT-Planungsrats wird ein Gleichklang der Verordnungsinhalte auf Bundes- und Landesebene im Interesse der Einheit der Rechtsordnung und der Interoperabilität zwischen verschiedenen Gebietskörperschaften gefördert. Die in der Rechtsverordnung festzulegenden sonstigen sicheren Verfahren haben die Barrierefreiheit zu gewährleisten.

Auf der Landesebene sollten im Wege der Simultangesetzgebung dem § 3a VwVfG (neu) entsprechende Regelungen in die Verwaltungsverfahrensgesetze der Länder aufgenommen werden.

2. Elektronische Abschrift bei Urkunden – § 33 Absatz 7 VwVfG (Nummer 2)

Im Rechtsverkehr – sowohl im Kontakt mit Behörden als auch im Zivilrecht – ist der Umgang mit von Behörden ausgestellten Urkunden von zentraler Bedeutung. Dabei besteht ein besonderes Bedürfnis an Ausfertigungen solcher Urkunden, die an Stelle des Originals verwendet werden können. § 33 VwVfG regelt dafür die Beglaubigung von Abschriften oder Kopien solcher Urkunden. Zwar können Urkunden auch elektronisch ausgestellt werden, regelmäßig werden aber herkömmlich in Papierform erstellte Urkunden verwendet. Auch die beglaubigten Kopien oder Abschriften sind in der Regel Schriftstücke.

Nach § 33 Absatz 4 Nummer 4a VwVfG gelten die Vorschriften über die Beglaubigung solcher Schriftstücke entsprechend für deren elektronische Abbilder. Bereits nach geltendem Recht kann also eine elektronische Ausfertigung einer schriftlichen Urkunde beglaubigt und mit dem Beweiswert einer herkömmlichen beglaubigten Kopie verwendet werden (§ 33 Absatz 6 VwVfG). Für eine vollständige elektronische Verfahrensabwicklung ist es erforderlich, dass bspw. zu Nachweiszecken vorzulegende Urkunden als beglaubigte Abschriften oder Abbilder in elektronischer Form zur Verfügung stehen. Das einmal erstellte und beglaubigte elektronische Dokument kann zudem mehrfach verwendet werden, ohne dass – wie beim herkömmlichen Schriftstück – eine Vielzahl von Abschriften oder Kopien zu fertigen und zu beglaubigen wären.

Dafür wird in § 33 VwVfG ein neuer Absatz 7 eingefügt, der die ausstellende Behörde verpflichtet, regelmäßig auf Anforderung entsprechende elektronische Dokumente zu erstellen und zu beglaubigen. Die „Soll"-Regelung trägt zum einen dem Umstand Rechnung, dass u. U. die technischen Voraussetzungen bei der Behörde nicht vorliegen, und hilft zum anderen, dass unverhältnismäßiger Aufwand vermieden wird, wenn z. B. kein berechtigtes Interesse glaubhaft gemacht werden kann.

3. Anfügen eines weiteren Satzes bei § 37 Absatz 3 VwVfG (Nummer 3)

Dieser Satz trägt den technischen Gegebenheiten der De-Mail-Infrastruktur Rechnung. Die Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes sieht vor, dass der akkreditierte Diensteanbieter im Auftrag des Senders bestätigt, dass er – der Sender – beim Versenden der Nachricht im Sinne des § 4 des De-Mail-Gesetzes sicher angemeldet war. Die Bestätigung erfolgt nach § 5 Absatz 5 Satz 1 des De-Mail-Gesetzes in der Nachricht selbst, konkret in den sogenannten Metadaten der Nachricht. Um dem Empfänger der Nachricht diese Bestätigung nachhaltig überprüfbar zu gestalten, ist der akkreditierte Diensteanbieter nach § 5 Absatz 5 Satz 3 verpflichtet, die Nachricht mit einer, und zwar „seiner" qualifizierten elektronischen Signatur zu versehen. Diese qualifizierte Signatur selbst enthält nicht die erlassende Behörde als Senderin. Dies ist nicht notwendig, weil sich die erlassende Behörde aus den Metadaten der Nachricht ergibt.

Einer Ergänzung von Absatz 4 bedarf es dagegen nicht, da dort bereits auf § 3a Absatz 2 insgesamt Bezug genommen wird.

Artikel 4

Änderung des Ersten Buches Sozialgesetzbuch

§ 36a Absatz 2 des Ersten Buches Sozialgesetzbuch – Allgemeiner Teil – (Artikel I des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015), das zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 15. Februar 2013 (BGBl. I S. 254) geändert worden ist, wird durch die folgenden Absätze 2 und 2a ersetzt:

„(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht unmittelbar durch die Behörde ermöglicht, ist nicht zulässig. Die Schriftform kann auch ersetzt werden

1. durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird;

2. bei Anträgen und Anzeigen durch Versendung eines elektronischen Dokuments an die Behörde mit der Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes;

3. bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörden durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt;

4. durch sonstige sichere Verfahren, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten; der IT-Planungsrat gibt Empfehlungen zu geeigneten Verfahren ab.

In den Fällen des Satzes 4 Nummer 1 muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen; in der Kommunikation zwischen dem Versicherten und seiner Krankenkasse kann die Identität auch mit der elektronischen Gesundheitskarte nach § 291 Absatz 2a Satz 4 des Fünften Buches elektronisch nachgewiesen werden.

(2a) Ist durch Rechtsvorschrift die Verwendung eines bestimmten Formulars vorgeschrieben, das ein Unterschriftsfeld vorsieht, wird allein dadurch nicht die Anordnung der Schriftform bewirkt. Bei einer für die elektronische Versendung an die Behörde bestimmten Fassung des Formulars entfällt das Unterschriftsfeld.“

Lesefassung § 36a SGB I – Elektronische Kommunikation

(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.

(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht unmittelbar durch die Behörde ermöglicht, ist nicht zulässig. Die Schriftform kann auch ersetzt werden

1. durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird;

2. bei Anträgen und Anzeigen durch Versendung eines elektronischen Dokuments an die Behörde mit der Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes;

3. bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörden durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt;

4. durch sonstige sichere Verfahren, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten; der IT-Planungsrat gibt Empfehlungen zu geeigneten Verfahren ab.

In den Fällen des Satzes 4 Nummer 1 muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen; in der Kommunikation zwischen dem Versicherten und seiner Krankenkasse kann die Identität auch mit der elektronischen Gesundheitskarte nach § 291 Absatz 2a Satz 4 des Fünften Buches elektronisch nachgewiesen werden.

(2a) Ist durch Rechtsvorschrift die Verwendung eines bestimmten Formulars vorgeschrieben, das ein Unterschriftsfeld vorsieht, wird allein dadurch nicht die Anordnung der Schriftform bewirkt. Bei einer für die elektronische Versendung an die Behörde bestimmten Fassung des Formulars entfällt das Unterschriftsfeld.“

(3) Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, übermittelt sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück.

(4) Die Träger der Sozialversicherung einschließlich der Bundesagentur für Arbeit, ihre Verbände und Arbeitsgemeinschaften verwenden unter Beachtung der Grundsätze der Wirtschaftlichkeit und Sparsamkeit im jeweiligen Sozialleistungsbereich Zertifizierungsdienste nach dem Signaturgesetz, die eine gemeinsame und bundeseinheitliche Kommunikation und Übermittlung der Daten und die Überprüfbarkeit der qualifizierten elektronischen Signatur auf Dauer sicherstellen. Diese Träger sollen über ihren jeweiligen Bereich hinaus Zertifizierungsdienste im Sinne des Satzes 1 verwenden. Die Sätze 1 und 2 gelten entsprechend für die Leistungserbringer nach dem Fünften und dem Elften Buch und die von ihnen gebildeten Organisationen.

Erläuterungen

Bei der Neufassung des Absatzes 2 handelt es sich um die Parallelregelung zur Änderung des § 3a VwVfG. Insoweit wird auf die entsprechende Begründung zu Artikel 3 Nummer 1 verwiesen.

Bei Absatz 2 Satz 2 Nummer 4 handelt es sich um die Parallelregelung zur Änderung des § 3a Absatz 2 Satz 4 Nummer 4 VwVfG. Insoweit wird auf die entsprechende Begründung verwiesen. Sollen für den Bereich der Sozialverwaltung sonstige sichere Verfahren zur Ersetzung der Schriftform geregelt werden, ist auf der Grundlage von § 36a Absatz 2 Satz 4 Nummer 4 SGB I eine gegenüber der Rechtsverordnung nach § 3a Absatz 2 Satz 4 Nummer 4 VwVfG eigenständige Rechtsverordnung zu erlassen. Aus Gründen der Einheitlichkeit sollte bei der Erarbeitung der beiden Rechtsverordnungen jedoch darauf geachtet werden, dass gleiche sichere Verfahren definiert werden, die jeweils sowohl die Schriftform nach § 3a Absatz 2 VwVfG als auch die nach § 36a Absatz 2 SGB I ersetzen können.

Abweichend von der Änderung des § 3a VwVfG wird in Satz 5 2. Halbsatz für die Kommunikation zwischen dem Versicherten und seiner Krankenkasse die elektronische Gesundheitskarte als möglicher weiterer elektronischer Nachweis der Identität zugelassen.

Die mit dem neuen Absatz 2a getroffene Regelung wird wortgleich aus Artikel 1 § 13 übernommen, um eine einheitliche Regelung für alle Bereiche des Sozialrechts zu gewährleisten. Satz 1 stellt klar, dass kein Schriftformerfordernis vorliegt, wenn dieses nicht explizit in einer Rechtsvorschrift geregelt ist. Allein aus der Tatsache, dass ein Formular ein Unterschriftsfeld enthält, lässt sich ein Schriftformerfordernis nicht herleiten.

Stellt die Behörde eine Fassung eines Formulars zur Verfügung, das für die elektronische Versendung bestimmt ist, entfällt in dieser Fassung das Unterschriftsfeld. Damit stellt Satz 2 klar, dass bei in Papierform ausgegebenen Formularen weiterhin die gesetzlich vorgesehene Form einschließlich des Unterschriftsfeldes beizubehalten ist. Im Übrigen wird auf die Begründung zu Artikel 1 § 13 verwiesen.

Artikel 5

Änderung des Vierten Buches Sozialgesetzbuch

Nach § 110c Absatz 1 Satz 1 des Vierten Buches Sozialgesetzbuch – Gemeinsame Vorschriften für die Sozialversicherung – in der Fassung der Bekanntmachung vom 12. November 2009 (BGBl. I S. 3710, 3973; 2011 I S. 363), das zuletzt durch Artikel 4 Absatz 2 des Gesetzes vom 20. April 2013 (BGBl. I S. 868) geändert worden ist, wird folgender Satz eingefügt:

„Dies gilt entsprechend für die ergänzenden Vorschriften des E-Government-Gesetzes.“

Lesefassung § 110c SGB IV – Verwaltungsvereinbarungen, Verordnungsermächtigung

(1) Die Spitzenverbände der Träger der Sozialversicherung und die Bundesagentur für Arbeit vereinbaren gemeinsam unter besonderer Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Voraussetzungen des Signaturgesetzes das Nähere zu den Grundsätzen ordnungsmäßiger Aufbewahrung im Sinne des § 110a, den Voraussetzungen der Rückgabe und Vernichtung von Unterlagen sowie die Aufbewahrungsfristen für Unterlagen. Dies gilt entsprechend für die ergänzenden Vorschriften des E-Government-Gesetzes. Die Vereinbarung kann auf bestimmte Sozialleistungsbereiche beschränkt werden; sie ist von den beteiligten Spitzenverbänden abzuschließen. Die Vereinbarungen bedürfen der Genehmigung der beteiligten Bundesministerien.

Erläuterungen

Aufgrund der Regelung in Artikel 1 § 1 Absatz 4 ist zwar davon auszugehen, dass die §§ 110a bis 110d SGB IV als entweder inhaltsgleiche oder entgegenstehende Normen den in Artikel 1 §§ 6, 7 und 8 enthaltenen Regelungen vorgehen. Sofern aber im EGovG weiter gehende Regelungen oder Neuerungen enthalten sind, würden diese jedenfalls für die dem Geltungsbereich des EGovG unterfallenden Träger der Sozialversicherung gelten. Mit der Ergänzung des § 110c SGB IV sollen die Spitzenverbände der Träger der Sozialversicherung und die Bundesagentur für Arbeit die Möglichkeit bekommen, auch zu diesen Vorschriften Verwaltungsvereinbarungen im Sinne des Satzes 1 zu treffen.

Artikel 6

Änderung des Zehnten Buches Sozialgesetzbuch

Das Zehnte Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), das zuletzt durch Artikel 2 Absatz 13 des Gesetzes vom 3. Mai 2013 (BGBl. I S. 1084) geändert worden ist, wird wie folgt geändert:

1. § 21 Absatz 1 wird wie folgt geändert:

a) In Satz 2 Nummer 1 werden nach dem Wort „Art“ die Wörter „, auch elektronisch und als elektronisches Dokument,“ eingefügt.

b) Folgender Satz wird angefügt:

„Urkunden und Akten können auch in elektronischer Form beigezogen werden, es sei denn, durch Rechtsvorschrift ist etwas anderes bestimmt.“

2. Nach § 25 Absatz 5 Satz 1 wird folgender Satz eingefügt:

„Soweit die Akteneinsicht in eine elektronische Akte zu gestatten ist, kann die Behörde Akteneinsicht gewähren, indem sie Unterlagen ganz oder teilweise ausdruckt, elektronische Dokumente auf einem Bildschirm wiedergibt, elektronische Dokumente zur Verfügung stellt oder den elektronischen Zugriff auf den Inhalt der Akte gestattet.“

3. Dem § 29 wird folgender Absatz 7 angefügt:

„(7) Soweit eine Behörde über die technischen Möglichkeiten verfügt, kann sie von Urkunden, die sie selbst ausgestellt hat, auf Verlangen ein elektronisches Dokument nach Absatz 4 Nummer 4 Buchstabe a oder eine elektronische Abschrift fertigen und beglaubigen.“

4. Dem § 33 Absatz 3 wird folgender Satz angefügt:

„Im Fall des § 36a Absatz 2 Satz 4 Nummer 3 des Ersten Buches muss die Bestätigung nach § 5 Absatz 5 des De-Mail-Gesetzes die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lassen.“

5. In § 67 Absatz 6 Satz 2 Nummer 3 wird in dem Satzteil nach Buchstabe b nach dem Wort „Sozialdaten“ das Komma gestrichen und werden die Wörter „; das Senden von Sozialdaten durch eine De-Mail-Nachricht an die jeweiligen akkreditierten Diensteanbieter – zur kurzfristigen automatisierten Entschlüsselung zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten der De-Mail-Nachricht – ist kein Übermitteln,“ eingefügt.

Lesefassung § 21 Absatz 1 SGB X – Beweismittel

(1) Die Behörde bedient sich der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält. Sie kann insbesondere

1. *Auskünfte jeder Art, auch elektronisch und als elektronisches Dokument, einholen,*

2. *Beteiligte anhören, Zeugen und Sachverständige vernehmen oder die schriftliche oder elektronische Äußerung von Beteiligten, Sachverständigen und Zeugen einholen,*

3. *Urkunden und Akten beiziehen,*

4. *den Augenschein einnehmen.*

Urkunden und Akten können auch in elektronischer Form beigezogen werden, es sei denn, durch Rechtsvorschrift ist etwas anderes bestimmt.

Lesefassung § 25 Absatz 5 SGB X

(5) Soweit die Akteneinsicht zu gestatten ist, können die Beteiligten Auszüge oder Abschriften selbst fertigen oder sich Ablichtungen durch die Behörde erteilen lassen. Soweit die Akteneinsicht in eine elektronische Akte zu gestatten ist, kann die Behörde Akteneinsicht gewähren, indem sie Unterlagen ganz oder teilweise ausdruckt, elektronische Dokumente auf einem Bildschirm wiedergibt, elektronische Dokumente zur Verfügung stellt oder den elektronischen Zugriff auf den Inhalt der Akte gestattet. Die Behörde kann Ersatz ihrer Aufwendungen in angemessenem Umfang verlangen.

Lesefassung § 67 Absatz 6 SGB X

(6) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen von Sozialdaten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren,

1. *Speichern das Erfassen, Aufnehmen oder Aufbewahren von Sozialdaten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,*

2. *Verändern das inhaltliche Umgestalten gespeicherter Sozialdaten,*

3. *Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Sozialdaten an einen Dritten in der Weise, dass*

   a) *die Daten an den Dritten weitergegeben werden oder*

   b) *der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft;*

Übermitteln im Sinne dieses Gesetzbuches ist auch das Bekanntgeben nicht gespeicherter Sozialdaten; das Senden von Sozialdaten durch eine De-Mail-Nachricht an die jeweiligen akkreditierten Diensteanbieter – zur kurzfristigen automatisierten Entschlüsselung zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten der De-Mail-Nachricht – ist kein Übermitteln,

4. *Sperren das vollständige oder teilweise Untersagen der weiteren Verarbeitung oder Nutzung von Sozialdaten durch entsprechende Kennzeichnung,*

5. *Löschen das Unkenntlichmachen gespeicherter Sozialdaten.*

Erläuterungen

1. Änderung des § 21 Absatz 1 SGB 10 (Nummer 1)

Mit der Ergänzung von Satz 2 Nummer 1 und der Ergänzung des Absatzes 1 um Satz 3 wird zur Etablierung durchgehend elektronischer Verfahrensabwicklung beigetragen. Medienbrüche werden vermieden, wenn die Verwaltung bereits eine Auskunft auf elektronischem Weg einholt und elektronische Dokumente übermittelt werden. Das gilt auch für Urkunden und Akten. Zukünftig werden immer mehr Verwaltungen ihre Akten elektronisch führen, so dass es zur Vermeidung von Medienbrüchen sinnvoll ist, auch die Beiziehung von Urkunden und Akten in elektronischer Form zuzulassen.

2. Elektronische Akteneinsicht – § 25 Absatz 5 SGB 10 (Nummer 2)

Bisher enthält das Sozialrecht nur in § 110a SGB IV für dessen Geltungsbereich Regelungen zur Ausgestaltung des Akteneinsichtsrechts für den Fall, dass Unterlagen, die lediglich elektronisch vorhanden sind, vorgelegt werden müssen. Da zunehmend auch in den anderen Sozialleistungsbereichen Akten elektronisch geführt werden, soll § 25 SGB X um eine Regelung zur Einsicht in eine elektronische Akte ergänzt werden. Die Vorschrift orientiert sich an Artikel 1 § 8. Daher wird auf die Begründung zu Artikel 1 § 8 verwiesen.

3. Elektronische Abschrift von Urkunden – § 29 Absatz 7 SGB 10 (Nummer 3)

Nach § 29 Absatz 4 Nummer 4 Buchstabe a SGB X gelten die Vorschriften über die Beglaubigung von Schriftstücken entsprechend für die Beglaubigung von elektronischen Dokumenten, die zur Abbildung eines Schriftstückes hergestellt wurden. Wie im Verwaltungsverfahrensrecht kann auch nach dem geltenden sozialrechtlichen Verfahrensrecht eine elektronische Ausfertigung einer schriftlichen Urkunde beglaubigt und mit dem Beweiswert einer herkömmlichen beglaubigten Kopie verwendet werden (§ 29 Absatz 6 SGB X). Um eine vollständige elektronische Verfahrensabwicklung zu fördern, sollen zukünftig beispielsweise zu Nachweiszwecken vorzulegende Urkunden als beglaubigte Abschriften oder Abbilder in elektronischer Form zur Verfügung stehen. So können einmal erstellte und beglaubigte elektronische Dokumente mehrfach verwendet werden, ohne dass eine Vielzahl von Abschriften oder Kopien zu fertigen und zu beglaubigen wären. Daher wird mit der Regelung in Absatz 7 das Ziel einer möglichst vollständigen elektronischen Verfahrensabwicklung gefördert. Zwar wird angesichts des Geltungsbereichs der Norm – sie gilt für alle Sozialleistungsträger in Bund, Ländern, Gemeinden und Gemeindeverbänden – keine Verpflichtung eingeführt. Wenn aber die Behörde über die technischen Voraussetzungen verfügt, kann die Behörde von der Urkunde, die sie ausgestellt hat, entsprechende elektronische Dokumente erstellen und beglaubigen, wenn der Bürger das verlangt.

4. Änderung des § 33 Absatz 3 SGB 10 (Nummer 4)

Es handelt sich um die Parallelregelung zur Änderung des § 37 Absatz 3 VwVfG. Insoweit wird auf die entsprechende Begründung verwiesen.

5. Änderung des § 67 Absatz 6 SGB 10 (Nummer 5)

Die Regelung enthält eine notwendige Klarstellung betreffend das Senden von Sozialdaten durch eine De-Mail-Nachricht. Akkreditierte Diensteanbieter im Sinne dieser Regelung sind solche, die eine Akkreditierung nach § 17 des De-Mail-Gesetzes vorweisen können.

Die Regelung ist im Zusammenhang mit dem durch dieses Gesetz geänderten § 5 Absatz 5 des De-Mail-Gesetzes zu sehen. Auf die dortige Begründung zu Artikel 2 Nummer 32 wird verwiesen.

Artikel 7

Änderung der Abgabenordnung

Die Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), die zuletzt durch Artikel 2 Absatz 10 des Gesetzes vom 3. Mai 2013 (BGBl. I S. 1084) geändert worden ist, wird wie folgt geändert:

1. Dem § 30 wird folgender Absatz 7 angefügt:

„(7) Werden dem Steuergeheimnis unterliegende Daten durch einen Amtsträger oder diesem nach Absatz 3 gleichgestellte Personen nach Maßgabe des § 87a Absatz 4 über De-Mail-Dienste im Sinne des § 1 des De-Mail-Gesetzes versendet, liegt keine unbefugte Offenbarung, Verwertung und kein unbefugter Abruf von dem Steuergeheimnis unterliegenden Daten vor, wenn beim Versenden eine kurzzeitige automatisierte Entschlüsselung durch den akkreditierten Diensteanbieter zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten der De-Mail-Nachricht stattfindet.“

2. § 87a wird wie folgt geändert:

a) Dem Absatz 1 wird folgender Satz angefügt:

„Die kurzzeitige automatisierte Entschlüsselung, die beim Versenden einer De-Mail-Nachricht durch den akkreditierten Diensteanbieter zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten der De-Mail-Nachricht erfolgt, verstößt nicht gegen das Verschlüsselungsgebot des Satzes 3.“

b) Die Absätze 3 und 4 werden wie folgt gefasst:

„(3) Eine durch Gesetz für Anträge, Erklärungen oder Mitteilungen an die Finanzbehörden angeordnete Schriftform kann, soweit nicht durch Gesetz etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist. Die Signierung mit einem Pseudonym ist nicht zulässig. Die Schriftform kann auch ersetzt werden

1. durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird;

2. durch Versendung eines elektronischen Dokuments an die Behörde mit der Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes.

In den Fällen des Satzes 4 Nummer 1 muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach § 18 des Per-

sonalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen.

(4) Eine durch Gesetz für Verwaltungsakte oder sonstige Maßnahmen der Finanzbehörden angeordnete Schriftform kann, soweit nicht durch Gesetz etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist. Die Schriftform kann auch ersetzt werden durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Finanzbehörde als Nutzer des De-Mail-Kontos erkennen lässt. Für von der Finanzbehörde aufzunehmende Niederschriften gelten die Sätze 1 und 3 nur, wenn dies durch Gesetz ausdrücklich zugelassen ist.“

3. Dem § 119 Absatz 3 wird folgender Satz angefügt:

„Im Falle des § 87a Absatz 4 Satz 3 muss die Bestätigung nach § 5 Absatz 5 des De-Mail-Gesetzes die erlassende Finanzbehörde als Nutzer des De-Mail-Kontos erkennen lassen.“

4. § 357 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 werden nach dem Wort „schriftlich“ die Wörter „oder elektronisch“ eingefügt.

bb) Satz 2 wird wie folgt gefasst:

„Es genügt, wenn aus dem Einspruch hervorgeht, wer ihn eingelegt hat.“

b) In Absatz 2 Satz 4 werden nach dem Wort „schriftliche“ die Wörter „oder elektronische“ eingefügt.

<u>Lesefassung § 357 Absatz 1, 2 AO – Einlegung des Einspruchs</u>

(1) Der Einspruch ist schriftlich oder elektronisch einzureichen oder zur Niederschrift zu erklären. Es genügt, wenn aus dem Einspruch hervorgeht, wer ihn eingelegt hat. Einlegung durch Telegramm ist zulässig. Unrichtige Bezeichnung des Einspruchs schadet nicht.

(2) Der Einspruch ist bei der Behörde anzubringen, deren Verwaltungsakt angefochten wird oder bei der ein Antrag auf Erlass eines Verwaltungsakts gestellt worden ist. Ein Einspruch, der sich gegen die Feststellung von Besteuerungsgrundlagen oder gegen die Festsetzung eines Steuermessbetrags richtet, kann auch bei der zur Erteilung des Steuerbescheids zuständigen Behörde angebracht werden. Ein Einspruch, der sich gegen einen Verwaltungsakt richtet, den eine Behörde auf Grund gesetzlicher Vorschrift für die zuständige Finanzbehörde erlassen hat, kann auch bei der zuständigen Finanzbehörde angebracht werden. Die schriftliche oder elektronische Anbringung bei einer anderen Behörde ist unschädlich, wenn der Einspruch vor Ablauf der Einspruchsfrist einer der Behörden übermittelt wird, bei der er nach den Sätzen 1 bis 3 angebracht werden kann.

Erläuterungen

1. Keine unbefugte Offenbarung – Neuer § 30 Absatz 7 AO (Nummer 1)

Die Regelung enthält eine notwendige Klarstellung. Akkreditierte Diensteanbieter im Sinne dieser Regelung sind solche, die eine Akkreditierung nach § 17 des De-Mail-Gesetzes vorweisen können.

Die Regelung ist im Zusammenhang mit dem durch dieses Gesetz geänderten § 5 Absatz 5 des De-Mail-Gesetzes zu sehen. Auf die dortige Begründung zu Artikel 2 Nummer 2 wird verwiesen.

2. Änderung des § 87a AO (Nummer 2)

a) Kein Verstoß gegen das Verschlüsselungsgebot (Buchstabe a)

Die Regelung enthält eine notwendige Klarstellung. Akkreditierte Diensteanbieter im Sinne dieser Regelung sind solche, die eine Akkreditierung nach § 17 des De-Mail-Gesetzes vorweisen können.

Die Regelung ist im Zusammenhang mit dem durch dieses Gesetz geänderten § 5 Absatz 5 des De-Mail-Gesetzes zu sehen. Auf die dortige Begründung zu Artikel 2 Nummer 3 wird verwiesen.

b) Ersetzung der Schriftform - § 87a Absatz 3, 4 AO (Buchstabe b)

Bei der Änderung des Absatzes 3 handelt es sich um die Parallelregelung zur Änderung des § 3a VwVfG. Insoweit wird auf die entsprechende Begründung zu Artikel 3 Nummer 1 verwiesen.

Bei der Änderung des Absatzes 4 handelt es sich um die Parallelregelung zur Änderung des § 3a VwVfG. Allerdings wird die Variante des Einsatzes des „elektronischen Formulars in Verbindung mit einem sicheren elektronischen Identitätsnachweis“ hier nicht vorgesehen, weil sich diese Variante nur für Kommunikation in Richtung einer Behörde eignet. Denn das Formular stellt die Behörde zur Verfügung. Da dieser Absatz aber die Kommunikation der Behörde hin zur Bürgerin/zum Bürger/zum Unternehmen/sonstigen Verfahrensbeteiligten regelt, ist die Variante der Vorgabe eines Formulars nicht geeignet.

3. Änderung des § 119 Absatz 3 AO (Nummer 3)

Es handelt sich um die Parallelregelung zur Änderung des § 37 Absatz 3 VwVfG. Insoweit wird auf die entsprechende Begründung verwiesen.

4. Änderung des § 357 AO (Nummer 4)

a) Elektronischer Einspruch (Buchstabe a)

Die Ergänzung in Satz 1 stellt klar, dass unter der Voraussetzung der Zugangseröffnung (§ 87a Absatz 1 AO) ein Einspruch auch elektronisch ohne qeS eingelegt werden kann. Eine Rechtsänderung ist hiermit nicht verbunden. Im Geltungsbereich der AO entspricht es bereits der derzeitigen Erlasslage, dass der Einspruch auch elektronisch ohne qeS eingelegt werden kann (Nummer 1 Satz 2 des AO-Anwendungserlasses zu § 357 AO, der insoweit auf den Beschluss des BFH vom 26. März 1991, VIII B 83/90 verweist). In diesem Beschluss hatte der BFH es für die Formgültigkeit einer Klageerhebung per Telefax

ausreichen lassen, wenn der Urheber der Rechtsmittelschrift eindeutig zu identifizieren und der ernstliche Wille zur Einlegung eines Rechtsmittels erkennbar war. Die bisherige Erlasslage zur AO hat sich bewährt und wird daher kodifiziert.

Die Neufassung des Satzes 2 berücksichtigt nunmehr auch im Wortlaut der Vorschrift die Möglichkeit der elektronischen Einspruchseinlegung.

b) Folgeänderung (Buchstabe b)

Es handelt sich um eine Folgeänderung zu Buchstabe a.

Artikel 8

Änderung des Passgesetzes

§ 25 des Passgesetzes vom 19. April 1986 (BGBl. I S. 537), das zuletzt durch Artikel 2 Absatz 4 des Gesetzes vom 3. Mai 2013 (BGBl. I S. 1084) geändert worden ist, wird wie folgt geändert:

1. In Absatz 4 wird die Angabe „Nr. 4 und 5“ durch die Wörter „Nummer 5 und 6“ ersetzt.

2. In Absatz 6 wird die Angabe „Nr. 1 und 3“ durch die Wörter „Nummer 2 und 4“ ersetzt.

Erläuterungen

Durch das Gesetz vom 18. Juni 2009 (BGBl. I S. 1346) wurde eine neue Nummer 1 in § 25 Absatz 2 eingefügt. Aufgrund eines redaktionellen Fehlers blieb der Einschub bei den Verweisen in den Absätzen 4 und 6 unberücksichtigt. Dies soll durch die Gesetzesänderung korrigiert werden.

Artikel 9

Änderung des Personalausweisgesetzes

Das Personalausweisgesetz vom 18. Juni 2009 (BGBl. I S. 1346), das durch Artikel 2 Absatz 4 des Gesetzes vom 3. Mai 2013 (BGBl. I S. 1084) geändert worden ist, wird wie folgt geändert:

1. Nach § 2 Absatz 6 wird folgender Absatz 6a eingefügt:

„(6a) Die Sperrsumme ist ein eindeutiges Merkmal, das aus dem Sperrkennwort, dem Familiennamen, den Vornamen und dem Tag der Geburt eines Ausweisinhabers errechnet wird. Es dient der Übermittlung einer Sperrung vom

Sperrnotruf oder einer Personalausweisbehörde an den Sperrlistenbetreiber. Mithilfe der Sperrsumme ermittelt der Sperrlistenbetreiber anhand der Referenzliste den Sperrschlüssel eines zu sperrenden elektronischen Identitätsnachweises.“

2. In § 9 Absatz 3 Satz 4 und 6 wird jeweils das Wort „schriftlich“ gestrichen.

3. § 10 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 wird das Wort „schriftlich“ gestrichen.

bb) In Satz 2 wird das Wort „schriftliche“ gestrichen.

b) In Absatz 5 werden in dem Satzteil nach Nummer 2 die Wörter „das Sperrkennwort“ durch die Wörter „die Sperrsumme“ ersetzt.

4. § 11 wird wie folgt geändert:

a) In Absatz 2 werden nach dem Wort „Informationsmaterial“ die Wörter „oder dessen Übersendung per De-Mail gemäß § 5 Absatz 8 des De-Mail-Gesetzes“ eingefügt.

b) Absatz 4 wird aufgehoben.

5. Nach § 18 Absatz 3 Satz 2 Nummer 1 wird folgende Nummer 1a eingefügt:

„1a. Geburtsname,“.

6. In § 19 Absatz 2 werden nach dem Wort „Sperrkennworts“ die Wörter „und der Sperrsumme“ eingefügt.

7. In § 21 Absatz 2 Satz 1 wird nach Nummer 2 folgende Nummer 2a eingefügt:

„2a eine Übermittlung an bestimmte Dritte zur Erfüllung eines Geschäftszwecks erforderlich ist, der nicht in der geschäftsmäßigen Übermittlung der Daten besteht und keine Anhaltspunkte für eine geschäftsmäßige oder unberechtigte Übermittlung der Daten vorliegen,“.

8. In § 23 Absatz 3 Nummer 12 werden nach dem Wort „Sperrkennwort“ die Wörter „und Sperrsumme“ eingefügt.

9. In § 32 Absatz 3 wird die Angabe „Nr. 2, 3 und 5“ durch die Wörter „Nummer 1, 2 und 4“ ersetzt.

Erläuterungen

1. Sperrsumme - § 2 Absatz 6a PAuswG (Nummer 1)

Die Legaldefinition des Begriffs Sperrsumme ist bislang in § 1 Absatz 1 der Personalausweisverordnung enthalten. Aufgrund der Bedeutung der Sperrsumme für das Sperrverfahren soll diese im Personalausweisregister gespeichert (siehe Nummer 6) und der Begriff damit in das Gesetz eingeführt werden. Aus diesem Grund soll auch die Begriffsbestimmung in das Gesetz aufgenommen werden.

2. Änderung des § 9 Absatz 3 PAuswG (Nummer 2)

Die vorgesehene Änderung greift den Vorschlag Nummer 22 der Stellungnahme des Bundesrates (BR Drucksache 557/12(B)) auf. Hinsichtlich der Änderung des Satzes 6 (Informationspflicht der Behörde gegenüber der antragstellenden Person hinsichtlich der Entscheidung der Aufnahme der Fingerabdrücke) wird darauf hingewiesen, dass es nunmehr ausschließlich der jeweiligen Personalausweisbehörde obliegt, im Rahmen ihrer Dokumentationspflicht die Information und die jeweils getroffene Entscheidung des Antragstellers gerichtsfest zu dokumentieren.

3. Änderung des § 10 PAuswG (Nummer 3)

a) Buchstabe a

Im Rahmen der Aushändigung des Personalausweises hat die antragstellende Person gegenüber der Personalausweisbehörde zu erklären, ob sie den elektronischen Identitätsnachweis nutzen möchte. Diese Erklärung erfolgt mündlich und wird aufgrund der rechtlichen Vorgabe schriftlich wiederholt. Auf dieses Formerfordernis kann verzichtet werden, weil die Erklärung im Fachverfahren dokumentiert wird. Dies gilt auch für eine spätere Erklärung zur Nutzung des elektronischen Identitätsnachweises. Durch den Wegfall des Erfordernisses der schriftlichen Bestätigung wird das Antragsverfahren beschleunigt und die Medienbruchfreiheit gefördert.

b) Buchstabe b

Folgeänderung zu Nummer 1.

4. Änderung des § 11 PAuswG (Nummer 4)

a) Buchstabe a

§ 11 Absatz 2 und 3 verpflichtet die Personalausweisbehörde, die antragstellende Person über die Funktion des elektronischen Identitätsnachweises sowie dessen sichere Nutzung zu unterrichten. Diesen Pflichten kommen die Personalausweisbehörden flächendeckend durch Übergabe einer vom BMI konzipierten Informationsbroschüre nach. Anstelle der Übergabe soll künftig auch die Versendung der Broschüre per De-Mail ermöglicht werden. Um sicherzustellen, dass der Bürger die De-Mail tatsächlich erhalten hat, ist die De-Mail mit einer Eingangsbestätigung gemäß § 5 Absatz 8 des De-Mail-Gesetzes zu versenden.

b) Buchstabe b

Die Übergabe wird im Rahmen des von der Behörde genutzten Fachverfahrens dokumentiert, so dass eine gesonderte Bestätigung durch die antragstellende Person entbehrlich ist. Durch den Wegfall des Erfordernisses der schriftlichen Bestätigung wird das Antragsverfahren beschleunigt und die Medienbruchfreiheit gefördert.

5. Geburtsname – Änderung des § 18 Absatz 3 PAuswG (Nummer 5)

Der Geburtsname wird nach § 5 Absatz 5 Nummer 1 in Verbindung mit Absatz 2 Nummer 1 auf dem Chip des Personalausweises gespeichert, ist in § 18 Absatz 3 aber nicht als zu übermittelndes Datum im Rahmen des elektronischen Identitätsnachweises vorgesehen. Bei zahlreichen Online-Anwendungen, insbesondere E-Government-Anwendungen, wird zur eindeutigen Identifizierung der Bürgerinnen und Bürger auch der Geburtsname benötigt. Wesentliche Anwendungen im Bereich des E-Government stellen z. B. die Möglichkeit zur Beantragung des Führungszeugnisses nach dem Bundeszentralregistergesetz und die Auskunft aus dem Verkehrszentralregister beim Kraftfahrtbundesamt dar. Beide Anwendungen benötigen zur eindeutigen Identifizierung einer Person die

Übermittlung des Geburtsnamens. Hierfür wird ein eigenes Datenfeld eingerichtet, so dass nicht bei jeder Übermittlung des Familiennamens auch zwangsläufig der Geburtsname übermittelt wird. Der Geburtsname kann also eigenständig abgefragt werden. Der Geburtsname wird nur dann ausgelesen, wenn die Vergabestelle für Berechtigungszertifikate zuvor die Erforderlichkeit der Übermittlung des Geburtsnamens für diesen Dienst festgestellt hat. § 18 Absatz 3 Satz 2 soll daher um den Geburtsnamen erweitert werden.

6. Änderung des § 19 Absatz 2 PAuswG (Nummer 6)

Es handelt sich um eine Folgeänderung zu Nummer 1. Die Sperrsumme ist eine Zeichenfolge, die den jeweiligen Personalausweis im Falle einer Sperrung oder Entsperrung beim Sperrlistenbetreiber eindeutig identifiziert und auch als temporäres Personenkennzeichen verwendet werden könnte.

7. Änderung des § 21 Absatz 2 PAuswG (Nummer 7)

§ 21 Absatz 2 Nummer 2 schließt Adresspools, Auskunfteien und mögliche Identitätsprovider, die verifizierte Daten aus dem Personalausweis einem beliebigen Kreis von Dritten zu Verfügung stellen, von der Nutzung des elektronischen Identitätsnachweises aus. Inzwischen sind Geschäftsprozesse entwickelt worden, in denen Diensteanbieter Daten aus dem Personalausweis für eigene Zwecke benötigen, diese zur vollständigen Erbringung des Dienstes aber auch an eindeutig bezeichnete Dritte weitergeben. Dabei handelt es sich um Dienste, in denen die Beteiligung Dritter dem endgültigen Abschluss des eigentlichen Geschäftszwecks dient, z. B. Beauftragung eines Unternehmens, um eine Kfz-Zulassung zu veranlassen. Die vorgesehene Gesetzesänderung bewirkt, dass in solchen Fällen die Erteilung einer Berechtigung nicht grundsätzlich ausgeschlossen ist, sofern der Diensteanbieter vorab gegenüber der Vergabestelle für Berechtigungszertifikate den Gesamtprozesses eindeutig definiert. Die Regelung entspricht dem Ziel des Gesetzgebers, mit der Online-Ausweisfunktion den Dienst für Nutzer transparent und für den Anbieter ohne Zwischenschritte den Dienst abwickeln zu können.

8. Änderung des § 23 Absatz 3 PAuswG (Nummer 8)

Die Sperrsumme ist zentraler Bestandteil des Sperrverfahrens im Falle des Ausweisverlustes. Die Kenntnis der Sperrsumme ist auf Seiten der Personalausweisbehörde neben dem Sperrkennwort erforderlich, um den Ausweis unverzüglich sperren zu können. Die Speicherung dient einem ordnungsgemäßen Sperrverfahren und damit dem Schutz des Ausweisinhabers bei Verlust seines Ausweises. Es wird sichergestellt, dass die vom Ausweishersteller im Rahmen des Produktionsprozesses errechnete Sperrsumme von der Personalausweisbehörde gespeichert werden kann, um sie für eine zukünftig eventuell erforderlich werdende Sperrung verwenden zu können.

9. Änderung des § 32 Absatz 3 PAuswG (Nummer 9)

Ordnungswidrigkeiten, deren Unrechtsgehalt sich im mittleren Bereich ansiedeln lässt, sind mit bis zu 30 000 Euro bußgeldbewehrt. Aufgrund eines redaktionellen Fehlers wurde die Zuordnung zu dieser Gruppe in Absatz 3 nach einer Änderung von Absatz 2 im Gesetzgebungsverfahren nicht angepasst. Durch die Gesetzesänderung soll die Zuordnung korrigiert werden.

Artikel 10

Änderung des Gesetzes über die Umweltverträglichkeitsprüfung

§ 9a Absatz 1 des Gesetzes über die Umweltverträglichkeitsprüfung in der Fassung der Bekanntmachung vom 24. Februar 2010 (BGBl. I S. 94), das zuletzt durch Artikel 6 des Gesetzes vom 8. April 2013 (BGBl. I S. 734) geändert worden ist, wird wie folgt geändert:

1. **In Satz 2 Nummer 2 werden nach den Wörtern „welcher Behörde“ die Wörter „und in welcher Form“ eingefügt.**

2. **Folgender Satz wird angefügt:**

   „In einem Beteiligungsverfahren nach Satz 1 kann die zuständige Behörde der betroffenen Öffentlichkeit des anderen Staates die elektronische Übermittlung von Äußerungen auch abweichend von den Voraussetzungen des § 3a Absatz 2 des Verwaltungsverfahrensgesetzes gestatten, sofern im Verhältnis zum anderen Staat hierfür die Voraussetzungen der Grundsätze von Gegenseitigkeit und Gleichwertigkeit erfüllt sind.“

Erläuterungen

Bei der Beteiligung der betroffenen Öffentlichkeit in einem Verfahren der grenzüberschreitenden Umweltverträglichkeitsprüfung kann die Nutzung der elektronischen Form einen effektiven und zügigen Verfahrensablauf bewirken. Grundsätzlich besteht nach dem Gesetz über die Umweltverträglichkeitsprüfung (UVPG) auf Grund des Verweises auf § 73 Absatz 4 Satz 1 VwVfG sowie nach dem Fachrecht (vgl. § 10 Absatz 3 Satz 4 des Bundes-Immissionsschutzgesetzes) ein Schriftformerfordernis. Eine Ersetzung durch die elektronische Form richtet sich nach § 3a Absatz 2 VwVfG. Für das auf Grund unions- und völkerrechtlicher Vorgaben bestehende Stellungnahmerecht der betroffenen Öffentlichkeit eines anderen Staates in einem deutschen Zulassungsverfahren können die Voraussetzungen von § 3a Absatz 2 VwVfG jedoch unüberwindbare Hürden darstellen. Daher könnte eine für Mitglieder der deutschen Öffentlichkeit bestehende Möglichkeit zur Nutzung der elektronischen Form, die Mitgliedern der betroffenen Öffentlichkeit eines anderen Staates im selben Beteiligungsverfahren nicht eröffnet ist, zur einer europarechtlich unzulässigen Diskriminierung führen. Um dies zu vermeiden, ermöglicht es die in Nummer 2 vorgesehene Ergänzung von § 9a Absatz 1 UVPG der zuständigen deutschen Behörde im Einzelfall, auch Äußerungen der betroffenen Öffentlichkeit des anderen Staates zuzulassen, die nicht den Voraussetzungen des § 3a Absatz 2 VwVfG entsprechen. Voraussetzung ist jedoch, dass die Grundsätze von Gegenseitigkeit und Gleichwertigkeit im bilateralen Verhältnis erfüllt sind, d. h., dass Mitglieder der deutschen Öffentlichkeit bei einem Verfahren des anderen Staates gegenüber der zuständigen Behörde des anderen Staates Äußerungen unter vergleichbaren Voraussetzungen elektronisch übermitteln können. Dies muss die zuständige Behörde prüfen, da nur sie die die Vergleichbarkeit der Zugangsvoraussetzungen, insbesondere technischer Art, feststellen kann. Damit die betroffene Öffentlichkeit des anderen Staates über die im konkreten Verfahren eröffnete Form für die Übermittlung von Äußerungen ausreichend informiert ist, wird durch die in Nummer 1 vorgesehene Änderung von § 9a Absatz 1 Satz 2 Nummer 2 UVPG ausdrücklich festgeschrieben, dass die Bekanntmachung im anderen Staat unter anderem diese Information beinhalten soll; dies entspricht bereits der bisherigen Verwaltungspraxis, wonach neben einer Postanschrift der zuständigen deutschen Behörde in Einzelfällen auch eine E-Mail-Adresse angegeben wird.

Artikel 11

Änderung des Umweltschutzprotokoll-Ausführungsgesetzes

Das Umweltschutzprotokoll-Ausführungsgesetz vom 22. September 1994 (BGBl. I S. 2593), das zuletzt durch Artikel 69 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407) geändert worden ist, wird wie folgt geändert:

1. In § 3 Absatz 1 Satz 2 und § 6 Absatz 1 Satz 1 werden jeweils nach dem Wort „schriftlich“ die Wörter „oder elektronisch“ eingefügt.

2. § 9 Absatz 1 wird wie folgt geändert:

a) Satz 2 wird wie folgt gefasst:

„Während der Auslegungsfrist können beim Umweltbundesamt Einwendungen zu der Untersuchung schriftlich, elektronisch oder zur Niederschrift abgegeben werden.“

b) In Satz 3 werden nach dem Wort „Schriftliche“ die Wörter „oder elektronische“ eingefügt und wird das Wort „vorgelegt“ durch das Wort „eingebracht“ ersetzt.

c) In Satz 4 wird das Wort „vorgelegt“ durch das Wort „eingebracht“ ersetzt.

Erläuterungen

1. Änderung der §§ 3, 6 (Nummer 1)

Mit den Änderungen wird bewirkt, dass der Antrag auf Erteilung der Genehmigung einer Tätigkeit nach § 3 Absatz 1 Satz 1 sowie die Anzeige einer Tätigkeit, die unter die Voraussetzungen des § 6 Absatz 1 Satz 1 fällt, auch elektronisch (also z. B. per E-Mail) gestellt werden bzw. erfolgen kann.

2. Änderung des § 9 Absatz 1 (Nummer 2)

a) Buchstabe a

Mit der Änderung wird bewirkt, dass Einwendungen zu der Untersuchung nach § 8 Absatz 3 auch elektronisch (also z. B. per E-Mail) abgegeben werden können.

b) Buchstabe b

Es handelt sich um Folgeänderungen. Das Erfordernis, dass Einwendungen auch in englischer Sprache vorgelegt werden sollen, soll auch für elektronisch abgegebene Einwendungen gelten.

c) Buchstabe c

Es handelt sich um eine Folgeänderung.

Artikel 12

Änderung des Aufenthaltsgesetzes

In § 91a Absatz 7 des Aufenthaltsgesetzes in der Fassung der Bekanntmachung vom 25. Februar 2008 (BGBl. I S. 162), das zuletzt durch Artikel 2 Absatz 5 des Gesetzes vom 15. Februar 2013 (BGBl. I S. 254) geändert worden ist, werden die Wörter „in elektronischer Form“ durch das Wort „elektronisch“ ersetzt.

Erläuterungen

Es handelt sich um eine redaktionelle Anpassung.

Bei der Datenübermittlung in Zusammenhang mit dem Register zum vorübergehenden Schutz soll als Alternative zum automatisierten Verfahren und zur schriftlichen Übermittlung auch eine Kommunikation per E-Mail möglich sein (vgl. Nummer 91a 7.1.1 der Allgemeinen Verwaltungsvorschrift zum Aufenthaltsgesetz). Durch die Formulierung „in elektronischer Form“ könnte hingegen der irrige Eindruck entstehen, dass die elektronische Form im Sinne von § 3a VwVfG gemeint ist, mit der Folge, dass die zu übermittelnden Dokumente mit einer qeS versehen werden müssten, was für die vorliegende Art der Datenübermittlung nicht intendiert war.

Artikel 13

Änderung des Bundesstatistikgesetzes

Das Bundesstatistikgesetz vom 22. Januar 1987 (BGBl. I S. 462, 565), das zuletzt durch Artikel 3 des Gesetzes vom 7. September 2007 (BGBl. I S. 2246) geändert worden ist, wird wie folgt geändert:

1. § 3 Absatz 1 wird wie folgt geändert:

a) Der Nummer 1 wird folgender Buchstabe d angefügt:

„d) Einzelangaben nach Maßgabe dieses Gesetzes oder einer anderen Rechtsvorschrift für wissenschaftliche Zwecke bereitzustellen; die Zuständigkeit der Länder, diese Aufgabe ebenfalls wahrzunehmen, bleibt unberührt,“.

b) In Nummer 4 wird das Wort „Gemeinschaften“ durch das Wort „Union“ ersetzt.

2. § 4 Absatz 3 Satz 1 wird wie folgt geändert:

a) In Nummer 1 werden nach dem Wort „Datenschutz“ die Wörter „und die Informationsfreiheit “ eingefügt.

b) In Nummer 3 wird das Wort „Gemeinschaften“ durch das Wort „Union“ ersetzt.

3. In § 9 Absatz 1 wird nach dem Wort „Berichtszeitraum“ das Komma durch das Wort „oder“ ersetzt.

4. § 10 wird wie folgt geändert:

a) Absatz 2 Satz 1 und 2 wird wie folgt gefasst:

„Der Name der Gemeinde, die Blockseite und die geografische Gitterzelle dürfen für die regionale Zuordnung der Erhebungsmerkmale genutzt werden. Die übrigen Teile der Anschrift dürfen für die Zuordnung zu Blockseiten und geografischen Gitterzellen für einen Zeitraum von bis zu vier Jahren nach Abschluss der jeweiligen Erhebung genutzt werden.“

b) Dem Absatz 3 wird folgender Satz angefügt:

„Eine geografische Gitterzelle ist eine Gebietseinheit, die bezogen auf eine vorgegebene Kartenprojektion quadratisch ist und mindestens 1 Hektar groß ist.“

5. Nach § 11 wird folgender § 11a eingefügt:

„§ 11a

Elektronische Datenübermittlung

(1) Soweit Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen, Daten mittels standardisierter elektronischer Datenaustauschformate übermitteln, sind diese auch bei der Übermittlung der für eine Bundesstatistik zu erhebenden Daten zu verwenden. Ansonsten sind elektronische Verfahren nach Absprache der statistischen Ämter mit den betroffenen Stellen zu verwenden.

(2) Werden Betrieben und Unternehmen für die Übermittlung der für eine Bundesstatistik zu erhebenden Daten elektronische Verfahren zur Verfügung gestellt, sind sie verpflichtet, diese Verfahren zu nutzen. Zur Vermeidung unbilliger Härten kann die zuständige Stelle auf Antrag eine Ausnahme zulassen.“

6. In § 13 Absatz 2 Satz 1 Nummer 1 werden nach dem Wort „Anschriften“ die Wörter „sowie die Geokoordinaten“ eingefügt.

7. In den §§ 18 und 19 wird jeweils das Wort „Gemeinschaften“ durch das Wort „Union“ ersetzt.

8. § 23 Absatz 2 wird wie folgt gefasst:

„(2) Ordnungswidrig handelt, wer

1. entgegen § 11 Absatz 1 eine Antwort nicht in der vorgeschriebenen Weise erteilt oder

2. entgegen § 11a Absatz 2 Satz 1 ein dort genanntes Verfahren nicht nutzt.“

Erläuterungen

1. Vorbemerkungen

Mit der Änderung des BStatG soll die Nutzung der elektronischen Datenübermittlung im Bereich der Statistik weiter forciert werden. Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen, aber auch privatwirtschaftliche Unternehmen und Betriebe werden künftig verpflichtet sein, elektronische Verfahren zur Datenübermittlung zu nutzen.

Weiterhin werden mit der Novellierung die Voraussetzungen dafür geschaffen, künftig Statistiken erheblich flexibler räumlich auswerten zu können als bislang, indem statistische Angaben georeferenziert gespeichert und statistische Ergebnisse georeferenziert verbreitet werden dürfen. Die Herstellung eines räumlichen Bezugs für statistische Daten ist bislang nur auf Ebene administrativer Gebietseinheiten und in Form von Blockseiten (Gebiet zwischen zwei Straßenmündungen) möglich. Dies entspricht aber nicht mehr den heutigen vielfältigen Bedürfnissen an Darstellung und Analyse statistischer Daten, z. B. für Zwecke des Katastrophenschutzes oder für die Planung einer bedarfsgerechten öffentlichen Infrastrukturversorgung. Die Gesetzesänderungen schaffen die Voraussetzungen dafür, dass zukünftig tiefere raumbezogene Darstellungen möglich und zulässig sind.

Weiterhin wird klargestellt, dass die Bereitstellung von Einzelangaben für wissenschaftliche Zwecke zu den Aufgaben des StBA gehört. Diese Klarstellung ist insbesondere im Hinblick auf den Zugang der Wissenschaft zu entsprechenden Daten geboten. Die Wahrung des Statistikgeheimnisses findet dabei selbstverständlich Beachtung.

Mit der Novellierung des BStatG werden schließlich noch einige Änderungen redaktioneller Art vorgenommen, unter anderem werden die Vorschriften des BStatG an den am 1. Dezember 2009 in Kraft getretenen Vertrag von Lissabon angepasst.

2. Änderung des § 3 Absatz 1 BStatG (Nummer 1)

a) Buchstabe a

Durch die vorgesehene Änderung des § 3 BStatG werden die Aufgaben des StBA nicht erweitert, sondern es wird lediglich klargestellt, dass die Bereitstellung von Einzelangaben für wissenschaftliche Zwecke zu den Aufgaben des StBA gehört. Diese Klarstellung ist, insbesondere im Hinblick auf den Zugang der Wissenschaft zu entsprechenden Daten, geboten. Das StBA hat diese Aufgabe stets wahrgenommen. Durch diese Regelung werden die Länder jedoch nicht von dieser Aufgabe ausgeschlossen. Sie stellen der Wissenschaft Einzeldaten, wie bisher, im Rahmen ihrer jeweiligen Zuständigkeit zur Verfügung.

Die Bereitstellung von Einzelangaben kann auf verschiedene Weise erfolgen. Der Gesetzgeber sieht dabei die Übermittlung absolut anonymisierter Einzelangaben nach § 16 Absatz 1 Satz 2 Nummer 4 BStatG und die Übermittlung faktisch anonymisierter Einzelangaben nach § 16 Absatz 6 BStatG vor.

Eine weitere Form der Bereitstellung besteht darin, formal anonymisierte Einzelangaben, d. h. Einzelangaben ohne Hilfsmerkmale, durch kontrollierte Datenfernverarbeitung für Auswertungen nutzbar zu machen. Bei diesem Verfahren werden dem Auftraggeber von den statistischen Ämtern jedoch keine Einzelangaben übermittelt und der Auftraggeber erlangt bei diesem Verfahren auch keine Kenntnis von den Einzelangaben. Bei der kontrollierten Datenfernverarbeitung schreibt der Auftraggeber ein Auswertungsprogramm, das auf dem Server des statistischen Amts mit den „originalen“ Einzelangaben der amtlichen Statistik, die lediglich formal anonymisiert sind, die Berechnungen durchführt. Die so errechneten Ergebnisse werden vom statistischen Amt auf Geheimhaltung überprüft und dem Auftraggeber übermittelt.

b) Buchstabe b

Hierbei handelt es sich um eine redaktionelle Änderung.

3. Änderung des § 4 Absatz 3 BStatG (Nummer 2)

a) Buchstabe a

Seit dem Inkrafttreten des IFG am 1. Januar 2006 nimmt der Bundesbeauftragte für den Datenschutz auch die Aufgaben des Bundesbeauftragten für die Informationsfreiheit wahr und trägt seitdem die Bezeichnung „Bundesbeauftragter für den Datenschutz und die Informationsfreiheit“.

b) Buchstabe b

Änderung redaktioneller Art.

4. Änderung des § 9 Absatz 1 BStatG (Nummer 3)

Hier handelt es sich um die Korrektur eines Redaktionsversehens. Die eine Bundesstatistik anordnende Rechtsvorschrift muss die Berichtszeit bestimmen, auf den sich die statistischen Daten beziehen. Dabei kann es sich entweder um einen Zeitraum oder um einen Zeitpunkt handeln. Dies wurde schon im Gesetzentwurf zur ursprünglichen Fassung des § 9 BStatG klargestellt (vgl. BT-Drs. 10/5345, S. 7, 17 und 24); die entsprechende Formulierung wurde allerdings im verabschiedeten Gesetzentwurf versehentlich nicht übernommen.

5. Änderung des § 10 BStatG (Nummer 4)

a) Absatz 2 (Buchstabe a)

In welcher Weise der Raumbezug von Einzeldatensätzen fachstatistischer Erhebungen dauerhaft gespeichert sowie für Auswertungen, Darstellungen und Veröffentlichungen der amtlichen Statistik genutzt werden darf, ist in § 10 Absatz 2 BStatG geregelt. Danach dürfen der Name der Gemeinde und die Blockseite für die regionale Zuordnung der Erhebungsmerkmale genutzt werden. Die Speicherung statistischer Daten auf von den Blockseiten abweichende räumliche Bausteine ist derzeit rechtlich nicht zulässig. Eine Ausnahme gilt für sog. Strukturerhebungen in land- und forstwirtschaftlichen Betrieben. Hier dürfen gemäß § 24 Absatz 4 des Agrarstatistikgesetzes statistische Ergebnisse Gebietseinheiten zugeordnet werden, die bezogen auf eine vorgegebene Kartenprojektion rechtwinklig, in der Regel quadratisch und mindestens 100 Hektar groß sind. Diese Spezialregelung bleibt von einer Änderung des § 10 Absatz 2 BStatG unberührt.

Für bundes- und landesweite statistische Auswertungen und Darstellungen sind intrakommunale Raumgliederungen, die auf den Bausteinen Blockseiten basieren, aus inhaltlich-fachlichen (keine flächendeckende Definition, hohe räumliche Heterogenität, zeitliche Variabilität) und aus technischen Gründen (extrem aufwändige Pflege einer Vektorgeometrie mit über einer Million Einheiten bundesweit) ungeeignet.

Die bisher kleinteiligste standardisierte Raumeinheit in der amtlichen Statistik des Bundes und der Länder ist die Ebene der Gemeinden. Durch eine Vielzahl von Gebietsreformen ändern sich deren räumliche Bezugsgrößen: Allein von 1990 bis 2012 sank die Zahl der Gemeinden in Deutschland von über 16 000 auf unter 12 000 (-25 %). Die Zahl der Gemeinden in Ostdeutschland hat sich in den letzten zwanzig Jahren mehr als halbiert. Die amtliche Statistik stellt daher unterhalb der Länderebene häufig keine Zeitreihen zur Verfügung. Die Zusammenlegungen größer werdender Gebietseinheiten führen zu einem zunehmenden Verlust an räumlicher Analyseschärfe und Vergleichbarkeit. Ein Datenangebot ohne einen Raumbezug unterhalb der Gemeindeebene, der auch von der amtlichen Statistik des Bundes und der Länder genutzt werden kann, erfüllt nicht mehr die heutigen Anforderungen an Analyse- und Darstellungsoptionen. Darüber hinaus verliert Deutschland hierdurch zunehmend den Anschluss an internationale Entwicklungen. Seit 2009

fördert Eurostat die Anstrengungen des European Forum for Geostatistics (EFGS) zur Etablierung einer europaweiten kleinräumigen Gliederung unterhalb der Gemeindeebene. Das EFGS favorisiert dabei das Konzept geografischer Gitter und daraus abgeleiteter Rasterkarten. Auch die europäische Kommission hat sich für die Zensusrunde 2011 und für die Schaffung einer Geodateninfrastruktur in der europäischen Gemeinschaft (INSPIRE) ebenfalls eindeutig dafür ausgesprochen, das Konzept eines geografischen Gitters zu nutzen. Die geografische Gitterzelle beschreibt eine quadratische Gebietseinheit in einem festgelegten geografischen Koordinatensystem. Für die Speicherung der Daten ist im BStatG eine Auflösung von mindestens 100 Meter x 100 Meter vorgesehen. Ausgehend von der 100 Meter x 100 Meter Gitterzelle, können die Daten unter Wahrung des statistischen Geheimnisses zielgenauer zu neuen Analyseeinheiten zusammengefasst und ausgewertet werden.

Der wesentliche Mehrwert des Konzepts liegt darin, Daten der amtlichen Statistik aus Vollerhebungen und Registern für vielfache bundesweite und regionale Verwaltungsaufgaben, beispielsweise für den Bevölkerungs- und Katastrophenschutz und die Gesundheitsvorsorge oder Umwelt- und Infrastrukturplanung, in ihrer räumlichen Auflösung erheblich flexibler bereitstellen zu können, als dies bei Beschränkung auf administrative Raumgliederungen möglich ist.

Die Umsetzung des Gitterkonzeptes erfordert eine Rechtslage, die es der amtlichen Statistik ermöglicht, den Raumbezug der Einzeldatensätze unmittelbar mit der Referenz auf ein geeignetes geografisches Gitter dauerhaft speichern zu dürfen. Dies bedeutet konkret, den Raumbezug der Einzeldatensätze vor der Löschung des Hilfsmerkmals „Anschrift“ durch die Referenz auf eine zugehörige Gitterzelle des Gitters zu vergröbern. Hierzu ist die Georeferenzierung der Adressen ein unverzichtbarer Zwischenschritt. Nach der Zuordnung der Adressen zu den Gitterzellen können sowohl die Adressen als auch die adressgenauen Geokoordinaten gelöscht werden. Das Maß der Vergröberung ist von der (einheitlichen) Gitterzellenweite des Gitters abhängig. Zu beachten ist, dass dieses Maß sich lediglich auf die Speicherung sowie die interne Verarbeitung der Daten in den statistischen Ämtern bezieht. Bei der Verbreitung von Ergebnissen ist selbstverständlich weiterhin die statistische Geheimhaltung maßgeblich, so dass hierbei im Regelfall größere Gebietseinheiten, z. B. abgeleitete Gitter mit größerer Gitterweite, zu bilden sein werden.

b) Absatz 3 (Buchstabe b)

Die Änderung der Regelung in § 10 Absatz 2 BStatG erlaubt es den statistischen Ämtern, die Angaben aus Bundesstatistiken mit Bezug auf quadratische Gitterzellen zu speichern. Nach der Regelung in § 10 Absatz 3 BStatG müssen diese Gitterzellen mindestens eine Fläche von einem Hektar (1 ha), also 100 Meter x 100 Meter, umfassen. Damit erfolgt bereits bei der Speicherung der Daten in den abgeschotteten Bereichen der statistischen Ämter eine Vergröberung des Raumbezugs der Einzeldatensätze von der Gebäudeadresse auf größere Raumeinheiten, um datenschutzrechtliche Belange zu berücksichtigen.

Die festgelegte Gitterweite des geografischen Gitters bezieht sich ausdrücklich auf die Speicherung des Raumbezugs der Daten und die interne Verarbeitung bzw. Auswertung der Daten bei den statistischen Ämtern.

Bei Veröffentlichungen ist, unabhängig von der gewählten Gitterweite, die statistische Geheimhaltung zu wahren. Für Zwecke der Veröffentlichung von statistischen Ergebnissen dürfen Gitterzellen als Grundlage genutzt werden; man spricht bei der Ausweisung von Ergebnissen mittels eines geografischen Gitters von Rasterkarten. Hierbei findet die statistische Geheimhaltung nach § 16 Absatz 1 BStatG strikte Anwendung, so dass die Größen der Gitterzellen, die für Veröffentlichungen Anwendung finden, meist größer als die gespeicherten Gitterzellen von 1 ha sein werden. Alternativ können, wie beispielsweise bei der Veröffentlichung von statistischen Ergebnissen in Tabellen üblich, Werte ge-

sperrt werden (keine Wertzuordnung zu einem Raster) oder auch andere Verfahren zur Wahrung der statistischen Geheimhaltung eingesetzt werden.

6. Elektronische Datenübermittlung - § 11a BStatG (Nummer 5)

Der Einsatz elektronischer Verfahren zur Übermittlung von Daten für statistische Zwecke führt zu einer deutlichen Kosten- und Zeitersparnis sowohl für die Auskunft Gebenden als auch für die statistischen Ämter. Daher sollen Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen, aber auch Unternehmen und Betriebe künftig verpflichtet werden, elektronische Verfahren zur Datenübermittlung zu nutzen.

Im Bereich der öffentlichen Verwaltung nutzen bereits einige Behörden die Möglichkeit des standardisierten elektronischen Datenaustausches (XÖV-Verfahren). Solche Standards sind beispielsweise im Meldewesen (XMeld), im Personenstandswesen (XPersonenstand) und im Ausländerwesen (XAusländer) im Einsatz. Die Regelung in Absatz 1 stellt klar, dass solche standardisierten Verfahren, die von den Daten übermittelnden Behörden genutzt werden, auch für die Übermittlung von Daten an die statistischen Ämter zu nutzen sind. Soweit Behörden keine standardisierten Verfahren für den Datenaustausch verwenden, sind elektronische Übermittlungsverfahren nach Absprache mit den zuständigen statistischen Ämtern zu nutzen.

Für Unternehmen und Betriebe gilt, dass künftig – z. B. mit Hilfe des Verfahrens „IDEV“ (Internet Datenerhebung im Verbund) – Online-Formulare auszufüllen und elektronisch zu übermitteln sind, wenn die Angaben bislang in Papiervordrucke eingetragen und per Post an die zuständigen Stellen übersandt wurden. Die statistischen Stellen bieten zudem mit dem „CORE.reporter“ ein Softwaremodul an, das dem Anwender die Übernahme von Angaben aus seinen eigenen Dateien erleichtert. Verschiedene Unternehmen und Betriebe haben in der bei ihnen betriebenen IT bereits ein spezielles Statistikmodul integriert, so dass sie über die Anwendung „eSTATISTIK.core“ die erfragten Daten direkt automatisiert aus den elektronischen Datenbeständen abrufen und aus ihrem IT-System heraus an die statistischen Stellen übermitteln können.

Die von den statistischen Stellen kostenfrei angebotenen elektronischen Übermittlungsverfahren geben sowohl den Übermittlungsweg als auch die für die amtliche Statistik geltenden Standards, insbesondere die Datenformate, vor und haben sich in der Praxis bewährt.

Soweit bei den befragten Unternehmen und Betrieben die technischen Voraussetzungen zur elektronischen Datenübermittlung nicht bzw. noch nicht vorliegen, kann das zuständige statistische Amt im Einzelfall die Datenübermittlung in einer anderen Form zulassen.

7. Änderung des § 13 Absatz 2 BStatG (Nummer 6)

Durch diese Regelung wird klargestellt, dass die dauerhafte Speicherung der Geokoordinate in von der Statistik genutzten Adressdateien, heute in der Regel als Register bezeichnet, zulässig ist. Die dauerhafte Speicherung der Anschrift ist bereits nach geltender nationaler Rechtslage zulässig und nach verbindlichen europarechtlichen Vorgaben sogar zwingend (Verordnung (EG) Nummer 177/2008 des Europäischen Parlaments und des Rates vom 20. Februar 2008 zur Schaffung eines gemeinsamen Rahmens für Unternehmensregister für statistische Zwecke und zur Aufhebung der Verordnung (EWG) Nummer 2186/93 des Rates, ABl. L 61 vom 5. März 2008, S. 6).

8. Änderung der §§ 18, 19 BStatG (Nummer 7)

Hierbei handelt es sich um eine redaktionelle Änderung.

9. Änderung des § 23 Absatz 2 BStatG (Nummer 8)

Es handelt sich um eine Folgeänderung, die aus der Einfügung von § 11a (vgl. Nummer 5) resultiert.

Artikel 14

Änderung des Rechtsdienstleistungsgesetzes

In § 13 Absatz 3 Satz 1 des Rechtsdienstleistungsgesetzes vom 12. Dezember 2007 (BGBl. I S. 2840), das zuletzt durch Artikel 16 des Gesetzes vom 6. Dezember 2011 (BGBl. I S. 2515) geändert worden ist, wird das Wort „schriftlich“ durch die Wörter „in Textform“ ersetzt.

Erläuterungen

Mit der Änderung kann die bislang ausschließlich schriftliche Mitteilung von Änderungen künftig auch elektronisch per einfacher E-Mail erfolgen. Dies ist von dem Begriff der Textform (§ 126b BGB) umfasst, der auch dem sonstigen Sprachgebrauch des Rechtsdienstleistungsgesetzes entspricht.

Artikel 15

Änderung der Rechtsdienstleistungsverordnung

In § 6 Absatz 1 Satz 1 der Rechtsdienstleistungsverordnung vom 19. Juni 2008 (BGBl. I S. 1069) werden nach dem Wort „schriftlich“ die Wörter „oder elektronisch“ eingefügt.

Erläuterungen

Die Änderung bewirkt, dass Anträge auf Registrierung nach § 13 Absatz 1 des Rechtsdienstleistungsgesetzes auch elektronisch (also z. B. per E-Mail) gestellt werden können. Dies ist eine Verfahrenserleichterung für den Antragsteller, die auch dem Anliegen der EU-Dienstleistungsrichtlinie entspricht. Die Änderung beruht auf einem Vorschlag seitens der Länder.

Artikel 16

Änderung des Satellitendatensicherheitsgesetzes

§ 25 des Satellitendatensicherheitsgesetzes vom 23. November 2007 (BGBl. I S. 2590) wird wie folgt geändert:

1. Absatz 1 wird wie folgt geändert:

a) In Satz 1 werden die Wörter „, § 19 Abs. 1 Satz 1 und 2 sowie nach § 20 Satz 1“ gestrichen.

b) Nach Satz 2 wird folgender Satz eingefügt:

„Eine Erlaubnis nach § 19 Absatz 1 Satz 1 und 2 sowie nach § 20 Satz 1 setzt einen schriftlichen oder elektronischen Antrag voraus.“

2. In Absatz 3 werden nach dem Wort „schriftlich“ die Wörter „oder elektronisch“ eingefügt und werden die Wörter „und zuzustellen“ gestrichen.

Erläuterungen

Die Regelung sieht vor, dass die Anträge auf eine Erteilung einer Erlaubnis zum Verbreiten von Daten eines hochwertigen Erdfernerkundungssystems nach den §§ 19 und 20 des Satellitendatensicherheitsgesetzes (SatDSiG) auch elektronisch (also z. B. per E-Mail) erfolgen können.

Darüber hinaus ist erforderlich, das Zustellungserfordernis für Verwaltungsakte des § 25 Absatz 3 SatDSiG aufzuheben, das aufgrund der fast durchgängig gegebenen hohen Eilbedürftigkeit zu hohen Kosten beim Datenanbieter, aber auch zu einem wenig effizienten Verwaltungshandeln im Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) geführt hat. Dabei ist insbesondere zu beachten, dass die ganz überwiegende Zahl der Erlaubnisanträge nach den §§ 19 und 20 vom BAFA in weniger als einer Stunde bearbeitet werden können. Zudem hat die bisherige Verwaltungspraxis gezeigt, dass das mit erheblichen Handhabungsschwierigkeiten verbundene Zustellungserfordernis nicht mit einem erhöhten Sicherheitserfordernis begründet werden kann, zumal die Verwaltungsakte (Erlaubniserteilung nach den §§ 19 und 20 SatDSiG) inhaltlich unkritisch sind. Grundsätzlich enthalten sie keine geheimhaltungsbedürftigen Tatsachen. Dem Bestimmtheitserfordernis des Verwaltungsaktes wird ohne Preisgabe sicherheitsrelevanter Tatsachen Rechnung getragen, indem im Wesentlichen auf Daten der Antragstellung Bezug genommen wird.

Artikel 17

Änderung des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern

Das Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern in der im Bundesgesetzblatt Teil III, Gliederungsnummer 701-1, veröffent-

lichten bereinigten Fassung, das zuletzt durch Artikel 2 Absatz 61 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044) geändert worden ist, wird wie folgt geändert:

1. § 3 Absatz 3 Satz 3 wird wie folgt gefasst:

„Natürliche Personen und Personengesellschaften, die nicht in das Handelsregister eingetragen sind, und eingetragene Vereine, wenn nach Art oder Umfang ein in kaufmännischer Weise eingerichteter Geschäftsbetrieb nicht erforderlich ist, sind vom Beitrag freigestellt, soweit ihr Gewerbeertrag nach dem Gewerbesteuergesetz oder, soweit für das Bemessungsjahr ein Gewerbesteuermessbetrag nicht festgesetzt wird, ihr nach dem Einkommensteuergesetz ermittelter Gewinn aus Gewerbebetrieb 5 200 Euro nicht übersteigt."

2. In § 10 Absatz 4 wird die Angabe „§ 3 Abs. 2" durch die Angabe „§ 3 Absatz 1, 2" ersetzt.

3. § 12 Absatz 1 wird wie folgt geändert:

a) In Nummer 8 wird das Komma am Ende durch einen Punkt ersetzt.

b) Nummer 9 wird aufgehoben.

Erläuterungen

1. Änderung des § 3 Absatz 3 IHKG (Nummer 1)

§ 3 Absatz 3 Satz 3 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHKG) bezweckt die Freistellung von Kleinstgewerben von der Beitragspflicht. Eingetragene Vereine mit geringfügiger wirtschaftlicher Betätigung sind nicht von dem Wortlaut der Vorschrift erfasst. Eine Ungleichbehandlung der eingetragenen Vereine ohne Kaufmannseigenschaft ist aber nicht gerechtfertigt. In seiner ab dem 1. Januar 2004 geltenden Fassung stellte § 3 Absatz 3 Satz 3 IHKG noch auf das Tatbestandsmerkmal „Kammerzugehörige, die nicht im Handelsregister oder im Genossenschaftsregister eingetragen sind" ab (seinerzeitige Neufassung der Vorschrift durch Gesetz vom 24. Dezember 2003, BGBl. I S. 2934). Die Vorschrift wurde dann durch Gesetz vom 7. September 2007 (BGBl. I S. 2246) mit der vom Gesetzgeber ausdrücklich benannten Zielrichtung geändert, lediglich ausländische Kapitalgesellschaften aus der Privilegierung herauszunehmen (BT-Drs. 16/4391, S. 31). Die Privilegierung der eingetragenen Vereine mit geringfügiger wirtschaftlicher Betätigung wollte der Gesetzgeber somit durch die letzte Änderung der Vorschrift nicht beenden. Damit dient die nunmehr angestrebte Neufassung der Vorschrift durch dieses Gesetz nur der Klarstellung der ohnehin geltenden Rechtslage.

Die eingetragenen Vereine profitieren als Kammermitglieder von der Nutzung moderner IT durch die Industrie- und Handelskammern, die durch das EGovG gefördert wird. Nach Artikel 1 § 1 Absatz 2 Satz 1 gilt das EGovG auch für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden der Länder einschließlich der ihrer Aufsicht unterstehenden juristischen Personen des öffentlichen Rechts, wenn sie Bundesrecht ausführen. Es gilt damit auch für die Industrie- und Handelskammern (siehe § 11 Absatz 1 Satz 1 IHK-Gesetz zur Länderaufsicht).

2. Änderung des § 10 Absatz 4 IHKG (Nummer 2)

Im IHKG ist die Rechtsform des öffentlich-rechtlichen Zusammenschlusses bislang nicht ausdrücklich festgelegt. Durch die entsprechende Anwendung von § 3 Absatz 1 IHKG wird bestimmt, dass der öffentlich-rechtliche Zusammenschluss in der Rechtsform einer Körperschaft des öffentlichen Rechts zu errichten ist. Diese Rechtsform ist erforderlich, damit die Industrie- und Handelskammern ihnen obliegende hoheitliche Aufgaben auf den Zusammenschluss übertragen können. Der Zusammenschluss als Teil der mittelbaren Staatsverwaltung kann moderne IT nutzen, deren Verwendung durch das EGovG gefördert wird.

3. Änderung des § 12 Absatz 1 IHKG (Nummer 3)

Der in § 12 Absatz 1 Nummer 9 IHKG in Bezug genommene Berufsbildungsausschuss ist nicht mehr im IHKG, sondern in den §§ 77 bis 80 des Berufsbildungsgesetzes (BBiG) geregelt. § 8 Absatz 2, auf den in § 12 Absatz 1 Nummer 9 verwiesen wird, ist aufgehoben. In den §§ 77 bis 80 BBiG werden Zuständigkeit und Verfahren für die Bestellung von Ausschussmitgliedern geregelt. Damit bedarf es einer Regelungskompetenz für den Landesgesetzgeber nicht mehr.

Artikel 18

Änderung der Gewerbeordnung

In § 35 Absatz 6 Satz 1 der Gewerbeordnung in der Fassung der Bekanntmachung vom 22. Februar 1999 (BGBl. I S. 202), die zuletzt durch Artikel 3 des Gesetzes vom 24. April 2013 (BGBl. I S. 930) geändert worden ist, werden nach dem Wort „schriftlichen“ die Wörter „oder elektronischen“ eingefügt.

Erläuterungen

Die Regelung sieht vor, dass ein Gewerbetreibender den Antrag auf Wiedergestattung der Ausübung des Gewerbes auch elektronisch (also z. B. per E-Mail) stellen kann, wenn Tatsachen die Annahme rechtfertigen, dass eine Unzuverlässigkeit nicht mehr vorliegt. Die Änderung beruht auf einem Vorschlag seitens der Länder.

Artikel 19

Änderung der Handwerksordnung

§ 30 Absatz 1 Satz 2 der Handwerksordnung in der Fassung der Bekanntmachung vom 24. September 1998 (BGBl. I S. 3074; 2006 I S. 2095), die zuletzt durch Artikel 2 des Gesetzes vom 5. Dezember 2012 (BGBl. I S. 2415) geändert worden ist, wird durch die folgenden Sätze ersetzt:

„Der Antrag kann schriftlich oder elektronisch gestellt werden; eine Kopie der Vertragsniederschrift ist jeweils beizufügen. Auf einen betrieblichen Ausbildungsplan

im Sinne des § 11 Absatz 1 Satz 2 Nummer 1 des Berufsbildungsgesetzes, der der zuständigen Stelle bereits vorliegt, kann dabei Bezug genommen werden.“

Erläuterungen

Nach der bisher geltenden Fassung ist jedem Antrag auf Eintragung eines Ausbildungsvertrages in die Lehrlingsrolle, die gemäß § 28 Absatz 1 der Handwerksordnung (HwO) von der Handwerkskammer geführt wird, eine Ausfertigung der nach § 11 Absatz 1 BBiG erforderlichen Vertragsniederschrift beizufügen; dies erfordert bisher eine zusätzliche Vertragsausfertigung und das Versenden der vollständigen Antragsunterlagen an die zuständigen Stellen im Sinne der §§ 71 bis 75 BBiG durch Briefpost. Die Änderung eröffnet nun auch die zeit- und kostensparende Form der elektronischen Übermittlung.

Rechtsklarheit und -sicherheit zwischen den Vertragsparteien werden dabei nicht in Frage gestellt; das Gebot der schriftlichen Niederlegung des wesentlichen Vertragsinhalts gemäß § 11 Absatz 1 BBiG bleibt unter Ausschluss der elektronischen Form erhalten. Der rechtsgültig unterschriebene Vertrag kann künftig dem Eintragungsantrag in elektronischer Kopie beigefügt werden.

Insbesondere durch den künftigen Verzicht auf die postalische Übersendung des zum Ausbildungsvertrag gehörenden und zumeist umfangreichen betrieblichen Ausbildungsplanes im Sinne von § 11 Absatz 1 Satz 2 Nummer 1 BBiG kann ein signifikanter Aufwand eingespart werden. Zudem stellt die Vorschrift nunmehr klar, dass eine jeweils erneute Übermittlung in denjenigen Fällen entfallen kann, in denen der Ausbildungsplan unverändert auf eine größere Zahl von Ausbildungsverhältnissen angewendet wird. Bei jedem weiteren Antrag im Sinne von § 30 Absatz 1 HwO reicht nun ein Bezug auf einen konkreten Ausbildungsplan aus, der der zuständigen Stelle bereits vorliegt und nun inhaltsgleich zu Grunde gelegt wird.

Die Änderungen erlauben eine wesentliche Verfahrensvereinfachung. Bei einer Zahl von ca. 600 000 jährlich neu abgeschlossenen Ausbildungsverträgen wird dies zu einer merkbaren Entlastung bei den Ausbildungsbetrieben führen, aber auch bei den jeweils für die Ausbildungsüberwachung zuständigen Stellen, in der Regel den Handwerkskammern sowie den Industrie- und Handelskammern.

Artikel 20

Änderung der Ersten Verordnung zum Sprengstoffgesetz

In § 23 Absatz 3 Satz 1 und Absatz 7 Satz 1 sowie § 25a Absatz 1 der Ersten Verordnung zum Sprengstoffgesetz in der Fassung der Bekanntmachung vom 31. Januar 1991 (BGBl. I S. 169), die zuletzt durch Artikel 1 der Verordnung vom 11. Oktober 2012 (BGBl. I S. 2171) geändert worden ist, werden jeweils nach dem Wort „schriftlich“ die Wörter „oder elektronisch“ eingefügt.

Erläuterungen

Die Änderung des § 23 Absatz 3 Satz 1 bewirkt, dass der Erlaubnis- oder Befähigungsscheininhaber das beabsichtigte Feuerwerk auch elektronisch (also z. B. per E-Mail) anzeigen kann. Die Änderung beruht auf einem Vorschlag seitens der Länder.

Die Änderung des § 23 Absatz 7 Satz 1 bewirkt, dass die erforderliche Anzeige der beabsichtigten Vorführung pyrotechnischer Effekte in Anwesenheit von Besuchern auch elektronisch (also z. B. per E-Mail) erfolgen kann. Die Änderung beruht auf einem Vorschlag seitens der Länder.

Die Änderung des § 25a Absatz 1 bewirkt, dass die Genehmigung zum Verbringen von Explosivstoffen nach § 15 Absatz 6 Satz 1 des Sprengstoffgesetzes vom Empfänger der Explosivstoffe oder seinem Bevollmächtigten auch elektronisch (also z. B. per E-Mail) bei der nach § 15 Absatz 7 des Sprengstoffgesetzes zuständigen Stelle beantragt werden kann. Die Änderung beruht auf einem Vorschlag seitens der Länder.

Artikel 21

Änderung der Dritten Verordnung zum Sprengstoffgesetz

In § 1 Absatz 1 Satz 1 in dem Satzteil vor Nummer 1 und in § 2 Satz 1 der Dritten Verordnung zum Sprengstoffgesetz vom 23. Juni 1978 (BGBl. I S. 783) werden jeweils nach dem Wort „Ausfertigung“ die Wörter „oder elektronisch“ eingefügt.

Erläuterungen

Die vorgesehene Änderung setzt die Anregung in Nummer 24 der Stellungnahme des Bundesrates (BR Drucksache 557/12(B)) um und ermöglicht künftig jeweils neben der schriftlichen auch die elektronische Anzeige.

Artikel 22

Änderung des Berufsbildungsgesetzes

§ 36 Absatz 1 Satz 2 des Berufsbildungsgesetzes vom 23. März 2005 (BGBl. I S. 931), das zuletzt durch Artikel 24 des Gesetzes vom 20. Dezember 2011 (BGBl. I S. 2854) geändert worden ist, wird durch die folgenden Sätze ersetzt:

„Der Antrag kann schriftlich oder elektronisch gestellt werden; eine Kopie der Vertragsniederschrift ist jeweils beizufügen. Auf einen betrieblichen Ausbildungsplan im Sinne von § 11 Absatz 1 Satz 2 Nummer 1, der der zuständigen Stelle bereits vorliegt, kann dabei Bezug genommen werden.“

Erläuterungen

Nach der bisher geltenden Fassung ist jedem Antrag auf Eintragung eines Ausbildungsvertrages in das Verzeichnis, das gemäß § 34 Absatz 1 BBiG von den zuständigen Stellen geführt wird, eine Ausfertigung der nach § 11 Absatz 1 erforderlichen Vertragsniederschrift beizufügen; dies erfordert bisher eine zusätzliche Vertragsausfertigung und das Versenden der vollständigen Antragsunterlagen an die zuständigen Stellen im Sinne der §§ 71 bis 75 durch Briefpost. Die Änderung eröffnet nun auch die heute weithin verfügbare, zeit- und kostensparende Form der elektronischen Übermittlung.

Rechtsklarheit und -sicherheit zwischen den Vertragsparteien werden dabei nicht in Frage gestellt; das Gebot der schriftlichen Niederlegung des wesentlichen Vertragsinhalts gemäß § 11 Absatz 1 bleibt unter Ausschluss der elektronischen Form erhalten. Der rechtsgültig unterschriebene Vertrag kann künftig dem Eintragungsantrag in elektronischer Kopie beigefügt werden.

Insbesondere durch den künftigen Verzicht auf die postalische Übersendung des zum Ausbildungsvertrag gehörenden und zumeist umfangreichen betrieblichen Ausbildungsplanes im Sinne von § 11 Absatz 1 Satz 2 Nummer 1 kann ein signifikanter Aufwand eingespart werden. Zudem stellt die Vorschrift nunmehr klar, dass eine jeweils erneute Übermittlung in denjenigen Fällen entfallen kann, in denen der Ausbildungsplan unverändert auf eine größere Zahl von Ausbildungsverhältnissen angewendet wird. Bei jedem weiteren Antrag im Sinne von § 36 Absatz 1 reicht nun ein Bezug auf einen konkreten Ausbildungsplan aus, der der zuständigen Stelle bereits vorliegt und nun inhaltsgleich zu Grunde gelegt wird.

Die Änderungen erlauben eine wesentliche Verfahrensvereinfachung. Bei einer Zahl von ca. 600 000 jährlich neu abgeschlossenen Ausbildungsverträgen wird dies zu einer merkbaren Entlastung bei den Ausbildungsbetrieben führen, aber auch bei den jeweils für die Ausbildungsüberwachung zuständigen Stellen, in der Regel den Industrie- und Handelskammern sowie den Handwerkskammern.

Artikel 23

Änderung des Berufsqualifikationsfeststellungsgesetzes

Das Berufsqualifikationsfeststellungsgesetz vom 6. Dezember 2011 (BGBl. I S. 2515) wird wie folgt geändert:

1. In § 6 Absatz 1 Satz 2 wird das Wort „schriftlich“ gestrichen.

2. Dem § 17 Absatz 2 Nummer 1 werden die Wörter „Wohnort des Antragstellers,“ angefügt.

Erläuterungen

1. Änderung des § 6 BQFG (Nummer 1)

Das Wort „schriftlich“ wurde gestrichen, um auch Anträge in anderer Form, insbesondere solche per E-Mail, zu ermöglichen. Es ist davon auszugehen, dass vor allem Antragsteller aus dem Ausland häufig auf diese Art der Antragstellung zurückgreifen werden. Sie ermöglicht einen schnellen und unbürokratischen Erstkontakt. Das Erfordernis, die Unterlagen nach § 5 Absatz 2 in der dort geforderten Form einzureichen, bleibt unberührt. Wenn

und soweit von der zuständigen Stelle nach § 5 Absatz 3 die einfache Kopie zugelassen wird, kann das Verfahren schnell und unbürokratisch betrieben werden.

2. Änderung des § 17 Absatz 2 BQFG (Nummer 2)

Für die Evaluation ist es wichtig, auch den Wohnort des Antragstellers zu erfassen, um die Statistik hinsichtlich der regionalen Antragssituation sowie der Anzahl der Anträge aus dem Ausland auswerten zu können. Daher wurde das Erhebungsmerkmal „Wohnort des Antragstellers“ aufgenommen.

Artikel 24

Änderung des Straßenverkehrsgesetzes

Das Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), das zuletzt durch Artikel 2 Absatz 118 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044) geändert worden ist, wird wie folgt geändert:

1. Dem § 30 Absatz 8 werden die folgenden Sätze angefügt:

„Die Auskunft kann elektronisch erteilt werden, wenn der Antrag unter Nutzung des elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes gestellt wird. Hinsichtlich der Protokollierung gilt § 30a Absatz 3 entsprechend.“

2. Dem § 58 werden die folgenden Sätze angefügt:

„Die Auskunft kann elektronisch erteilt werden, wenn der Antrag unter Nutzung des elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes gestellt wird. Hinsichtlich der Protokollierung gilt § 53 Absatz 3 entsprechend.“

3. § 64 wird wie folgt geändert:

a) Der Wortlaut wird Absatz 1.

b) Folgender Absatz 2 wird angefügt:

„(2) Unbeschadet anderer landesrechtlicher Regelungen können durch Landesrecht Aufgaben der Zulassung von Kraftfahrzeugen auf die für das Meldewesen zuständigen Behörden übertragen werden, sofern kein neues Kennzeichen erteilt werden muss oder sich die technischen Daten des Fahrzeugs nicht ändern.“

Erläuterungen

1. Elektronisches Auskunftsverfahren - § 30 Absatz 8 StVG (Nummer 1)

Die Aufnahme von Satz 3 und 4 in § 30 Absatz 8 StVG leistet einen Beitrag zur Reform der Vorschriften des Verkehrszentralregisters und gleichzeitig zur Erweiterung des E-

Government-Angebots der Bundesregierung. Durch die Schaffung eines elektronischen Auskunftsverfahrens soll das System für den Betroffenen transparenter gemacht werden. Der Antrag auf Auskunft aus dem Verkehrszentralregister kann bereits seit dem 02. Mai 2011 beim Kraftfahrt-Bundesamt mittels eines elektronischen Identitätsnachweises nach § 18 PAuswG gestellt werden.

Die Transparenz des Systems soll nun dadurch weiter erhöht werden, dass auch die Auskunftserteilung elektronisch erfolgen kann. Die Neuregelung bestimmt die dafür einzuhaltenden Bedingungen. § 30 Absatz 8 StVG regelt bisher, unter welchen Bedingungen die schriftliche Auskunft an den Betroffenen erfolgt. Sie bestehen darin, dass der Antrag schriftlich gestellt wird und der Antragsteller einen Identitätsnachweis dem Antrag beigefügt hat. In diesem Fall erhält er vom Kraftfahrt-Bundesamt schriftlich Auskunft. Dieselben Bedingungen werden nun für die Alternative der elektronischen Auskunft aufgestellt. Dabei wird die schriftliche Antragstellung durch die elektronische Antragstellung mittels der eID-Funktion des nPA ersetzt, wie dies die Erste Verordnung über Ausnahmen von den Vorschriften der Fahrerlaubnis-Verordnung vorsieht.

Dies deckt auch die im schriftlichen Verfahren vorgesehene Identifizierung des Betroffenen ab, die hier durch Beifügung des Identitätsnachweises und im elektronischen Verfahren durch das Auslesen der Daten aus dem elektronischen Speicher- und Verarbeitungsmedium des nPA erfolgt. Damit sind die Anforderungen an die Identifizierung der anfragenden Person wie im schriftlichen Verfahren erfüllt. Außerdem erfolgt die bei Online-Anfragen übliche Protokollierung (§ 30a Absatz 3 StVG).

Zusätzlicher Anforderungen auch an die Auskunftserteilung bedarf es nicht. Diese hätten lediglich den Zweck, die Auskunft erteilende Behörde gegenüber den Betroffenen zu identifizieren und sicherzustellen, dass die übermittelte Auskunft nicht verfälscht werden kann. Im Vergleich zur weiterhin möglichen schriftlichen Auskunftserteilung (Schreiben ohne Unterschrift) erhöht die elektronische Auskunftserteilung das Risiko von Verfälschungen nicht. Um einen Verwaltungsakt handelt es sich bei der Auskunftserteilung ebenfalls nicht, so dass die aufgestellten Anforderungen ausreichen.

2. Änderung des § 58 StVG (Nummer 2)

Die Änderung ermöglicht die elektronische Auskunft aus dem Zentralen Fahrerlaubnisregister. Diese wird bisher nur einer Privatperson auf Antrag schriftlich über den sie betreffenden Inhalt des örtlichen oder des Zentralen Fahrerlaubnisregisters unter Vorlage eines Identitätsnachweises erteilt.

3. Änderung des § 64 StVG (Nummer 3)

Mit der vorgeschlagenen Änderung soll erreicht werden, dass die Bürgerinnen und Bürger bei einer Adressänderung nur eine Behörde, hier die Meldebehörde, aufsuchen müssen. Die Möglichkeit einer entsprechenden Verwaltungsorganisation steht den Ländern bereits nach Artikel 84 Absatz 1 Satz 1 GG zu. Die Meldebehörde muss der Zulassungsbehörde dann die erforderlichen Daten weiterleiten. Dies dient dem Bürokratieabbau.

Verwaltungsorganisation ist grundsätzlich Ländersache. Mit der Regelung „Unbeschadet anderweitiger landesrechtlicher Regelungen" wird vermieden, dass eine „Sperrwirkung" für andere organisationsrechtliche Entscheidungen entsteht oder dies jedenfalls so wahrgenommen wird.

Artikel 25

Änderung der Fahrzeug-Zulassungsverordnung

Nach § 13 Absatz 1 der Fahrzeug-Zulassungsverordnung vom 3. Februar 2011 (BGBl. I S. 139), die zuletzt durch Artikel 2a der Verordnung vom 22. Mai 2013 (BGBl. I S. 1395) geändert worden ist, wird folgender Absatz 1a eingefügt:

„(1a) Der Mitteilungspflicht nach Absatz 1 Satz 1 Nummer 1 wird auch genügt, wenn diese Änderungen über eine Meldebehörde mitgeteilt werden, sofern bei der Meldebehörde ein solches Verfahren eröffnet ist.“

Erläuterungen

Es handelt sich um eine Klarstellung, dass die Mitteilung der Meldebehörde diejenige bei der Zulassungsbehörde ersetzt. Eine Verpflichtung aller Meldebehörden, dieses Verfahren durchzuführen, ergibt sich aus der Regelung jedoch nicht.

Artikel 26

Änderung des Bundeswasserstraßengesetzes

§ 28 Absatz 2 Satz 1 des Bundeswasserstraßengesetzes in der Fassung der Bekanntmachung vom 23. Mai 2007 (BGBl. I S. 962; 2008 I S. 1980), das zuletzt durch Artikel 11 des Gesetzes vom 31. Mai 2013 (BGBl. I S. 1388) geändert worden ist, wird wie folgt geändert:

1. **In Satz 1 werden nach dem Wort „schriftlich“ ein Komma und das Wort „elektronisch“ eingefügt.**

2. **Satz 3 wird aufgehoben.**

Erläuterungen

Da für eine strom- und schifffahrtspolizeiliche Genehmigung mangels spezialgesetzlicher Regelungen schon heute die Formvorschrift des § 37 VwVfG gilt, führt die Ergänzung um das Wort „elektronisch“ zu einer Vereinheitlichung.

Aufgrund des Beweiswerts in Bezug auf die Zustellung des Verwaltungsaktes ist jedoch damit zu rechnen, dass die elektronische Form nur in Ausnahmefällen Anwendung findet bzw. im Nachgang in schriftlicher Form bestätigt wird.

Ein Vorteil kann sich hier gegenüber dem mündlichen Verwaltungsakt aus der zusätzlichen (elektronischen) Verkörperung ergeben.

Mit der Streichung des Satzes 3 wird nicht bereichsspezifisch im Bundeswasserstraßengesetz (WaStrG) das Begründungserfordernis für schriftliche auf elektronische Verwal-

tungsakte ausgeweitet, sondern es greift die Grundregel des § 39 Absatz 1 VwVfG, wonach auch elektronische Verwaltungsakte zu begründen sind.

Die Streichung ist auch darin begründet, dass der seit dem Inkrafttreten des WaStrG 1968 unveränderte § 28 Absatz 2 WaStrG durch den Erlass des VwVfG 1976 nicht länger erforderlich ist, soweit es für ihn – als Regelung im Spezialgesetz – eine allgemeine Regelung im VwVfG gibt. Die Streichung dient somit auch der besseren Rechtssetzung.

Artikel 27

Änderung des Luftverkehrsgesetzes

Nach § 32c des Luftverkehrsgesetzes in der Fassung der Bekanntmachung vom 10. Mai 2007 (BGBl. I S. 698), das zuletzt durch Artikel 13 des Gesetzes vom 31. Mai 2013 (BGBl. I S. 1388) geändert worden ist, wird folgender § 32d eingefügt:

„§ 32d

Elektronische Veröffentlichungen

Unbeschadet der Regelungen von § 15 Absatz 1 des E-Government-Gesetzes kann eine durch Verordnung des Bundesministeriums für Verkehr, Bau und Stadtentwicklung bestimmte Pflicht zur Publikation in den Nachrichten für Luftfahrer oder im Luftfahrthandbuch der Bundesrepublik Deutschland zusätzlich oder ausschließlich durch eine elektronische Ausgabe erfüllt werden, wenn diese über öffentlich zugängliche Netze angeboten wird. In diesem Fall gilt § 15 Absatz 2 des E-Government-Gesetzes entsprechend.“

Erläuterungen

Die Regelung von Artikel 1 § 15 Absatz 1 erlaubt der Verwaltung ihrer Pflicht zur Publikation von bestimmten Umständen oder Unterlagen auch durch eine elektronische Veröffentlichung nachzukommen. Artikel 1 § 15 Absatz 1 bezieht sich jedoch nur auf amtliche Mitteilungs- oder Verkündungsblätter des Bundes, der Länder und Gemeinden. Nichtamtliche Verkündungsblätter sind von dieser Regelung ausgenommen. Im Bereich der Luftfahrt werden jedoch im großen Umfang Festlegungen, Bekanntmachungen, Hinweise, Umstände und Unterlagen auch in nichtamtlichen Verkündungsblättern bekannt gegeben. Es handelt sich hierbei um die Nachrichten für Luftfahrer und das Luftfahrthandbuch der Bundesrepublik Deutschland. Beide Veröffentlichungsblätter haben für die Luftfahrt eine große Bedeutung. Sie stellen die Nachrichten- und Informationsquelle für die Luftfahrt schlechthin dar. In zahlreichen Vorschriften auf Ebene der Rechtsverordnung des Bundesministeriums für Verkehr, Bau und Stadtentwicklung wird auf die Notwendigkeit der Veröffentlichung bestimmter Sachverhalte und Umstände in diesen beiden Veröffentlichungsblättern hingewiesen. Auch in der Luftfahrt ist ein Prozess zu beobachten, der dahin geht, dass die Papierform zunehmend verdrängt wird. Vor diesem Hintergrund erscheint es sachgerecht, mit Absatz 1 die in § 15 des Gesetzes zur Förderung der elektronischen Verwaltung enthaltenen Rechtsregelungen auch auf die Nachrichten für Luftfahrer und das Luftfahrthandbuch der Bundesrepublik Deutschland zu erstrecken.

Artikel 28

Änderung der Luftverkehrs-Zulassungs-Ordnung

In § 63d Nummer 4 der Luftverkehrs-Zulassungs-Ordnung in der Fassung der Bekanntmachung vom 10. Juli 2008 (BGBl. I S. 1229), die zuletzt durch Artikel 2 der Verordnung vom 15. Februar 2013 (BGBl. I S. 293) geändert worden ist, werden in dem Satzteil vor Satz 2 nach dem Wort „schriftlich“ die Wörter „oder elektronisch“ eingefügt.

Erläuterungen

Nach § 63d Nummer 4 Satz 1 der Luftverkehrs-Zulassungs-Ordnung (LuftVZO) haben die Luftfahrtunternehmen zur Durchführung der Verordnung (EG) Nummer 261/2004 ihren Passagieren sowie dem Luftfahrt-Bundesamt auf Verlangen die für die Abwicklung von Ansprüchen und zur Entgegennahme von Beschwerden verantwortliche Stelle im Unternehmen mit allen notwendigen Kontaktangaben schriftlich mitzuteilen.

Durch die Neuregelung erhalten die Luftfahrtunternehmen die Möglichkeit, die Mitteilung künftig auch in elektronischer Form, also per E-Mail, zu versenden, sofern die Passagiere über einen E-Mail-Zugang verfügen und dem Luftfahrtunternehmen die E-Mail-Adresse zur Verfügung gestellt haben.

Artikel 29

Änderung schifffahrtrechtlicher Vorschriften

Folgende Vorschriften werden aufgehoben:

1. **§ 4a der Ölhaftungsbescheinigungs-Verordnung vom 30. Mai 1996 (BGBl. I S. 707), die zuletzt durch Artikel 3 des Gesetzes vom 12. Juli 2006 (BGBl. I S. 1461; 2008 I S. 2070) geändert worden ist,**

2. **§ 1 Absatz 3 des Binnenschifffahrtsaufgabengesetzes in der Fassung der Bekanntmachung vom 5. Juli 2001 (BGBl. I S. 2026), das zuletzt durch Artikel 2 Absatz 125 des Gesetzes vom 22. November 2011 (BGBl. I S. 3044) geändert worden ist,**

3. **§ 18 des Seeaufgabengesetzes in der Fassung der Bekanntmachung vom 26. Juli 2002 (BGBl. I S. 2876), das zuletzt durch Artikel 2 des Gesetzes vom 4. Juni 2013 (BGBl. I S. 1471) geändert worden ist,**

4. **§ 33a der Schiffsmechaniker-Ausbildungsverordnung vom 12. April 1994 (BGBl. I S. 797), die zuletzt durch Artikel 520 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407) geändert worden ist,**

5. **§ 19 der Schiffsoffizier-Ausbildungsverordnung in der Fassung der Bekanntmachung vom 15. Januar 1992 (BGBl. I S. 22, 227), die zuletzt durch Artikel 1 der Verordnung vom 2. Mai 2011 (BGBl. I S. 746) geändert worden ist,**

6. § 22c des Flaggenrechtsgesetzes in der Fassung der Bekanntmachung vom 26. Oktober 1994 (BGBl. I S. 3140), das zuletzt durch Artikel 1 des Gesetzes vom 20. Dezember 2012 (BGBl. I S. 2792) geändert worden ist, und

7. § 1a des Seelotsgesetzes in der Fassung der Bekanntmachung vom 13. September 1984 (BGBl. I S. 1213), das zuletzt durch Artikel 105 des Gesetzes vom 8. Dezember 2010 (BGBl. I S. 1864) geändert worden ist.

Erläuterungen

In den aufgelisteten Vorschriften wird die elektronische Form pauschal ausgeschlossen. Die Änderung bewirkt, dass Anträge und Anzeigen, für die die Schriftform vorgeschrieben ist, zukünftig auch in einer elektronisch sicheren, die Schriftform ersetzenden Form erfolgen können. Formulare können dann elektronisch ausgefüllt werden, wenn die zuständige Behörde sie in elektronischer Form im Internet zur Verfügung stellt. Zeugnisse, Bescheinigungen und andere Dokumente sollten entweder aufgrund internationalen oder europäischen Rechts oder wegen ihrer Eigenart als Originalurkunde in einer bestimmten vorgeschriebene Form zunächst weiterhin als körperliche Schriftstücke vorgelegt, ausgestellt und mitgeführt werden.

Artikel 30

Evaluierung

(1) Die Bundesregierung berichtet dem Deutschen Bundestag innerhalb von fünf Jahren nach Inkrafttreten dieses Gesetzes über die durch das Gesetz erzielten Wirkungen und unterbreitet ihm Vorschläge für seine Weiterentwicklung.

(2) Die Bundesregierung berichtet dem Deutschen Bundestag innerhalb von drei Jahren nach Inkrafttreten dieses Gesetzes,

1. in welchen verwaltungsrechtlichen Rechtsvorschriften des Bundes die Anordnung der Schriftform verzichtbar ist und

2. in welchen verwaltungsrechtlichen Rechtsvorschriften des Bundes auf die Anordnung des persönlichen Erscheinens zugunsten einer elektronischen Identifikation verzichtet werden kann.

Erläuterungen

1. Evaluierung (Absatz 1)

Die Berichtspflicht nach diesem Absatz dient der Evaluierung des Gesetzes. Zur Förderung eines nachhaltigen Ausbaus elektronischer Verwaltungsdienste soll der Bericht auch Vorschläge für die Weiterentwicklung der gesetzlichen Grundlagen enthalten. Die erzielten Wirkungen umfassen dabei auch den Erfüllungsaufwand, der bei Bürgerinnen und Bürgern, Wirtschaft und Verwaltung durch die Rechtsänderungen dieses Gesetzes entsteht.

Ergänzend könnten auf Grund eines entsprechenden Beschlusses des IT-Planungsrats die Fortschritte bei der Umsetzung der nationalen E-Government-Strategie einer Berichterstattung zugeführt werden.

2. Normenscreening (Absatz 2)

a) Schriftform verzichtbar (Nummer 1)

Durch die Einführung alternativer Techniken neben der qeS zur Ersetzung der Schriftform in diesem Gesetz wird die Erfüllung der Schriftform bereits erheblich erleichtert. Allerdings ist bei der Vielzahl der Schriftformerfordernisse in den Fachgesetzen (mehrere Tausend) zu vermuten, dass in einigen Fällen nach heutigen Kriterien eine Übermittlung durch einfache E-Mail ausreichend ist, so dass das Schriftformerfordernis verzichtbar ist. In anderen Fällen wird möglicherweise nur ein Teil der Schriftformfunktionen benötigt, so dass diese Tatsache in der Norm abzubilden ist. Hierzu bedarf es einer Überprüfung des gesamten Rechtsbestandes. Da diese Überprüfung auf die mit diesem Gesetz geänderten Querschnittsnormen zur Schriftform aufbaut (§ 3a VwVfG, § 36a SGB I, § 87a AO), sollte sie erst in einem zweiten Schritt nach Inkrafttreten dieses Gesetzes vorgenommen werden. Das Ergebnis der Prüfung ist in einem Bericht an den Deutschen Bundestag niederzulegen und wird im Anschluss Gegenstand eines gesonderten Gesetzgebungsverfahrens. Eine Abfrage des IT-Planungsrates hat jedoch ergeben, dass sich in der Praxis einige Normen als besonders änderungsbedürftig erwiesen haben. Diese Änderungen werden daher bereits mit diesem Gesetz vorgenommen.

b) Persönliches Erscheinen verzichtbar (Nummer 2)

Durch die Einführung des nPA ist eine sichere elektronische Identifikation auch in Fällen möglich geworden, in denen bisher ein persönliches Erscheinen bei einer Behörde nötig ist. Es ist daher eine Überprüfung des Rechtsbestands daraufhin angezeigt, in welchen Fällen das persönliche Erscheinen lediglich den Zweck der sicheren Identifikation verfolgt und daher künftig zugunsten einer elektronischen Identifikation entfallen kann. Die Verpflichtung zum persönlichen Erscheinen muss dagegen beibehalten werden, wenn sie primär anderen Zwecken dient, z. B. dem beratenden oder motivierenden Gespräch mit der Bürgerin oder dem Bürger oder wenn es darauf ankommt, dass sich der Behördenmitarbeiter einen persönlichen Eindruck von der Person verschaffen kann. Auch diese Überprüfung soll in einen Bericht an den Deutschen Bundestag münden, der dann Grundlage für entsprechende gesetzliche Änderungen wird.

Artikel 31

Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich der Absätze 2 bis 5 am Tag nach der Verkündung in Kraft.

(2) In Artikel 1 tritt § 2 Absatz 1 des E-Government-Gesetzes, in Artikel 2 tritt Nummer 3, in Artikel 3 Nummer 1 tritt § 3a Absatz 2 Satz 4 Nummer 2 und 3 des Verwaltungsverfahrensgesetzes, in Artikel 4 tritt § 36a Absatz 2 Satz 4 Nummer 2 und 3 des Ersten Buches Sozialgesetzbuch, in Artikel 7 Nummer 2 tritt § 87a Absatz 3 Satz 4 Nummer 2 und Absatz 4 der Abgabenordnung am 1. Juli 2014 in Kraft.

(3) In Artikel 1 tritt § 2 Absatz 3 und § 14 des E-Government-Gesetzes am 1. Januar 2015 in Kraft.

(4) In Artikel 1 tritt § 2 Absatz 2 des E-Government-Gesetzes ein Kalenderjahr nach Aufnahme des Betriebes des zentral für die Bundesverwaltung angebotenen IT-Verfahrens, über das De-Mail-Dienste für Bundesbehörden angeboten werden, in Kraft. Das Bundesministerium des Innern gibt den Tag des Inkrafttretens im Bundesgesetzblatt bekannt.

(5) In Artikel 1 tritt § 6 Satz 1 des E-Government-Gesetzes am 1. Januar 2020 in Kraft.

Erläuterungen

Die Vorschrift regelt zeitlich gestaffelt das Inkrafttreten des Gesetzes. Nach Absatz 2 wird festgelegt, dass die Änderung des De-Mail-Gesetzes in Artikel 2 Nummer 3 erst am 1. Juli 2014 in Kraft tritt, damit die De-Mail-Provider diese Anforderung aus Gründen der Investitionssicherheit erst mit den technisch erforderlichen Änderungen an ihrer De-Mail-Infrastruktur beginnen müssen, wenn das Gesetz in Kraft getreten ist. Da die Artikel 3 Nummer 1, Artikel 4 und Artikel 7 Nummer 2 die Änderung des De-Mail-Gesetzes voraussetzen, soweit sie De-Mail als Schriftformersatz regeln, wird in Absatz 2 auch insoweit der spätere Termin des Inkrafttretens geregelt. Die in diesen Artikeln ebenfalls geregelte Ersetzung der Schriftform durch die Verwendung elektronischer Formulare in Verbindung mit einem sicheren Identitätsnachweis kann dagegen sofort nach der Verkündung in Kraft treten, so dass die Behörden, die bereits über eine entsprechende Infrastruktur verfügen, diese Verfahren ab Inkrafttreten des Gesetzes anbieten können.

Außerdem wird in Absatz 2 bzw. Absatz 3 festgelegt, dass Artikel 1 § 2 Absatz 1 am 1. Juli 2014 und § 2 Absatz 3 am 1. Januar 2015 in Kraft tritt. Dies trägt dem Umstand Rechnung, dass die betroffenen Behörden zunächst die technisch-organisatorischen Voraussetzungen für die vorgesehene Zugangseröffnung bzw. die Identifikationsmöglichkeit nach § 18 PAuswG schaffen müssen, bevor sie der gesetzlichen Verpflichtung nachkommen können. Nach Absatz 4 wird schließlich festgelegt, dass die Verpflichtung, den elektronischen Zugang zusätzlich durch eine De-Mail-Adresse im Sinne des De-Mail-Gesetzes zu eröffnen (§ 2 Absatz 2), ein Kalenderjahr nach Aufnahme des Betriebes des zentral für die Bundesverwaltung angebotenen IT-Verfahrens, über das De-Mail-Dienste für Bundesbehörden angeboten werden, in Kraft tritt. Der Übergangszeitraum ist für die Anbindung der einzelnen Behörden des Bundes erforderlich. Mit dem Inkrafttreten von § 14 am 1. Januar 2015 wird dem notwendigen Vorlauf Rechnung getragen, eine Festlegung für die Georeferenzierung in Bund-Länder-Gremien zur erarbeiten und im IT-Planungsrat zu beschließen.

Absatz 5 regelt das Inkrafttreten der Soll-Vorschrift für die elektronische Aktenführung in Artikel 1 § 6 Satz 1. Damit soll den Behörden Zeit gegeben werden, die haushalterischen und organisatorischen Vorkehrungen zu treffen, um sich – falls noch nicht geschehen – auf den Übergang zur elektronischen Aktenführung vorzubereiten. Bis dahin bleibt die Führung von elektronischen Akten wie bisher im Ermessen der Behörden. Dabei ist Artikel 1 § 6 Satz 2 zu beachten, der am Tag nach der Verkündung in Kraft tritt.

Der neue
Personalausweis
Meine wichtigste Karte.

Alles Wissenswerte zum neuen Personalausweis.

BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
MUSTERMANN
ERIK
12.08.1964
BERLIN
31.10.2020
938568
Zutrittskontrollen
an Automaten ausweisen
Zugang mit Pseudonym
Barrierefreie Internetdienste
Online unterschreiben
Online-Behördengänge
Online-Registrierung
Altersbestätigung
Online-Formulare ausfüllen

Inhalt

Der neue Personalausweis

Auf einen Blick 4
Der Ausweis im Detail 6
Das Lichtbild 8
Neuer Ausweis, neue Möglichkeiten 10
Spezielle Funktionen 11
Die Online-Ausweisfunktion 12
Zubehör für die Online-Ausweisfunktion 14
Der PIN-Brief 15
Die Unterschriftsfunktion 16
Datenschutz, Datensicherheit und Selbstbestimmung 17
Ausweis weg? – Das ist zu tun! 18
Sicherer Umgang mit den neuen Funktionen 20
Fragen und Antworten 22
Gebühren 23

Steckbriefe

ePass 24
Vorläufiger Reisepass 26
Kinderreisepass 28

Bürgerservice und Sperrnotruf 31

Auf einen Blick

Was ist neu am Personalausweis?

- Scheckkartenformat
- Postleitzahl
- Chip im Ausweis
- Online-Ausweisfunktion für den Einsatz im Internet und an Automaten (auf Wunsch, nutzbar ab 16 Jahren)
- Digitales Lichtbild und freiwillige Fingerabdrücke zur eindeutigen Zuordnung von Ausweis und Inhaber
- Vorbereitet für die Unterschriftsfunktion mit der qualifizierten elektronischen Signatur (separat zu erwerben)
- Erweiterte Sicherheitsmerkmale und besonderer Schutz der biometrischen Daten
- Personalausweis-Logo auf der Rückseite (kennzeichnet ebenfalls Einsatzmöglichkeiten und Zubehör)

Weitere Informationen sind im Internet unter www.personalausweisportal.de oder telefonisch über den Bürgerservice unter 0180-1-33 33 33 erhältlich. (Mo–Fr 7–20 Uhr; 3,9 ct/Min. aus dem dt. Festnetz, aus dem Mobilfunknetz maximal 42 ct/Min., auch aus dem Ausland erreichbar)

Für wen wird das Dokument ausgestellt?

Für deutsche Staatsangehörige ab 16 Jahren. Für Kinder und Jugendliche unter 16 Jahren kann ebenfalls ein Personalausweis ausgestellt werden, jedoch ohne eingeschaltete Online-Ausweisfunktion.

Was kostet der Personalausweis?

Für Personen ab 24 Jahren 28,80 Euro (10 Jahre gültig), für Personen unter 24 Jahren 22,80 Euro (6 Jahre gültig).

Was ist bei der Beantragung vorzulegen?

Benötigt werden ein aktuelles Lichtbild und ein gültiges Identitätsdokument (z. B. alter Personalausweis, Reisepass, Kinderausweis, Kinderreisepass oder Geburtsurkunde). Bei Antragstellern unter 16 Jahren ist die Einverständniserklärung beider Erziehungsberechtigter oder der Sorgerechtsnachweis bei nur einem Erziehungsberechtigten erforderlich.

Anforderungen an das Lichtbild:

- Aktuelle Aufnahme
- Gesicht zentriert auf dem Foto, Frontalaufnahme, kein Halbprofil
- Augen offen und deutlich sichtbar
- Mund geschlossen, neutraler Gesichtsausdruck

Weitere Informationen sind unter www.personalausweisportal.de/fotomustertafel aufgeführt.

Kann die Online-Ausweisfunktion nachträglich eingeschaltet werden?

Die Online-Ausweisfunktion kann jederzeit im Bürgeramt ein- oder ausgeschaltet werden, solange der Personalausweis gültig ist. Für das nachträgliche Einschalten wird eine Gebühr von 6 Euro erhoben. Das nachträgliche Ausschalten ist gebührenfrei.

Werden die Fingerabdrücke gespeichert?

Die freiwillig aufgenommenen Fingerabdrücke werden ausschließlich auf dem Ausweis und nicht in Registern oder Datenbanken gespeichert. Nur hoheitliche Stellen verfügen über die Berechtigung und die technische Möglichkeit, diese Informationen abzufragen.

Der Ausweis im Detail

Diese Daten sind regelmäßig auf dem Chip des Personalausweises abgelegt und können nach Freigabe durch den Ausweisinhaber mit der Online-Ausweisfunktion übermittelt werden:

- Familienname und Vornamen
- Geburtsdatum und -ort
- Anschrift und Postleitzahl
- Wenn angegeben: Ordens- bzw. Künstlername
- Wenn angegeben: Doktorgrad

Die Angaben, ob der Ausweis noch gültig und nicht gesperrt ist, werden im Zusammenhang mit einer Freigabe der oben aufgeführten Daten auch übermittelt.

Für die Nutzung ausschließlich im Rahmen einer hoheitlichen Identitätskontrolle werden zusätzlich die folgenden Daten im Chip abgelegt:

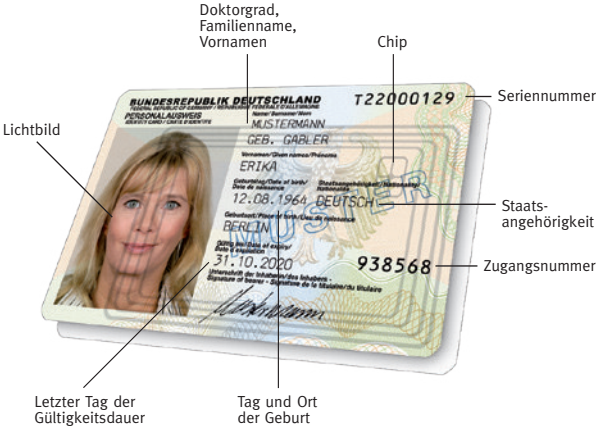
- Das digitale Lichtbild
- Die Seriennummer

Zusätzlich können für die Nutzung ausschließlich im Rahmen einer hoheitlichen Identitätskontrolle auf Wunsch zwei Fingerabdrücke gespeichert werden.

Grundsätzlich nicht gespeichert werden:

- Die eigenhändige Unterschrift
- Die Körpergröße
- Die Augenfarbe

Die Online-Ausweisfunktion wird auf Wunsch des Inhabers in der Personalausweisbehörde vollständig deaktiviert.
Auf Wunsch des Inhabers kann ein Zertifikat für die qualifizierte elektronische Signatur nachgeladen werden (erhältlich bei sogenannten Zertifizierungsdiensteanbietern, siehe Seite 16).



(IDD = Personalausweis der Bundesrepublik Deutschland, Seriennummer, Tag der Geburt, letzter Tag der Gültigkeit, Prüfziffer, Leerstellen, Name, Vorname)

Das Lichtbild

Für das Lichtbild auf dem neuen Personalausweis gelten die gleichen Bestimmungen wie für den aktuellen Reisepass:

- Das Bild muss aktuell sein.
- Das Gesicht muss zentriert auf dem Foto erkennbar sein, Frontalaufnahme, kein Halbprofil.
- Die Augen müssen offen und deutlich sichtbar sein.
- Der Mund muss geschlossen sein, der Gesichtsausdruck neutral.

Selbstverständlich sind Ausnahmen möglich, z. B. aus medizinischen Gründen. Weitere Informationen sind unter www.personalausweisportal.de/fotomustertafel aufgeführt.

Bitte beachten: Das Lichtbild ist das einzige biometrische Merkmal, das auf dem Chip im Personalausweis verpflichtend abgelegt ist. Alle anderen biometrischen Daten des Ausweises, wie die eigenhändige Unterschrift, die Körpergröße und die Augenfarbe, sind lediglich aufgedruckt.

Die Fingerabdrücke

Im Chip des Personalausweises können auf Wunsch zwei Fingerabdrücke gespeichert werden. Sie bieten z. B. nach einem Ausweisdiebstahl besseren Schutz vor Identitätsmissbrauch, da einfacher festgestellt werden kann, ob ein Ausweis auch vom tatsächlichen Ausweisinhaber vorgelegt wird. Die Fingerabdruckdaten werden ausschließlich auf dem Ausweis und nicht in Registern oder Datenbanken gespeichert.

Bitte beachten: Nur hoheitliche Stellen wie Polizei, Zollverwaltung, Pass- und Personalausweisbehörden sowie Meldebehörden verfügen über die Berechtigung und die technischen Möglichkeiten, das Lichtbild und die Fingerabdruckdaten einzusehen. Die Übertragung mit der Online-Ausweisfunktion ist ausgeschlossen.

Die Person muss mit neutralem Gesichtsausdruck und geschlossenem Mund gerade in die Kamera blicken.

Der Hintergrund muss einfarbig hell sein (idealerweise neutral grau). Auf dem Hintergrund dürfen keine Schatten entstehen.

Die Augen müssen klar und deutlich erkennbar sein. Reflexionen auf den Brillengläsern, getönte Gläser oder Sonnenbrillen sind nicht zulässig. Der Rand der Gläser oder das Gestell dürfen die Augen nicht verdecken.

Neuer Ausweis, neue Möglichkeiten

Grundsätzlich kann man sich mit dem neuen Personalausweis wie bisher z. B. bei Polizei- und Grenzkontrollen ausweisen. Mit der neuen Online-Ausweisfunktion (auch eID-Funktion genannt) ist darüber hinaus die einfache und sichere Kommunikation über das Internet zwischen Ausweisinhaber, Verwaltungen und Unternehmen ohne Papier und lange Wartezeiten möglich.

Immer mehr Dinge des täglichen Lebens verlagern sich in die Online-Welt. Einige Transaktionen konnten bislang nicht allein über das Internet abgeschlossen werden, da ein zusätzlicher Identitäts- oder Altersnachweis durch Vorlage des Personalausweises erforderlich war. Darüber hinaus sind für viele Internetdienste eigene Passwörter, Benutzernamen oder Zugangsnummern nötig. Einen Standard-Identitätsnachweis für die Online-Welt gab es nicht. Der neue Personalausweis schließt diese Lücke.

Der Chip in der Ausweiskarte kann erforderliche Daten – nach Zustimmung des Ausweisinhabers durch Eingabe der PIN – über sicher verschlüsselte Verbindungen übermitteln. Berechtigungszertifikate regeln, welche persönlichen Daten an Anbieter von Internetanwendungen und Online-Verwaltungsdienstleistungen übertragen werden dürfen.

Im Gegensatz zu bisherigen Anmelde- und Registrierungsverfahren im Internet, bei denen sich der Nutzer durch die Kenntnis einer Kombination aus Nutzername und Passwort identifiziert, wird das Sicherheitsniveau mit dem neuen Personalausweis erhöht: Hier ist nicht nur die Kenntnis der 6-stelligen PIN, sondern zusätzlich der Besitz des Ausweises erforderlich. Auf diese Weise werden Identitätsdiebstahl und -missbrauch deutlich erschwert.

Spezielle Funktionen

Mit der Online-Ausweisfunktion bietet der Ausweis weitere Funktionalitäten, die ebenfalls freiwillig nutzbar sind.

Pseudonymer Zugang

Der Ausweis kann ein dienste- und kartenspezifisches Merkmal generieren, mit dessen Hilfe sich der Ausweisinhaber mit seinem neuen Personalausweis auch pseudonym bei Internetdiensten anmelden kann, ohne dass persönliche Angaben wie Name und Adresse übermittelt werden. Trotzdem kann der Anbieter den Ausweisinhaber bei jeder späteren Anmeldung anhand dieses Merkmals wiedererkennen. Eine Verbindung zu anderen Diensten, die auch mit dem Personalausweis genutzt werden, kann aufgrund dieses Merkmals jedoch nicht hergestellt werden.

Alters- und Wohnortbestätigung

Für einige Dienste und Anwendungen benötigen die Anbieter lediglich Angaben zum Alter oder zum Wohnort des Ausweisinhabers. Der neue Personalausweis kann statt des gesamten Geburtsdatums für diese Zwecke die Information übermitteln, ob das angefragte Alter (z. B. 16 oder 18 Jahre) erreicht ist oder nicht. Ähnlich wird verfahren, wenn ein Anbieter seine Dienste nur in einem Bundesland oder in einer bestimmten Stadt anbietet. Statt der vollständigen Übermittlung der Anschrift wird bei der Wohnortbestätigung ein einfaches „Ja“ oder „Nein“ übermittelt.

Außerdem ist der Personalausweis für das elektronische rechtsverbindliche Unterzeichnen von Verträgen und Urkunden mit der qualifizierten elektronischen Signatur über das Internet vorbereitet (siehe Seite 16).

Die Online-Ausweisfunktion

Mit der Online-Ausweisfunktion können erforderliche persönliche Angaben elektronisch übermittelt werden. Diese Art der Datenübermittlung hat jedoch keinen Einfluss auf den Vertragsabschluss selbst. Hier gelten weiterhin die Regeln für Online-Geschäfte. So funktioniert das Online-Ausweisen beispielsweise in einem Online-Shop:

Sie suchen sich beim Online-Händler ein Produkt zum Kauf aus. Der Online-Händler benötigt für den Vertragsabschluss, zur Rechnungsstellung und zum Zusenden der Ware Ihren Namen, Vornamen und Ihre Anschrift. Diese Daten können mithilfe der Online-Ausweisfunktion übermittelt werden.

Dazu wird Ihnen das Berechtigungszertifikat des Online-Händlers angezeigt. Es enthält Angaben zum Anbieter, zur Gültigkeit und dazu, welche Daten der Anbieter von Ihnen erhalten möchte. Mit der Eingabe Ihrer 6-stelligen PIN stimmen Sie der Datenübertragung zu. Wenn Sie wünschen, können Sie einzelne Daten von der Übertragung ausschließen.

Das Berechtigungszertifikat des Online-Händlers wird im Chip des Personalausweises geprüft. Dann werden die von Ihnen freigegebenen Daten verschlüsselt an den Online-Händler übertragen. Das System des Online-Händlers wiederum überprüft, ob Ihr Personalausweis gültig und nicht gesperrt ist.

Der Online-Händler empfängt Ihre Daten. Im Regelfall werden Ihnen diese noch einmal angezeigt. Den Kaufvertrag schließen Sie wie bisher durch eine separate Willenserklärung ab, z. B. durch die Schaltfläche „Bestellung abschicken“.

Zubehör für die Online-Ausweisfunktion

Für die Verwendung der Online-Ausweisfunktion am eigenen Computer werden ein Lesegerät und eine Treiber-Software benötigt.

Lesegerät

Das Lesegerät liest die jeweils ausgewählten Daten aus dem Chip und überträgt diese – nach Eingabe der 6-stelligen PIN durch den Ausweisinhaber – an den Anbieter. Empfohlen werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierte Lesegeräte mit Personalausweis-Logo. Zu unterscheiden sind:

- Standard- und Komfortlesegeräte mit eigener Tastatur zur PIN-Eingabe. Für die Nutzung der Unterschriftsfunktion sind Komfortlesegeräte erforderlich.
- Basislesegeräte mit PIN-Eingabe über die Computer- oder Bildschirmtastatur.

Software

Eine Software – zum Beispiel die „AusweisApp“ – stellt die Verbindung zwischen Ausweis und Computer her und ermöglicht den verschlüsselten Datenaustausch über das Lesegerät. Die „AusweisApp“ kann kostenlos unter www.ausweisapp.bund.de heruntergeladen werden.

Der PIN-Brief

Wie auch bei EC- oder Kreditkarten erhält der Antragsteller nach der Beantragung eines Ausweises für die Verwendung der Online-Ausweisfunktion einen PIN-Brief mit einer 5-stelligen Aktivierungs-PIN, der PUK-Nummer und einem Sperrkennwort per Post zugestellt.

Von der Aktivierungs-PIN zur persönlichen PIN

Die 5-stellige Aktivierungs-PIN (auch Transport-PIN genannt) muss vor der ersten Verwendung der Online-Ausweisfunktion durch eine persönliche 6-stellige PIN ersetzt werden. Entweder mithilfe eines Lesegeräts von zu Hause aus oder in der Personalausweisbehörde (bei der Abholung des Ausweises gebührenfrei). Ohne eine persönliche 6-stellige PIN ist die Online-Ausweisfunktion nicht nutzbar.

PUK-Nummer

Wenn die persönliche PIN dreimal hintereinander falsch eingegeben wurde, wird die Online-Ausweisfunktion blockiert. Mit der PUK-Nummer kann die Blockierung wieder aufgehoben werden.

Sperrkennwort

Das Sperrkennwort wird benötigt, wenn der Personalausweis abhandengekommen ist und die Online-Ausweisfunktion gesperrt werden muss (siehe Seite 18).

Die Unterschriftsfunktion

Die Unterschriftsfunktion mit der qualifizierten elektronischen Signatur dient dazu, digital vorliegende Verträge oder Urkunden rechtsverbindlich zu unterzeichnen. Gleiches gilt für Erklärungen und Anträge gegenüber Behörden, die zur Rechtsverbindlichkeit schriftlich erfolgen müssen.

Mit der Unterschriftsfunktion entfällt die handschriftliche Unterschrift. Zusätzlich kann erkannt werden, ob Dokumente nach dem digitalen Unterschreiben verändert worden sind. Im Gegensatz zur Online-Ausweisfunktion können mit der Unterschriftsfunktion rechtsverbindliche Willenserklärungen, beispielsweise zum Vertragsabschluss oder zum Erteilen einer Vollmacht, abgegeben werden.

Signaturzertifikat und Komfortlesegerät

Für die Verwendung der Unterschriftsfunktion mit dem neuen Personalausweis werden ein Signaturzertifikat, eine Signatur-PIN und ein Komfortlesegerät mit PIN-Pad benötigt.

Ein Signaturzertifikat kann bei einem Zertifizierungsdiensteanbieter erworben und auf den Personalausweis nachgeladen werden (siehe www.nrca-ds.de).

Datenschutz, Datensicherheit und Selbstbestimmung

Der neue Personalausweis bietet maximale Sicherheit für die persönlichen Daten und ermöglicht selbstbestimmte Datenübermittlung.

Im Gegensatz zu einfachen Funkchips, wie sie beispielsweise in Schlüsselkarten oder Skipässen verwendet werden, sendet der Personalausweis die auf ihm gespeicherten Informationen nicht an jedes beliebige Lesegerät. Vor der Datenübermittlung prüft der Chip im Ausweis, ob der anfragende Anbieter oder die anfragende Behörde dazu berechtigt sind, welche Daten im Einzelfall übermittelt werden sollen und ob der Ausweisinhaber dieser Datenübermittlung zustimmt.

Bei jeder Datenübermittlung werden die Daten verschlüsselt. Alle Informationen und Übermittlungen werden mit international anerkannten und etablierten technischen Verfahren sicher geschützt. Außerdem muss trotz Funkverbindung der Personalausweis auf dem Lesegerät aufliegen. Ein Auslesen aus der Ferne ist daher nicht möglich.

Mehr Sicherheit gibt es damit vor allem im Internet: Nur wer den Ausweis besitzt und die zugehörige PIN kennt, kann Informationen zur Übermittlung freigeben. Der Ausweisinhaber behält die volle Kontrolle, weiß jederzeit, wem er seine Identität preisgibt, da jeder Anbieter erst behördlich zugelassen werden muss. Letztendlich entscheidet immer der Ausweisinhaber selbst, ob und wem er welche Daten übermittelt.

Ausweis weg? – Das ist zu tun!

Sperrnotruf – rund um die Uhr erreichbar

0180-1-33 33 33

(3,9 ct/Min. aus dem dt. Festnetz,
aus dem Mobilfunknetz maximal 42 ct/Min.)

Wenn ein Personalausweis mit eingeschalteter Online-Ausweisfunktion gestohlen wurde oder abhanden gekommen ist, muss die Online-Ausweisfunktion so schnell wie möglich gesperrt werden. Das geht im Bürgeramt oder über den 24-Stunden-Sperrnotruf 0180-1-33 33 33 (3,9 ct/Min. aus dem dt. Festnetz, aus dem Mobilfunknetz maximal 42 ct/Min., auch aus dem Ausland erreichbar).

Zum Sperren der Online-Ausweisfunktion über den Sperrnotruf werden der Familienname, der erste Vorname, das Geburtsdatum und das Sperrkennwort telefonisch abgefragt. Diese Angaben sind im PIN-Brief notiert. Weitere Informationen sind unter www.personalausweisportal.de/verlustfall nachzulesen.

Bitte beachten: Der Ausweisinhaber ist zusätzlich verpflichtet, den Verlust seines Personalausweises, egal ob die Online-Ausweisfunktion eingeschaltet ist oder nicht, der zuständigen Personalausweisbehörde zu melden.

Sperren der Unterschriftsfunktion

Für den Fall, dass der Personalausweis auch für die elektronische Signatur genutzt wurde, muss das Signaturzertifikat über den jeweiligen Anbieter gesondert gesperrt werden.

BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
T22000129
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE
Name/Surname/Nom
MUSTERMANN
GEB. GABLER
Vornamen/Given names/Prénoms
ERIKA
Geburtstag/Date of birth/
Date de naissance
12.08.1964
Staatsangehörigkeit/Nationality/
Nationalité
DEUTSCH
MUSTER
Geburtsort/Place of birth/Lieu de naissance
BERLIN
938568
Gültig bis/Date of expiry/
Date d'expiration
31.10.2020
Unterschrift der Inhaberin/des Inhabers -
Signature of bearer - Signature de la titulaire/du titulaire

Sicherer Umgang mit den neuen Funktionen

Bitte gehen Sie mit Ihrem neuen Personalausweis und den neuen Funktionen genauso sorgsam um wie mit Ihrer EC- oder Kreditkarte und beachten Sie unbedingt folgende Hinweise:

- Bewahren Sie den Ausweis immer sicher auf. Lassen Sie ihn nicht unbeaufsichtigt zurück, wenn ein anderer Zugriff darauf haben könnte.

- Geben Sie Ihre PIN nicht an Dritte weiter. Wenn Sie sich die PIN aufschreiben oder anderweitig notieren, bewahren Sie diese nicht zusammen mit dem Ausweis – zum Beispiel im Portemonnaie – auf. Notieren Sie die PIN auch keinesfalls auf Ihrem Ausweis.

- Wenn Ihr Ausweis abhandengekommen ist, müssen Sie die Online-Ausweisfunktion – wenn diese eingeschaltet ist – so schnell wie möglich sperren lassen. Dies ist in Ihrer Personalausweisbehörde oder über den 24-Stunden-Sperrnotruf möglich (siehe Seite 18).

Bitte beachten Sie auch die Hinweise zum sicheren Umgang mit Ihrem Ausweis am eigenen Computer:

- Aktualisieren Sie regelmäßig das Virenschutzprogramm, die Firewall, das Betriebssystem und die Software (z. B. AusweisApp). Nutzen Sie die Sicherheitsupdates der jeweiligen Softwarehersteller.

- Ändern Sie Ihre PIN regelmäßig. Wählen Sie als PIN keine Zahlenfolge, die auf dem Ausweis aufgedruckt ist (z. B. das Geburtsdatum oder die Zugangsnummer) oder leicht zu erraten wäre (z. B. „123456“).

Weitere Informationen

Weitere Informationen finden Sie unter www.bsi-fuer-buerger.de. Dort informiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) über Gefahren im Internet und gibt Tipps für ein sicheres Online-Verhalten.

Fragen und Antworten

Behalten alte Ausweise ihre Gültigkeit?

Alle alten Personalausweise behalten ihre Gültigkeit bis zum Ablaufdatum. Ein vorzeitiger Umtausch des alten Personalausweises gegen den neuen Ausweis ist aber jederzeit möglich.

Was ist beim Lichtbild zu beachten?

Erlaubt sind nur Frontalaufnahmen, keine Halbprofile. Das Gesicht muss zentriert auf dem Foto erkennbar sein. Die Augen müssen offen, der Mund geschlossen und der Gesichtsausdruck neutral sein. Weitere Informationen sind unter www.personalausweisportal.de/fotomustertafel aufgeführt.

Wozu dienen die Fingerabdrücke?

Als zusätzliches Sicherheitsmerkmal ist es möglich, zwei Fingerabdrücke auf dem Chip im Ausweis aufzunehmen. Die Fingerabdrücke werden nicht in Registern oder Datenbanken gespeichert und können nur von hoheitlichen Stellen wie der Polizei, der Zollverwaltung, den Pass- und Personalausweisbehörden sowie den Meldebehörden zur Überprüfung der Echtheit des Ausweises und der Identität des Ausweisinhabers genutzt werden.

Was ist zu tun bei Diebstahl und Verlust?

Siehe Seite 18.

Muss bei einem Umzug ein neuer Ausweis beantragt werden?

Nach dem Umzug wird im Rahmen der Ummeldung im Bürgeramt auch die Anschrift auf dem Personalausweis kostenlos geändert. Dazu werden die Daten auf dem Chip des Ausweises aktualisiert und ein Änderungsaufkleber auf der Rückseite der Ausweiskarte angebracht.

Gebühren

Ausstellung von Personalausweisen ab 1. November 2010

Antragstellende Person ab 24 Jahren	28,80 Euro (10 Jahre gültig)
Antragstellende Person unter 24 Jahren	22,80 Euro (6 Jahre gültig)
Vorläufiger Personalausweis	10 Euro

Weitere Gebührenregelungen

Erstmaliges Einschalten der Online-Ausweisfunktion bei der Ausgabe oder bei der Vollendung des 16. Lebensjahres	gebührenfrei
Nachträgliches Einschalten der Online-Ausweisfunktion	6 Euro
Ausschalten der Online-Ausweisfunktion	gebührenfrei
Ändern der PIN im Bürgeramt (z. B. PIN vergessen)*	6 Euro
Ändern der Anschrift bei Umzügen	gebührenfrei
Sperren der Online-Ausweisfunktion im Verlustfall	gebührenfrei
Entsperren der Online-Ausweisfunktion	6 Euro
Kosten für das Aufbringen eines elektronischen Signaturzertifikates	Festlegung durch Anbieter

* Ändern der PIN mit eigenem Kartenlesegerät ist jederzeit möglich.

Steckbrief

ePass

(Elektronischer Reisepass)

Für wen wird das Dokument ausgestellt?

Im Regelfall für Personen ab zwölf Jahren. Auf Wunsch kann auch für Kinder unter zwölf Jahren ein ePass beantragt werden. Bei Kindern unter sechs Jahren werden jedoch keine Fingerabdrücke erfasst.

Was ist bei der Beantragung vorzulegen?

Ein aktuelles Lichtbild und ein gültiges Identitätsdokument (alter Reisepass oder Personalausweis bei Erstbeantragung, Kinderreisepass, Kinderausweis oder Geburtsurkunde).

Lichtbild und Fingerabdrücke

Lichtbild: siehe Seite 8. Weitere Informationen sind unter www.personalausweisportal.de/fotomustertafel aufgeführt.
Fingerabdrücke: Bei der Beantragung des ePass werden zwei Fingerabdrücke aufgenommen. Die Fingerabdrücke werden nur auf dem ePass gespeichert, nicht in Registern oder Datenbanken. Sie können nur von hoheitlichen Stellen abgefragt werden.

Kosten und Gültigkeit

59 Euro für Pässe, die für Personen ab 24 Jahren ausgestellt werden (10 Jahre gültig), und 37,50 Euro für Personen unter 24 Jahren (6 Jahre gültig).

Steckbrief

Vorläufiger Reisepass

Für wen wird das Dokument ausgestellt?

Der vorläufige Reisepass wird nur in Einzelfällen ausgestellt, beispielsweise wenn sofort ein Pass benötigt wird und die Ausstellung eines regulären Passes nicht bis zum Zeitpunkt des erstmaligen Gebrauchs möglich ist.

Was ist bei der Beantragung vorzulegen?

Ein aktuelles Lichtbild und ein gültiges Identitätsdokument (alter Reisepass oder Personalausweis, Kinderreisepass, Kinderausweis oder Geburtsurkunde). Die Passbehörden können die Vorlage von geeigneten Belegen zum Nachweis der Dringlichkeit (z. B. Flugticket für eine kurzfristig anstehende Reise) verlangen.

Anforderungen an das Lichtbild

Siehe Seite 8. Weitere Informationen sind unter www.personalausweisportal.de/fotomustertafel aufgeführt.

Kosten und Gültigkeit

26 Euro (bis zu ein Jahr gültig).

Bitte beachten:

Der vorläufige Reisepass ist nicht für die visumfreie Einreise in die Vereinigten Staaten von Amerika zugelassen.

Steckbrief

Kinderreisepass

Für wen wird das Dokument ausgestellt?

Für Kinder unter zwölf Jahren.

Was ist bei der Beantragung vorzulegen?

Ein aktuelles Lichtbild und ein gültiges Identitätsdokument (z. B. alter Kinderreisepass, Kinderausweis oder Geburtsurkunde sowie die Einverständniserklärung beider Erziehungsberechtigten oder der Sorgerechtsnachweis bei nur einem Erziehungsberechtigten.

Anforderungen an das Lichtbild

Siehe Seite 8. Weitere Informationen sind unter www.personalausweisportal.de/fotomustertafel aufgeführt.

Kosten und Gültigkeit

13 Euro (6 Jahre gültig) und 6 Euro für eine Verlängerung (längstens bis zum zwölften Geburtstag).

Extra-Hinweis

Der frühere Kinderausweis wird seit dem 1. Januar 2006 nicht mehr ausgestellt bzw. verlängert. Seit dem 1. November 2007 können Kinder nicht mehr in den Reisepass ihrer Eltern eingetragen werden. Es ist jedoch möglich, für Kinder einen Personalausweis (z. B. für Reisen innerhalb der Europäischen Union) zu beantragen.

Bitte beachten:

Der Kinderreisepass ist nicht für die visumfreie Einreise in die Vereinigten Staaten von Amerika zugelassen.

BUNDESREPUBLIK DEUTSCHLAND
T22
PERSONALAUSWEIS
MUSTERMANN
GEB. GABLER
ERIKA
12.08.1964, BERTSCH
BERLIN
31.10.2020
938568
MUSTER

Bürgerservice und Sperrnotruf

Der Bürgerservice (Mo–Fr 7–20 Uhr) und der Sperrnotruf (rund um die Uhr) sind unter 0180-1-33 33 33 erreichbar (3,9 ct/Min. aus dem dt. Festnetz, aus dem Mobilfunknetz maximal 42 ct/Min., auch aus dem Ausland erreichbar).

Weitere Informationen sind unter www.personalausweisportal.de/buergerservice aufgeführt.

Bestellservice

Diese Broschüre kann kostenlos bestellt werden bei:
Publikationsversand der Bundesregierung
Postfach 48 10 09 // 18132 Rostock
Telefon: 0180-5-77 80 90 // Fax: 0180-5-77 80 94
publikationen@bundesregierung.de
Artikelnummer: BMI10004
Die zum Versand der Publikation angegebenen personenbezogenen Daten werden nach erfolgreicher Lieferung gelöscht.

Diese Broschüre wird im Rahmen der Öffentlichkeitsarbeit des Bundesministeriums des Innern kostenlos herausgegeben. Sie darf weder von Parteien noch von Wahlbewerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Das gilt für Europa-, Bundestags-, Landtags- und Kommunalwahlen. Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung. Unabhängig davon, wann, auf welchem Weg und in welcher Anzahl diese Schrift dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme der Bundesregierung zugunsten einzelner politischer Gruppen verstanden werden könnte.

Bundesministerium
des Innern

Herausgeber:
Bundesministerium des Innern // 11014 Berlin
Redaktion: BMI
www.bmi.bund.de // www.cio.bund.de
www.personalausweisportal.de
5. Auflage // Stand: November 2010
Bildnachweis: BMI

Bundesamt
für Sicherheit in der
Informationstechnik

Certificate Policy für die eID-Anwendung des ePA

Elektronischer Identitätsnachweis mit dem elektronischen Personalausweis

Version 1.29, 23.05.2012

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: cvca-eID@bsi.bund.de
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2012

Inhaltsverzeichnis

1 Einleitung ... 7
1.1 Überblick ... 9
1.2 Name und Identifizierung des Dokuments ... 12
1.3 PKI-Teilnehmer ... 12
1.4 Verwendung von Zertifikaten ... 15
1.5 Administration der Policy ... 17
2 Verantwortlichkeit für Veröffentlichungen und Verzeichnisse ... 18
2.1 Verzeichnisse ... 18
2.2 Veröffentlichung von Informationen zur Zertifikatserstellung ... 18
2.3 Zeitpunkt und Häufigkeit der Veröffentlichungen ... 19
2.4 Zugriffskontrollen auf Verzeichnisse ... 19
3 Identifizierung und Authentifizierung ... 20
3.1 Regeln für die Namensgebung ... 20
3.2 Initiale Überprüfung der Identität ... 24
3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung ... 30
3.4 Identifizierung und Authentifizierung von Anträgen auf Sperrung ... 31
4 Betriebsanforderungen für den Zertifikatslebenszyklus ... 32
4.1 Zertifikatsantrag ... 32
4.2 Verarbeitung von Zertifikatsanträgen ... 38
4.3 Ausgabe von Zertifikaten ... 40
4.4 Annahme von Zertifikaten ... 40
4.5 Verwendung von Schlüsselpaar und Zertifikat ... 41
4.6 Zertifikatserneuerung ... 42
4.7 Zertifizierung nach Schlüsselerneuerung ... 42
4.8 Änderungen am Zertifikat ... 43
4.9 Sperrung und Suspendierung von Zertifikaten ... 43
4.10 Service zur Statusabfrage von Zertifikaten ... 43
4.11 Beendigung der Teilnahme ... 44
4.12 Hinterlegung und Wiederherstellung von Schlüsseln ... 44
5 Organisatorische, betriebliche und physikalische Sicherheitsmaßnahmen ... 45
5.1 Physikalische Sicherheitsmaßnahmen ... 45
5.2 Verfahrensanweisungen ... 46
5.3 Personalkontrolle ... 46
5.4 Überwachungsmaßnahmen ... 47
5.5 Archivierung von Aufzeichnungen ... 47
5.6 Schlüsselwechsel einer Zertifizierungsstelle ... 47
5.7 Notfall-Management ... 48
6 Technische Sicherheitsmaßnahmen ... 50
6.1 Erzeugung und Installation von Schlüsselpaaren ... 50

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module....52
6.3 Andere Aspekte des Managements von Schlüsselpaaren....56
6.4 Aktivierungsdaten....59
6.5 Sicherheitsmaßnahmen für die Rechneranlagen....59
6.6 Zeitstempel....60
6.7 Validierungsmodell....60
7 Profile für Zertifikate und Sperrlisten....61
7.1 Profile für Zertifikate und Zertifikats-Requests....61
7.2 Profile für Sperrlisten....63
7.3 Profile für OCSP-Dienste....63
8 Überprüfung und andere Bewertungen....64
8.1 Inhalte, Häufigkeit und Methodik....64
8.2 Reaktionen auf identifizierte Vorfälle....67
9 Sonstige finanzielle und rechtliche Regelungen....68
9.1 Preise....68
9.2 Finanzielle Zuständigkeiten....68
10 Anhang....69
Definitionen....69
Literaturverzeichnis....73

Tabellenverzeichnis

Tabelle 1: Identifikation des Dokuments....12
Tabelle 2: Übersicht der PKI-Teilnehmer....12
Tabelle 3: Certificate Authorities (CAs) der CVCA-eID PKI....13
Tabelle 4: Registration Authorities (RAs) der CVCA-eID PKI....14
Tabelle 5: Erlaubter Verwendungszweck von Zertifikaten und zugehöriger privater Schlüssel....16
Tabelle 6: Kontaktadresse....17
Tabelle 7: Belegung CHR-Feld der CVCA-Zertifikate....20
Tabelle 8: Belegung CHR-Feld der CVCA-Zertifikate / Anteil Antragsteller....20
Tabelle 9: Belegung CHR-Feld des hoheitlichen DV-Zertifikats....21
Tabelle 10: Belegung CHR-Feld des hoheitlichen DV-Zertifikats / Anteil Antragsteller....21
Tabelle 11: Belegung CHR-Feld des nicht hoheitlichen DV-Zertifikats....22
Tabelle 12: Belegung CHR-Feld des nicht hoheitlichen DV-Zertifikats / Anteil Antragsteller....22
Tabelle 13: Zur Zertifikatsantragsstellung berechtigte hoheitliche Organisationen....33
Tabelle 14: Zur Zertifikatsantragsstellung berechtigte nicht hoheitliche Organisationen....33
Tabelle 15: Fristen zur Bearbeitung von hoheitlichen Zertifikatsanträgen....39
Tabelle 16: Fristen zur Bearbeitung von nicht hoheitlichen Zertifikatsanträgen....39
Tabelle 17: Archivierung öffentlicher Schlüssel....56
Tabelle 18: Setzen von Gültigkeitszeiten in CV-Zertifikaten der CVCA-eID PKI....57
Tabelle 19: Gültigkeitszeiten CVCA-eID- und DV-Ebene....57
Tabelle 20: Gültigkeitszeiten hoheitliche Terminals....58
Tabelle 21: Gültigkeitszeiten nicht hoheitliche Terminals....59
Tabelle 22: Übersicht Felder CV-Zertifikat mit vorgegebener Wertebelegung....61
Tabelle 23: Erlaubte Zugriffsrechte für CVCA-/DV-Zertifikate....62
Tabelle 24: Prüfanforderungen Hoheitlicher Document Verifier....65
Tabelle 25: Prüfanforderungen Hoheitlicher Terminalbetreiber....65
Tabelle 26: Prüfanforderungen BerCA....66
Tabelle 27: Prüfanforderungen Diensteanbieter....66
Tabelle 28: Prüfanforderungen eID-Service Provider....67
Tabelle 29: Begriffsbestimmung....71
Tabelle 30: Abkürzungen....73

Abbildungsverzeichnis

Abbildung 1: Gesamtübersicht CVCA-eID PKI.....8
Abbildung 2: Terminal-Gerätetypen (On-/Offline-Terminal).....11

1 Einleitung

Der **elektronische Personalausweis (ePA)** beinhaltet die drei Anwendungen „Biometrie Anwendung (ePass)“, „elektronischer Identitätsnachweis (eID) und „elektronische Signatur (eSign)“.

Der elektronische Identitätsnachweis (eID) des ePA ermöglicht die verbindliche elektronische Übermittlung von Identitätsmerkmalen (ohne biometrische Daten) in Online-Anwendungen und in lokalen Verarbeitungsprozessen. Für einen Zugriff auf diese im Chip des ePA gespeicherten Daten ist ein digitales Berechtigungszertifikat erforderlich. Bei diesen Zertifikaten handelt es sich um sogenannte CV- (Card Verifiable) Zertifikate in welchen explizit festgelegt ist, auf welche Daten im Chip des Ausweises zugegriffen werden darf.

Das vorliegende Dokument beschreibt die **Certificate Policy (CP)** unter welcher die Berechtigungszertifikate in der Country Verifying Certificate Authority -electronic Identity PKI (**CVCA-eID PKI**) zum Zugriff auf die eID-Funktion des elektronischen Personalausweises ausgestellt werden. Des Weiteren ist die CP in der Verordnung „Über Personalausweise und den elektronischen Identitätsnachweis“ verankert.

Innerhalb dieser CP werden organisatorische und technische Anforderungen für das Anerkennen, Ausstellen, Verwalten, Benutzen, Zurückziehen und Erneuern von Zertifikaten zum Zugriff auf die eID-Anwendung des elektronischen Personalausweises definiert.

Die Ausführungen in dieser CP beziehen sich über den Sachzusammenhang mit dem ePA hinaus auf weitere zukünftig einzuführende elektronische Ausweise wie z.B. den **elektronischen Aufenthaltstitel (eAT)**.

Regelungen hinsichtlich der Anwendungen ePass und eSign sind nicht Gegenstand der vorliegenden Certificate Policy.

Inhaltliche Grundlagen für die Erstellung der Certificate Policy bilden insbesondere die folgenden Dokumente:

- Architektur Elektronischer Personalausweis [TR-03127],
- Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI) - [TR-03110],
- EAC-PKI'n für den elektronischen Personalausweis [TR-03128]
- Gesetz über den Personalausweis und den elektronischen Identitätsnachweis (Personalausweisgesetz, PAuswG) [PAuswG]
- Verordnung über Personalausweise und den elektronischen Identitätsnachweis [PAuswV]
- PKI for the Extended Access Control (EAC), Protocol for the Management of Certificates and CRLs [TR-03129]

Die Struktur dieses Dokuments orientiert sich an dem Request for Comments (RFC) 3647 [RFC 3647], um eine zweckdienliche Vergleichbarkeit mit anderen Policies zu unterstützen.

Die Schlüsselworte „MUSS“ / „MÜSSEN“, „DARF KEIN“ / „DÜRFEN KEIN“, „DARF NICHT“ / „DÜRFEN NICHT“, „SOLL“/ „SOLLEN“, „SOLL NICHT“/ „SOLLEN NICHT“, „SOLLTE“ / „SOLLTE“, „SOLLTE NICHT“ / „SOLLTEN NICHT“, „EMPFOHLEN“ und „KANN“ / „KÖNNEN“ in diesem Dokument sind wie in [RFC 2119] definiert zu interpretieren.

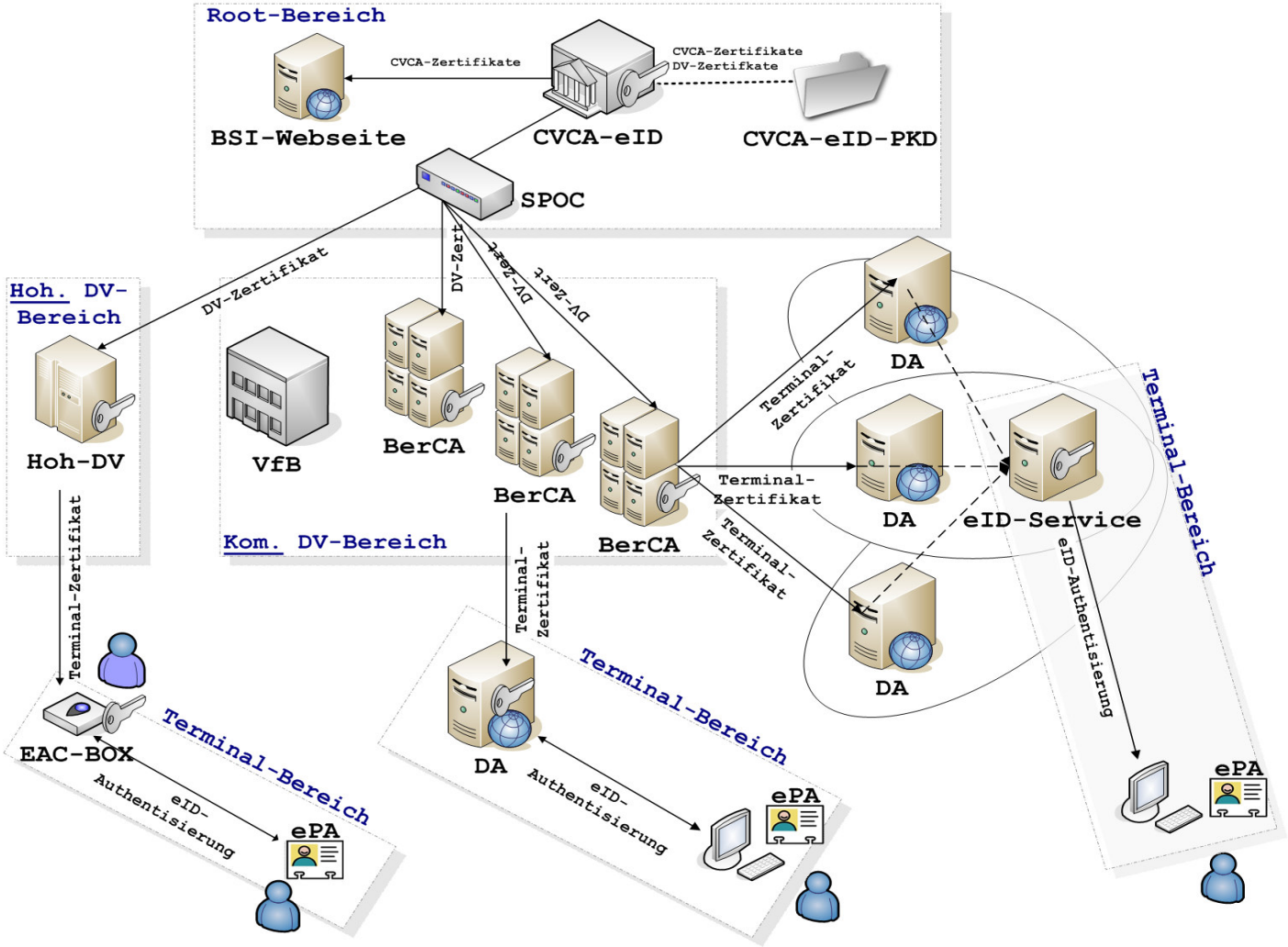


Abbildung 1: Gesamtübersicht CVCA-eID PKI

1.1 Überblick

Der elektronische Identitätsnachweis (eID) des ePA ermöglicht die verbindliche elektronische Übermittlung von Identitätsmerkmalen (ohne biometrische Daten) in Online-Anwendungen und in lokalen Verarbeitungsprozessen. Für einen Zugriff auf diese im Chip des ePA gespeicherten Daten ist ein Berechtigungsnachweis notwendig. Die Berechtigungen und somit auch die Zugriffsrechte auf die gespeicherten Daten werden durch die Vergabe von Zertifikaten über eine **Public Key Infrastruktur (PKI)** geregelt.

Die Public Key Infrastruktur für die eID-Anwendung des elektronischen Personalausweises, die **CVCA-eID PKI,** ist gemäß [TR-03110] in drei Stufen unterteilt. Diese PKI Stufen sind in Abbildung 1 als „Bereiche“ gekennzeichnet und werden nachfolgend erläutert.

Root-Bereich

Die oberste Stufe der CVCA-eID PKI bildet der Root Bereich mit dem nationalen Vertrauensanker für die eID-Funktion der **CVCA-eID**. Die CVCA-eID betreibt einen eigenen nicht öffentlichen Verzeichnisdienst, in dem alle ausgestellten Zertifikate archiviert werden, genannt **CVCA-eID PKD**. Darüber hinaus verfügt die CVCA-eID über eine einheitliche Kommunikationsschnittstelle, den sogenannten Single Point of Contact (**SPOC),** über welchen die Kommunikation zu den Document Verifiern (DVs) abgewickelt wird. Ferner werden den PKI-Teilnehmern über die **BSI-CVCA-eID Webseite** verschiedene Informationen zur PKI sowie Zertifikate zur Verfügung gestellt (siehe Abschnitt 2.2). Alle Systeme des Root-Bereichs werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) betrieben.

Die Aufgabe der CVCA-eID ist die Berechtigung von DVs zur Vergabe von Terminal-Zertifikaten durch das Ausstellen eines DV-Zertifikats. Innerhalb des DV-Zertifikats ist definiert, welche Zugriffsrechte der DV mit der Vergabe seiner Terminal-Zertifikate einräumen darf und für welchen Zeitraum der DV zum Ausstellen berechtigt ist. Neben der Ausgabe von DV-Zertifikaten (C_{DV}) stellt die CVCA als Root selbst-signierte CVCA-Zertifikate (C_{CVCA}) und CVCA-Link-Zertifikate (Link-C_{CVCA}) aus.

Document Verifier (DV)-Bereich

Grundsätzlich wird im DV-Bereich zwischen hoheitlicher und nicht hoheitlicher Verwendung unterschieden [TR-03128].

Hoheitlicher DV-Bereich

Die Document Verifier im hoheitlichen Bereich werden von oder im Auftrag der öffentlichen Verwaltung betrieben und stellen ausschließlich Zertifikate für Ausweis- und Kontrollbehörden hinsichtlich folgender Nutzungsszenarien aus:

- Qualitätssicherung bei der Ausgabe des Ausweises
- Auskunftsbegehren des Bürgers
- Änderungen der Daten der eID-Funktion auf einem ePA-Chip

Eine Besonderheit des hoheitlichen Document Verifiers ist, das dieser auch Zertifikate ausstellen kann, die Schreibrechte auf die eID-Anwendung gewähren, bspw. zur Realisierung der Adressänderungen in den Ausweisbehörden.

Aufgabe eines hoheitlichen Document Verifiers ist die Prüfung der eingehenden Zertifikatsanträge (Registration Authority) und das Ausstellen der Terminal-Zertifikate (Certification Authority) $C_{Terminal}$.

Eine detaillierte Beschreibung, der von hoheitlichen Document Verifier zu erfüllenden Anforderungen ist in [TR-03128] zu finden.

Nicht hoheitlicher DV-Bereich

Der Document Verifier im nicht hoheitlichen Bereich stellt Zertifikate für

- eBusiness- und
- eGoverment-Diensteanbieter

zum Zugriff auf die eID-Funktion des ePA aus. Hierbei strukturiert sich der DV in eine „Vergabestelle für Berechtigungszertifikate, VfB“ (Registration Authority), und eine oder mehrere Dienstleister als zugehöriger Zertifizierungsdienst (Certification Authority), die „Berechtigungs-CA(s), BerCA(s)“ genannt werden.

Die Aufgaben der **VfB** (Registration Authority) lauten:

- Entgegennahme Anzeige geeigneter Zertifizierungsdienstleister (BerCAs)
  - Die BerCAs erhalten ein DV-Zertifikat von der CVCA-eID ausschließlich nach Erfüllung der im vorliegenden Dokument und der [TR-03128] enthaltenen Anforderungen.
  - Auf Basis des DV-Zertifikats stellen die BerCAs die Terminal-Zertifikate für die Diensteanbieter aus, die von der VfB bestätigt wurden.
- die Bestätigung geeigneter Diensteanbieter.
  - die Erteilung und Aufhebung von Berechtigungen zur Abfrage von Daten des elektronischen Personalausweises über die eID-Funktion für Diensteanbieter.
  - Die Entscheidungen der VfB werden von den BerCAs durch das Aus- oder Nichtausstellen von Terminal-Zertifikaten mit spezifischen Zugriffsrechten umgesetzt.

Die VfB nimmt technisch keine Zertifikats-Request entgegen. Diese gehen abhängig vom Antragssteller (BerCA oder Diensteanbieter) an die jeweils zuständige PKI-Instanz.

Aufgabe der **BerCAs** (Certification Authority) ist die Annahme von Zertifikats-Requests und das Ausstellen von Berechtigungszertifikaten (Terminal-Zertifikaten) für Diensteanbieter nach deren erfolgreicher Bestätigung durch die VfB. Stellvertretend für einen Diensteanbieter kann auch ein von ihm beauftragter eID-Service-Provider nach erfolgreicher Bestätigung des Diensteanbieters durch die VfB von einer BerCA zertifiziert werden, um in seinem Auftrag die technische Realisierung der eID-Authentisierung durchzuführen.

Eine detaillierte Beschreibung, der von nicht hoheitlichen Document Verifier zu erfüllenden Anforderungen ist in [TR-03128] geben.

Terminal-Bereich

Die Unterscheidung zwischen hoheitlicher und nicht hoheitlicher Verwendung setzt sich durch die unterschiedliche Bezugsquelle der Terminal-Zertifikate im Terminal-Bereich fort.

Hoheitliche Terminals

beziehen die Terminal-Zertifikate von einem hoheitlichen DV. In der Regel werden im hoheitlichen Bereich von den Ausweis- und Kontrollbehörden Spezialgeräte zum Zugriff auf den ePA verwendet. Zur Realisierung der Visualisierung und des Änderungsdienstes (schreibender Zugriff) in den Ausweisbehörden, werden sogenannte EAC-Boxen nach [TR-03131] verwendet.

Nicht hoheitliche Terminals

beziehen die Terminal-Zertifikate von einer BerCA.

Im nicht hoheitlichen Bereich kommen zur Nutzung der eID-Anwendungen grundsätzlich zwei verschiedene Realisierungsformen von Terminals zum Einsatz, welche in der nachfolgenden Abbildung dargestellt sind:

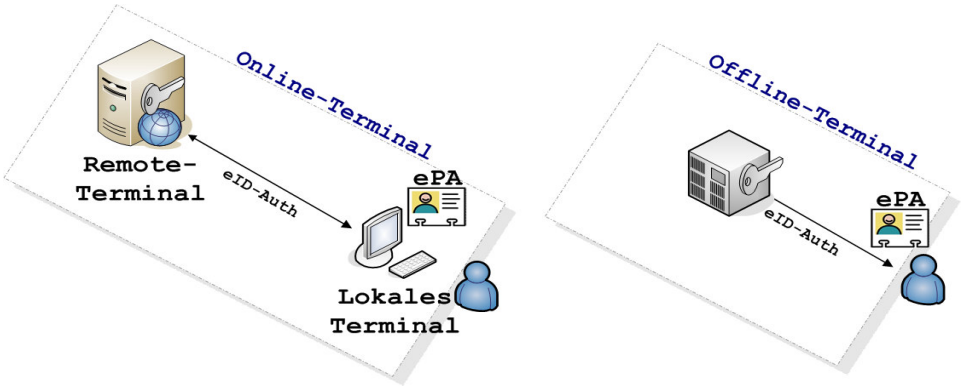


Abbildung 2: Terminal-Gerätetypen (On-/Offline-Terminal)

- **Online Terminals** bestehen aus zwei Terminal-Typen:
  - **Remote Terminal**: Das Remote-Terminal (zu verstehen als Web-Anwendung) wird auf einem Web-Server betrieben, welcher über einen integrierten Terminal-Schlüssel sowie eine zugehörige EAC-Zertifikatskette verfügt. Vom Remote-Terminal werden dem lokalen Lesegerät die EAC-Zertifikatskette sowie die über die vom ePA-Chip angeforderte Challenge erforderliche Signatur zum Nachweis der Berechtigung zur Verfügung gestellt. Dies geschieht typischerweise über eine online Verbindung.
  - **Local Terminal**: Demgegenüber besteht das lokale Terminal als vorgelagerte Stelle aus einem Lesegerät und einem privat genutzten IT-System mit der speziellen Vermittlungssoftware, welche zwischen dem RF-Chip im ePA und dem Remote-Terminal eine Verbindung etabliert. Ein Zugriff auf die eID-Daten erhält letztendlich nur das Remote-Lesegerät.
- **Offline Terminals** (bspw. alleinstehende Verkaufsautomaten) sind vollständig in sich gekapselte Geräte. Diese Geräte verfügen über einen integrierten Terminal-Schlüssel und die zugehörige vollständige EAC-Zertifikatskette und können somit selbstständig die eID-Authentisierung mit einem ePA durchführen.

Die Authentisierungsprotokolle der Terminals sind in der [TR-03110] spezifiziert.

1.2 Name und Identifizierung des Dokuments

Dieses Dokument ist die Certificate Policy (CP) der deutschen Country Verifying Certificate Authority - electronic Identity (CVCA-eID).

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat diesem CP/CPS folgenden Object Identifier (OID) zugeordnet: `0.4.0.127.0.7.3.1.1.2.2`.

Dieses Dokument kann unter https://www.bsi.bund.de/cvca-eID bezogen werden.

Identifikator	Wert
Titel	Certificate Policy für die eID-Anwendung des ePA (CP CVCA-eID)
Version	1.29
OID	0.4.0.127.0.7.3.1.1.2.2

Tabelle 1: Identifikation des Dokuments

1.3 PKI-Teilnehmer

In diesem Unterkapitel werden die Teilnehmer (Zertifizierungsstellen, Registrierungsstellen, Zertifikatsnehmer und Zertifikatsnutzer), der CVCA-eID PKI aufgeführt. Die nachfolgende Tabelle zeigt einen Überblick über die PKI-Teilnehmer:

Instanz der PKI	Zert.-Stelle	Reg.-Stelle	Zert.-Nehmer	Zert.-Nutzer
CVCA-eID	■	■	■	■
DV	■	■	■	■
Terminal			■	■
ePA				■

Tabelle 2: Übersicht der PKI-Teilnehmer

1.3.1 Zertifizierungsstellen

Zertifizierungsstellen (Certification Authority, CA), welche die Anforderungen dieser Certificate Policy erfüllen, stellen Zertifikate für den Zugriff auf die eID-Anwendung des elektronischen Personalausweises aus.

Die **Country Verifying Certification Authority – electronic Identity (CVCA-eID)** bildet den nationalen Vertrauensanker (Root) der CVCA-eID PKI für die Berechtigung zum Zugriff auf die eID-Funktion des ePA. Folgende Zertifikate werden von der CVCA-eID ausgestellt:

- selbst-signierte CVCA-Zertifikate (C_{CVCA}),
- DV-Zertifikate (C_{DV}) sowie
- CVCA-Linkzertifikate (Link-C_{CVCA})

Die **Document Verifying Certification Authority** (DVCA), auch als **Document Verifier** (DV) oder bei nicht-hoheitlicher Tätigkeit als **Berechtigungs-CA** (BerCA) bezeichnet, ist eine organisatorische Einheit, welche einen Verbund von Terminals und Dienstleistern betreut, die als teilnehmendes Terminal eingestuft werden. Der DV ist von der CVCA-eID zur Ausgabe von Berechtigungszertifikaten (Terminal-Zertifikate) für Terminals autorisiert. Sowohl die Zugriffsrechte als auch die Gültigkeitsdauer der ausgestellten Zertifikate werden vom DV auf Basis der Entscheidung der VfB (nicht hoheitliche Verwendung) und den Anforderungen dieser CP definiert.

Von einem DV ausgestellte Zertifikate:

- Berechtigungszertifikate ($C_{Terminal}$)

Die folgende Tabelle enthält eine Übersicht der CVCA-eID PKI mit deren CAs und der hiervon ausgestellten Zertifikate.

PKI-Instanz	Zertifizierungsstelle	Auszustellende Zertifikate
CVCA-eID	CVCA-eID-CA	C_{CVCA}, Link-C_{CVCA}, C_{DV}
DV	DVCA	$C_{Terminal}$
Terminal	keine	keine
ePA	keine	keine

Tabelle 3: Certificate Authorities (CAs) der CVCA-eID PKI

1.3.2 Registrierungsstellen

Registrierungsstellen (Registration Authority, RA) führen vor der Ausstellung eines Zertifikats die zweifelsfreie Identifizierung und Authentifizierung des Antragstellers durch.

Die Registrierungsstelle der CVCA-eID bildet die CVCA-eID RA. Diese ist für die Bearbeitung der initialen Registrierungen sowie der möglichen Wiederholungsanträge von Document Verifiern zuständig.

Eine Registrierungsstelle der DVCA (Document Verifying Registration Authority, DVRA), bei nicht-hoheitlicher Tätigkeit auch als **Vergabestelle für Berechtigungszertifikate (VfB)** bezeichnet, ist hingegen für die Bearbeitung der initialen Registrierung sowie der möglichen Wiederholungsanträge von Terminals bzw. Diensteanbietern zuständig.

Die Kommunikation zwischen Zertifizierungs- und Registrierungsstellen muss durch angemessene Maßnahmen abgesichert werden.

PKI-Instanz	Registrierungsstellen	Eingehende Anträge
CVCA-eID	CVCA-eID-RA	Initialer C_{DV} Request Wiederhol. C_{DV} Request
DV hoheitlich	DVRA	Initialer $C_{Terminal}$ Request Wiederhol $C_{Terminal}$ Request
DV nicht hoheitlich	VfB	Initialer $C_{Terminal}$ Request Wiederhol $C_{Terminal}$ Request
Terminal	keine	keine
ePA	keine	keine

Tabelle 4: Registration Authorities (RAs) der CVCA-eID PKI

1.3.3 Zertifikatsnehmer

Zertifikatsnehmer sind CVCA-eID, die Document Verifier und Terminals.

Als Vertrauensanker stellt sich die CVCA-eID ein selbst-signiertes Zertifikat aus.

Für die Ausstellung von Zertifikaten zum Zugriff auf die eID-Anwendung für Terminals benötigt ein Document Verifier die Berechtigung durch die CVCA-eID. Diese stellt dem DV hierfür ein DV-Zertifikat aus.

Damit ein Terminal Zugriff auf die Daten eines elektronischen Personalausweises erhält, muss es hierzu über die Terminal Authentication [TR-03110] seine Berechtigung nachweisen. Diese Berechtigung wird in von einem DV ausgestellten Terminal-Zertifikat festgehalten und bestätigt.

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer sind alle Einheiten, welche auf den Vertrauensanker der CVCA-eID zurückgreifen, um Zertifikate der PKI zur Überprüfung von Berechtigungen zu verwenden.

Somit existieren die folgenden Zertifikatsnutzer in der CVCA-eID PKI:

- CVCA-eID, überprüft die Signatur der Wiederholungsanträge der DV,
- Document Verifier, überprüfen die Signatur der Wiederholungsanträge der Diensteanbieter, sowie
- elektronische Personalausweise, überprüfen die Zertifikatskette zur Bestätigung der Zugriffsberechtigung eines Terminals.

1.3.5 Andere Teilnehmer

Teilnehmer, welche keine Verpflichtungen im Rahmen dieser Certificate Policy eingegangen sind, sind nicht Bestandteil der Policy und werden daher nicht weiter berücksichtigt. Ergeben sich beispielsweise durch die internationale Anbindung von Terminals weitere Teilnehmer, so dürfen weder deren Rollen noch deren Interaktionen gegen die Sicherheitsanforderungen dieser Policy verstoßen.

1.4 Verwendung von Zertifikaten

In diesem Abschnitt wird die erlaubte und verbotene Verwendung von Zertifikaten in der CVCA-eID PKI definiert.

1.4.1 Erlaubte Verwendung von Zertifikaten

Schlüssel bzw. Zertifikate können von Zertifikatsnehmern zur Authentisierung sowie zur Erzeugung von elektronischen Signaturen verwendet werden.

Zertifikatsnutzer können Schlüssel bzw. Zertifikate zur Validierung von Authentisierungen und elektronischen Signaturen verwenden.

Daraus ergeben sich die folgenden Verwendungszwecke:

Zertifikat	Verwendungszweck und Eigenschaften
C_{CVCA}	- Vertrauensanker der PKI. Der zugehörige öffentliche Schlüssel wird zur Überprüfung von Zertifikatsketten benötigt und daher bei der Produktion im ePA gespeichert. - Mit dem privaten Schlüssel werden das initiale C_{CVCA}, die nachfolgenden Link-C_{CVCA} sowie alle C_{DV} signiert.
Link-C_{CVCA}	- Mit dem privaten Schlüssel des zuletzt gültigen C_{CVCA} oder Link-C_{CVCA} signiert. - Aktualisiert den Vertrauensanker eines elektronischen Personalausweises.
C_{DV}	- Der zugehörige öffentliche Schlüssel wird zur Überprüfung von Zertifikatsketten benötigt. - Mit dem privaten Schlüssel werden Wiederholungsanträge signiert. - Mit dem privaten Schlüssel werden $C_{Terminal}$ signiert.
$C_{Terminal}$	- Der zugehörige öffentliche Schlüssel wird zur Überprüfung von Zertifikatsketten benötigt. - Mit dem privaten Schlüssel werden Wiederholungsanträge signiert. - Mit dem privaten Schlüssel wird im Rahmen der Authentisierung gegenüber dem ePA eine Signatur erzeugt (siehe EAC-Protokollbeschreibung in [TR-03110]).

Tabelle 5: Erlaubter Verwendungszweck von Zertifikaten und zugehöriger privater Schlüssel

Hinweis: Berechtigungszertifikate werden im nachfolgenden Text gemäß deren technischer Funktion als Terminal-Zertifikate ($C_{Terminal}$) bezeichnet.

1.4.2 Verbotene Verwendung von Zertifikaten

Die Zertifikate dürfen ausschließlich gemäß ihres Verwendungszwecks (siehe Abschnitt 1.4.1) eingesetzt werden.

1.5 Administration der Policy

Die für dieses Dokument verantwortliche Organisation ist das Bundesamt für Sicherheit in der Informationstechnik (BSI). Das BSI kann über folgende Adresse kontaktiert werden:

Organisation	Bundesamt für Sicherheit in der Informationstechnik
Einheit	Referat 312 „Hoheitliche Dokumente und elektronische Ausweise“
Adresse	Godesberger Allee 185-189 53175 Bonn
Fax	+49 228 9582 55722
E-Mail	cvca-eID@bsi.bund.de
Webseite	https://www.bsi.bund.de/cvca-eID

Tabelle 6: Kontaktadresse

1.5.1 Pflege der Certificate Policy

Jede aktualisierte Version der Certificate Policy wird den Anwendern unverzüglich über die Internetseite des BSI (siehe Abschnitt 1.5) zur Verfügung gestellt.

1.5.2 Zuständigkeit für das Dokument

Zuständig für Erweiterung und oder nachträgliche Änderungen dieser CP ist das BSI.

1.5.3 Ansprechpartner / Kontaktperson

Siehe Abschnitt 1.5.

1.5.4 Zuständiger für die Anerkennung eines CPS

Das CPS ist ein internes Dokument. Dieses KANN aber bei Prüfungen herangezogen werden (siehe Abschnitt 8.1).

1.5.5 CPS-Aufnahmeverfahren

Das CPS MUSS die Anforderungen dieser CP umsetzen.

2 Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

2.1 Verzeichnisse

CVCA-eID

Das BSI betreibt ein zentrales Verzeichnis, das **CVCA-eID PKD,** als Bestandteil der CA. In diesem Verzeichnis werden alle produzierten Zertifikate gespeichert. Es beinhaltet:

- C_{CVCA} / Link-C_{CVCA}
- C_{DV}

DV-Ebene

Die Document Verifier MÜSSEN jeweils ein Verzeichnis mit Einträgen zu den von ihnen verwalteten Terminals und den hierzu ausgestellten Zertifikaten einrichten. Diese Verzeichnisse werden im Sinne einer Bestandsführung und eines Archivs geführt und sind kontinuierlich zu pflegen (siehe [TR-03128]).

Das Verzeichnis der CVCA-eID sowie die Verzeichnisse der DVs sind nicht öffentlich.

Die einzuhaltenden Aufbewahrungszeiten von Zertifikaten sind in Abschnitt 6.3.1 definiert.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

CVCA-eID

Folgende Informationen MÜSSEN durch die CVCA-eID auf der **BSI CVCA-eID Webseite** (https://www.bsi.bund.de/cvca-eID) veröffentlicht werden:

- CVCA-eID PKI Certificate Policy
- Verlinkung auf die mit dieser Policy in Verbindung stehenden technischen Richtlinien.
- Informationen zur Kommunikationsverbindung zum SPOC
- Zertifikate (siehe Abschnitt 4.4.1).

Das Certificate Practice Statement (CPS) der CVCA-eID wird nicht veröffentlicht.

DV-Ebene

Die Veröffentlichung der für den Betrieb der DV erforderlichen Dokumente, beschrieben in [SigG, SigV] und [TR-03128] liegt in der Entscheidung des DV.

Die Ausnahme bildet die **DV Certificate Policy** (siehe Abschnitt 5.1.2). Diese MUSS veröffentlicht werden.

2.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

CVCA-eID

Die CVCA-eID MUSS zu jeder Zeit alle weiteren für die eID-Authentisierung (siehe [TR-03110]) erforderlichen Root-Zertifikate (C_{CVCA}, Link-C_{CVCA}) bereitstellen. Dies erfolgt über die Kommunikationsschnittstelle gemäß [TR-03129] sowie über die BSI-Webseite.

Bei Änderungen an dieser CP MUSS die aktualisierte CP auf der BSI-CVCA-eID Webseite veröffentlicht werden.

DV-Ebene

Ein Document Verifier MUSS dem Terminalbetreiber zu jeder Zeit alle weiteren für die eID-Authentisierung (siehe [TR-03110]) erforderlichen Zertifikate (C_{CVCA}, Link- C_{CVCA}, C_{DV}, C_{CSCA} und CRL) bereitstellen. Dies erfolgt über die Kommunikationsschnittstelle gemäß [TR-03129].

Eine geänderte DV CP MUSS veröffentlicht werden und MUSS weiterhin die Anforderungen der CVCA-eID CP übernehmen (siehe Abschnitt 2.2).

2.4 Zugriffskontrollen auf Verzeichnisse

Die CVCA-eID und die Document Verifier MÜSSEN durch geeignete organisatorische und technische Maßnahmen sicherstellen, dass die Vertraulichkeit und Integrität der Informationen in ihren Verzeichnissen gewahrt bleibt.

3 Identifizierung und Authentifizierung

Dieses Kapitel beschreibt die durchzuführenden Prozeduren, um die Identität und Berechtigung eines Antragsstellers bei der **CVCA-eID**, **DVRA** oder **VfB** vor dem Ausstellen eines Zertifikats festzustellen.

Das allgemeine Profil eines Zertifikats-Requests MUSS konform zu [TR-03110] sein.

3.1 Regeln für die Namensgebung

Der Bezeichner eines Zertifikats der CVCA-eID-PKI MUSS dem Profil in [TR-03110] entsprechen und wird im Feld `Certificate Holder Reference` angegeben.

3.1.1 Arten von Namen

In diesem Abschnitt werden die Inhalte für die Bezeichner im Feld `Certificate Holder Reference(CHR)` der verschiedenen CV-Zertifikate der CVCA-eID PKI spezifiziert.

CVCA-Zertifikat

Das Feld `Certificate Holder Reference` MUSS aus den folgenden verketteten Elementen bestehen.

Certificate Holder Reference		
Ländercode	Besitzerkürzel	Seriennummer
DE	CVCAeID	<SN>

Tabelle 7: Belegung CHR-Feld der CVCA-Zertifikate

Nachfolgend die Erläuterung des durch den Antragssteller zu definierenden Anteils:

Variabler Anteil	**Zeichen**	**Codierung**	**Inhalt**
<SN>	5 Zeichen	ISO/IEC 8859-1	Fortlaufende Seriennummer (00001 bis 99999). Bei Überlauf Neubeginn bei 00001

Tabelle 8: Belegung CHR-Feld der CVCA-Zertifikate / Anteil Antragsteller

Hoheitlicher Bereich

Hoheitliches DV-Zertifikat

Das Feld `Certificate Holder Reference` MUSS aus den folgenden verketteten Elementen bestehen.

Certificate Holder Reference		
Ländercode	Besitzerkürzel	Seriennummer
DE	DVeID<Betreiberkürzel>	<SN>

Tabelle 9: Belegung CHR-Feld des hoheitlichen DV-Zertifikats

Nachfolgend die Erläuterung des durch den Antragssteller zu definierenden Anteils:

Variabler Anteil	**Zeichen**	**Codierung**	**Inhalt**
<Betreiberkürzel>	2-4 Zeichen	ISO/IEC 8859-1	Name des Betreibers des hoheitlichen DVs
<SN>	5 Zeichen	ISO/IEC 8859-1	Fortlaufende Seriennummer (00001 bis 99999).

Tabelle 10: Belegung CHR-Feld des hoheitlichen DV-Zertifikats / Anteil Antragsteller

Ein Betreiberkürzel MUSS den Betreiber des hoheitlichen DVs eindeutig identifizieren. Sollten zwei oder mehr DVs das gleiche Besitzerkürzel anstreben, so erhält der DV das Besitzerkürzel, der als Erstes einen entsprechend gültigen Zertifikats-Request der CVCA-RA zustellt.

Hoheitliches Terminal-Zertifikat

Ein Terminal-Zertifikat MUSS immer eindeutig über die Kombination der Werte der beiden folgenden Zertifikatsfelder identifizierbar sein (siehe [TR-03110]):

- `Certification Authority Reference (CAR)`
  - Der Wert des CAR-Feldes MUSS dem des CHR-Feldes aus dem DV-Zertifikat des hoheitlichen DVs entsprechen.
- `Certificate Holder Reference (CHR)`
  - Der gesamte Inhalt des Feldes `Certificate Holder Reference (CHR)` wird vom ausstellenden DV selbst bestimmt, unter Berücksichtigung der Anforderungen aus [TR-03110]

Nicht hoheitlicher Bereich

Nicht hoheitliches DV-Zertifikat

Das Feld `Certificate Holder Reference` MUSS aus den folgenden verketteten Elementen bestehen.

Certificate Holder Reference		
Ländercode	Besitzerkürzel	Seriennummer
DE	DVeID<Betreiberkürzel>	<SN>

Tabelle 11: Belegung CHR-Feld des nicht hoheitlichen DV-Zertifikats

Nachfolgend die Erläuterung des durch den Antragssteller zu definierenden Anteils:

Variabler Anteil	**Zeichen**	**Codierung**	**Inhalt**
<Betreiberkürzel>	2-4 Zeichen	ISO/IEC 8859-1	Name des Betreibers des nicht hoheitlichen DVs
<SN>	5 Zeichen	ISO/IEC 8859-1	Aufsteigende Seriennummer (00001 bis 99999).

Tabelle 12: Belegung CHR-Feld des nicht hoheitlichen DV-Zertifikats / Anteil Antragsteller

Ein Betreiberkürzel MUSS den Betreiber des hoheitlichen DVs eindeutig identifizieren. Sollten zwei oder mehr DVs das gleiche Besitzerkürzel anstreben, so erhält der DV das Besitzerkürzel, der als Erstes einen entsprechend gültigen Zertifikats-Request der CVCA-RA zustellt.

Nicht hoheitliches Terminal-Zertifikat

Ein Terminal-Zertifikat MUSS immer eindeutig über die Kombination der Werte der beiden folgenden Zertifikatsfelder identifizierbar sein (siehe [TR-03110]):

- `Certification Authority Reference (CAR)`
  - Der Wert des CAR-Feldes MUSS dem des CHR-Feldes aus dem DV-Zertifikat des nicht hoheitlichen DVs entsprechen.
- `Certificate Holder Reference (CHR)`
  - Der gesamte Inhalt des Feldes `Certificate Holder Reference (CHR)` wird von der ausstellenden BerCA selbst bestimmt, unter Berücksichtigung der Anforderungen aus [TR-03110]

3.1.2 Notwendigkeit für aussagefähige Namen

Der Bezeichner im Feld `Certificate Holder Reference` MUSS den Zertifikatsnehmer eindeutig identifizieren.

3.1.3 Anonymität oder Pseudonyme von Zertifikatsnehmern

Anonymität oder Pseudonymität des Zertifikatsnehmers ist nicht erlaubt.

3.1.4 Interpretationsregeln für verschiedene Namensformen

Der Bezeichner im Feld `Certificate Holder Reference` MUSS für die Zertifizierungsstelle eindeutig sein.

3.1.5 Eindeutigkeit von Namen

Der Wert des Feldes `Certificate Holder Reference` MUSS den Zertifikatsnehmer bei seiner Zertifizierungsstelle eindeutig identifizieren.

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

Entfällt.

3.2 Initiale Überprüfung der Identität

Dieser Abschnitt enthält Informationen über die Identifizierungs- und Authentifizierungsprozeduren für den initialen Zertifikatsantrag des Zertifikatsnehmers.

Bestandteil dieser Prozeduren sind auch die Prüfungen nach den Anforderungen aus Abschnitt 8.1.

Auf der **Root-Ebene** wird das Ausstellen des selbst-signierten CVCA- und von CVCA-Link Zertifikaten nicht betrachtet, da die CVCA-eID RA und CVCA-eID CA eine organisatorische Einheit, die CVCA-eID, bilden. Somit ist eine Identifizierung und Authentifizierung auf Root-Ebene gegeben.

3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Zum Nachweis des Besitzes des privaten Schlüssels MUSS der Zertifikats-Request gemäß [TR-03110] eine sogenannte innere Signatur beinhalten.

Hierdurch MUSS bei der Antragsprüfung durch Verifikation der inneren Signatur mit dem im Zertifikats-Request enthaltenden zugehörigen öffentlichen Schlüssel nachgewiesen werden, dass der Antragsteller im Besitz des privaten Schlüssels ist.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Die nachfolgenden Organisationen DÜRFEN innerhalb der CVCA-eID PKI Zertifikatsanträge stellen. Hierbei wird speziell zwischen dem hoheitlichen und dem nicht hoheitlichen Bereich unterschieden. Die in diesem Abschnitt beschriebenen Anforderungen und Abläufe gelten für die **initiale** Identifizierung und Authentifizierung von Zertifikatsanträgen.

Die in dieser CP speziell in diesem Abschnitt angeführten Kommunikationszertifikate zur Absicherung der Kommunikationsverbindung zwischen den PKI-Instanzen MÜSSEN vergleichbar mit dem Sicherheitsniveau der V-PKI [CP V-PKI] sein. Jeder Teilnehmer der CVCA-eID PKI MUSS mindestens eine Kommunikationsschnittstelle nach [TR-03129] besitzen, die über Kommunikationszertifikate zur Authentisierung verfügen MUSS.

Hoheitlicher Bereich

Hoheitlicher DV

Zur initialen Identifizierung und Authentifizierung eines hoheitlichen Document Verifiers durch die CVCA-eID RA MUSS ein bevollmächtigter Vertreter des Betreibers persönlich erscheinen.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Zertifizierung durch die CVCA-eID mit
  - Name der einsetzenden Behörde und
  - Kontaktdaten der Ansprechpartner.
- Vertretungsvollmacht
- Bestätigung der hoheitlichen Verwendung des DVs.
  - MUSS von der obersten Bundes- oder Landesbehörde ausgestellt werden und mit dem Dienstsiegel versehen sein.
- Certificate Policy des hoheitlichen DVs
  - MUSS die Anforderungen aus der CVCA-eID CP berücksichtigen.
- Vereinbarung mit der CVCA-eID, beinhaltet die
  - Erklärung der Einhaltung der Anforderungen der CVCA-eID.
- Bestätigung der erfolgreichen Testzertifizierung
  - Vor der initialen Identifizierung und Authentifizierung MUSS die Zertifikatsausstellung von der CVCA-eID zum hoheitlichen DV im Rahmen einer Testzertifizierung erfolgreich erprobt worden sein.
  - Die Testzertifizierung erfolgt auf Basis von Testschlüsseln unter Einhaltung der Anforderungen an den Wirkbetrieb aus [TR-03128] und dieser Certificate Policy.
  - Die verwendeten Testschlüssel (CVCA-eID / hoh. DV) werden ausschließlich für den Testbetrieb erzeugt und DÜRFEN NICHT in den Wirkbetrieb zur Kommunikation mit elektronischen Personalausweisen überführt werden.

- Kommunikationszertifikate (inklusive der zur Verifikation erforderlichen Zertifikatskette).
- Initialer Zertifikats-Request (Initialer C_{DV} Request, gemäß [TR-03110])
  - KANN vom DV, nach der Einrichtung des sicheren SSL-Kanals, direkt an die CVCA-eID gesendet werden.
  - EMPFOHLEN wird die Übergabe des Zertifikats-Requests durch den bevollmächtigten Vertreter.

Sollte ein privatwirtschaftlicher Dienstleister für den Betrieb des hoheitlichen Document Verifiers **beauftragt** werden, MUSS zusätzlich zu den genannten Unterlagen der CVCA-eID RA eine schriftliche Bestätigung durch den Auftraggeber mit Benennung der autorisierten Ansprechpartner vorgelegt werden.

Hoheitliche Terminals

Der hoheitliche DV verantwortet den Einsatz der Terminals in seinem Zuständigkeitsbereich, indem dieser berechtigten Terminals Terminal-Zertifikate ausstellt. Somit MUSS der hoheitliche DV die Zertifikatsanträge der Terminals prüfen. Des Weiteren MUSS dieser ein **Bestandsverzeichnis** aller von ihm verwalteten Terminals und der zugehörigen Zertifikate führen.

Zur Identifizierung und Authentifizierung eines Terminals MUSS dessen Betreiber bei der hoheitlichen DVRA folgende Unterlagen und Daten einreichen:

- Antragsschreiben zur Zertifizierung durch den hoheitlichen DV, beinhaltet:
  - Name der einsetzenden Behörde
  - Kontaktdaten der Ansprechpartner
- Technische Beschreibung des Terminals, beinhaltet:
  - Hersteller und Modellbezeichnung
  - Informationen zum Kryptografiemodul, inwiefern dies hinsichtlich Sicherheitseigenschaften geprüft wurde, bspw. Common Criteria Zertifizierung.
  - Eindeutige Kennung des Terminals
  - Einsatzort
- Kommunikationszertifikate (inklusive der zur Verifikation erforderlichen Zertifikatskette).
- Initialer Zertifikats-Request (Initialer $C_{Terminal}$, gemäß [TR-03110])
  - Wird vom Terminal direkt an den DV gesendet, nachdem der sichere SSL-Kanal durch Registrieren der Kommunikationszertifikate durch die hoheitlichen DVRA eingerichtet wurde. Die Kommunikation mit dem DV MUSS gemäß [TR-03129] erfolgen.

Die Registrierungsinformation aus den Unterlagen des Terminalbetreibers MÜSSEN vom DV in dessen Bestandsverzeichnis vor dem Ausstellen eines Zertifikats für ein Terminal erfasst werden.

Sonderfall: Visualisierung / Änderungsdienst durch **EAC-Boxen**

EAC-Boxen dienen zur Realisierung der Visualisierung und des Änderungsdiensts in **Ausweisbehörden**. Daher werden diese Geräte ausschließlich an authentifizierte Ausweisbehörden (organisatorische Authentifizierungsprozeduren beinhaltet Antragsschreiben mit Dienstsiegel der Ausweisbehörde) ausgeliefert.

Bei der Produktion einer EAC-Box wird diese mit einem privaten Schlüssel versehen ($SKey_{EAC\text{-}Box}$) zur Signatur des initialen Zertifikats-Request. Der zugehörige öffentliche Schlüssel ($PKey_{EAC\text{-}Box}$) wird im Bestandsverzeichnis des zuständigen hoheitlichen DVs unter der vorgesehenen Ausweisbehörde registriert. Zusätzlich werden Kommunikationszertifikate für eine sichere Kommunikation hinterlegt und an die Ausweisbehörde ausgeliefert.

Die Identifizierung und Authentifizierung eines initialen Zertifikats-Request durch den hoheitlichen DV erfolgt dann wie folgt:

- Die SSL-Verbindung zum hoheitlichen DV MUSS mittels der hinterlegten Kommunikationszertifikate authentisiert werden.
- Der Zertifikats-Request MUSS mit $SKey_{EAC\text{-}Box}$ signiert sein. Die Prüfung erfolgt mit $PKey_{EAC\text{-}Box}$ aus dem Verzeichnisdienst des hoheitlichen DV der unter der entsprechenden Ausweisbehörde registriert sein MUSS.
- Der Wert des Felds `Certificate Holder Reference` MUSS dem vom hoheitlichen DV vorgegebenen Namensschema entsprechen.

<u>Nicht hoheitlicher Bereich</u>

BerCA

Zur initialen Identifizierung und Authentifizierung einer BerCA durch die CVCA-eID RA MUSS ein bevollmächtigter Vertreter der BerCA persönlich erscheinen.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antrag auf Zertifizierung durch die CVCA-eID mit
  - Name der Organisation und
  - Kontaktdaten der Ansprechpartner
- Vertretungsvollmacht
- Mitteilung der VfB über die Anzeige [BVA01]
- DV Certificate Policy der BerCA
  - MUSS die Anforderungen aus der CVCA-eID CP berücksichtigen.
- Vereinbarung mit der Root CVCA-eID, beinhaltet die
  - Erklärung der Einhaltung der Anforderungen der CVCA-eID.
- Bestätigung der erfolgreichen Testzertifizierung durch die CVCA-eID nach den Anforderungen aus [TR-03128].
- Kommunikationszertifikate (inklusive der zur Verifikation erforderlichen Zertifikatskette).
- Initialer Zertifikats-Request (Initialer C_{DV} Request, gemäß [TR-03110])

- KANN von der BerCA, nach Einrichtung des sicheren SSL-Kanals, direkt an die CVCA-eID gesendet werden.
- EMPFOHLEN wird die Übergabe des Zertifikats-Requests durch den bevollmächtigten Vertreter.

Nach Ausstellen des initialen DV-Zertifikats für die BerCA MUSS die CVCA-eID die VfB über die Aufnahme des Wirkbetriebs informieren.

Diensteanbieter

Die initiale Identifizierung und Authentifizierung eines **Diensteanbieters**, zum Erhalt von Terminal-Zertifikaten von einer BerCA, erfolgt durch die **VfB** (siehe [TR-03128]).

Sollte der Diensteanbieter einen **eID-Service-Provider** zur Durchführung der eID-Authentisierung beauftragen, MUSS er dies ebenfalls schriftlich bei der VfB angeben.

Zur Authentisierung MUSS der Diensteanbieter ein Antragsverfahren gemäß [BVA02] erfolgreich durchlaufen. Der erfolgreiche Durchlauf MUSS der BerCA von der VfB auf elektronischem Wege mitgeteilt werden. Das Antragsverfahren beinhaltet insbesondere eine Prüfung des Unternehmens und seiner Tätigkeitsfelder sowie die Zuordnung zu einer Datenschutzbehörde.

Unabhängig von der Erteilung der notwendigen Berechtigung, durch die VfB MUSS der Diensteanbieter noch erfolgreich eine Testzertifizierung durch die BerCA auf Basis von Testschlüsseln unter Einhaltung der Anforderungen aus [TR-03128] und dieser Certificate Policy durchlaufen.

Nachdem die BerCA von der VfB über den erteilten Bescheid zum Diensteanbieter informiert wurde, MUSS der Diensteanbieter noch folgende Schritte durchführen, um ein Zertifikat erhalten zu können:

- Beantragung / Mitteilung von Kommunikationszertifikaten (inklusive der zur Verifikation erforderlichen Zertifikatskette).
  - Die Kommunikationszertifikate authentisieren den Diensteanbieter / eID-Service-Provider innerhalb der SSL-Verbindung mit der BerCA.
  - Die Kommunikationszertifikate KÖNNEN durch die BerCA vergeben oder vom Betreiber des Terminals erzeugt oder beschafft und bei der BerCA registriert werden.
  - Die BerCA MUSS die Echtheit der Kommunikationszertifikate des Diensteanbieters sorgfältig prüfen.
- Initialer Zertifikats-Request (Initialer $C_{Terminal}$, gemäß [TR-03110]) MUSS über die Schnittstelle der BerCA gemäß [TR-03129] zugestellt werden. Dabei MÜSSEN die vorher registrierten Kommunikationszertifikate genutzt werden.
  - Der Inhalt des Zertifikats-Requests (Initialer $C_{Terminal)}$ MUSS von der BerCA auf Basis der Bestätigung durch die VfB auf Korrektheit geprüft werden.
  - Die BerCA MUSS die VfB nach Ausstellen des Zertifikats (Initial $C_{Terminal}$) für den Dienstleister / eID-Service Provider über den hiermit verbundenen Beginn des Echtbetriebes informieren.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers

Ein Zertifikats-Request DARF NICHT von einer Einzelperson, sondern nur von einer Organisation gestellt werden.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Die Registrierungsstelle MUSS die Angaben zum Zertifikatsnehmer im Zertifikats-Request gegen die eingereichten Unterlagen auf Korrektheit prüfen (siehe Abschnitt 3.2.2).

3.2.5 Prüfung der Berechtigung zur Antragstellung

Siehe Abschnitt 3.2.

3.2.6 Kriterien für den Einsatz interoperierender Systeme/Einheiten

Entfällt.

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung

Nach der initialen Zertifikatsausstellung erfolgen sogenannte Wiederholungsanträge. Diese MÜSSEN ebenso wie die initialen Zertifikatsanträge (siehe Abschnitt 3.2) zweifelsfrei durch die Registrierungsstelle identifiziert und authentisiert werden.

Diese Certificate Policy unterscheidet zwei Arten von Wiederholungsanträgen:

- **Routinemäßige Wiederholungsanträge**: Der Antragssteller besitzt einen gültigen privaten Schlüssel dessen aktueller Einsatzzeitpunkt innerhalb des im zugehörigen Zertifikat definierten Gültigkeitszeitraums (d.h. zwischen den beiden Zeitpunkten definiert durch die Felder `Certificate Effective Date` und `Certificate Expiration Date`) liegt.
- **Nicht routinemäßige Wiederholungsanträge**: Der Antragssteller besitzt einen nicht mehr gültigen privaten Schlüssel dahingehend, dass dessen Einsatzzeitpunkt nicht innerhalb des im zugehörigen Zertifikat definierten Gültigkeitszeitraums (d.h. nicht zwischen den beiden Zeitpunkten definiert durch die Felder `Certificate Effective Date` und `Certificate Expiration Date`) liegt **oder** das sein Zertifikat von der übergeordneten Instanz für einen Wiederholungsantrag intern gesperrt wurde (interne Sperrliste).

Jede Certificate Authority der CVCA-eID PKI MUSS einen Sperrdienst (interne Sperrliste) betreiben, um nicht routinemäßige Wiederholungsanträge erkennen zu können.

3.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung

Routinemäßige Wiederholungsanträge MÜSSEN folgende Eigenschaften zur Identifizierung und Authentifizierung durch die Registrierungsstelle erfüllen:

- Zustellung über die in [TR-03129] definierten Kommunikationsprotokolle.
- Verbindungsauthentisierung über die bei der initialen Registrierung festgelegten Kommunikationszertifikate.
- Signatur des Zertifikats-Requests durch den Antragssteller mit einem noch gültigen bei der CA registrierten Schlüsselpaar (gemäß Profil [TR-03110]).
- Der Bezeichner des Zertifikats (Wert des CHR-Feldes) MUSS den Vorgaben entsprechen (siehe Abschnitt 3.1).

Die genannten Anforderungen MÜSSEN durch die Registrierungsstelle geprüft werden. Hierzu verfügt diese über geeignete Mechanismen.

Diensteanbieter / eID-Service Provider stellen ihre routinemäßigen Wiederholungsanträge direkt an die BerCA (technische Request Annahme), welche die entsprechenden Prüfungen durchführt.

3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen

Nach einem **nicht routinemäßigen Wiederholungsantrag** (siehe Einleitung 3.3) ist der Zertifikatsnehmer gesperrt. Der Bezug weiterer Zertifikate ist nicht möglich.

Um wieder Zertifikate erhalten zu können, MUSS der Zertifikatsnehmer die Gründe, warum kein routinemäßiger Wiederholungsantrag mehr durchgeführt wurde, melden (siehe Abschnitt 5.7). Danach MUSS der Zertifikatsnehmer einen neuen initialen Zertifikats-Request übermitteln.

Die Identifizierung und Authentifizierung des neuen initialen Zertifikats-Requests MUSS über die SSL-Verbindung zwischen den beiden PKI-Teilnehmern, mit den bei der initialen Registrierung festgelegten Kommunikationszertifikaten, erfolgen. Zusätzlich MUSS eine Prüfung des korrekten Fingerprints des neuen initialen Zertifikats-Requests durchgeführt werden. Die Übermittlung des Fingerprints MUSS über einen zur Internetverbindung unabhängigen Kommunikationskanal erfolgen, bspw. Telefon oder Fax.

Sollte der nicht routinemäßigen Wiederholungsantrag durch Probleme mit den Kommunikationszertifikaten des Zertifikatsnehmers begründet sein, so ist ein erneuter vertrauenswürdiger Austausch der Kommunikationszertifikate erforderlich.

3.4 Identifizierung und Authentifizierung von Anträgen auf Sperrung

Zertifikatsnehmer können sich selbst sperren, indem sie keinen routinemäßigen Wiederholungsantrag mehr stellen.

Sollte der Zertifikatsnehmer die Sperrung wieder aufheben wollen, MUSS der Grund für die Selbstsperrung gemeldet werden (siehe Abschnitt 5.7). Danach MUSS ein neuer initialer Zertifikats-Request übersendet werden (siehe Abschnitt 3.3.2).

4 Betriebsanforderungen für den Zertifikatslebenszyklus

In diesem Kapitel werden die Prozeduren und Verantwortlichkeiten für den Lebenszyklus von Zertifikaten definiert. Dies umfasst insbesondere folgende Bereiche:

- Zertifikatsbeantragung
- Verarbeitung von Zertifikatsanträgen
- Zertifikatsausstellung

4.1 Zertifikatsantrag

Zertifikatsanträge für CVCA-Zertifikate werden von der CVCA-eID selbst getätigt.

Ab der DV-Ebene gliedert sich die CVCA-eID PKI durch die beiden unterschiedlichen Aufgabenstellungen in einen **hoheitlichen** und einen **nicht hoheitlichen Bereich**.

Generell sind in beiden Bereichen die folgenden Prozesse zu unterscheiden:

- Beantragung eines DV-Zertifikats (C_{DV})
- Beantragung eines Terminal-Zertifikats ($C_{Terminal}$)

Hierbei ist hinsichtlich des Registrierungsdienstes zu berücksichtigen, ob es sich bei der Registrierung um einen initialen (Erstantrag) oder einen Wiederholungsantrag handelt.

4.1.1 Wer kann einen Zertifikatsantrag stellen?

Zertifikatsanträge MÜSSEN über die in Kapitel 3 definierten Prozesse gestellt werden. In den in diesem Abschnitt aufgeführten Tabellen wird dargestellt, welche Organisationen Zertifikatsanträge stellen dürfen. Zur Antragstellung berechtigte hoheitliche und nicht hoheitliche Document Verifier MÜSSEN alle Anforderungen gemäß [TR-03128] erfüllen.

Hoheitlicher Bereich

Im Falle hoheitlicher Aufgabenstellungen erfolgt die Beantragung eines DV-Zertifikats (C_{DV}) bei der CVCA-eID immer durch den hoheitlichen Betreiber selbst, d.h. sowohl bei einem Erst- als auch bei einem Wiederholungsantrag.

Der Document Verifier ist selbst Antragsteller und Verantwortlicher für den Betrieb der ihm zugeordneten Terminals. Deshalb werden die Terminal-Zertifikate ($C_{Terminal}$) mittels eines Zertifikats-Requests des Terminals bei dem Document Verifier beantragt. Im Falle eines initialen Requests wird das Terminal in die Bestandsführung des Document Verifiers übernommen. Ausgenommen EAC-Boxen, diese sind schon vorher im Bestandsverzeichnis registriert (siehe Abschnitt 3.2.2).

Berechtigte Organisationen	Zert-Typ	Erstantrag		Wiederholungsantrag	
		Technische Annahme Request	Identifikation und Authenfi-zierung	Technische Annahme Request	Identifikation und Authenfi-zierung
DV	C_{DV}	CVCA-eID RA	CVCA-eID RA	CVCA-eID RA	CVCA-eID RA
Terminalbetreiber	$C_{Terminal}$	DVRA	DVRA	DVRA	DVRA

Tabelle 13: Zur Zertifikatsantragsstellung berechtigte hoheitliche Organisationen

Nicht hoheitlicher Bereich

Die initiale Beantragung eines DV-Zertifikats (C_{DV}) erfolgt, nach eingereichter Anzeige bei der VfB, durch die BerCA direkt bei der CVCA-eID. Der technische Zertifikats-Request ist der CVCA-eID zuzustellen (siehe Abschnitt 3.2). Wiederholungsanträge werden ebenfalls direkt an die CVCA-eID gesendet.

Die initiale Beantragung eines Terminal-Zertifikats ($C_{Terminal}$) erfolgt durch den Diensteanbieter bei der VfB (Verwaltungsverfahren). Der technische Zertifikats-Request wird erteilter Berechtigung (Bescheid) direkt an die BerCA gesendet. Die BerCA wird von der VfB über einen positiven Bescheid an den DA informiert. Wiederholungsanträge werden direkt an die BerCA gesendet. Eine weitere Prüfung durch die VfB ist nicht erforderlich (siehe Abschnitt 3.3.1). Sofern ein eID-Service Anbieter Bestandteil des Szenarios ist, ist diese Instanz entsprechend zu berücksichtigen.

Berechtigte Organisationen	Zert-Typ	Erstantrag		Wiederholungsantrag	
		Technische Annahme Request	Identifikation und Authenfi-zierung	Technische Annahme Request	Identifikation und Authenfi-zierung
BerCA	C_{DV}	CVCA-eID RA	CVCA-eID RA	CVCA-eID RA	CVCA-eID RA
Diensteanbieter	$C_{Terminal}$	BerCA	VfB u. BerCA	BerCA	BerCA
eID-Service Provider (im Auftrag eines Diensteanbieters)	$C_{Terminal}$	BerCA	VfB u. BerCA	BerCA	BerCA

Tabelle 14: Zur Zertifikatsantragsstellung berechtigte nicht hoheitliche Organisationen

4.1.2 Beantragungsprozess und Zuständigkeiten

Der Registrierungsprozess für ein Zertifikat wird durch den Zertifikatsantrag eines Antragsstellers initiiert. Der Zertifikatsantrag und der technische Zertifikats-Request MÜSSEN durch die jeweils zuständige RA auf Basis des 4-Augenprinzips geprüft werden. Sollte die Identifizierung und die Authentifizierung des Antragsstellers erfolgreich abgeschlossen worden sein, wird das entsprechende Zertifikat von der jeweiligen CA ausgestellt.

In diesem Abschnitt wird der Beantragungs- und Austellungsprozess sowie die Verantwortlichkeiten der verschiedenen CVCA-eID PKI Instanzen definiert.

Genereller Beantragungsprozess

Der generelle Beantragungsprozess von Zertifikaten ($C_{Terminal}$,C_{DV}) bei der übergeordneten PKI-Instanz MUSS wie nachfolgend beschrieben erfolgen:

1. Der Antragsteller generiert ein Schlüsselpaar unter Verwendung eines entsprechend sicheren Kryptografiemoduls (siehe Abschnitt 6.2).
   - Auf DV- und Root-Ebene MÜSSEN die Schlüsselpaare in einer sicheren Umgebung erzeugt werden (siehe Abschnitt 5.1).
2. Der Antragsteller generiert den zugehörigen Zertifikats-Request gemäß den Anforderungen aus Abschnitt 7.1.
3. Der Antragsteller sendet den Zertifikats-Request an die entsprechende zuständige Stelle (siehe Tabellen in Abschnitt 4.1.1) über das entsprechende Kommunikationsprotokoll gemäß [TR-03129].
4. Die zuständige RA führt eine Identifikation und Authentifizierung des Antragsstellers (beschrieben in Kapitel 3) durch. Die Vorgehensweise unterscheidet hier zwischen initialer Beantragung oder einem routinemäßigen Wiederholungsantrag.
5. Die zuständige CA erstellt nach der erfolgreichen Prüfung des Antragsstellers und dessen Zertifikats-Request (beschrieben in Kapitel 3) das entsprechende Zertifikat.
6. Zustellung des Zertifikats über das entsprechende Kommunikationsprotokoll gemäß [TR-03129].

Die beschriebenen Schritte SOLLEN auf Basis des 4-Augenprinzips durchgeführt werden.

Im nicht hoheitlichen Bereich MUSS der beschriebene Beantragungsprozess im Rahmen der initialen Identifikation und Authentifizierung zunächst mit Testschlüsseln durchgeführt werden.

Verantwortlichkeiten

Nachfolgend werden die Hauptverantwortlichkeiten der RA und CA der jeweiligen PKI-Instanzen definiert. Hinzukommen die in Kapitel 8 definierten Prüfanforderungen.

CVCA-eID RA

Die CVCA-eID RA MUSS die folgenden Aufgaben wahrnehmen:

- Empfang von Zertifikats-Requests für die CVCA-eID über die in [TR-03129] definierte Schnittstelle.
  - Die Kommunikationsverbindung MUSS gegenseitig authentisiert und verschlüsselt sein.
- Überprüfung der Korrektheit des Zertifikats-Requests (gemäß Abschnitt 3.2) speziell unter folgenden Gesichtspunkten:
  - Ist der Antragssteller berechtigt, einen Zertifikatsantrag zu stellen?
  - Ist der Antrag konsistent?
  - Ist die vorgegebene Identität korrekt?
  - Besitzt der Antragssteller den zugehörigen privaten Schlüssel?
  - Ist der Antrag technisch konform (siehe Abschnitt 7.1)?
- Weiterleiten des technischen Zertifikats-Requests an die CVCA-eID CA über eine gesicherte Verbindung.

CVCA-eID CA

Die CVCA-eID CA MUSS die folgenden Aufgaben wahrnehmen:

- Generierung von CVCA-eID Schlüsselpaaren in einer sicheren Umgebung unter Verwendung eines sicheren Kryptografiemoduls (siehe Abschnitt 6.2).
- Ausstellen der CVCA-Zertifikate: C_{CVCA} und Link-C_{CVCA}.
- Veröffentlichen der Zertifikate C_{CVCA} und Link-C_{CVCA} auf der BSI-Webseite.
- Ausstellen von DV-Zertifikaten (C_{DV}) für hoheitliche DVs und BerCAs.
- Speicherung aller ausgestellten Zertifikate im CVCA-eID PKD.

Hoheitlicher Bereich

DVRA

Die DVRA MUSS die folgenden Aufgaben wahrnehmen:

- Entgegennahme von Terminal-Zertifikats-Requests über die in [TR-03129] definierte Schnittstelle.
  - Die Kommunikationsverbindung MUSS gegenseitig authentisiert und verschlüsselt sein.
- Identifizieren und Authentifizieren des Terminal-Betreibers gemäß der in Kapitel 3.2 aufgeführten Prozeduren, speziell unter den folgenden Gesichtspunkten:
  - Ist der Antragssteller berechtigt, einen Zertifikatsantrag zu stellen?
  - Ist der Antrag technisch konform (siehe Abschnitt 7.1)?
  - Ist die vorgebende Identität korrekt?
  - Besitzt der Antragssteller den zugehörigen privaten Schlüssel?
- Weiterleiten des technischen Zertifikats-Requests an die DVCA über eine gesicherte Verbindung.
- Führen eines Bestandsverzeichnisses in dem alle zur Zertifizierung berechtigten Terminals und die hierfür ausgestellten Zertifikate registriert sind.

DVCA

Die DVCA MUSS die folgenden Aufgaben wahrnehmen:

- Generieren von DV Schlüsselpaaren in einer sicheren Umgebung (siehe Abschnitt 5.1) unter Benutzung eines sicheren Kryptografiemoduls (siehe Abschnitt 6.2).
- Ausstellen von Terminal-Zertifikaten ($C_{Terminal}$) für von der DVRA authentifizierte hoheitliche Terminalbetreiber.
- Archivieren der ausgestellten Zertifikate (siehe Abschnitt 6.3.1).
- Zustellen des erzeugten Terminal-Zertifikats ($C_{Terminal}$) und der gesamten Zertifikatskette an den Terminalbetreiber über die in [TR-03129] definierte Schnittstelle.

Terminalbetreiber

Der Terminalbetreiber MUSS die folgenden Aufgaben wahrnehmen:

- Generieren von Terminal-Schlüsselpaaren mithilfe eines sicheren Kryptografiemoduls (siehe Anforderungen in Abschnitt 6.2).
- Durchführen der in Kapitel 3 aufgeführten Identifizierungs- und Authentifizierungs-prozeduren.
- Prüfen von erhaltenen Zertifikaten auf Korrektheit.

Nicht Hoheitlicher Bereich

VfB

Die VfB MUSS die folgenden Aufgaben wahrnehmen:

- Identifizieren und Authentifizieren von ZDAs, die als **BerCA** im Rahmen dieser Policy tätig werden wollen (Anzeige), speziell unter dem Gesichtspunkt:
  - Ist die vorgebende Identität korrekt?
- Die VfB informiert die CVCA-eID über die erfolgte Anzeige.

- Identifizieren und Authentifizieren von **Diensteanbietern** (oder beauftragten eID-Service-Provider) gemäß der in Kapitel 3.2 aufgeführt Prozeduren speziell unter den folgenden Gesichtspunkten:
  - Ist der Antragssteller berechtigt, einen Zertifikatsantrag zu stellen?
  - Ist die vorgegebene Identität korrekt?
- Mitteilen des erfolgreichen Prüfungsergebnisses auf elektronischem Wege an die BerCA. Die Authentizität und Integrität der Mittlung MUSS geschützt werden. Das Sicherheitsniveau MUSS hierbei vergleichbar mit der V-PKI [CP V-PKI] sein.

BerCA

Die BerCA MUSS die folgenden Aufgaben wahrnehmen:

- Generieren von DV-Schlüsselpaaren in einer sicheren Umgebung (siehe Abschnitt 5.1) unter Benutzung eines sicheren Kryptografiemoduls (siehe Abschnitt 6.2).
- Prüfen eingehender Terminal-Zertifikats-Requests speziell hinsichtlich:
  - Ist der Antrag technisch konform (siehe Abschnitt 7.1)?
  - Besitzt der Antragssteller den zugehörigen privaten Schlüssel?
  - Gehört der Zertifikats-Request zu dem bei der VfB registrierten Diensteanbieter (ermittelt durch die bei der Antragsstellung registrierten Kommunikationszertifikate)?
- Ausstellen von Terminal-Zertifikaten für Diensteanbieter (oder beauftragte eID-Service-Provider) nach Erhalt der Bestätigung durch die VfB.
- Identifizieren und Authentifizieren von Wiederholungsanträgen gemäß Abschnitt 3.3.1.
- Führen eines Bestandsverzeichnisses in dem alle zur Zertifizierung berechtigten Diensteanbieter und die hierfür ausgestellten Zertifikate registriert sind.
  - Archivieren der ausgestellten Zertifikate (siehe Abschnitt 6.3.1).
- Zustellen des erzeugten Terminal-Zertifikats und der gesamten Zertifikatskette an den Diensteanbieter (oder beauftragte eID-Service-Provider) über die in [TR-03129] definierte Schnittstelle.

Diensteanbieter

Der Diensteanbieter MUSS die folgenden Aufgaben wahrnehmen:

- Generieren von Terminal-Schlüsselpaaren über ein sicheres Kryptografiemodul.
- Durchführen der in Kapitel 3 aufgeführten Identifizierungs- und Authentifizierungsprozeduren.
- Prüfen von erhaltenen Zertifikaten auf Korrektheit.

Sollten zwischen Diensteanbieter und eID-Service Provider personenbezogene Daten aus der eID-Authentisierung übertragen werden, MUSS die Sicherheit deren Kommunikationsverbindung mit dem Sicherheitsniveau der ePA-Authentisierung vergleichbar sein.

4.2 Verarbeitung von Zertifikatsanträgen

In diesem Abschnitt werden die Prozeduren zur Verarbeitung von Zertifikatsanträgen beschrieben. Grundlage für die Verarbeitung ist die in Abschnitt 4.1 beschriebene Beantragung.

4.2.1 Durchführung der Identifizierung und Authentifizierung

Zertifikatsanträge MÜSSEN zur Prüfung der Gültigkeit des Zertifikatsantrags die entsprechenden Identifikations- und Authentifizierungsprozeduren durchlaufen. Hierbei werden zwei Fälle unterschieden:

- Initialer Zertifikatsantrag, Prozeduren beschrieben in Abschnitt 3.2
- Wiederholungsanträge, Prozeduren beschrieben in Abschnitt 3.3

Zertifikatsanträge dürfen ausschließlich an die nächsthöhere PKI-Instanz gestellt werden. Ferner wird hierbei zwischen dem hoheitlichen und dem nicht hoheitlichen PKI-Bereich unterschieden.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Sollte eine Prüfung auf Basis der Identifikations- und Authentifizierungsprozeduren eines Zertifikatsantrags nicht erfolgreich verlaufen sein, so erhält der Antragssteller kein Zertifikat.

Im Falle eines nicht routinemäßigen Wiederholungsantrag ist gemäß Abschnitt 3.3 zu verfahren.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

In den Tabellen dieses Abschnitts sind die Fristen zur Reaktion auf einen Zertifikatsantrag aufgeführt. Hierbei wird insbesondere zwischen dem initialen Zertifikatsantrag und einem Wiederholungsantrag unterschieden.

Mit **Reaktionszeit** ist hier der Zeitraum nach Eingang des Zertifikats-Requests bis zur Erstellung des Zertifikats, nach einer erfolgreichen Identifizierung und Authentifizierung, zu verstehen.

Hoheitlicher Bereich

Beantragter Zertifikatstyp	Technische Annahme Request	Reaktionsfrist	
		Initialer Antrag	Wiederholungsantrag
C_{DV}	CVCA-eID RA	3 Werktage	3 Werktage
$C_{Terminal}$	DVRA	3 Werktage	unverzüglich

Tabelle 15: Fristen zur Bearbeitung von hoheitlichen Zertifikatsanträgen

Nicht hoheitlicher Bereich

Beantragter Zertifikatstyp	Technische Annahme Request	Reaktionsfrist	
		Initialer Antrag	Wiederholungsantrag
C_{DV}	CVCA-eID RA	3 Werktage	3 Werktage
$C_{Terminal}$	BerCA	3 Werktage	unverzüglich

Tabelle 16: Fristen zur Bearbeitung von nicht hoheitlichen Zertifikatsanträgen

4.3 Ausgabe von Zertifikaten

In diesem Abschnitt werden die Prozeduren zur Ausgabe von Zertifikaten beschrieben. Grundlage für die Ausgabe ist die in Abschnitt 4.2 beschriebene Verarbeitung von Zertifikatsanträgen.

Die CVCA-eID stellt für sich selbst CVCA-eID Zertifikate (C_{CVCA} und Link-C_{CVCA}) aus.

Alle anderen PKI-Instanzen MÜSSEN Antragssteller erfolgreich als berechtigt identifizieren und authentifizieren (gemäß der in Kapitel 3 definierten Prozeduren), um diesen ein Zertifikat auszustellen zu können.

4.3.1 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

Das ausgestellte Zertifikat wird dem Antragssteller über die in [TR-03129] definierten Kommunikationsprotokolle zur Verfügung gestellt. Die Verbindung wird über die bei der initialen Registrierung hinterlegten Kommunikationszertifikate der Teilnehmer authentisiert und verschlüsselt.

4.4 Annahme von Zertifikaten

Nach Erhalt MUSS der Zertifikatsinhaber die Angaben im Zertifikat auf Korrektheit und Vollständigkeit prüfen. Um ein Zertifikat zurück zuweisen, MUSS der Inhaber eine Nachricht an die Zertifizierungsstelle schicken. In einer solchen Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Bei fehlerhaften Zertifikaten sind, soweit möglich, die fehlerhaften bzw. unvollständigen Einträge zu benennen.

Sonderfall EAC-Box

Im Falle einer Zurückweisung eines Zertifikats durch eine EAC-Box MUSS diese über die in [TR-03129] definierten Protokolle zur Fehlerübermittlung eine Nachricht an den DV senden. In einer solchen Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Zusätzlich sind soweit möglich die fehlerhaften bzw. unvollständigen Einträge im Zertifikat zu benennen. Die Absicherung der Integrität und Authentizität der Nachricht erfolgt durch die direkte SSL-Verbindung zwischen EAC-Box und DV.

4.4.1 Veröffentlichung von Zertifikaten durch die CA

Die CVCA-eID MUSS deren CVCA-eID Zertifikate (C_{CVCA} und Link-C_{CVCA}) auf der BSI-CVCA-eID Webseite veröffentlichen (www.bsi.bund.de/cvca-eID).

Überdies werden auf der BSI-Webseite (www.bsi.bund.de/csca) die CSCA-Zertifikate, CSCA Link-Zertifikate und die zugehörige Sperr-/ DefectListen zum Abruf bereitgestellt, welche zur Durchführung der passiven Authentisierung (siehe [TR-03110]) benötigt werden.

Die hoheitlichen DVs und die BerCAs MÜSSEN deren Zertifikatsnehmer zusätzlich zu dem erstellten Zertifikat ($C_{Terminal}$) die gesamte für die eID-Authentisierung erforderliche Zertifikatskette (siehe [TR-03110]) über die Schnittstelle gemäß [TR-03129] zur Verfügung stellen.

4.5 Verwendung von Schlüsselpaar und Zertifikat

Die Zertifikate DÜRFEN NUR gemäß ihres Verwendungszwecks eingesetzt werden. Der Verwendungszweck für die Zertifikate ist in Abschnitt 1.4 beschrieben.

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Schlüssel bzw. Zertifikate können von Zertifikatsnehmern zum Nachweis einer Berechtigung sowie zur Erzeugung von elektronischen Signaturen verwendet werden. Nachfolgend werden für die verschiedenen PKI-Ebenen die erlaubten Verwendungen des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer definiert:

Root-Ebene

Das Zertifikat der CVCA-eID bildet den Vertrauensanker der CVCA-eID PKI. Mit dem CVCA-Zertifikat (C_{CVCA}) wird durch die CVCA-eID die Berechtigung zur Ausstellung von DV-Zertifikaten nachgewiesen. Mit dem privaten Schlüssel werden das selbst signierte CVCA-eID-Zertifikat (C_{CVCA}) und die nachfolgenden Link-Zertifikate (Link-C_{CVCA}) sowie alle DV-Zertifikate (C_{DV}) signiert.

DV-Ebene

Ein Document Verifier (Hoheitlicher DV, BerCA) erbringt mit seinem DV-Zertifikat (C_{DV}) den Nachweis der Berechtigung zur Ausstellung von Terminal-Zertifikaten. Mit dem privaten Schlüssel werden Terminal-Zertifikate ($C_{Terminal}$) und Wiederholungsanträge an die CVCA-eID signiert.

Terminal-Ebene

Mit seinem Zertifikat ($C_{Terminal}$) wird durch ein Terminal der Nachweis der Berechtigung erbracht, auf die Daten der eID-Anwendung eines ePA zugreifen zu dürfen. Dazu wird mit dem privaten Schlüssel im Rahmen der Authentisierung gegenüber dem ePA eine Signatur erzeugt (Protokollbeschreibung siehe [TR-03110] Terminal Authentication). Zudem werden mit dem privaten Schlüssel Wiederholungsanträge an den zuständigen DV signiert.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Zertifikatsnutzer können Schlüssel bzw. Zertifikate zur Validierung von Authentisierungen und elektronischen Signaturen verwenden.

Zertifikatsnutzer können die öffentlichen Schlüssel von Terminal, Document Verifier und CVCA-eID nutzen, um Zertifikatsketten und somit die Gültigkeit einer Berechtigung zu überprüfen.

4.6 Zertifikatserneuerung

Zertifikatserneuerung bedeutet das Ausstellen eines neuen Zertifikats für einen öffentlichen Schlüssel, der bereits zertifiziert wurde.

Zertifikatserneuerung IST NICHT erlaubt.

4.7 Zertifizierung nach Schlüsselerneuerung

Zertifizierung nach Schlüsselerneuerung bedeutet, dass ein Antragssteller (DV- oder Terminal-Ebene) ein neues Schlüsselpaar generiert und einen Zertifikats-Request mit dem neuen öffentlichen Schlüssel einreicht. Dieser Zertifikats-Request ist mit dem privaten Schlüssel signiert, welcher zum letzten von der CA ausgestellten Zertifikat gehört.

Somit handelt es sich um einen Wiederholungsantrag.

4.7.1 Bedingungen der Zertifizierung nach Schlüsselerneuerungen

Es muss sich um einen **routinemäßigen Wiederholungsantrag** gemäß Abschnitt 3.3 handeln.

4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Die initiale Identifikation und Authentifizierung des Antragsstellers MUSS erfolgreich durchgeführt worden sein. Überdies muss der Antragssteller im Besitz eines noch gültigen privaten Schlüssels zur Signatur des neuen Zertifikats-Requests sein (siehe Abschnitt 3.3).

4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Die Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen entspricht der Bearbeitung eines Wiederholungsantrags. Dieser Prozess ist in Abschnitt 3.3 beschrieben.

4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Die Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats erfolgt, wie in Abschnitt 4.3.1 beschrieben.

4.7.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Das Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen wird in Abschnitt 4.4 beschrieben.

4.7.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA

Die Veröffentlichung von Zertifikaten für Schlüsselerneuerungen entspricht den Regelungen beschrieben in Abschnitt 4.4.1.

4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Die Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats entspricht den Regelungen, beschrieben in Abschnitt 4.4.1.

4.8 Änderungen am Zertifikat

Änderungen am Zertifikat bedeutet das Ausstellen eines neuen Zertifikats mit geänderten Zertifikatsinformationen aber gleich bleibendem öffentlichen Schlüssel.

Änderungen am Zertifikat SIND NICHT erlaubt.

4.9 Sperrung und Suspendierung von Zertifikaten

Das Sperren von Zertifikaten über eine Sperrliste ist in der CVCA-eID PKI nicht vorgesehen.

Eine Sperrung erfolgt durch die Rücknahme einer erteilten Berechtigung. Eine Rücknahme löst aufgrund der kurzen Zertifikatslaufzeiten eine Sperrung in Form der Ablehnung weiterer Zertifikatsanträge bzw. von Wiederholungsanträgen aus (siehe Prozeduren in den Abschnitten 3.3 und 3.4).

Jede PKI-Instanz, die Zertifikate ausstellt, MUSS Wiederholungsanträge sperren können (bspw. über eine interne Sperrliste).

4.10 Service zur Statusabfrage von Zertifikaten

In der CVCA-eID PKI ist kein Service zur Statusabfrage von Zertifikaten vorgesehen.

Jede PKI-Instanz, die Zertifikate ausstellt, MUSS Wiederholungsanträge sperren können (bspw. über eine interne Sperrliste).

Den Document Verifiern (DV, BerCA) MUSS es jederzeit möglich sein, den aktuellen Bestand der betreuten Terminals mit den zugehörigen Zertifikaten sowie deren Historie festzustellen.

4.11 Beendigung der Teilnahme

Die Beendigung der Teilnahme erfolgt durch das nicht mehr Stellen von routinemäßigen Wiederholungsanträgen (siehe Einleitung 3.3). Überdies MUSS die zuständige höhere PKI-Instanz entsprechend informiert werden (vergleiche hierzu die "Anforderungen an die Einstellung des Betriebs", Kapitel 4.3.2 in [TR-03128]).Eine erneute initiale Überprüfung des Antragsstellers, wie in Abschnitt 3.2 definiert, ist erforderlich, um wieder an der CVCA-eID PKI teilnehmen zu können.

4.12 Hinterlegung und Wiederherstellung von Schlüsseln

Die Hinterlegung und Wiederherstellung von Schlüsseln IST NICHT erlaubt.

5 Organisatorische, betriebliche und physikalische Sicherheitsmaßnahmen

5.1 Physikalische Sicherheitsmaßnahmen

In diesem Abschnitt werden die Anforderungen an die physikalischen Sicherheitsmaßnahmen der CVCA-eID PKI Teilnehmer definiert.

5.1.1 Generelle Sicherheitsmaßnahmen

Die nachfolgenden generellen Sicherheitsmaßnahmen MÜSSEN von

- der **CVCA-eID** sowie
- den **Document Verifiern** (hoheitliche DVs, BerCAs)

der CVCA-eID PKI realisiert werden.

Die Anforderungen beziehen sich insbesondere auf eine sichere Betriebsumgebung sowie die Betriebsabläufe von CA und RA:

- **Lage und Gebäude**

  Die CA und RA werden beide in einem physikalisch geschützten Bereich betrieben.

- **Zugang**

  Der Zugang zu CA und RA wird kontrolliert und auditiert. Überdies wird der Zugang ausschließlich berechtigten Personen gewährt.

- **Stromversorgung**

  Eine unterbrechungsfreie Stromversorgung wird gewährleistet.

- **Wassergefährdung**

  Die IT-Infrastruktur der CA und RA wird gegen Wasserschäden aller Art geschützt.

- **Brandschutz**

  Gebräuchliche Methoden zum Schutz gegen Schäden durch Feuer werden umgesetzt.

- **Speichermedien**

  Die Speichermedien werden gegen nicht autorisierten oder unbeabsichtigten Gebrauch, hinsichtlich Zugang und Freigabe oder Schaden durch Personen oder andere Bedrohungen (z.B. Feuer oder Wasser) geschützt.

- **Abfallbeseitigung**

  Verfahren zur Beseitigung von Abfall werden eingeführt, um unautorisierten Gebrauch, Zugang oder Freigabe von/zu vertraulichen Daten zu vermeiden.

- **Notfall-Backup**
  - Die Daten der CA und RA MÜSSEN gesichert werden (bspw. das Bestandsverzeichnis eines DV), sodass die Systeme nach einem Notfall/Unfall auf Basis dieser Daten wieder operativ betrieben werden können.
  - Backup- und Wiederherstellungsprozeduren dürfen ausschließlich von vertrauenswürdigen Betriebspersonal durchgeführt werden.
  - Ein Offsite-Backup kritischer Daten wird durchgeführt. Dies betrifft insbesondere die Backup-Schlüssel und Zertifikate (siehe Abschnitt 5.6).

Es wird EMPFOHLEN, dass **Diensteanbieter** und **hoheitliche Terminalbetreibe**r ein entsprechendes Sicherheitsniveau angelehnt an die beschriebenen Anforderungen gewährleisten.

5.1.2 Erweiterte Sicherheitsmaßnahmen

Document Verifier unterliegen aufgrund deren Rolle gemäß [TR-03128] erweiterten Anforderungen bzgl. deren Sicherheitsmaßnahmen:

- **Hoheitliche Document Verifier**

  MÜSSEN ein Sicherheitskonzept nach IT-Grundschutz erstellen. Darüber hinaus wird EMPFOHLEN, eine entsprechende Auditierung durchführen zu lassen.

- **BerCAs**

  MÜSSEN alle Sicherheitsmaßnahmen einhalten, die nach SigV [SigG, SigV] erforderlich sind.

Darüber hinaus MÜSSEN alle Document Verifier eine DV Certificate Policy erstellen, welche alle Anforderungen dieser Certificate Policy berücksichtigt. Eine Übersicht der erforderlichen Prüfungen, die ein DV durchführen MUSS, ist in Abschnitt 8.1 enthalten.

5.2 Verfahrensanweisungen

Verfahrensanweisungen MÜSSEN umgesetzt werden, welche insbesondere die Trennung von Verantwortlichkeiten und die gegenseitige Kontrolle für kritische Vorgänge beinhalten. Die vertrauenswürdigen Rollen, die Anzahl an Personal die für die Aufgabe benötigt wird und die Identifikation und Authentifizierung jeder Rolle sind in einem entsprechenden Konzept festzuhalten.

5.3 Personalkontrolle

Die PKI-relevanten Systeme der Teilnehmer an der CVCA-eID-PKI MÜSSEN von qualifiziertem und erfahrenem Personal betrieben werden.

Das Betriebspersonal der CVCA-eID MUSS eine erfolgreiche Sicherheitsüberprüfung nach Sicherheitsüberprüfungsgesetz (SÜV) nachweisen.

5.4 Überwachungsmaßnahmen

Die Teilnehmer an der CVCA-eID-PKI MÜSSEN sicherstellen, dass deren Systeme über Protokollierungsmechanismen verfügen, um eine unberechtigte oder fehlerhafte Nutzung ihrer Systeme erkennen und analysieren zu können.

5.5 Archivierung von Aufzeichnungen

Die Teilnehmer an der CVCA-eID-PKI MÜSSEN sicherstellen, dass deren Systeme über angemessene Archivierungsfunktionen verfügen.

5.6 Schlüsselwechsel einer Zertifizierungsstelle

CVCA-eID (Root-Ebene)

Bei der Aufnahme des Wirkbetriebs generiert die CVCA-eID das initiale **Root-Schlüsselpaar** und ein zugehöriges selbst-signiertes Zertifikat (Init C_{CVCA}). Dieses selbst-signierte Zertifikat wird dem Ausweisproduzenten durch einen autorisierten Repräsentanten der CVCA-eID übergeben und bei der Produktion in jeden ePA als Vertrauensanker eingebracht.

Überdies MÜSSEN mindestens **drei** weitere **Backup-Schlüsselpaare** in entsprechend sicheren Hardwaremodulen generiert werden, welche die folgenden Anforderungen erfüllen:

- Alle Backup-Schlüsselpaare MÜSSEN Zertifikate erhalten, die mit dem aktiven privaten Root-Schlüssel signiert sind.
- Alle Schlüsselpaare und zugehörige Zertifikate MÜSSEN sicher gelagert werden, entsprechend den diesbezüglichen Anforderungen dieser Policy.
- Zwei Backup-Schlüsselpaare und die zugehörigen Zertifikate MÜSSEN in einer sicheren Umgebung gelagert werden, welche nicht zum Gebäude der CVCA-eID gehört.

Vor Ablauf des aktiven Root-Schlüsselpaars (siehe Abschnitt 6.3.2) MUSS ein neues Root-Schlüsselpaar erzeugt werden. Das zugehörige **Link-Zertifikat** (Link-C_{CVCA}) MUSS folgende Anforderungen erfüllen:

- Das Link-Zertifikat MUSS vom noch aktiven privaten Root-Schlüssel signiert werden.
- Das erste selbst-signierte CVCA-Zertifikat und alle folgenden LINK-Zertifikate (**Zertifikatskette**) MÜSSEN auf der BSI-Webseite veröffentlicht werden.

Alle für die Schlüsselgenerierung und -speicherung verwendeten Kryptografiemodule MÜSSEN die Anforderungen aus Abschnitt 6.2 erfüllen.

Die Gültigkeitszeiten für die Zertifikate sind in Abschnitt 6.3.2 definiert.

DV- / Terminal-Ebene

Teilnehmer auf DV- und Terminal-Ebene MÜSSEN für jeden Zertifikats-Request ein neues Schlüsselpaar generieren (siehe Abschnitt 4.1.2) und die Anforderungen an einen routinemäßigen Wiederholungsantrag erfüllen (siehe Abschnitt 3.3).

5.7 Notfall-Management

In diesem Abschnitt werden Anforderungen an das Notfall-Management definiert. Insbesondere wird beschrieben, wie zu verfahren ist, wenn aufgrund eines Vorfalls kein routinemäßiger Wiederholungsantrag gestellt werden kann oder der Verdacht auf Kompromittierung oder Missbrauch des privaten Schlüssels besteht.

5.7.1 Behandlung von Vorfällen und Kompromittierung

Generell MÜSSEN alle Zertifikatsnehmer der CVCA-eID PKI:

- **CVCA-eID**
- **Hoheitlich**: DV (siehe [TR-03128]) und Terminalbetreiber
- **Nicht Hoheitlich**: BerCA (siehe [TR-03128]), Diensteanbieter und eID-Service-Provider

ein Sicherheitskonzept erstellen, welches insbesondere die Kompromittierung des privaten Schlüssels berücksichtigt.

Die nachfolgend beschriebenen Prozesse MÜSSEN bei einem Vorfall oder einem Verdacht auf solchen eingehalten werden:

Vorfall auf Root-Ebene

Besteht Verdacht auf Kompromittierung oder Missbrauch seines privaten Schlüssel, MUSS die CVCA-eID den Vorfall sorgfältig aufklären. Ein entsprechender Bericht ist zu erstellen. Ist die Integrität des privaten Schlüssels nicht mehr geben, MUSS unverzüglich auf ein neues initiales CVCA-Schlüsselpaar gewechselt werden. Das alte Schlüsselpaar DARF NICHT mehr verwendet werden. Alle Document Verifier MÜSSEN hierüber informiert werden. Zusätzlich MUSS der Schlüsselwechsel auf der CVCA-eID Webseite veröffentlicht werden.

Vorfall auf DV-Ebene

Kann aufgrund eines Vorfalls kein routinemäßiger Wiederholungsantrag gestellt werden oder besteht Verdacht auf Kompromittierung oder Missbrauch seines privaten Schlüssel, MUSS der Document Verifier unverzüglich die CVCA-eID informieren. Handelt es sich beim DV um eine BerCA, MUSS gleichzeitig die VfB in Kenntnis gesetzt werden.

Zur Klärung des Vorfalls und der weiteren Vorgehensweise MUSS der DV der CVCA-eID folgende Unterlagen bereitstellen:

- Bericht über den Vorfall,
- Protokolldaten,
- in Relation stehende Betriebsdokumente.

Vorfall auf Terminal-Ebene

Kann aufgrund eines Vorfalls kein routinemäßiger Wiederholungsantrag gestellt werden oder besteht Verdacht auf Kompromittierung oder Missbrauch seines privaten Schlüssels, MUSS der Terminalbetreiber unverzüglich den zuständigen DV informieren. Der DV KANN dies wiederum unverzüglich an die CVCA-eID weitergeben. Handelt es sich um einen nicht hoheitlichen Schlüssel, MUSS gleichzeitig die VfB informiert werden.

Zur Klärung des Vorfalls und der weiteren Vorgehensweise MUSS der Terminalbetreiber dem DV folgende Unterlagen bereitstellen:

- Bericht über den Vorfall,
- Protokolldaten,
- in Relation stehende Betriebsdokumente.

Die entsprechenden Dokumente sind vom DV an die CVCA-eID weiterzugeben.

Wie die zuständige übergeordnete PKI-Instanz bei einem Vorfall zu verfahren hat, ist in Abschnitt 8.2 beschrieben.

5.7.2 Kompromittierung des privaten Schlüssels einer CA

Bei Kompromittierung des privaten Schlüssels einer CA ist wie in Abschnitt 5.7.1 beschrieben zu verfahren.

6 Technische Sicherheitsmaßnahmen

6.1 Erzeugung und Installation von Schlüsselpaaren

Jeder Zertifikatsnehmer MUSS sein eigenes Schlüsselpaar generieren. Dies betrifft folgende Instanzen der CVCA-eID PKI:

- CVCA-eID (zertifiziert Schlüsselpaar selbst)
- **Hoheitlicher Bereich:** DVs und Terminalbetreiber
- **Nicht hoheitlicher Bereich**: BerCAs, Diensteanbieter und eID-Service Provider (generiert ein Schlüsselpaar im Auftrag des Diensteanbieters)

6.1.1 Erzeugung von Schlüsselpaaren

In der CVCA-eID PKI dürfen ausschließlich kryptografische Algorithmen gemäß [TR-03110] eingesetzt werden. Die konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen sind in [TR-03116-2] angegeben.

Das jeweilige kryptografische Schlüsselpaar MUSS in einem sicheren Kryptografiemodul generiert werden (siehe Abschnitt 6.2).

Der technische Zugriff auf die Kryptografiemodule aller Zertifikatsnehmer ist durch ein Geheimnis geschützt (Passwort, PIN, o.ä.), welches nur die jeweiligen Operatoren kennen. Der Zugriff auf das Kryptografiemodul, insbesondere zur Schlüsselerzeugung, ist auf ein Minimum an Operatoren beschränkt.

Die Generierung von Schlüsseln durch die CVCA-eID oder auf DV-Ebene erfordert die Einhaltung des 4-Augenprinzips. Zusätzlich MUSS die Generierung in einer sicheren Umgebung erfolgen.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Der Zertifikatsnehmer generiert seinen privaten Schlüssel selbst. Daher wird keine Lieferung von privaten Schlüsseln vorgenommen.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

Die Zertifikats-Requests MÜSSEN der zuständigen Annahmestelle (siehe Abschnitt 4.1) über die in [TR-03129] definierten Kommunikationsprotokolle zugestellt werden.

Die Kommunikationsverbindung MUSS durch einen SSL-Kanal geschützt werden. Die Kommunikationspartner MÜSSEN sich dabei gegenseitig über die bei der initialen Registrierung festgelegten Kommunikationszertifikate authentisieren.

6.1.4 Lieferung öffentlicher Schlüssel der CA an Zertifikatsnutzer

Die Zertifikate MÜSSEN dem Zertifikatsnehmer (siehe Abschnitt 4.1) über die in [TR-03129] definierten Kommunikationsprotokolle zugestellt werden.

Die Kommunikationsverbindung MUSS durch einen SSL-Kanal geschützt werden. Die Kommunikationspartner MÜSSEN sich dabei gegenseitig authentisieren. Diese erfolgt über die bei der initialen Registrierung festgelegten Kommunikationszertifikate.

6.1.5 Schlüssellängen und kryptografische Algorithmen

Die zu verwendenden kryptografischen Algorithmen und Schlüssellängen sind in [TR-03116-2] und [TR-02102] definiert. Diese technischen Richtlinien werden fortlaufend aktualisiert unter Berücksichtigung des aktuellen Technologie- und Wissensstands.

6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Der Antragssteller MUSS sicherstellen, dass sein Zertifikats-Request konform zu dem geforderten Profil in [TR-03110] und den Anforderungen dieser Policy ist.

Ferner MÜSSEN die Systeme des Antragsstellers eine automatische diesbezügliche Prüfung anschließend an die Generierung durchführen.

6.1.7 Verwendungszweck der Schlüssel

Die Schlüssel dürfen ausschließlich wie in Kapitel 4 beschrieben verwendet werden.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

Der private Schlüssel MUSS in einem kryptografischen Hardwaremodul generiert, gespeichert und genutzt werden. Die **Kryptografiemodule** MÜSSEN nach den folgenden Common Criteria Protection Profiles (PPs) durch das BSI zertifiziert sein.

- High Security Module (HSM): PP-Cryptographic Modules "moderate“ [PP-CM-m]
- Chipkarten: PP-Secure Signature-Creation Device [PP-SSCD].

Diese Anforderung KANN bis auf Widerruf alternativ durch den Nachweis

- eines sicheren Zufallszahlengenerators aus einer der folgenden Klassen (siehe [AIS 20/31]):
  - DRG.3 (bzw. DRG.4),
  - PTG.3,
  - NTG.1;
- eines Tamper-Schutzes gegen Attack Potential "moderate";
- der Seitenkanalresistenz gegen Attack Potential "moderate"

erfüllt werden. Der Nachweis MUSS durch eine durch das BSI für Common Criteria-Evaluierungen akkreditierte Prüfstelle erbracht werden.

Diensteanbieter und eID-Service Provider MÜSSEN zur eID-Authentisierung Systeme mit einem sicheren Kryptografiemodul (s.o.) verwenden. Ferner gelten zum Betrieb des Systems zur eID-Authentisierung die Anforderungen aus [TR-03130], Anhang C.

Eine EAC-Box MUSS konform zu [TR-03131] und nach [PP-IS] zertifiziert sein.

6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

Das Prinzip der gegenseitigen Kontrolle MUSS bei der Zertifikatsausstellung durchgesetzt werden. Ein Operator für die Zertifikatsausstellung DARF KEIN Operator bei der RA sein.

6.2.2 Hinterlegung privater Schlüssel

Es DARF KEINE Hinterlegung privater Schlüssel geben.

6.2.3 Backup privater Schlüssel

Eine PKI-Instanz der CVCA-eID PKI DARF NUR über einen aktiven Schlüssel verfügen, der im Kryptografiemodul oder in einem Verbund (siehe Abschnitt 6.2.5) aus mehreren Kryptografiemodulen betrieben wird.

Dieser private Schlüssel KANN als Backup wie folgt exportiert werden:

- Verschlüsselter Dateicontainer
  - Datenstruktur, die den geheimen Schlüssel enthält und mit einem KEK (Key Encryption Key) verschlüsselt ist.
    - Die Anforderungen an die Verschlüsselung ergeben sich aus [TR-02102].
  - Die Nutzung des Dateicontainers erfordert den Import in ein Kryptografiemodul, das die Anforderungen aus Abschnitt 6.2 erfüllt.
  - Der Zugriff auf den verschlüsselten Dateicontainer MUSS auf das Betriebspersonal beschränkt sein.
- Backup Kryptografiemodul
  - Der private Schlüssel wird verschlüsselt direkt in das Backup-Kryptografiemodul transferiert (siehe Abschnitt 6.2.5).
  - Der Zugang zum Backup-Kryptografiemodul MUSS auf das Betriebspersonal beschränkt sein.

Der KEK der Kryptografiemodule zur Ver-/Entschlüsselung des privaten Schlüssels MUSS vertrauensvoll ausgetauscht werden.

Der private Schlüssel darf zu keinem Zeitpunkt außerhalb des Kryptografiemoduls im Klartext vorliegen.

Bei der Durchführung des Backups MUSS das Prinzip der gegenseitigen Kontrolle durchgesetzt werden.

6.2.4 Archivierung privater Schlüssel

Es DARF KEINE Archivierung privater Schlüssel geben.

6.2.5 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Der private Schlüssel DARF zwischen kryptografischen Modulen transferiert werden. Hierdurch KANN ein Verbund aus Kryptografiemodulen gebildet werden bspw. zur Erhöhung der Ausfallsicherheit oder aus Lastverteilungsgründen.

Voraussetzung für den Transfer privater Schlüssel ist, dass nur Kryptografiemodule verwendet werden, welche die Anforderungen aus Abschnitt 6.2 erfüllen.

Der private Schlüssel MUSS hierbei verschlüsselt transferiert werden. Die Anforderungen an die Verschlüsselung ergeben sich aus [TR-02102]. Die Ver-/Entschlüsselung MUSS in den Kryptografiemodulen erfolgen.

Der KEK zur Ver-/Entschlüsselung des privaten Schlüssels MUSS vertrauensvoll ausgetauscht werden.

Bei der Durchführung des Transfers MUSS das Prinzip der gegenseitigen Kontrolle durchgesetzt werden.

6.2.6 Speicherung privater Schlüssel in kryptographischen Modulen

Das Kryptografiemodul MUSS die Anforderungen aus Abschnitt 6.2, welche eine sichere Speicherung des Schlüssels beinhaltet, berücksichtigen.

6.2.7 Aktivierung privater Schlüssel

Bei der Aktivierung wird der private Schlüssel in den Zustand versetzt, Signaturen erstellen zu können.

Die Aktivierung erfordert eine vorherige Authentisierung durch Eingabe eines Geheimnisses (Passwort oder PIN), EMPFOHLEN in Verbindung mit einem Hardware-Token.

Bei der Zertifikatsausstellung auf CVCA-Ebene MUSS das Prinzip der gegenseitigen Kontrolle durchgesetzt werden.

6.2.8 Deaktivierung privater Schlüssel

Bei der Deaktivierung wird der private Schlüssel in einen Zustand versetzt, in dem er ohne erneute Aktivierung keine Signaturen erstellen kann.

6.2.9 Zerstörung privater Schlüssel

Private Schlüssel auf Root- und DV-Ebene MÜSSEN zerstört werden, wenn deren Gültigkeitszeit abgelaufen ist.

Die Zerstörung erfolgt durch einen entsprechenden Mechanismus im HSM. Sollte der private Schlüssel auf einer Chipkarte gespeichert sein, MUSS diese physikalisch vernichtet werden.

6.2.10 Beurteilung kryptographischer Module

Die Anforderungen an Kryptografiemodule sind in Abschnitt 6.2 definiert.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Die PKI-Instanzen MÜSSEN verschiedene Zertifikate zur Durchführung deren Aufgabenstellung speichern. Die nachfolgende Tabelle zeigt eine Übersicht der Archivierungsdauer pro Ebene.

Ebene	Archivierungsort	Zertifikatstyp	Archivierungsdauer
CVCA-eID	Internes CVCA-eID PKD	C_{CVCA}, LINK-C_{CVCA}	Zertifikatslaufzeit + 10 1/2 Jahre
		Alle ausgestellten C_{DV}	Zertifikatslaufzeit + 10 1/2 Jahre
DV	Internes DV PKD	C_{CVCA} und alle LINK-C_{CVCA}	Zertifikatslaufzeit + 2 Jahre
		Alle bezogenen C_{DV}	Zertifikatslaufzeit + 2 Jahre
		Alle ausgestellten $C_{Terminal}$	Zertifikatslaufzeit + 2 Jahre
Terminal	Zertifikatsspeicher	C_{CVCA} und alle LINK-C_{CVCA}	Zertifikatslaufzeit + 6 Monate
		Aktuelle C_{DV}	Zertifikatslaufzeit + 6 Monate
		Aktuelle $C_{Terminal}$	Zertifikatslaufzeit + 6 Monate
ePA	Chipkarten-Speicher	C_{CVCA}, LINK-C_{CVCA}	Gesamte Laufzeit

Tabelle 17: Archivierung öffentlicher Schlüssel

Die Zertifikatslaufzeit entspricht der Gültigkeitszeit des Zertifikats, beschrieben in Abschnitt 6.3.2.

6.3.2 Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren

In diesem Abschnitt wird der Gültigkeitszeitraum der Schlüssel der CVCA-eID PKI definiert. Der Verwendungszweck der Schüssel und Zertifikate wird in Tabelle 5 angegeben.

Technisch wird der Gültigkeitszeitraum der Schlüssel durch die Zertifikatsgültigkeit bestimmt. Hierzu MUSS die jeweilige CA die entsprechenden Werte im auszustellenden CV-Zertifikat in den folgenden Feldern setzen:

Feld	Inhalt
`Certificate Effective Date`	Datum der Zertifikatsgenerierung
`Certificate Expiration Date`	Datum, an dem das Zertifikat abläuft.

Tabelle 18: Setzen von Gültigkeitszeiten in CV-Zertifikaten der CVCA-eID PKI

Die nachfolgend aufgeführten Gültigkeitszeiten für die Zertifikate der CVCA-eID PKI MÜSSEN von der entsprechenden ausstellenden Instanz unter Einhaltung der Kodierungsanforderungen aus [TR-03110] gesetzt werden.

CVCA- und DV-Ebene

Die Gültigkeitszeiten auf CVCA- und DV-Ebene sind für den hoheitlichen und nicht hoheitlichen Bereich identisch und werden in der folgenden Tabelle dargestellt.

Ebene	Gültigkeitszeitraum
CVCA-eID	3 Jahre
DV	90 Tage

Tabelle 19: Gültigkeitszeiten CVCA-eID- und DV-Ebene

Die CVCA-eID und die Document Verifier sollten darauf achten, rechtzeitig vor Ablauf ihrer Zertifikate ein neues Zertifikat zu beantragen, damit diese über die gesamte Betriebszeit, Zertifikate mit dem vollen Gültigkeitszeitraum für ihre Zertifikatsnehmer ausstellen können.

Weitere Informationen zum Zeitmanagement von Zertifikaten sind in [TR-03110] enthalten.

Terminal-Ebene

Auf Terminal-Ebene sind die Gültigkeitszeiten von Zertifikaten je nach Verwendungszweck und Betriebsart unterschiedlich. Die verschiedenen Terminal-Typen werden in Abschnitt 1.1 und [TR-03128] beschrieben.

Zertifikate auf Terminal-Ebene werden ausschließlich für die eID-Authentisierung verwendet. Hier setzt sich der Gültigkeitsraum aus einer **Addition** von Zeiträumen zusammen, die wie folgt definiert sind:

- Nutzungszeit: Zeitraum, in dem das Zertifikat zur ePA-Authentisierung verwendet wird.
  - Beginnt am Tag der Ausstellung des Zertifikats.
- Überlappungszeit: Zeitraum zur Beantragung eines neuen Zertifikats. Das Zertifikat kann innerhalb dieser Zeit noch zur Authentisierung verwendet werden.

<u>Hoheitlicher Bereich</u>

Terminal	Anwendung	Betriebsart	Gültigkeitszeitraum	
			Nutzung	Überlappung
Inspektionssystem	Kontrollprozess (Lesen der eID-Daten)	verteilt	30 Tage	2 Tage
Inspektionssystem	Kontrollprozess (Lesen der eID-Daten)	integriert	1 Tag	1 Tag
Visualisierung / Änderungsterminal	Auskunftsbegehren / Änderungsdienst (Lesen/Schreiben eID-Daten)	verteilt	30 Tage	2 Tage
Visualisierung / Änderungsterminal EAC-Box	Auskunftsbegehren / Änderungsdienst (Lesen/Schreiben eID-Daten)	integriert	1 Tag	1 Tag
Sonderfall				
Qualitätskontroll-Terminal[1]	Produktionsprozess Qualitätssicherung (Lesen von eID-Daten)	integriert/ verteilt	90 Tage	14 Tage

Tabelle 20: Gültigkeitszeiten hoheitliche Terminals

[1]Das Qualitätskontroll-Terminal DARF NUR vom Ausweisproduzenten in dessen sicherer Produktionsumgebung betrieben werden.

Nicht hoheitlicher Bereich

Für nicht hoheitliche Terminals entfällt die Unterscheidung der Betriebsart in verteilt/integriert (wie in Abschnitt 1.1 beschrieben).

Terminal	Anwendung	Gültigkeitszeitraum	
		Nutzung	Überlappung
Remote-Terminal Diensteanbieter	Online-Authentisierung (Lesen der eID-Daten)	1 Tag	1 Tag
Remote-Terminal Diensteanbieter	Online-Authentisierung (Verifizieren von Alter und Wohnort)	30 Tage	2 Tage
Remote-Terminal Diensteanbieter	Online-Authentisierung (Nachladen QES)	30 Tage	2 Tage
Offline Terminal Automatenbetrieb	Offline-Authentisierung (Altersverifikation)	30 Tage	7 Tage
Offline Terminal Automatenbetrieb	Offline-Authentisierung (Lesen der eID-Daten)	In Abstimmung mit der Root	

Tabelle 21: Gültigkeitszeiten nicht hoheitliche Terminals

6.4 Aktivierungsdaten

Siehe Abschnitt 6.2.7.

6.5 Sicherheitsmaßnahmen für die Rechneranlagen

Generell MÜSSEN alle an der CVCA-eID PKI teilnehmenden Organisationen für ein angemessenes Sicherheitsniveau ihrer Rechneranlagen sorgen. Dies betrifft insbesondere:

- Implementierung und Pflege von Sicherheitskomponenten (Virenscanner, Firewalls)
- Updatemanagement (regelmäßiges Installieren von Sicherheitsupdates)
- Umsetzung der Rollentrennung
- Implementierung und Betrieb von Protokollierungsmechanismen

Hoheitliche Document Verifier und BerCAs MÜSSEN zusätzlich die in Abschnitt 5.1.2 definierten Anforderungen erfüllen.

6.6 Zeitstempel

Entfällt.

6.7 Validierungsmodell

Die Validierung der Zertifikate basiert auf dem Schalenmodell.

7 Profile für Zertifikate und Sperrlisten

7.1 Profile für Zertifikate und Zertifikats-Requests

Die in der CVCA-eID PKI verwendeten Zertifikate sind selbst-beschreibende Card Verifiable Zertifikate (CV-Zertifikate) konform zum ISO Standard 7816 (ISO/IEC 7816-4:2005, ISO/IEC 7816-6:2004, ISO/IEC 7816-8:2004).

Das zu verwendende Profil für Zertifikate und Zertifikats-Requests ist in [TR-03110] spezifiziert. Unter anderem werden in dieser Richtlinie auch die Anforderungen an die Kodierung sowie die OIDs definiert.

Welche kryptografischen Verfahren und Schlüssellängen zu verwenden sind, ist in [TR-03116-2] festgelegt. Diese technische Richtlinie ist entscheidend für das Sicherheitsniveau des ePA und wird daher fortlaufend aktualisiert.

Darüber hinaus enthält diese Policy Anforderungen für die Belegung folgender Zertifikats-Felder.

Feld	Bedeutung	Abschnitt
`Certificate Holder Reference`	Antragssteller	3.1
`Certificate Effective Date` `Certificate Expiration Date`	Gültigkeitszeitraum	6.3.2
`Certificate Holder Authorization Template`	Zugriffsrechte	7.1.1

Tabelle 22: Übersicht Felder CV-Zertifikat mit vorgegebener Wertebelegung

7.1.1 Zugriffsrechte

Die CVCA-eID MUSS die angegebenen Zugriffsrechte in den von ihr ausgestellten DV-Zertifikaten (C_{DV}) im Feld `Certificate Holder Authorization Template (CHAT)` setzen. Diese Zugriffsrechte stellen das Maximum an Zugriffsrechten dar, die vom jeweiligen DV an ein Terminal über das Terminal-Zertifikat ($C_{Terminal}$) weitergeben werden kann.

Document Verifier sind im Sinne der Datensparsamkeit angehalten, für Terminal-Zertifikate immer die minimal erforderlichen Zugriffsrechte zu gewähren. Im nicht hoheitlichen Bereich werden diese durch die VfB bestimmt.

Die Rechte zur Installation eines qualifizierten Signaturzertifikates und zum Auslesen des Ablaufdatums darf gewährt werden, wenn im Bescheid der VfB als Verwendungszweck "Nachladen der qualifizierten Signatur auf dem Personalausweis" angegeben ist.

Die folgende Tabelle 23 definiert, welche Zugriffsrechte über die Zertifikate der CVCA-eID PKI gesetzt werden dürfen. Wie die Zugriffsrechte im CHAT zu kodieren sind, ist in Anhang C der [TR-03110] spezifiziert.

Erlaubte Zugriffsrechte für CVCA-/DV-Zertifikate[1]			
Auszustellender Zertifikatstyp	**CVCA-eID** C_{CVCA}	**Nicht Hoheitlich** C_{DV}	**Hoheitlich** C_{DV}
Schreibzugriff			
DG 17 (Anschrift)	ja	nein	ja
DG 18 (Wohnort-ID)	ja	nein	ja
DG 19 (Nebenbestimmungen I – eAT)	ja	nein	ja
DG 20 (Nebenbestimmungen II – eAT)	ja	nein	ja
DG 21 (unbenutzt)	ja	nein	nein
Lesezugriff			
DG 1 (Dokumententyp)	ja	ja	ja
DG 2 (Ausgebender Staat)	ja	ja	ja
DG 3 (Ablaufdatum)	ja	ja	nein
DG 4 (Vorname(n))	ja	ja	ja
DG 5 (Familienname)	ja	ja	ja
DG 6 (Ordens-/Künstlername)	ja	ja	ja
DG 7 (Doktorgrad)	ja	ja	ja
DG 8 (Geburtsdatum)	ja	ja	ja
DG 9 (Geburtsort)	ja	ja	ja
DG 10 (Staatsangehörigkeit)	ja	ja	ja
DG 11 – DG 12 (unbenutzt)	nein	nein	nein
DG 13 (Geburtsname)	ja	ja	ja
DG 14 – DG 16 (unbenutzt)	nein	nein	nein
DG 17 (Anschrift)	ja	ja	ja
DG 18 (Wohnort-ID)	ja	nein	ja
DG 19 (Nebenbestimmungen I – eAT)	ja	ja	ja
DG 20 (Nebenbestimmungen II – eAT)	ja	nein	ja
DG 21 (unbenutzt)	nein	nein	nein
Spezielle Funktionen			
Installation qualifiziertes Signaturzertifikat	ja	ja	nein
Installation Signaturzertifikat	ja	nein	nein
PIN-Management	ja	nein	ja
CAN allowed	ja	nein	ja
Privilegiertes Terminal	ja	nein	ja
Pseudonym	ja	ja	nein
Wohnortverifikation	ja	ja	nein
Altersverifikation	ja	ja	nein

Tabelle 23: Erlaubte Zugriffsrechte für CVCA-/DV-Zertifikate

1 Die Darstellung in der Tabelle entspricht nicht dem CHAT Aufbau (siehe [TR-03110]).

7.1.2 Zertifikatserweiterung

Jedes Zertifikat, welches von einer BerCA ausgestellt wird, MUSS die folgenden Certificate Extensions enthalten:

- `CertificateDescription` (spezifiziert in [TR-03110]). Diese Extension enthält Informationen zum Diensteanbieter. Der Inhalt MUSS dem durch die VfB in der Berechtigung enthaltenen Inhalt entsprechen.

  Wird das Zertifikat zur Verwendung bei einer Online-Authentisierung ausgestellt, MUSS diese Extension zusätzlich eine Liste von Hash-Werten der vom Diensteanbieter für die Kommunikation zwischen Web-Browser und Diensteanbieter-Server(n) sowie zwischen eID-Server und eCard-API Softwareimplementierung (bspw. AusweisApp) verwendeten Kommunikationszertifikate enthalten. Die BerCA MUSS beim Ausstellen der Certificate Extension sorgfältig prüfen, dass die Hash-Werte der korrekten Kommunikationszertifikate des Diensteanbieters aufgenommen werden.
- `TerminalSector` (spezifiziert in [TR-03110]). Diese Extension enthält den öffentlichen Schlüssel des Diensteanbieters für die Erzeugung von Sperrmerkmal und Pseudonym. Das entsprechende Schlüsselpaar wird durch die BerCA erzeugt, der private Schlüssel wird durch die BerCA für die Berechnung von diensteanbieterspezifischen Sperrlisten gespeichert (siehe [TR-03127]/[TR-03128]).

Zertifikatserweiterungen, die über die aufgeführten Zertifikatserweiterungen hinausgehen, MÜSSEN mit der CVCA-eID abgestimmt werden.

7.2 Profile für Sperrlisten

In der CVCA-eID PKI werden keine Sperrlisten ausgestellt.

Ausgenommen sind hiervon die internen Sperrlisten der RAs zum Sperren von Wiederholungsanträgen (siehe Abschnitt 3.3). Für diese wird kein Profil vorgegeben.

7.3 Profile für OCSP-Dienste

In der CVCA-eID PKI werden keine OSCP-Dienste eingesetzt.

8 Überprüfung und andere Bewertungen

Jeder Betreiber einer PKI-Instanz der CVCA-eID PKI verpflichtet sich zur Einhaltung dieser von der Root (CVCA-eID) herausgegebenen CP zur Durchführung eines ordnungsgemäßen Betriebs. Überdies ist diese Policy in der für den ePA maßgebenden Verordnung „Über Personalausweise und den elektronischen Identitätsnachweis“ [PAuswV] verankert.

Die grundlegenden Prüfungsanforderungen an die verschiedenen PKI-Instanzen werden in Abschnitt 8.1 beschrieben.

Das Vorgehen bei identifizierten Mängeln ist in Abschnitt 8.2 definiert.

8.1 Inhalte, Häufigkeit und Methodik

In diesem Abschnitt werden die grundlegenden Prüfanforderungen für die PKI-Instanzen der CVCA-eID PKI beschrieben.

CVCA-eID (Root-Ebene)

Der Betrieb der CVCA-eID MUSS in der sicheren Betriebsumgebung des BSI erfolgen. Diese erfüllt alle in dieser Certificate Policy definierten Anforderungen sowie die Sicherheits-anforderungen des IT-Grundschutzes.

DV-Ebene

Ab der DV-Ebene unterscheidet die Prüfsystematik zwischen der **hoheitlichen** und der **nicht hoheitlichen** Verwendung.

Für die DV-Ebene ist ein „**Audit“** ohne Zusatz wie bspw. „IT-Grundschutz“ wie folgt definiert:

> „Systematische unabhängige Untersuchung, inwieweit die realisierten, qualitätsbezogenen Tätigkeiten und die hieraus resultierenden Ergebnisse mit den geplanten Anforderungen übereinstimmen und geeignet sind, die Zielstellung zu erreichen.“
>
> Status des Auditors: 3rd Party = unabhängiger Auditor einer akkreditierten Zertifizierungsstelle (Akkreditierung nach DIN EN 45000 ff. und DIN EN/ISO 17000 ff.)
>
> Vorgehensweise: nach DIN ISO 19011 (Leitfaden für Audits von QMS/UMS)
>
> Informationssammlung mittels
>
> - Auswertung von Dokumenten
> - Befragung/Beobachtung von Tätigkeiten
> - Stichprobenartige Verifizierung insbesondere IT-gestützter Abläufe
>
> Untersuchungsgegenstand: Eingerichteter Betrieb der PKI-Instanz DV
>
> Prüftiefe: Wird im Einzelfall im Auditplan fixiert und ist system- und verfahrensorientiert.
>
> Systemorientierung = Struktur- und Funktionsaspekte (Aufbauorganisation, Dienste, Aufgaben, Personaleinsatz)
>
> Verfahrensorientierung = Prozessabläufe und Tätigkeiten (Ablauforganisation, Rollen)

Hoheitlicher Bereich

Die nachfolgenden Tabellen enthalten die Prüfanforderungen für die PKI-Instanzen des hoheitlichen Bereichs von der DV-Ebene bis zum Terminalbetreiber.

Hoheitlicher Document Verifier				
Häufigkeit	**Inhalt**	**Grundlage**	**Nachweis**	**Durchführung**
(Vor Aufnahme Wirkbetrieb) Bei **Änderungen** am Pflichtenheft / DV CP	Abstimmung Pflichtenheft[1], IT-Sicherheitskonzept[2] und DV CP	DV CP, CVCA-eID CP, TRs, IT-Sicherheitskonzept, Pflichtenheft	Bestätigung	BSI
	Audit	CVCA-eID CP, IT-Sicherheitskonzept, Pflichtenheft, CPS	Prüfbericht	DV beauftragt externe Prüfstelle
Optional (Empfohlen)	IT-Grundschutz Audit nach 27001	CVCA-eID CP, TRs, IT-Sicherheitskonzept, Pflichtenheft, CPS	Zertifikat	DV beauftragt externen IT-Grundschutz Auditor

Tabelle 24: Prüfanforderungen Hoheitlicher Document Verifier

[1] Im Rahmen eines Auftragsverhältnisses für einen hoheitlichen DV verpflichtend, sonst auf Wunsch (siehe [TR-03128]).

[2] Sichtung auf Eignung.

Hoheitlicher Terminalbetreiber				
Häufigkeit	**Inhalt**	**Grundlage**	**Nachweis**	**Durchführung**
Initial (Vor Aufnahme Wirkbetrieb)	Prüfung hoheitlicher Einsatz und Terminaleignung	DV CP, TRs, Einsatz und Gerätebeschreibung	Berechtigung	Hoheitlicher DV im Rahmen der Registrierung

Tabelle 25: Prüfanforderungen Hoheitlicher Terminalbetreiber

Nicht hoheitlicher Bereich

Die nachfolgenden Tabellen enthalten die Prüfanforderungen für die PKI-Instanzen des nicht hoheitlichen Bereichs von der BerCA-Ebene bis zum Diensteanbieter / eID-Service Provider.

BerCA				
Häufigkeit	**Inhalt**	**Grundlage**	**Nachweis**	**Durchführung**
Initial (Vor Aufnahme Wirkbetrieb)	Formale Prüfung der Voraussetzungen gemäß [BVA01] und [TR-03128]	Anzeige von ZDAs nach SigG u. SigV	Berechtigung	Anzeige VfB / BSI
	Einhaltung der Anforderung der CVCA-eID CP.	DV Certificate Policy	Bestätigung	BSI
Optional (Empfohlen)	IT-Grundschutz Audit nach 27001	CVCA-eID CP, TRs, IT-Sicherheits-konzept, Pflichten-heft, CPS	Zertifikat	BerCA beauftragt externen IT-Grundschutz Auditor

Tabelle 26: Prüfanforderungen BerCA

Diensteanbieter				
Häufigkeit	**Inhalt**	**Grundlage**	**Nachweis**	**Durchführung**
Initial (Vor Aufnahme Wirkbetrieb)	Eignung des Diensteanbieters gem. § 21 PAuswG	Verwaltungsverfahren nach PAuswG [PAuswG]	Berechtigung	VfB

Tabelle 27: Prüfanforderungen Diensteanbieter

eID-Service Provider (beauftragt durch Diensteanbieter)				
Häufigkeit	**Inhalt**	**Grundlage**	**Nachweis**	**Durchführung**
Initial (Vor Aufnahme Wirkbetrieb)	Eignung des eID-Service Provider gem. § 21 PAuswG	§11 BDSG, Berechtigung	Vertragliche Vereinbarung.	Diensteanbieter

Tabelle 28: Prüfanforderungen eID-Service Provider

8.2 Reaktionen auf identifizierte Vorfälle

Initiale Prüfung

Die Teilnehmer der CVCA-eID PKI MÜSSEN die entsprechenden in Abschnitt 8.1 aufgeführten Anforderungen an die initiale Prüfung ohne Mängel erfüllen, um mit dem Wirkbetrieb beginnen zu können.

Vorfall im Betrieb

Ein Vorfall im Betrieb ist wie in Abschnitt 5.7.1 beschrieben, an die übergeordnete PKI-Instanz zu melden.

Zeigt der Vorfall einen sicherheitskritischen Mangel auf, ist eine sorgfältige Prüfung des Vorfalls erforderlich. Die Beseitigung des Mangels MUSS nachgewiesen werden, bevor ein neues Zertifikat ausgestellt werden darf.

Ist der Vorfall nicht sicherheitskritisch, KANN ein erneuter initialer Zertifikats-Request über die bestehende sichere SSL-Verbindung zugestellt werden (siehe Abschnitt 3.3.2).

9 Sonstige finanzielle und rechtliche Regelungen

9.1 Preise

Nachfolgend werden die preislichen Regelungen für die PKI-Instanzen der CVCA-eID PKI angegeben.

CVCA-eID (Root-Ebene)

Das Bundesamt für Sicherheit in der Informationstechnik, hier in seiner Funktion als Root der Public Key Infrastrukturen für hoheitliche Dokumente, erhebt gemäß § 1 BSI-KostV für Amtshandlungen nach § 3 Abs. 1 Nr. 3, 5, 6 und 7 des BSI-Errichtungsgesetzes Kosten nach der BSI-Kostenverordnung (BSI-KostV).

Zertifizierungen von Certification Authorities sind als solche Amtshandlungen anzusehen und mit einem festen Gebührensatz im Gebührenverzeichnis zur BSI-KostV verankert. Da Document Verifier ihrer Aufgabenstellung entsprechend CAs sind, besteht grundsätzlich eine Kostenerstattungspflicht für die Ausstellung von Berechtigungszertifikaten durch die Root.

Inwieweit sachlich oder persönlich begründete Gebührenfreiheit bzw. Ausnahmen nach dem Verwaltungskostengesetz (VwKostG) bestehen, wird im Einzelfall geprüft.

DV- und Terminal-Ebene

An die Betreiber von PKI-Instanzen auf DV- und Terminal-Ebene sowohl hoheitlich als auch nicht hoheitlich werden **keine preislichen Anforderungen** gestellt.

9.2 Finanzielle Zuständigkeiten

Die finanzielle Zuständigkeit des BSI obliegt den entsprechenden Regelungen der Bundesverwaltung.

Die Betreiber von PKI-Instanzen auf DV- und Terminal-Ebene sowohl hoheitlich als auch nicht hoheitlich sind finanziell für sich selbst zuständig.

10 Anhang

Definitionen

Begriff	Erläuterung
Änderungsdienst	Hoheitlicher Funktionsumfang zur Aktualisierung der Angaben zur Adresse und im Rahmen des PIN-Managements.
Altersverifikation	Im ePA verfügbare Funktionalität zum Nachweis einer geforderten Altersgrenze, ohne das tatsächliche Alter preiszugeben.
Antragssteller	Ein Zertifikatsnehmer, der einen Zertifikatsantrag stellt.
Auskunftsbegehren	Recht des Dokumenten-Inhabers zur Visualisierung der im Chip des ePA gespeicherten, persönlichen Daten.
Authentifizierungsterminal	Terminaltyp zum berechtigten Zugriff/Nutzung der eID-Anwendung im hoheitlichen (hoh.) und nicht-hoheitlichen (nhoh.) Einsatzszenario.
Berechtigungs Certification Authority	Aufgabe der BerCAs (Certification Authorities) ist die Annahme von Zertifikats-Requests und das Ausstellen von Berechtigungszertifikaten (Terminal-Zertifikaten) für Diensteanbieter.
Country Verifying Certification Authority	Die CVCA ist der einzige nationale Sicherheitsanker, der Document Verifier (DV) zum Ausstellen von Terminal-Zertifikaten autorisieren darf. Die deutsche CVCA stellt also Zertifikate für DVs aus, damit die von dieser Organisationseinheit verwalteten Terminals auf die im Chip des ePA's gespeicherten Daten zugreifen können.
DefectListe	Datenstruktur mit Informationen zum Korrigieren, Sperren und Austauschen von CSCA- und DS-Zertifikaten gemäß [TR-03129]. DefectListen sollen zukünftig Sperrlisten nach X.509 zum Sperren von CSCA- und DS-Zertifikaten ablösen.
Diensteanbieter	Begriff gemäß § 2, Absatz 2 PAuswG. Alle Anbieter, die ihre Dienstleistung(en) IT-gestützt online oder offline bereitstellen bzw. die Abwicklung durch IT unterstützen. Diese sind die verantwortlichen Terminal-Betreiber (Instanz auf Terminal-Ebene). Der Betrieb von Terminals kann an Dritte übertragen werden (z.B. an einen eID-Service).
Document Verifier	Ein DV ist eine Organisationseinheit zur Verwaltung von Terminals. Technisch betrachtet ist der DV eine CERTIFICATION AUTHORITY, die im Rahmen der EAC-PKI (Berechtigungs-)Zertifikate für Terminals ausstellt.
eBusiness	Online basiertes Dienstleistungs-Portfolio der Wirtschaft.
eGovernment	Online basiertes Dienstleistungs-Portfolio der öffentlichen Verwaltung.

eID-Anwendung	Funktionalität und Datenstruktur für Online-Identitätsnachweise mit dem elektronischen Personalausweis.
eID-Service Provider	Dienstleister, die die eID-Funktionalitäten im Auftrag eines oder mehrerer Diensteanbieter für diese abwickeln.
ePass-Anwendung	Funktionalität und Datenstruktur entsprechend dem deutschen elektronischen Reisepass nach ICAO 9303.
eSign-Anwendung	Funktionalität und Datenstruktur zur Schlüsselgenerierung, Zertifikatsbeantragung und –speicherung sowie Signaturerstellung für qualifizierte elektronische Signaturen.
elektronische Identität	Die in der elektronischen Kommunikation eingenommene Empfänger-/Absender-Identität.
elektronischer Personalausweis	Der elektronische Personalausweis (ePA) enthält einen RF-Chip, auf welchem biografische und biometrische Angaben zum Inhaber in digitaler Form gespeichert sind. Als multifunktionales Identitätsdokument sind optional eine elektronische Identitäts- (eID) und eine Signatur-Funktion integrativ vorbereitet. Inhaber sind Bürger der BRD.
Fingerprint	Hashwert über ein Zertifikat oder einen Zertifikats-Request.
Kryptografiemodul	Funktionseinheit zur Erzeugung und sicheren Speicherung kryptografischen Schlüsselmaterials, Erstellung von Zertifikats-Requests sowie Leistung elektronischer Signaturen.
Kommunikations-zertifikate	Zertifikate zur Verbindungsauthentisierung innerhalb einer SSL/TLS-Verbindung. Jeder Kommunikationspartner muss zur Verbindungsauthentisierung grundlegend über zwei Zertifikate (Client- und Server-Zertifikat) verfügen. Der jeweilige Initiator verwendet das Client-Zertifikat die Gegenstelle das Server-Zertifikat.
Lokales Lesegerät	Im Zusammenhang mit der Online-Authentisierung im nicht-hoheitlichen Einsatzszenario eingesetztes Lesegerät vor Ort beim Nutzer, über welches der MRTD-Chip mit dem Remote-Lesegerät interagiert.
Password Authenticated Connection Establishment	Passwort-basiertes Zugriffsprotokoll zum sicheren Zugriff von autorisierten Lesegeräten auf Daten und Anwendungen in MRTD-Chips.
qualifizierte Signatur	Qualifizierte elektronische Signatur entsprechend dem Signaturgesetz (SigG).
Remote-Lesegerät	Im Zusammenhang mit der Online-Authentisierung im nicht-hoheitlichen Einsatzszenario eingesetztes Lesegerät vor Ort beim Diensteanbieter, welches zusammen mit dem Nutzer über das lokale Lesegerät mit dem MRTD-Chip interagiert.

Regierungsnetz	Kommunikationsinfrastruktur für die zuverlässige und sichere Sprach- und Datenkommunikation zwischen den obersten Bundesbehörden und Verfassungsorganen in Berlin und Bonn
RF-Chip	Chip mit kontaktloser Schnittstelle auf Basis von Hochfrequenztechnik (Radio Frequency). Hier: in das maschinenlesbare Dokument (ePA) eingebrachter RF-Chip zur Speicherung der dokumenten- und personenbezogenen Daten.
Sperrdienst	Zuständige Stelle für die Bereitstellung von Sperrlisten zu den von Ausweisinhabern ausgelösten eID-Sperren.
Terminal	Ein Terminal ist ein Lesegerät, dass mit dem RF-Chip im ePA kommuniziert.
Trust-Point	Bei Produktion gesetzter und bei Gültigkeitsprüfungen von Terminal-Zertifikaten aktualisierter Sicherheitsanker im Chip des ePAs (CVCA- resp. CVCA-Link-Zertifikate).
Vergabestelle für Berechtigungszertifikate	Für die Erteilung und Aufhebung von Berechtigungen nach §21 PAuswG zuständige Stelle.
Visualisierung	Sichtbarmachung der elektronisch auf dem Chip eines ePA‘s gespeicherten dokumenten- und personenbezogenen Daten.
Zertifikatsantrag	Vorgang der Beantragung eines Zertifikats.
Zertifikatsnehmer	Ist eine Instanz der PKI, die von einer übergeordneten Instanz Zertifikate bezieht (siehe Abschnitt 1.3.3). Ausnahme bildet die CVCA-eID diese stellt sich selbst Zertifikate (selbst-signierte Zertifikate) aus.
Zertifikats-Request	Der technische Antrag auf ein Zertifikat (siehe Certificate Request in [TR-03110])

Tabelle 29: Begriffsbestimmung

Abkürzung	Begriff
AuthT	Terminaltyp: Authentisierungsterminal
BerCA	Berechtigungs Certificate Authority
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
CAR	Certification Authority Reference
CHAT	Certificate Holder Authorization Template
CHR	Certificate Holder Reference
C_{NN}	Berechtigungs-Zertifikat der jeweiligen (PKI-) Hierarchiestufe (NN= CVCA, DV oder Terminaltyp: IS, hoh./nhoh. AuthT, SignT)
CPS	Certifcate Practise Statement
CRL	Zertifikatssperrliste
CVCA	Country Verifying Certification Authority
DG	Datengruppe
DIN	Deutsches Institut für Normung
DV	Document Verifier
DVCA	Document Verifying Certification Authority
EAC	Extended Access Control
EAL	Common Criteria Prüftiefe
eID	elektronischer Identitätsnachweis (Anwendung im ePA)
ePA	elektronischer Personalausweis
ePass	elektronischer Reisepass (Anwendung im ePA)
eSign	elektronische Signatur (Anwendung im ePA)
hoh.	hoheitlich(es Einsatzszenario)
HSM	Hardware Sicherheitsmodul
IS	Inspektionssystem
ISO	International Organization for Standardization
KEK	Key Encryption Key
KM	Kryptografiemodul (siehe HSM)
MRTD	Machine Readable Travel Document
nhoh.	nicht-hoheitlich(es Einsatzszenario)
OID	Object Identifier
OSCP	Sperrabfragedienst
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number
PKey	Öffentlicher Schlüssel
PKI	Public Key Infrastruktur
PUK	PIN Unblocking Key
QES	qualifizierte elektronische Signatur
RA	Registration Authority

RF	Radio Frequency
RFC	Requests for Comments (Technischer Standard)
SigG	Gesetz zur digitalen Signatur (Signaturgesetz)
SignT	Signaturterminal
SigV	Verordnung zur elektronischen Signatur (Signaturverordnung)
SKey	Geheimer Schlüssel
SPOC	Kommunikationsschnittstelle zur CVCA-eÍD
SSL	Protokoll Verbindungsauthentisierung/Verschlüsselung
TLS	Protokoll Verbindungsauthentisierung/Verschlüsselung
TR	Technische Richtlinie
URL	Uniform Resource Locator (hier Internetadresse)
VfB	Vergabestelle für Berechtigungszertifikate
ZDA	Zertifizierungsdiensteanbieter

Tabelle 30: Abkürzungen

Literaturverzeichnis

TR-03127	BSI: Technische Richtlinie TR-03127, Architektur Elektronischer Personalausweis
TR-03110	BSI: Technische Richtlinie TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)
TR-03128	BSI: Technische Richtlinie TR-03128. EAC-PKI'n für den elektronischen Personalausweis
PAuswG	Gesetz über den Personalausweis und den elektronischen Identitätsnachweis(Personalausweisgesetz, PersAuswG)
PAuswV	Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung, PersAuswV)
TR-03129	BSI: Technische Richtlinie TR-03129. PKI for the Extended Access Control (EAC), Protocol for the Management of Certificates and CRLs
RFC 3647	Chokhani, S.; Ford, W.; Sabett, R.; Merrill, C.; Wu, S.:Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework
RFC 2119	Bradner, S.: Key words for use in RFCs to indicate requirement levels
TR-03131	BSI: Technische Richtlinie TR-03131. EAC-Box Architecture and Interfaces
SigG, SigV	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) und Verordnung zur elektronischen Signatur (Signaturverordnung – SigV)
CP V-PKI	BSI: Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung
BVA01	BVA: Aufbau eines Test-Sperregisters für den ePA - Anzeigeverfahren für das Bundesverwaltungsamt
BVA02	BVA: Antragsvefahren für Diensteanbieter
TR-03116-2	BSI: Technische Richtlinie TR-03116-2. eCard-Projekte der Bundesregierung
TR-02102	BSI: Technische Richtlinie TR-02102. Kryptografische Verfahren: Empfehlungen und Schlüssellängen
PP-CM-m	BSI: Protection Profile - Cryptografic Modules, Security Level "Moderate"
PP-SSCD	CEN/ISSS: Protection Profile - Secure Signature-Creation Device
AIS 20/31:	Wolfgang Killmann (T-Systems GEI GmbH), Werner Schindler (Bundesamt für Sicherheit in der Informationstechnik), A proposal for:Functionality classes for random number generators, September 2011
TR-03130	BSI: Technische Richtlinie TR-03130. eID-Server
PP-IS	BSI: Protection Profile for Inspection Systems (IS)

Fw: Bachelorarbeit: Elektronische Identifikation

09.08.2015 15:42

Von Tanja Dinkel <tanjadinkel@gmx.de>

An Lea Miene <leamiene@t-online.de>

From: KUSTOR, Peter
Sent: Monday, June 22, 2015 4:55 PM
To: Tanja Dinkel
Cc: jens.bender@bsi.bund.de
Subject: AW: Bachelorarbeit: Elektronische Identifikation

Sehr geehrte Frau Dinkel,

habe nun auch Infos direkt aus berufenem Mund in Deutschland. Jens Bender vom BSI war so freundlich, die folgenden Infos zur Verfügung zu stellen und bietet freundlicherweise auch an, sich direkt an ihn zu wenden bei allfälligen weiteren Fragen (mail in :cc). Ich gebe die Info direkt so weiter, wie ich sie erhielt:

***

Vorbemerkung: In DE sind Identifizierung und Signatur zwei unterschiedliche Funktionen (sowohl technologisch als auch "logisch"). Die folgenden Angaben sind nur für die eID-Funktion. Zahlen für die Signatur auf dem Ausweis oder auf getrennten Signaturkarten habe ich nicht.

Ausgegebene eID-Karten (Personalausweise + Aufenthaltstitel): ~40 Millionen

Die eID-Funktion kann kartenseitig abgeschaltet werden. Zur Zeit haben wir etwa 30% Einschaltquote (etwas schwankend je nach Kommune), d.h. über den Daumen geschätzte ~ 12 Millionen aktivierte eID-Karten.

Konkrete Nutzung können wir (aus dem gleichen Grund wie bei der AT-Karte) nicht zählen.

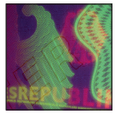
***

Beste Grüße,
Peter Kustor

SICHERHEITSMERKMALE DES PERSONALAUSWEISES

1+14 Mehrfarbige Guillochen. Guillochen sind Schutzmuster aus feinen, ineinander verschlungenen Linien. Bei Reproduktionen werden die Linienstrukturen des Originals in punktierte Rasterstrukturen aufgelöst. Die Guillochen zeigen als zentrale Motive auf der Vorderseite den Bundesadler und auf der Rückseite das Brandenburger Tor.

2+15 Mikroschriften. In das Sicherheitsdruckdesign ist als Positiv- und Negativmikroschrift der Schriftzug „BUNDESREPUBLIK DEUTSCHLAND“ integriert.



3+16 UV-Aufdruck. Unter UV-Beleuchtung lumineszieren das Guillochenmotiv in mehreren Farben. Auf der Vorderseite ist zusätzlich ein UV-Aufdruck mit Bundesadlern und der Endlosschrift „BUNDESREPUBLIK DEUTSCHLAND“ enthalten.

4 Optischvariable Farben. Das Erscheinungsbild der Titelzeile „BUNDESREPUBLIK DEUTSCHLAND“ geht beim Kippen der Karte – je nach Betrachtungswinkel – von Grün in Blau über.

5 Holografisches Porträt. Das Lichtbild wird bei Betrachtung unter flacherem Winkel rechts neben dem herkömmlichen Bild in holografischer Form sichtbar. In diese Sekundärdarstellung des Ausweisfotos sind vier Bundesadlermotive eingearbeitet.

6 3D-Bundesadler. Eine 3D-Darstellung des Bundesadlers ist unter bestimmten Betrachtungswinkeln in roter Farbe über der sechsstelligen Kartenzugangsnummer erkennbar.

7 Kinematische Bewegungsstrukturen. Die über dem herkömmlichen Lichtbild angeordneten Bewegungsstrukturen zeigen einen von zwölf Sternen umgebenen Bundesadler.

Durch Kippen der Ausweiskarte verwandelt sich das Adlermotiv über eine Sechseckstruktur in den Buchstaben „D“. Außerdem bewegen sich die Sechsecke; die Sterne verändern abwechselnd ihre Größe.

8 Makroschriften. Über dem linken Rand des herkömmlichen Lichtbildes erscheint im Hologramm ein geschwungenes Makroschriftband mit dem Text „BUNDESREPUBLIK DEUTSCHLAND“, an das sich mehrere Mikroschriftzeilen mit gleichem Inhalt anschließen.

9 Kontrastumkehr. Beim Kippen der Karte erfolgt beim kinematischen Adlermotiv eine Kontrastumkehr: Der zunächst helle Adler erscheint nun dunkel in einer hellen Sechseckfläche.

10 Maschinell prüfbare Struktur. Das Identigram® enthält eine Struktur, die neben der Sichtkontrolle auch eine maschinelle Echtheitsprüfung des Ausweises ermöglicht. Diese Struktur beinhaltet keine personenbezogenen oder dokumentenspezifischen Daten.

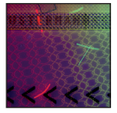
11 Farbintegrationstechnik (InnoSec®FUSION). Das Lichtbild wird über das Personalisierungssystem InnoSec®FUSION

farbig dargestellt und sicher in das Material der Karte integriert. Mit der gleichen Technik wird die alphanumerische Seriennummer (in OCR-B-Schrift) eingebracht.

12+20 Lasergravur. Alle Personalisierungsdaten – außer Lichtbild und Seriennummer – sind mittels Lasergravur kontrastreich in die inneren Kartenschichten des Ausweiskörpers integriert.

13 Taktile Merkmale. Das Gültigkeitsdatum und die sechsstellige Kartenzugangsnummer auf der Vorderseite des Personalausweises werden per Lasergravur als fühlbare Schrift aufgebracht.

17 Personalausweislogo. Dieses Logo wird auf der Rückseite der Ausweiskarte abgebildet. Es kennzeichnet seit November 2010 auch Anwendungen und Lesegeräte, die den neuen Personalausweis unterstützen.

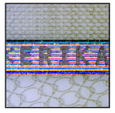


18 Melierfasern. Auf der Ausweisrückseite sind transparente Melierfasern in das Kartenmaterial integriert. Diese sind unregelmäßig verteilt und lumineszieren unter UV-Beleuchtung.

19 Oberflächenprägung. Eine Sicherheitsprägung von Mikroschriften und einer Deutschlandkarte auf der Kartenrückseite verleihen dem Dokument im linken oberen Bereich eine reliefartig fühlbare Oberfläche.

21 Laserkippbild. Im so genannten Changeable Laser Image (CLI) werden – je nach Betrachtungswinkel – das Gültigkeitsdatum des Dokuments oder das Porträt des Ausweisinhabers sichtbar.

22 Maschinenlesbare Zone. Die maschinenlesbaren Zeilen auf der Ausweisrückseite enthalten Dokumententyp, Ausstellungsland, Seriennummer, Geburtsdatum, Gültigkeitsdatum, Staatsangehörigkeit, Namen sowie Prüfziffern in maschinell lesbarer Form (OCR-B).



23 Personalisierter Sicherheitsfaden. Auf der Ausweisrückseite verläuft horizontal ein maschinell prüfbarer Sicherheitsfaden, der mit der Dokumentennummer sowie dem Namen des Ausweisinhabers personalisiert wird.

Nachträgliche Adressänderungen werden auch beim neuen Personalausweis mittels eines Aufklebers verzeichnet, der durch eine transparente Folie geschützt sein kann. Das für den Aufkleber verwendete Sicherheitspapier ist mit einem zweifarbigen Guillochenmotiv bedruckt und enthält spezielle Fasern, die unter UV-Beleuchtung mehrfarbig lumineszieren. Neben der neuen Anschrift wird auf dem Adressaufkleber auch die Seriennummer des Ausweises eingetragen sowie das Dienstsiegel der zuständigen Behörde angebracht.

SICHERHEIT IM SCHECKKARTENFORMAT

Der Personalausweis mit eID enthält zahlreiche Sicherheitsmerkmale, die bestmöglichen Schutz vor Fälschung und Missbrauch bieten. Diese Merkmale machen den Ausweis zu einem der sichersten der Welt.

Auf den folgenden Seiten werden alle wesentlichen Sicherheitsmerkmale des Personalausweises kurz erläutert und dargestellt. Unter anderem zählen dazu der komplexe Sicherheitsdruck mit mehrfarbigen Linienstrukturen, Mikroschriften, taktile Merkmale, feine Oberflächenprägungen sowie ein Laserkippbild und ein integrierter Sicherheitsfaden. Das bereits bewährte Identigram®, ein komplexes holografisches Reproduktionsschutzmerkmal, enthält folgende Elemente: kinematische Bewegungsstrukturen über dem herkömmlichen Lichtbild, das Lichtbild des Ausweisinhabers in holografischer Form, den Bundesadler in dreidimensionaler Darstellung, den Namen des Ausweisinhabers sowie die Seriennummer des Ausweises.

Der Personalausweis mit eID bietet zahlreiche Möglichkeiten, den Vorgang des Sichausweisens außer in der analogen Welt auch in der digitalen Welt des Internets zu etablieren – einfach, komfortabel und dank seiner vielfältigen Sicherheitsmerkmale jederzeit bestens geschützt.

KONTAKT

Bundesdruckerei GmbH
Kommandantenstr. 15
10969 Berlin
Tel.: +49 (0) 30 25 98 0
Fax: +49 (0) 30 25 98 22 05
E-Mail: info@bdr.de
www.bundesdruckerei.de

© 2014 Bundesdruckerei GmbH

Der neue Personalausweis
Meine wichtigste Karte.

DER PERSONALAUSWEIS

Sicherheitsmerkmale

Stand: Januar 2014

Bundesministerium des Innern

BUNDES DRUCKEREI

SICHERHEIT IN DER REALEN UND DIGITALEN WELT

Mit Inkrafttreten des „Gesetzes über Personalausweise und den elektronischen Identitätsnachweis“ wird seit dem 1. November 2010 der Personalausweis mit elektronischer Identitätsfunktion (eID) in Deutschland ausgegeben. Allen Ausweisinhabern bietet dieser Ausweis drei zusätzliche Funktionen: die Online-Ausweisfunktion, die Unterschriftsfunktion für den Einsatz in der digitalen Welt und die hoheitliche Biometriefunktion für behördliche Identitätsprüfungen.

Seit November 2010 werden im integrierten Sicherheits-Chip des Personalausweises mit eID u. a. ein digitales Foto und auf Wunsch des Ausweisinhabers zwei digitale Fingerabdrücke gespeichert. Diese separat geschützten persönlichen Daten sind Bestandteil der hoheitlichen Biometriefunktion und dienen ausschließlich der behördlichen Identitätsprüfung.

Mit der Online-Ausweisfunktion und einer sechsstelligen Geheimnummer (PIN) können Bürger ihre Identität bei elektronischen Anwendungen im Internet einfach, sicher und zuverlässig belegen. Darüber hinaus ist jeder Personalausweis mit eID für die Nutzung der Qualifizierten Elektronischen Signatur (QES) vorbereitet. Mit dieser hochsicheren Unterschriftsfunktion können digitale Dokumente rechtskräftig unterzeichnet werden.

newzealand.govt.nz

DOCUMENT VERIFICATION GUIDE:

Version 3 2012

INTERNAL AFFAIRS
Te Tari Taiwhenua

FOREWORD:

As the government's authoritative source of identity data for New Zealand citizens, the Department of Internal Affairs plays an important role in assisting organisations to verify customers' identities and prevent identity fraud.

The Department of Internal Affairs has conservatively estimated the financial costs of identity crime to the New Zealand economy at $136 million to $204 million per annum, and the costs to public sector agencies at $22 million to $33 million. Whether perpetrated by employees, contractors, customers or suppliers, it has significant and often long-term economic and social costs - not only for the organisations themselves, but for those affected through its flow-on effects.

New Zealand does not currently have a single document carried by all residents to prove identity. The majority of the documents included in this Guide are not specifically intended to serve as proof of identity (for example, a New Zealand Passport enables international travel, a birth certificate records a birth).

This Document Verification Guide has been produced to help organisations quickly and accurately verify the authenticity of a number of common documents. The ability to verify the authenticity of identity documents will assist in reducing identity fraud, a serious issue for New Zealand.

Factsheets for additional documents have been included into this third version of the Guide.

The documents included in this Guide are:

- New Zealand Birth Certificate (same as previous version)
- New Zealand Citizenship Certificate (same as previous version)
- New Zealand Passport (same as previous version)
- New Zealand Marriage or Civil Union Certificate (new factsheet)
- New Zealand Name Change Certificate (new factsheet)
- New Zealand Driver Licence (same as previous version)
- New Zealand Pink Driver Licenses (Limited licence, Zero Alcohol Licence and Alcohol Interlock Licence) (new factsheet)
- Immigration New Zealand Visa, Immigration Act 2009, blue label (same as previous version)
- Immigration New Zealand Visa, Immigration Act 1987, blue label (same as previous version)
- Immigration New Zealand Visa, Immigration Act 1987, orange label (same as previous version)
- New Zealand Firearm Licence (same as previous version)
- Hospitality New Zealand, 18+ Card (new factsheet).

This Guide will be updated regularly, as documents change frequently. It is recommended that you register for alerts, which will be sent when a new version becomes available. Register by emailing *docverify@dia.govt.nz*.

GENERAL TIPS TO SPOT A FRAUDULENT DOCUMENT

There are three main types of document fraud, listed in order of likelihood:

1. Someone uses a genuine document, which may have been lost or stolen, but they are not the person the document refers to (for example, someone alters their appearance to look like the photo on someone else's passport). To target this sort of fraud, you should check more than one document, especially if the document being used does not include a photo (like a birth certificate).
2. A person presents a genuine document that they have altered in some way (for example, changing a photograph or name). Check that the document:
   - looks like the photo on the document factsheet in this Guide
   - is consistent (the names are all the same, the lettering is the same)
   - does not have unusual wear and tear (peeling plastic covering, etc.).
3. Someone presents a completely fake document. Check that the document:
   - looks like the photo on the document factsheet in this Guide
   - is consistent (the names are all the same, the lettering is the same)
   - does not have unusual wear and tear (peeling plastic covering, etc.)
   - feels right (paper thickness and plastic covering).

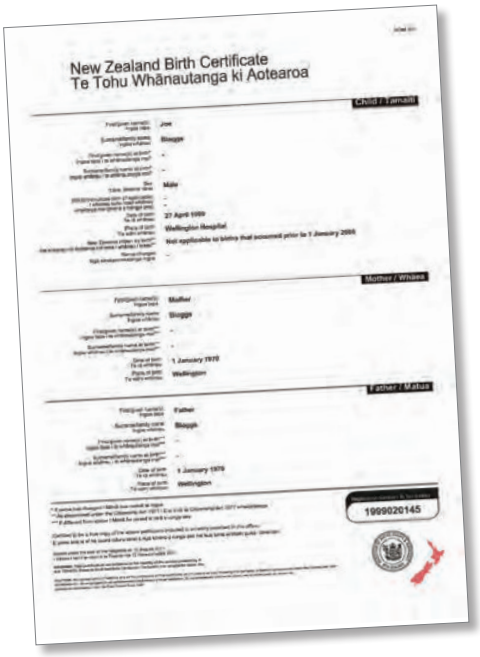
It is always a good idea, particularly when the potential risk is high, to check more than one document (such as a driver licence and a birth certificate). Ensure the details provided are realistic (for example, the person looks to be the age they claim) and, where possible, verify the information via another source.

For further advice or assistance with identity verification processes email *eoistandard@dia.govt.nz.*

INTERNAL AFFAIRS
Te Tari Taiwhenua

NEW ZEALAND BIRTH CERTIFICATE

VERIFICATION



Quick steps to verify a Birth Certificate

Over the years there have been a number of different designs and layouts of the New Zealand Birth Certificate.

Check for Registrar's seal and/or signature

All Birth Certificates should be stamped with a Registrar's seal, or signed by the Registrar, or have both the Registrar's seal and signature.

Check for watermark

A Birth Certificate issued from 1985 is printed on paper that has a 'block wave watermark' visible when the certificate is held up to the light.

A Birth Certificate issued from late 2011 on glossy paper has a watermark of a kiwi and two ferns visible when the certificate is held up to the light. It also has a red map of New Zealand that feels slightly raised in the bottom right-hand corner.

Check registration number

A birth certificate issued from 1/10/1999 will have a 10-digit registration number. The first four digits will usually be the year of birth or a subsequent year.

Description of the document:

Purpose

A New Zealand Birth Certificate is an official document containing registered information about a person's birth as at the date of issue. It is not to be used on its own as evidence of identity.

Information

Contains registered information about an individual's birth, including the child and parents' given names, surnames, date of birth and place of birth. Certificates issued on or after 01/01/2006 will also verify New Zealand citizenship by birth.

Validity

Valid indefinitely.

Versions

Current Birth Certificates are issued in standard and decorative (beach and forest) designs on glossy A4 portrait paper (see images). There have been a number of different layouts and designs, however all should contain the same information and features listed.

Note, certificates issued from a separate Māori register (1913-1961) will have a Te Reo Māori heading first and English second.

There are currently two choices of decorative Birth Certificates available, depicting a forest or a beach.

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-BC-V2-2012

INTERNAL AFFAIRS
Te Tari Taiwhenua

CERTIFICATE OF CITIZENSHIP
VERIFICATION

Quick steps to verify a citizenship certificate

A4 portrait version

This version of the citizenship certificate has been issued from early 2012 and replaces the previous landscape version. All citizenship documents are printed on this certificate, apart from certified copies, confirmation of citizenship by grant and renunciation of citizenship, which are printed on A4 speckled brown paper.

Hold up to light and look for a watermark of a kiwi and two ferns.

Feel the raised red map of New Zealand in the bottom right-hand corner.

Check for the words 'NEW ZEALAND DEPARTMENT OF INTERNAL AFFAIRS TE TARI TAIWHENUA' repeated with no spaces in the background.

Check that the title in Māori now reads 'Te Tohu Kiriraraunga,' as it has been retranslated for this version.

Check that you can see a silver fern, the words New Zealand and Aotearoa and a kowhaiwhai (koru) pattern in the background.

Description of the document:

Purpose

A New Zealand citizenship certificate provides confirmation that the person is a New Zealand citizen either by descent or grant. It is not an identity document, you should check other documents as well. For further information on eligibility criteria for New Zealand citizenship, please go to *www.dia.govt.nz/new-zealand-citizenship*.

Information

The citizenship certificate includes a person's full name, gender, date of birth, place of birth, effective date of citizenship and certificate number.

Validity

Valid indefinitely.

Versions

The features of the previous citizenship certificates can be found on the next factsheet. There are also some earlier versions of the citizenship certificate, including different sizes that are smaller than A4, but are landscape.

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-CC-V2-2012

INTERNAL AFFAIRS
Te Tari Taiwhenua

CERTIFICATE OF CITIZENSHIP

VERIFICATION

Quick steps to verify a citizenship certificate

There are three different types of certificates:

- A New Zealand citizenship certificate – A4 landscape
- Confirmation of New Zealand Citizenship – A4 portrait on speckled brown paper
- Certified Copy of Registration of New Zealand Citizenship by Descent – A4 portrait on cream paper with a bluish hue.

Certificate

Hold up to the light and look for a floral watermark.

Feel the raised security printing around the border.

Check for an embossed seal on the bottom left-hand corner, in the form of a circle with the New Zealand Coat of Arms in the centre and the words 'NEW ZEALAND DEPARTMENT OF INTERNAL AFFAIRS' written around it.

The certificates for citizens by descent are signed (in the bottom left-hand corner), whereas those for citizens by grant are not signed.

Confirmation of New Zealand Citizenship

Check for a New Zealand Coat of Arms printed in the top left-hand corner and a lighter New Zealand Coat of Arms in the centre of the page.

Certified Copy of Registration of New Zealand Citizenship by Descent

Hold up to the light and look for a watermark of horizontal lines 2.5cm apart.

Description of the document:

Purpose

A New Zealand citizenship certificate provides confirmation that the person is a New Zealand citizen either by descent or grant. It is not an identity document, you should check other documents as well. For further information on eligibility criteria for New Zealand citizenship please go to *www.dia.govt.nz/new-zealand-citizenship.*

Information

The citizenship certificate includes a person's full name, gender, date of birth, place of birth, effective date of citizenship and certificate number.

Validity

Valid indefinitely.

Versions

There are some earlier versions of the citizenship certificate, including different sizes that are smaller than A4, but are landscape.

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-CC-V1-2011

INTERNAL AFFAIRS
Te Tari Taiwhenua

NEW ZEALAND PASSPORT

Black cover, laser engraved photo

VERIFICATION

Quick steps to verify a New Zealand Passport

These points apply to passports, which began being issued in November 2009 and are the only type of passport issued since February 2010. They have a black cover with a silver fern design.

The person's photo appears twice, and their personal details are engraved onto a hard plastic insert, which is stitched into the passport. Further information about the security features is given in the passport on page three.

Check the same photo appears twice on the photo page and that it matches the person presenting the passport.

Check the passport identification number begins with L and another letter and is followed by six numbers.

Check the passport number is perforated into the book from page three through to the back cover and that it matches the number on the photo page.

Check the numbers and letters at the bottom of the photo page. The second line should follow this pattern:
Passport number< random number, NZL, date of birth backwards, random number, gender (M, F or <), expiry date backwards.

Feel the raised passport identification number on the photo page.

Tilt the back inside cover to see the letters NZ change to NZL in the picture of the North Island.

Description of the document:

Purpose

The specific purpose of a New Zealand passport is to verify a New Zealand citizen when they travel outside the country. You should check other documents as well.

Information

A passport includes the person's image, full name, date of birth, place of birth and gender.

Validity

This version of the New Zealand passport is valid for a maximum of five years. Where it is valid for a shorter period, there is usually a notation on page six.

Versions

Factsheets for previous passport versions are also available, as these differ substantially.

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-LAPP-V1-2011

Internal Affairs
Te Tari Taiwhenua

NEW ZEALAND PASSPORT

Blue cover, photo printed on page

VERIFICATION

Quick steps to verify a New Zealand Passport

These points apply to most passports issued from December 2000 until February 2010. They have a dark blue cover embossed with the New Zealand crest.

Feel the raised security printing on the inside back cover.

Check the inside pages under light to view the kiwi watermark.

Tilt the inside back cover to see the words 'NEW ZEALAND' in the design at the base of the page.

The passport identification number should begin with AA, AB, EA or EB. The person's photo is printed directly into the book and blends with the background.

Check the numbers and letters at the bottom of the photo page, the second line should follow the pattern: Passport number< random number, NZL, date of birth backwards, random number, gender (M, F or <), expiry date backwards.

Description of the document:

Purpose

The specific purpose of a New Zealand passport is to verify a New Zealand citizen when they travel outside the country. You should check other documents as well.

Information

A passport includes the person's image, full name, date of birth, place of birth and gender.

Validity

Passports issued from 21 April 2005 are valid for a maximum of five years.

Passports issued prior to 21 April 2005 are valid for a maximum of ten years.

In either case, where it is valid for a shorter period there is usually a notation on page four.

Versions

Factsheets for newer and older passport versions are also available, as these differ substantially.

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-AAPP-V1-2011

INTERNAL AFFAIRS
Te Tari Taiwhenua

NEW ZEALAND PASSPORT

Blue cover, photo inserted on page

VERIFICATION

Quick steps to verify a New Zealand Passport

These points apply to most passports issued between 1992 and mid 2000. They have a dark blue cover embossed with the New Zealand crest.

Check the border of the design on the inside back cover for the words 'NEW ZEALAND' in small text.

Check the blue design in the laminate over the personal information and the photo is unbroken.

Check the perforated number matches the passport number and begins on page five, continuing to page 48.

The passport identification number should begin with F, L, N or X followed by six numbers. The person's photo is inserted into the book and laminated.

Check the numbers and letters at the bottom of the photo page, the second line should follow the pattern: Passport number< random number, NZL, date of birth backwards, random number, gender (M, F or <), expiry date backwards.

Description of the document:

Purpose

The specific purpose of a New Zealand passport is to verify a New Zealand citizen when they travel outside the country. You should check other documents as well.

Information

A passport includes the person's photo, full name, date of birth, place of birth and gender.

Validity

This version of the New Zealand passport is valid for a maximum of ten years.

Where it is valid for a shorter period, there is usually a notation on page four.

Versions

Factsheets for newer and older passport versions are also available, as these differ substantially.

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-FPP-V1-2011

INTERNAL AFFAIRS
Te Tari Taiwhenua

NEW ZEALAND PASSPORT

Blue cover, photo and personal details inserted on page

VERIFICATION

Quick steps to verify a New Zealand Passport

These points apply to some passports issued until November 2004. They have a dark blue cover embossed with a silver New Zealand crest.

Check the border of the design at the base of the inside back cover for the words 'NEW ZEALAND' in small text.

Check the photo page to see the New Zealand crest embossed in the laminate over the photo, and through to the page behind.

Check the perforated number matches the passport number and begins on page five, continuing to page 48.

The passport identification number should begin with M followed by six numbers. The person's photo is inserted into the book. The personal details are typed on a coloured paper slip, which is inserted and the page is laminated. This type of passport does not include a machine-readable zone of letters and numbers.

Description of the document:

Purpose

The specific purpose of a New Zealand passport is to verify a New Zealand citizen when they travel outside the country. You should check other documents as well.

Information

A passport includes the person's photo, full name, date of birth, place of birth and gender.

Validity

This version of the New Zealand passport is valid for a maximum of ten years.

Where it is valid for a shorter period, there is usually a notation on page four.

Versions

Factsheets for other passport versions are also available, as these differ substantially.

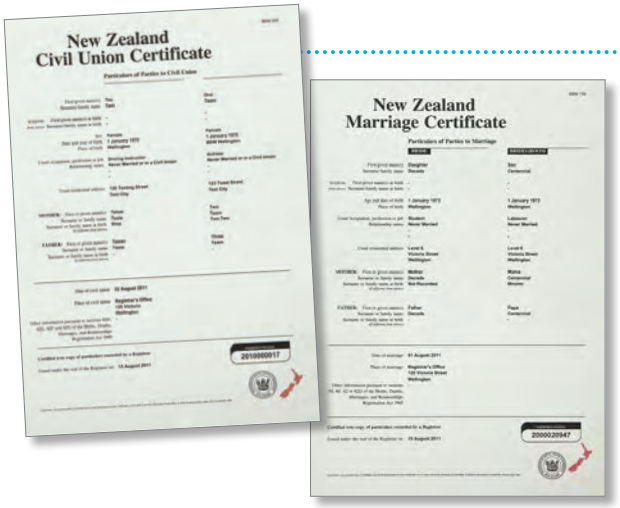
Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-MPP-V1-2011

INTERNAL AFFAIRS
Te Tari Taiwhenua

NEW ZEALAND MARRIAGE & CIVIL UNION CERTIFICATE

VERIFICATION



Quick steps to verify a Marriage or Civil Union Certificate

Over the years there have been a number of different designs and layouts of the New Zealand Marriage and Civil Union Certificate. New Zealand Civil Union Certificates have only been issued since 26 April 2005.

Check for Registrar's seal and/or signature

All Marriage and Civil Union Certificates should be stamped with a Registrar's seal, or signed by the Registrar, or have both the Registrar's seal and signature.

Check for watermark

A Marriage Certificate issued from 1985 or a Civil Union Certificate issued from 26 April 2005 is printed on paper that has a 'block wave watermark' visible when the certificate is held up to the light.

A Marriage or Civil Union Certificate issued from late 2011 on glossy paper has a watermark of a kiwi and two ferns visible when the certificate is held up to the light. It also has a red map of New Zealand that feels slightly raised in the bottom right-hand corner.

Check registration number

A Marriage Certificate issued from 2001 or a Civil Union Certificate issued from 26/04/2005 will have a 10-digit registration number. The first four digits will usually be the year that the marriage or civil union was registered.

Description of the document:

Purpose

New Zealand Marriage and Civil Union Certificates are official documents containing registered information about a couple's New Zealand marriage or civil union. The certificate may generally be used as evidence that one party has assumed the other party's surname (or a combination of both surnames) by usage and reputation. It should not be used on its own as evidence of identity.

Information

Contains the following details about the couple – both parties full name and names at birth (if different), sex (only for civil unions), date and place of birth, usual occupation, relationship status, usual residential address, date and place of marriage or civil union, name(s) of parents, change of relationship and dissolution details (if applicable).

Validity

Valid indefinitely.

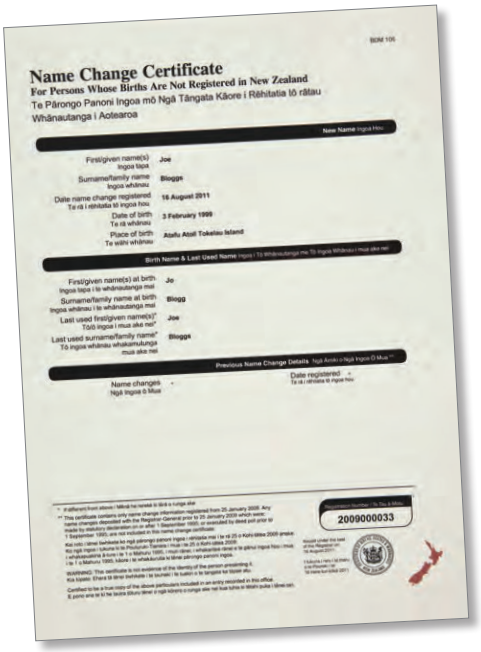
Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-MCU-V3-2012

INTERNAL AFFAIRS
Te Tari Taiwhenua

NEW ZEALAND NAME CHANGE CERTIFICATE

VERIFICATION


Name Change Certificate
For Persons Whose Births Are Not Registered in New Zealand
Te Pārongo Panoni Ingoa mō Ngā Tāngata Kāore i Rāhitatia tō rātau Whānautanga i Aotearoa

New Name Ingoa Hou

First/given name(s) Ingoa tapa: Joe
Surname/family name Ingoa whānau: Bloggs
Date name change registered Te rā i rēhita tō ingoa hou: 16 August 2011
Date of birth Te rā whānau: 3 February 1999
Place of birth Te wāhi whānau: Atafu Atoll Tokelau Island

Birth Name & Last Used Name

First/given name(s) at birth Ingoa tapa i te whānautanga mai: Jo
Surname/family name at birth Ingoa whānau i te whānautanga mai: Blogg
Last used first/given name(s)* Tōrō ingoa i mua ake nei: Joe
Last used surname/family name* Tō ingoa whānau whakamutunga mua ake nei: Bloggs

Previous Name Change Details

Name changes Ngā Ingoa ō Mua: -
Date registered Te rā i rēhitea tō ingoa hou: -

2009000033

* If different from above / Mēnā he rerekē i tēnā e tūnga atu

** This certificate contains only name change information registered from 25 January 2009. Any name changes deposited with the Registrar-General prior to 25 January 2009 which were: made by statutory declaration on or after 1 September 1995; or executed by deed poll prior to 1 September 1995, are not included in this name change certificate

Kia rōki i tēnei tuhinga ki te Pūkoputaki Tianara i mua i te 25 o Kohi-tātea 2009 anake. Kia ngā ingoa i tukuna ki te Pūkoputaki Tianara i mua i te 25 o Kohi-tātea 2009 ka whakatakoto rānei i te pānga ingoa hou i mua i te 1 o Mahuru 1995, i mua rānei, i whakaritea rānei e te pānga ingoa hou i mua i te 1 o Mahuru 1995, kāore i te whakauru i tēnei pānga panoni ingoa.

WARNING: The certificate is not evidence of the identity of the person presenting it.
Kia tūpato: Ehara tō tēnei tuhituhi i te taunaki i te tuakiri o te tangata ka tūtaki ahu.

Certified to be a true copy of the above particulars included in an entry recorded in this office.
E pono ana ka tū ka tuna ōkuru tēnei e ngā kōrero o runga ake nei kua tuhia ki tēnāi auka i tēnei oti.

Quick steps to verify a Name Change Certificate

The New Zealand Name Change Certificate has been available since 25 January 2009.

Check for Registrar's seal and/or signature

All Name Change Certificates should be stamped with a Registrar's seal.

Check for watermark

A Name Change Certificate issued from 25 January 2009 is printed on paper that has a 'block wave watermark' visible when the certificate is held up to the light.

A Name Change Certificate issued from late 2011 on glossy paper has a watermark of a kiwi and two ferns visible when the certificate is held up to the light. It also has a red map of New Zealand that feels slightly raised in the bottom right-hand corner.

Check registration number

A Name Change Certificate issued from 25/01/2009 will have a 10-digit registration number. The first four digits will usually be the year the first name change was registered since 2009.

Description of the document:

Purpose

A New Zealand Name Change Certificate is an official document containing registered information about a person's name change, as at the date of issue. It is only issued for people whose births are not recorded in New Zealand and who are New Zealand citizens, or who are entitled to be in New Zealand indefinitely. It should not be used on its own as evidence of identity.

Information

Contains registered information about an individual's name change, including the individual's first name(s), surname(s), name at birth, as well as last used name if different, date and place of birth, date the name change was registered and list of name changes registered on or after 25 January 2009.

Validity

Valid indefinitely.

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-NC-V3-2012

NZ TRANSPORT AGENCY
WAKA KOTAHI

NEW ZEALAND DRIVER LICENCE

VERIFICATION

Quick steps to verify a Driver Licence

New Zealand driver licences have been issued in the current credit card sized version since May 1999. The previous paper licences should not be accepted as identification. The layout of photo driver licences has changed slightly over the years.

There are **four licence colours**, full (green), restricted (yellow), learner (blue) and pink (limited), which shows that a person can only drive under certain conditions.

Check limited (pink) licences issued prior to mid 2012 do not have 'limited' printed between the flag and the photo.

Check that the licence is plastic, not cardboard. Licences issued since early 2011 will feel like a credit card, previous versions were more flexible.

Check recently issued licences for the newzealand.govt.nz logo in silver when the licence is tilted. In previous versions there will be either the Land Transport New Zealand logo in silver or the Land Transport Safety Authority logo in gold. The concentration of ink in the Land Transport New Zealand logo may cause a bubble effect under the laminated surface of the licence.

Check that printed lines can be seen over the person's photo.

Check with a magnifying glass that the words 'New Zealand' can be seen around the New Zealand flag.

Check that the licence number in 5a matches the first part of the information printed directly below the barcode on the back of the card.

Description of the document:

Purpose

A New Zealand driver licence is issued as evidence that a person is allowed to drive in this country and contains some identity information. It is a good idea to check this against another document that a person holds.

Information

Contains name, date of birth, date of licence issue, date of licence expiry, donor indicator, driver licence number, card version number, signature, licence classes and, in some cases, address.

Validity

Most licences are issued for ten years. However licences can be issued for anywhere between 1 and 11 years. Check the expiry date is no more than 11 years in the future.

Versions

The photo driver licence has had some changes in layout and type of plastic since its introduction, but the information provided will still apply to older versions.

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-DL-V2-2012

NZ TRANSPORT AGENCY
WAKA KOTAHI

NEW ZEALAND PINK DRIVER LICENCE

VERIFICATION

Quick steps to verify a Pink Driver Licence

New Zealand driver licences have been issued in the current credit card sized version since May 1999. The previous paper licences should not be accepted as identification. The layout of photo driver licences has changed slightly over the years.

There are four main types of licence, green (full), yellow (restricted), blue (learner) and a pink licence. This factsheet focuses on the pink licence. A pink licence shows the driver is subject to special conditions as the result of a suspension or disqualification.

There are three different pink licences:

- Limited licence - The driver is currently suspended or disqualified and driving under the conditions of a court order.
- Alcohol interlock licence - The driver can only drive vehicles which are fitted with an alcohol interlock device.
- Zero alcohol licence - The driver must maintain a zero alcohol limit when they are driving.

Check that the licence is plastic, not cardboard. Licences issued since early 2011 will feel like a credit card, previous versions were more flexible.

Check recently issued licences for the newzealand.govt.nz logo in silver when the licence is tilted. On previous versions there will be either Land Transport New Zealand logo or the Land Transport Safety Authority logo in gold. The concentration of ink in the Land Transport New Zealand logo may cause a bubble effect under the laminated surface of the licence.

Check that printed lines can be seen over the person's photo.

Check with a magnifying glass that the words 'New Zealand' can be seen around the New Zealand flag.

Check that the licence number in 5a matches the first part of the information printed directly below the barcode on the back of the card.

Description of the document:

Purpose

A New Zealand Driver Licence is issued as evidence that a person is allowed to drive in this country and contains some identity information. It is a good idea to check this against another document that a person holds.

Information

Contains name, date of birth, date of licence issue, date of licence expiry, donor indicator, driver licence number, card version number, signature, licence classes and, in some cases, address.

Validity

The zero alcohol licence can be issued for up to three years while all other licences can be issued for up to 11 years. The validity period of driver licences is dependent on court orders, in the case of a limited licence, and the age of the driver in the case of an alcohol Interlock licence. Check the expiry date is no more than 11 years in the future.

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-PDL-V3-2012

Department of Labour
TE TARI MAHI

IMMIGRATION NEW ZEALAND VISA

Immigration Act 2009, blue label

VERIFICATION

Quick steps to verify an Immigration New Zealand Visa

Issued from November 2010

Immigration New Zealand issue visas under the New Zealand Immigration Act 2009 (effective late 2010).

The visas are a label contained within the person's passport from their country of origin. The details on a visa may be printed by machine or written by hand, however no details are written by hand on machine-printed labels.

There are many different types of visas issued: work, resident, visitor, and student are the most common. The type of visa issued will depend on the purpose of the individual entering New Zealand.
The different types of visas all look the same, the only difference being the type of visa is shown across the top of the label.

Visas issued under the New Zealand Immigration Act 1987 may still be in circulation, but will be phased out over time.

Check for a silver hologram in the top left hand corner of the visa.

Check for 'New Zealand Immigration Act 2009' printed on a silver background across the top of the label.

Check that the information on the visa is consistent with the information on the photo page of the passport.

Look for a unique label number. On machine-printed labels, the unique label number is in the white space, above the blue background.

Check no details are written by hand on machine-printed labels.

If you think that someone is presenting a fraudulent visa, contact Immigration New Zealand on 0508 558 855.

Description of the document:

Purpose

A New Zealand visa is issued as evidence that a person is permitted to enter New Zealand and to undertake the activities as listed on the visa, such as, to study or work. The visa contains some identity information, however it is a good idea to check this against another document that a person holds.

Information

Contains name, date of birth, gender, passport number, visa start and expiry date, number of entries permitted into New Zealand and conditions of the visa.

Validity

The validity of a visa depends on what kind of visa it is. Some, such as resident visas, are valid indefinitely. Some are valid for a fixed period, such as the duration a person is studying in New Zealand, or a short-term work contract.

Versions

The layout of the visa label has remained relatively consistent, although there are some differences between those issued from late 2010 and previously. See other visa factsheets for more information.

VisaView *Employers can use VisaView to check whether people who aren't New Zealand citizens are entitled to work in New Zealand. Go to www.immigration.govt.nz/visaview*

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-V09B-V2-2012

Department of Labour
TE TARI MAHI

IMMIGRATION NEW ZEALAND VISA

Immigration Act 1987, blue label

VERIFICATION

Quick steps to verify an Immigration New Zealand Visa

Issued between 1997 and 2010

Visas issued under the New Zealand Immigration Act 1987 may still be in circulation, but will be phased out over time. Visually the visas issued between 1997 to 2004 appear similar to recently issued visas under the Immigration Act 2009.

Visas are a label contained in the person's passport from their country of origin. The details on a visa may be printed by machine or written by hand, however no details are written by hand on machine-printed labels.

There are many different types of visas issued: work, resident, visitor, and student are the most common. The type of visa issued will depend on the purpose of the person entering New Zealand. The different types of visas all look the same, the only difference being the type of visa is shown across the top of the label.

Check for a silver hologram in the top left hand corner of the visa.

Check for 'New Zealand Immigration Act 1987' printed on a silver background across the top of the label.

Check that the information on the visa is consistent with the information on the photo page of the passport.

Look for a unique label number. On machine-printed labels, the unique label number is in the blue background.

Check no details are written by hand on machine-printed labels.

If you think that someone is presenting a fraudulent visa, contact Immigration New Zealand on 0508 558 855.

Description of the document:

Purpose

A New Zealand visa is issued as evidence that a person is permitted to enter New Zealand and to undertake the activities as listed on the visa, such as, to study or work. The visa contains some identity information, however it is a good idea to check this against another document that a person holds.

Information

Contains name, date of birth, gender, passport number, visa start and expiry date, number of entries permitted into New Zealand and conditions of the visa.

Validity

The validity of a visa depends on what kind of visa it is. Some, such as resident visas, are valid indefinitely. Some are valid for a fixed period, such as the duration a person is studying in New Zealand, or a short-term work contract.

Versions

The layout of the visa label has remained relatively consistent, although there are some differences between those issued from late 2010 and previously. See other visa factsheets for more information.

VisaView *Employers can use VisaView to check whether people who aren't New Zealand citizens are entitled to work in New Zealand. Go to www.immigration.govt.nz/visaview*

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-V87B-V2-2012

newzealand.govt.nz

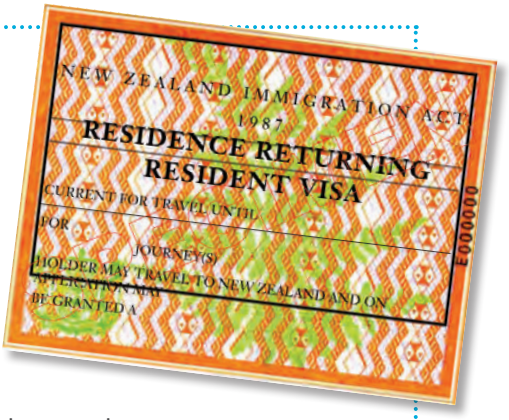
INTERNAL AFFAIRS
Te Tari Taiwhenua

Department of Labour
TE TARI MAHI

IMMIGRATION NEW ZEALAND VISA

Immigration Act 1987, orange label

VERIFICATION



Quick steps to verify an Immigration New Zealand Visa

Issued between 1990 and 1997

Visas issued under the New Zealand Immigration Act 1987 may still be in circulation, but will be phased out over time. Those issued between 1990 and 1997 are an orange label.

The visas are a label contained in the person's passport from their country of origin. The details on a visa may be printed by machine or written by hand, however no details are written by hand on machine-printed labels.

There are many different types of visas issued: work, resident, visitor, and student are the most common. The type of visa issued will depend on the purpose of the person entering New Zealand. The different types of visas all look the same, the only difference being the type of visa is shown across the top of the label.

Check for 'New Zealand Immigration Act 1987' printed across the top of the label.

Check that the information on the visa is consistent with the information on the photo page of the passport.

Check there is an image of a green fern behind the orange pattern.

Look for a unique label number down the right-hand side of the label.

Check no details are written by hand on machine-printed labels.

If you think that someone is presenting a fraudulent visa, contact Immigration New Zealand on 0508 558 855.

Description of the document:

Purpose

A New Zealand visa is issued as evidence that a person is permitted to enter New Zealand and to undertake the activities as listed on the visa, such as, to study, or to work. The visa contains some identity information, however it is a good idea to check this against another document that a person holds.

Information

Contains name, date of birth, gender, passport number, visa start and expiry date, number of entries permitted into New Zealand and conditions of the visa.

Validity

The validity of a visa depends on what kind of visa it is. Some, such as resident visas, are valid indefinitely. Some are valid for a fixed period, such as the duration a person is studying in New Zealand, or a short-term work contract.

Versions

The layout of the visa label has remained relatively consistent, although there are some differences between those issued from late 2010 and previously. See other visa factsheets for more information.

VisaView *Employers can use VisaView to check whether people who aren't New Zealand citizens are entitled to work in New Zealand. Go to www.immigration.govt.nz/visaview*

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-V87O-V2-2012

NEW ZEALAND FIREARMS LICENCE

VERIFICATION

Quick steps to verify a Firearms Licence

Firearms licences are issued to people 16 years or older, who have passed a checking process to ensure they are suitable to possess firearms. The issuance process is thorough and includes a visit to their home address and interviews with two referees.

Check that the licence is plastic, like a New Zealand driver licence, not cardboard. Licences issued since early 2011 will feel like a credit card, previous versions were more flexible.

Check that the photo is part of the printing on the licence.

Check the title New Zealand Firearms Licence. The card has the full name, date of birth, licence number and expiry date.

Check the fern pattern runs behind the written details with a fine swirl running in concentric lines horizontally across the licence card.

Check the hologram. This is the police crest in small size intermittently across the whole front of the card.

Description of the document:

Purpose

A New Zealand Firearms Licence proves that a person is allowed to possess a firearm and has passed the necessary checks by the New Zealand Police.

Information

Contains a photo, name, date of birth, licence number, expiry date and details of endorsements held (if any).

Validity

Valid for a maximum of ten years.

Versions

The firearms licence has had some changes in layout and type of plastic since its introduction, but the information provided will still apply licences issued since 2002.

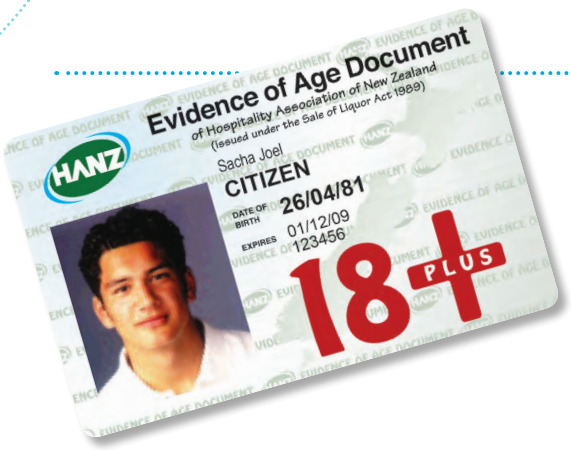
Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-FL-V2-2012

Hospitality NEW ZEALAND

HOSPITALITY NEW ZEALAND 18+ CARD

VERIFICATION



Quick steps to verify a Hospitality New Zealand 18+ Card

The Hospitality NZ 18+ card is an approved photographic evidence of age document under the Sale of Liquor Act 1989. It verifies the named person is over 18 and is entitled to purchase alcohol.

Check that the licence is plastic, like a New Zealand driver licence, not cardboard.

Check that the photo is part of the printing on the licence.

Check the title "Evidence of Age Document". The card has the full name, date of birth and expiry date.

Check for a six-digit registration number running underneath the expiry date.

Check the HANZ logo, "Evidence of Age Document" and a map of New Zealand is printed on the background of the card.

Note that a hologram of the old HANZ logo is visible under UV light.

Description of the document:

Purpose

A Hospitality New Zealand 18+ Card is an evidence of age document that shows a person is old enough to purchase alcohol in New Zealand. It is a good idea to check this against another document that a person holds.

Information

Contains name, date of birth, expiry date and a photo of the individual.

Validity

The 18+ Card is issued for 10 years. It is expected that after this time the holder will not be required to show evidence of their age.

Versions

The design and layout of the 18+ Card has remained constant since it was introduced in 1999.

Crown copyright ©. This Guide is licensed under the Creative Commons Attribution 3.0 New Zealand licence, available at http://creativecommons.org/licenses/by/3.0/nz/. No emblem or logo may be used in any way which infringes *the Flags, Emblems, and Names Protection Act 1981*. This Guide is not intended to provide an exhaustive treatment of all issues that can arise in the context of document verification. The Department of Internal Affairs has taken all due care in preparing it but will not be liable on any legal basis (including negligence) for consequences arising from reliance on it. **If you have feedback on this Guide, you can email docverify@dia.govt.nz.**

VG-18-V3-2012

RE: Email enquiry -please respond to customer

19.08.2015 05:00

Von William Hopgood <William.Hopgood@dia.govt.nz>

An 'leamiene@t-online.de' <leamiene@t-online.de>

Hello Lea,

I am a Business Support Officer for the Identity Verification Service and have been forwarded your query from the NZ Passport Office.

One method of online identification in New Zealand is with RealMe. RealMe at is core is a login service used across multiple government agencies to access online services i.e. Renew passport online, open a bank account.
RealMe also provides the option of upgrading to a RealMe verified account which you can attach a â€˜verified identityâ€™ to.

> **RealMe verified identity**
> A verified identity allows customers to â€˜assertâ€™ or prove their identity online to participating agencies where proof of identification is required. For example:
>
> *To open a bank account a customer is traditionally required to provide a form of identification to a bank employee in person if they wish to open an account. With a RealMe verified identity the customer is able to open a bank account online and as part of the new account application they can assert their verified identity via RealMe.*

This is a relatively new service and has only been running since 2009, The *Electronic Identity Verification Act 2012* governs the identity verification service

For more information on RealMe please visit our website www.realme.govt.nz

Another interesting piece of legislation that stipulates the use of identification is the *Anti-Money Laundering and Counter Financing of Terrorism Act 2009* which require organisations to perform identity check against originators of wire transfers

When proving identity we adhere to the Government Evidence of Identity Standard. More information about it can be accessed here. The EOI standard provides best practice guidance on the authentication component of online services. If you would like more information on the EOI standard I can pass your question on to the Senior Business Advisor that knows more about that field. *Please note: she is currently on leave until next week though.*

You may also wish to refer to the Privacy Act or contact the Office of the Privacy Commissioner for more information around why New Zealand doesnâ€™t have national ID cards.

I hope this has been helpful. If you have any more questions please feel free to ask

Regards

William Hopgood | Business Support Officer | Identity & Passport Services
The Department of Internal Affairs Te Tari Taiwhenua
Direct Dial: +64 4 382 3576 | Extn: 4576
120 Victoria Street, Wellington 6011, New Zealand | www.dia.govt.nz

INTERNAL AFFAIRS
Te Tari Taiwhenua

From: Erin Carter
Sent: Wednesday, 12 August 2015 5:50 p.m.
To: Passport Correspondence
Subject: Email enquiry -please respond to customer

Hey guys,

Unsure if you can help with this enquiry, if not could you please forward to the appropriate person?

Cheers, Erin

Dear Lea

Thank you for your email.

Due to the nature of your enquiry, your email has been forwarded to a senior staff member who will respond within 15 working days.

For any other enquiries please reply to this email, visit our website at www.passports.govt.nz <http://www.passports.govt.nz> or contact us by phone.

Kind regards
Erin Carter
Client Information Officer | Passport Office
NZ: 0800 22 50 50 | Outside NZ: +64 4 463 9360
Mon to Thu 8am - 10pm | Fri 9am - 10pm | Sat 9am - 2pm
Department of Internal Affairs Te Tari Taiwhenua

> **From:** leamiene@t-online.de [mailto:leamiene@t-online.de]

> **Sent:** Tuesday, 11 August 2015 1:28 a.m.

> **To:** Telephon Telephon

> **Subject:** Enquiry bachelor thesis
>
>
>
> Dear Sir or Madam,

>
>
>
> my Name is Lea and I am from Germany, currently writing my bachelor thesis,
>
> which is a comparison of New Zealands and Germanys ways of (online) identification.
>
>
>
> As I am writing a chapter about how you can prove your identityin NZ, I came across the fact that having an identity
> document is optional in NZ.
>
>
>
> Now, can you tell me if there´s any Act about what Kind of documents can be used for proving your identity?
>
> Or is there any Act saying that having a identity document is optional?
>
>
>
> Thanks so much for your help! ðŸ˜Š
>
>
>
> Best wishes from Germany,
>
>
>
> Lea
>
>
>

RE: enquiry bachelor thesis - Nachricht (HTML)

Datei | Nachricht | Lernen

Ignorieren | Junk-E-Mail | Löschen | Antworten | Allen antworten | Weiterleiten | Besprechung | Weitere | Ablage | Team-E-Mail | Antworten und l... | An Vorgesetzte(n) | Erledigt | Neu erstellen | Verschieben | Regeln | Aktionen | Als ungelesen markieren | Kategorisieren | Nachverfolgung | Übersetzen | Suchen | Verwandt | Markieren | Zoom

Sie haben am 11.06.2015 07:06 auf diese Nachricht geantwortet.

Von: RealMe Business <business@realme.govt.nz>
An: Miene, Lea Denise (RPS)
Cc:
Betreff: RE: enquiry bachelor thesis

Gesendet: Do 11.06.2015 06:23

Nachricht | The RealMe Story - May 2015.docx (181 KB)

Hi Lea,

Thank you for your enquiry about RealMe. I've attached a document that I hope will be of some assistance. I also suggest that you check out our website, (www.realme.govt.nz) which is being totally refreshed and is expected to "go live" by the end of June.

Good luck with your bachelor thesis!

Regards
Julie, on behalf of the RealMe team

From: Miene, Lea Denise (RPS) [mailto:LeaDenise.Miene@rps.bwl.de]
Sent: Wednesday, 10 June 2015 12:47 a.m.
To: RealMe Business
Subject: enquiry bachelor thesis

Dear RealMe team,

I have recently been to New Zealand for an internship.
Back home in Germany I am now working on my bachelor thesis which is a comparison between NZ and Germanys ways of online identification, with focus on RealMe as a service to prove who you are online.

Regarding that, it would be great to have some statistics or charts about
- RealMe in general
- its development
- its users (of course no personal data!)

to put into my bachelor thesis!

Can you offer me any statistics or charts to use for my thesis?

I´m thankful for any help ☺

Best regards from Germany,

Lea

09:35
15.06.2015

About RealMe

1. RealMe is the Government's common login and online identity verification service, provided by the Department of Internal Affairs in partnership with New Zealand Post.
2. RealMe provides a secure and privacy protected way for New Zealanders to access online services, prove their identity and assert personal information online. It is designed to facilitate the online transactions of citizens and make peoples' relationship with government throughout their lifetime a much easier and more integrated experience than it is currently.
3. RealMe services currently include:
   - **RealMe login** (previously the igovt login service): an authentication service that allows customers to use the same login details securely to access 61 online services from **20** public-sector agencies (as at May 2015). Both low and moderate strength login is available to meet requirements for different levels of risk.
   - **RealMe verified identity** (launched July 2013): where customers who have verified information about themselves can share that information with **six** participating public and private-sector organisations in a secure way. Currently customers can verify their identity (name, date of birth, place of birth, gender) and address. In future we plan to add more attributes (e.g. citizenship status).

RealMe design and development history

4. RealMe login started as the Government Logon Service, which went live in April 2007. It was rebranded under the igovt brand in July 2009 when the service transferred from the State Services Commission to the Department of Internal Affairs. In 2011 New Zealand Post became the private sector commercialisation partner, and in July 2013 the igovt login service was rebranded as RealMe, and the RealMe verified account was launched.

RealMe meets strict design and operating requirements

5. RealMe has been developed to operate within strict requirements for privacy protection and information security. RealMe is a world class solution tailored to the New Zealand environment and is consistent with

- *the Electronic Identity Verificatio*n Act 2013, which enables electronic identity verification online;
- the Privacy Act 1993, which only allows data matching between departments in very limited circumstances;
- the Anti-Money Laundering and Countering Financing of Terrorism Act 2009;
- the international OASIS SAML 2.0 and WS-Trust standards; and
- NZ e-GIF Identity Management and Authentication Standards, New Zealand Government Web Standards, New Zealand Secure Web Services Standards, New Zealand Security Manual (NZSIM) and Security in the Government Sector (SIGS).

How RealMe Works

Process of getting a RealMe login

1. Customers set up a **RealMe login** by choosing their unique username and password. They must provide an email address, the answers to three security questions, and agree to RealMe terms of use. They may also provide their mobile phone number and an alternative contact number.

Process of establishing a RealMe verified identity

2. Currently customers undertake a two-step process to verify their identity:

   (1) an online application; and **(2)** a personal visit to a participating PostShop within 14 days of starting the process, to get their photo taken.

Step 1: Customers submit information online and choose how to verify their identity

3. Customers first login at www.realme.govt.nz by using their username and password. They provide a **mobile phone number** which is then used for second-factor authentication (i.e. customers receive a text message with a code when conducting some transactions). Each phone number can be associated only with one RealMe login.
4. Customers verify their identity and provide information relating to one of the following four official records :
   - Passport (77 % of all approved applications use this method)
   - New Zealand birth details (12 %)
   - Immigration records (9.6%)
   - Citizenship (1.4%).
5. Each customer receives an email and text with a unique reference code for the second stage of the process at a participating PostShop.

Step 2: Customers visit New Zealand PostShop for photo capture (and to provide hard-copy documents if required)

6. At the PostShop customers present the reference code and have their photo taken by a PostShop employee. If they are applying via a Birth or immigration record they are also required to provide a supplemental photo ID (e.g. a driver's or firearms licence[1]) and an additional document (e.g. evidence of an IRD number, bank or Community Services Card) which are scanned and provided to the Department along with the electronic photo.

---

[1] A driver's licence, Student ID, Firearms licence or HANZ card is not in itself sufficient proof of identity, but provides evidence of ongoing use of an identity in the community by the person pictured in the photograph. When combined with other documents linked to official records (e.g. Birth Certificate or Immigration Record) the result provides sufficient confidence an individual's identity to meet the Evidence of Identity Standard.

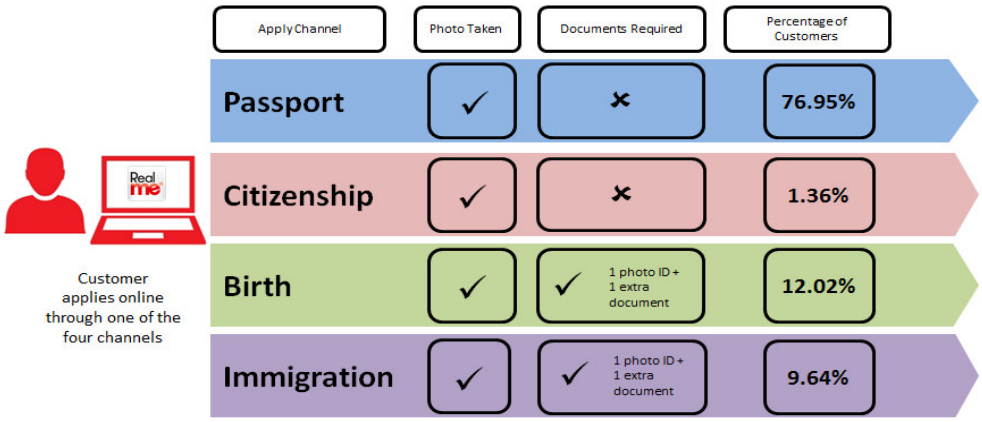


Figure 1: RealMe Verified account evidence requirements

7. The Department checks the biometric match to photo records, checks the material supplied against relevant databases[2] and creates a RealMe verified identity.

8. In addition to checking that the photograph from the PostShop matches the passport, citizenship or secondary ID, the Department also checks Birth, Death, Marriage, Immigration, Passport and Citizenship records related to that individual, and then binds/links each record to prevent them being used or reused by a fraudster.

Progress to Date

Since RealMe was launched in July 2013:

- 1,014,826 logins have been created (bringing the total to 2.02 million logins) with around 12 million transactions over the last 12 months.
- The reuse rate of RealMe logins has been showing a steady increase, from 20% at the time RealMe launched in July 2013 to 51% in February 2015 (shown in red in Figure 2 below).

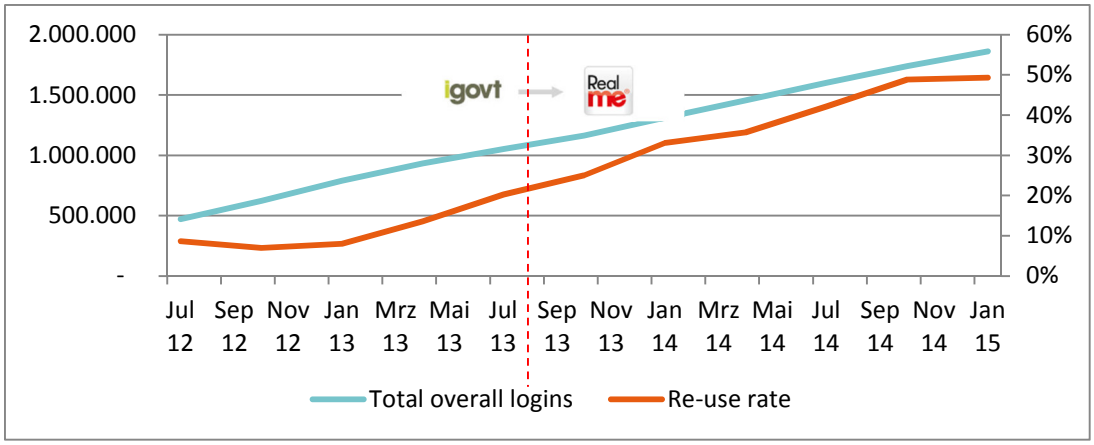


Figure 2: RealMe Login cumulative uptake and reuse rate

[2]Databases checked include Passports, Citizenship, Births, Deaths, Marriages, Immigration, Hotel Association of New Zealand 18+ Card, NZTA Driver Licences, and NZ Police Firearms Licences.

Verified identity uptake

Figure 3 shows the increasing growth in uptake of RealMe verified accounts – almost 42,000 have been created since its launch in July 2013. New options such as being able to apply for a verified identity at the same time as renewing an adult passport online have just been introduced to drive further uptake of verified identity.

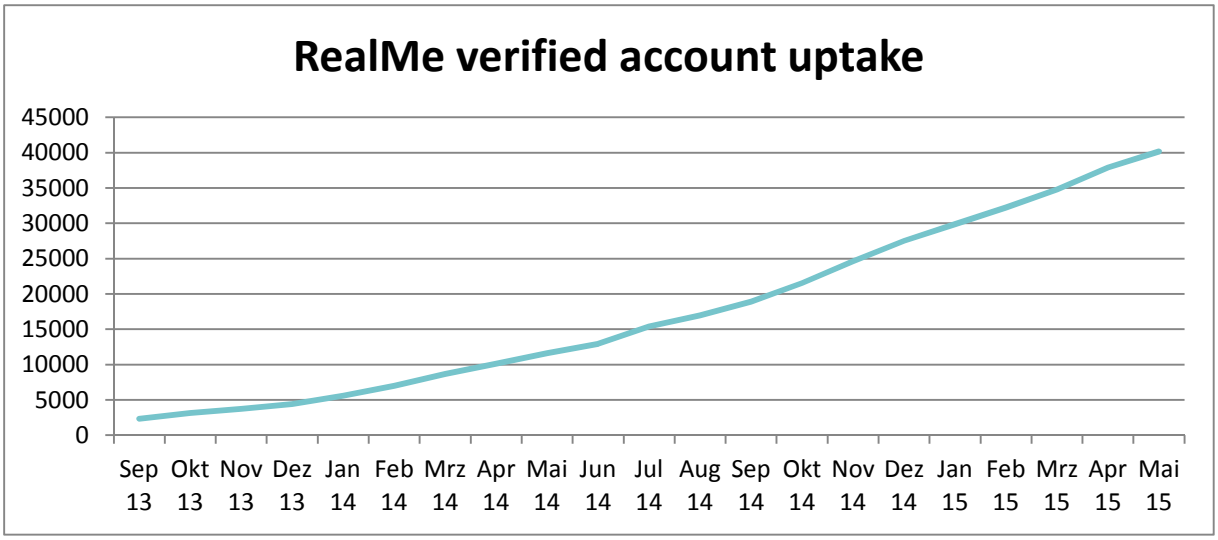


Figure 3: Uptake of RealMe Verified Accounts

Services available:

Customers with a verified identity can use services offered by the following organisations:-

These organisations have signed up for the verified service already — and we're adding more all the time.

bnz Westpac TSB Bank

STUDYLINK Hoto Akoranga A service of the Ministry of Social Development

INTERNAL AFFAIRS Te Tari Taiwhenua

NZFOREX FOREIGN EXCHANGE SERVICES

ELECTIONS ELECTORAL COMMISSION Te Kaitiaki Take Kôwhiri

MOBILE
FOKUSGRUPPE IM BVDW

BVDW
Wir sind das Netz

Faszination Mobile

Verbreitung, Nutzungsmuster und Trends

Bundesverband Digitale Wirtschaft in Kooperation mit Google und TNS Infratest

Carola Lopez

Zielsetzung und Methodik der Befragung

- Das vorliegende Studienband ist im Rahmen einer Studienkooperation des Bundesverband Digitale Wirtschaft (BVDW) e.V., Google und TNS Infratest entstanden. Die Studie beleuchtet die Verbreitung, Nutzungsmuster und Trends mobiler Endgeräte in Deutschland mit speziellem Fokus auf Smartphone-Nutzer.
- Das Studienband setzt sich aus zentralen Ergebnissen der TNS/Google Global Connected Consumer Studie und einer TNS Dual-Frame Telefonbefragung zusammen, die im Januar / Februar 2014 durchgeführt wurden.

MOBILE
FOKUSGRUPPE IM BVDW

Google TNS

TNS Infratest

BVDW
Wir sind das Netz

Verwendung mobiler Endgeräte bei der Internetnutzung in Deutschland

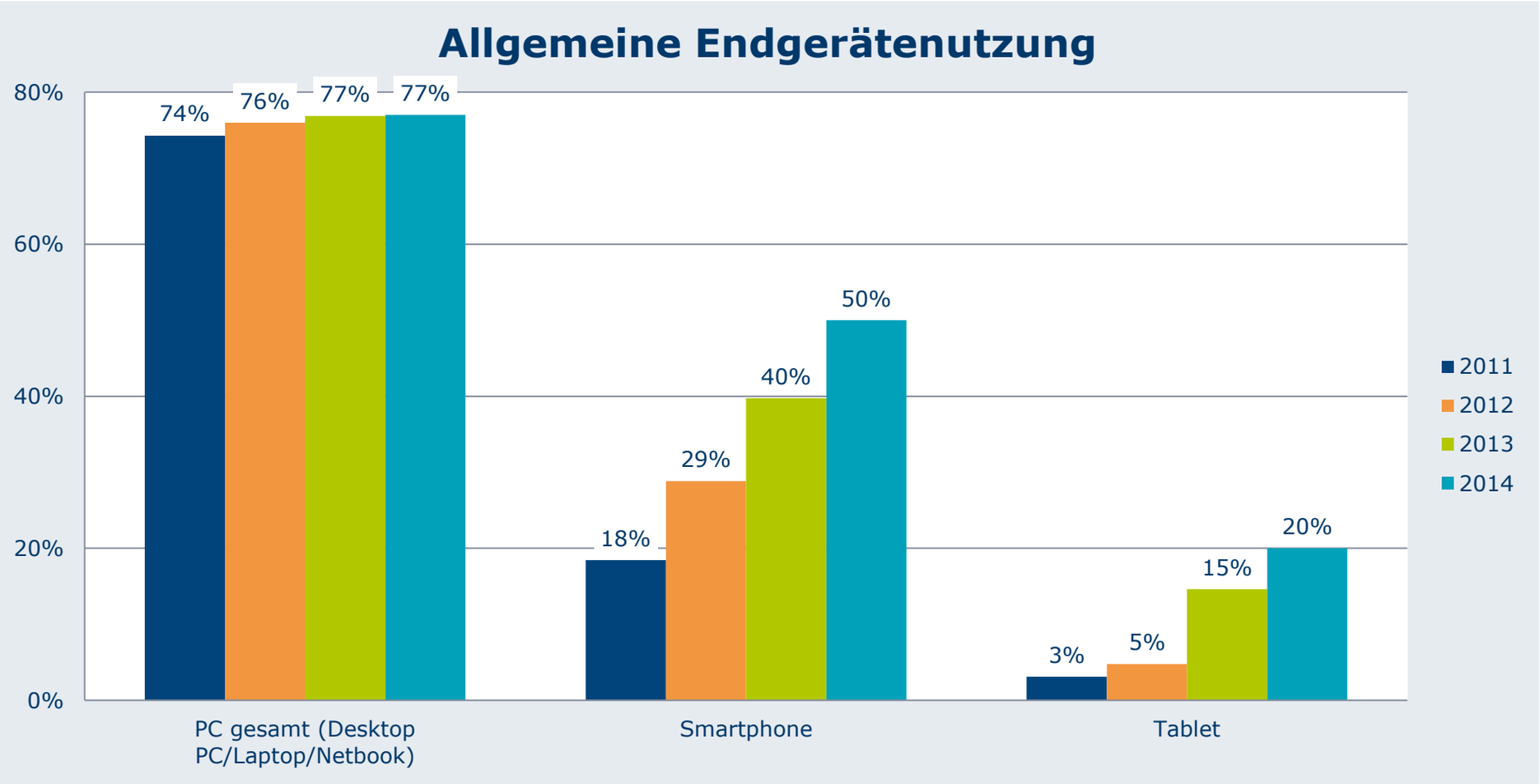
Mobile treibt die Onlinenutzung voran. 50 Prozent der Deutschen verwenden ein Smartphone (+25 Prozent 2014 zu 2013), 63 Prozent hiervon täglich (+21 Prozent 2014 zu 2013) (ca. 25 Mio. Menschen in Deutschland).

Durchschnittlich werden mehr als zwei internetfähige Endgeräte genutzt. 14 Prozent nutzen ein Tablet, ein Smartphone und einen PC.

MOBILE
FOKUSGRUPPE IM BVDW

Google TNS TNS Infratest BVDW Wir sind das Netz

Die Smartphone-Nutzung wächst in Deutschland weiter stark an, allein 2013 auf 2014 um +25 Prozent.

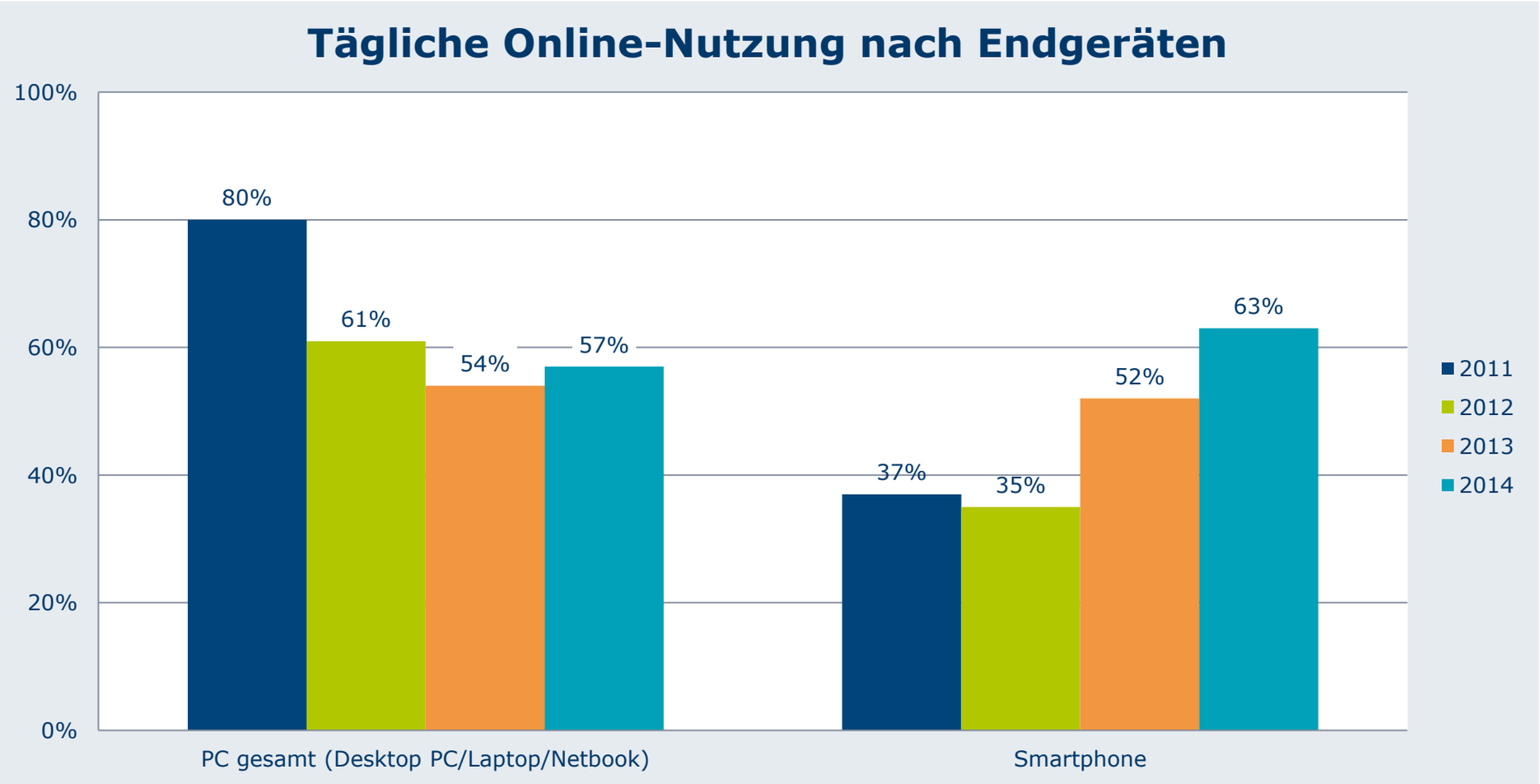


Quelle: Google (2013), Connected Consumer Study, TNS, Q1 2014, Q1 2013, Q1 2012, Q1 2011; Basis (gewichtet): Alle Befragten n=1,000; Frage: Welche der folgenden Geräte , wenn überhaupt, nutzen Sie gerade?

MOBILE
FOKUSGRUPPE IM BVDW

Google TNS TNS Infratest BVDW Wir sind das Netz

Der Anteil an täglichen Nutzern unter den Smartphone-Usern ist allein 2013 auf 2014 um +21 Prozent angestiegen.

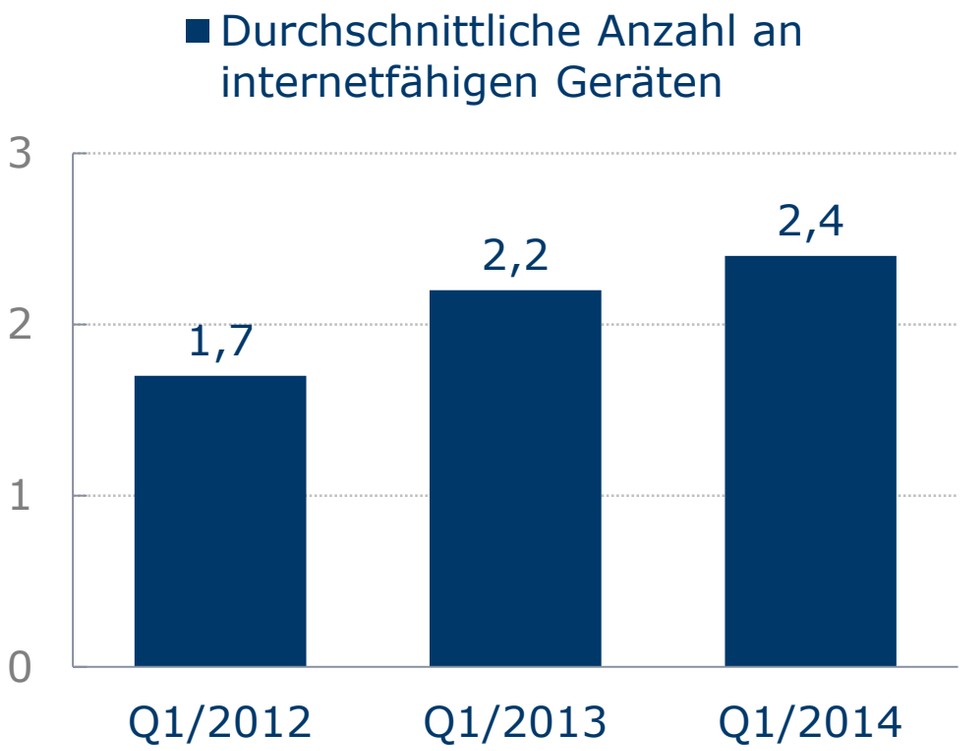


Quelle: Google (2013), Connected Consumer Study, TNS, Q1 2014, Q1 2013, Q1 2012, Q1 2011; Basis (gewichtet): Alle Befragten n=1,000; Frage: „Wie häufig nutzen Sie per .... das Internet (…) für private Zwecke? Bitte denken Sie hierbei an Ihre Nutzungsgewohnheiten im letzten Monat."

MOBILE FOKUSGRUPPE IM BVDW

Google TNS TNS Infratest BVDW Wir sind das Netz

Aktuell verwendet die Gesamtbevölkerung im Durchschnitt 2,4 internetfähige Internetgeräte.



14%

der Deutschen ab 16 Jahren nutzen ein Tablet, ein Smartphone und einen PC.

Quelle: Google (2013), Connected Consumer Study, TNS, Q1 2014, Q1 2013, Q1 2012, Q1 2011; Basis (gewichtet): Alle Befragten n=1,000; Frage: „Wie häufig nutzen Sie per .... das Internet (…) für private Zwecke? Bitte denken Sie hierbei an Ihre Nutzungsgewohnheiten im letzten Monat."

MOBILE
FOKUSGRUPPE IM BVDW

Google TNS TNS Infratest BVDW Wir sind das Netz

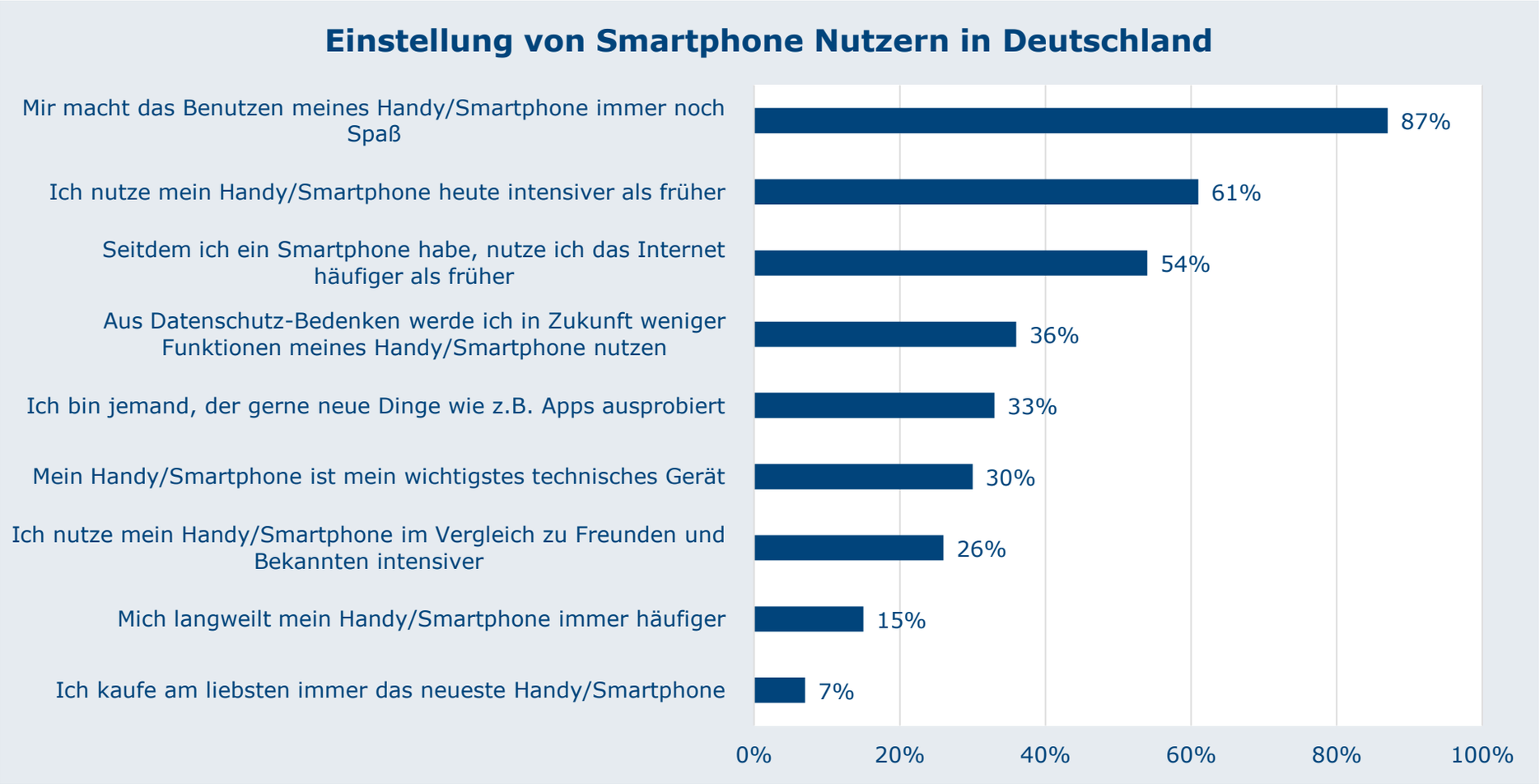
Einstellungen und Muster der Smartphone Nutzung

Die Mehrheit der Smartphone-Nutzer (87 Prozent) hat noch immer Spaß an der Nutzung

60 Prozent der Befragten weisen eine intensivere Nutzung als früher auf.

Mehr als die Hälfte (54 Prozent) der Befragten sind durch das Smartphone häufiger online als in der Vergangenheit

Die Mehrheit der Smartphone-Nutzer hat noch immer Spaß an der Nutzung, 60 Prozent weisen eine intensivere Nutzung als früher auf.

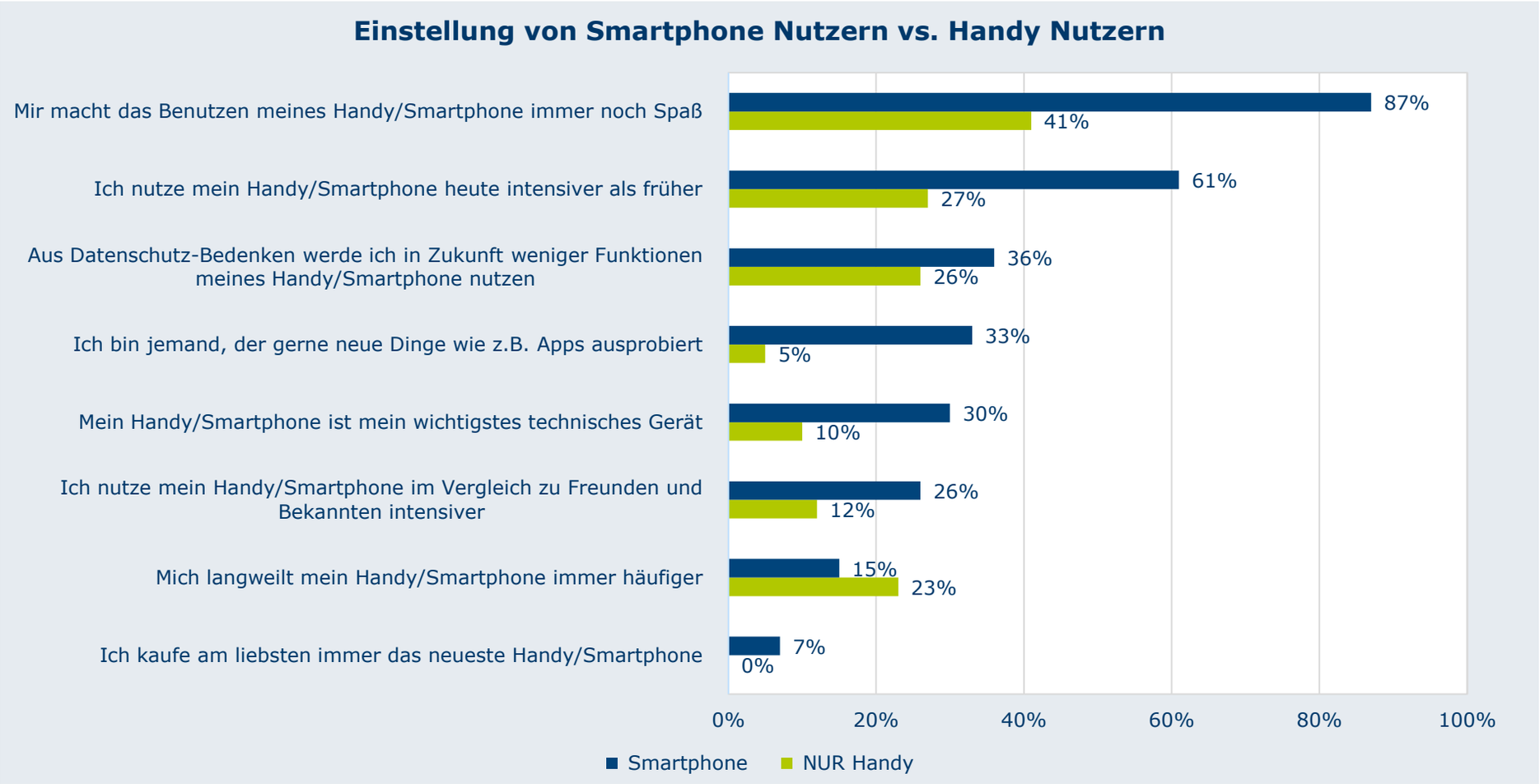


Quelle: TNS Infratest (2014), CATI 100 Omnibus, Basis: N=228 (Besitzer eines Smartphones); Frage: „Ich lese Ihnen jetzt einige Aussagen zu Nutzung und Einstellungen rund ums Handy/Smartphone vor. Sagen Sie mir jeweils, ob die Aussagen auf Sie persönlich eher zutreffen oder eher nicht zutreffen."

Einstellungen und Muster der Nutzung
Smartphone vs. Handy-Nutzer

Verglichen mit Smartphone-Nutzern haben Handy-Nutzer eine deutlich geringere Bindung zu ihrem Handy: Sie nutzen das Handy weniger intensiv und haben weniger Spaß an der Nutzung.

Verglichen mit Smartphone-Nutzern haben Handy-Nutzer eine deutlich geringere Bindung zu ihrem Handy und sind weniger offen für Neues.



Quelle: TNS Infratest (2014), CATI 100 Omnibus, Basis: N=228 (Besitzer Smartphone);N=210 (Besitzer Handy); Frage: „Ich lese Ihnen jetzt einige Aussagen zu Nutzung und Einstellungen rund ums Handy/Smartphone vor. Sagen Sie mir jeweils, ob die Aussagen auf Sie persönlich eher zutreffen oder eher nicht zutreffen."

MOBILE
FOKUSGRUPPE IM BVDW

Google TNS

TNS Infratest

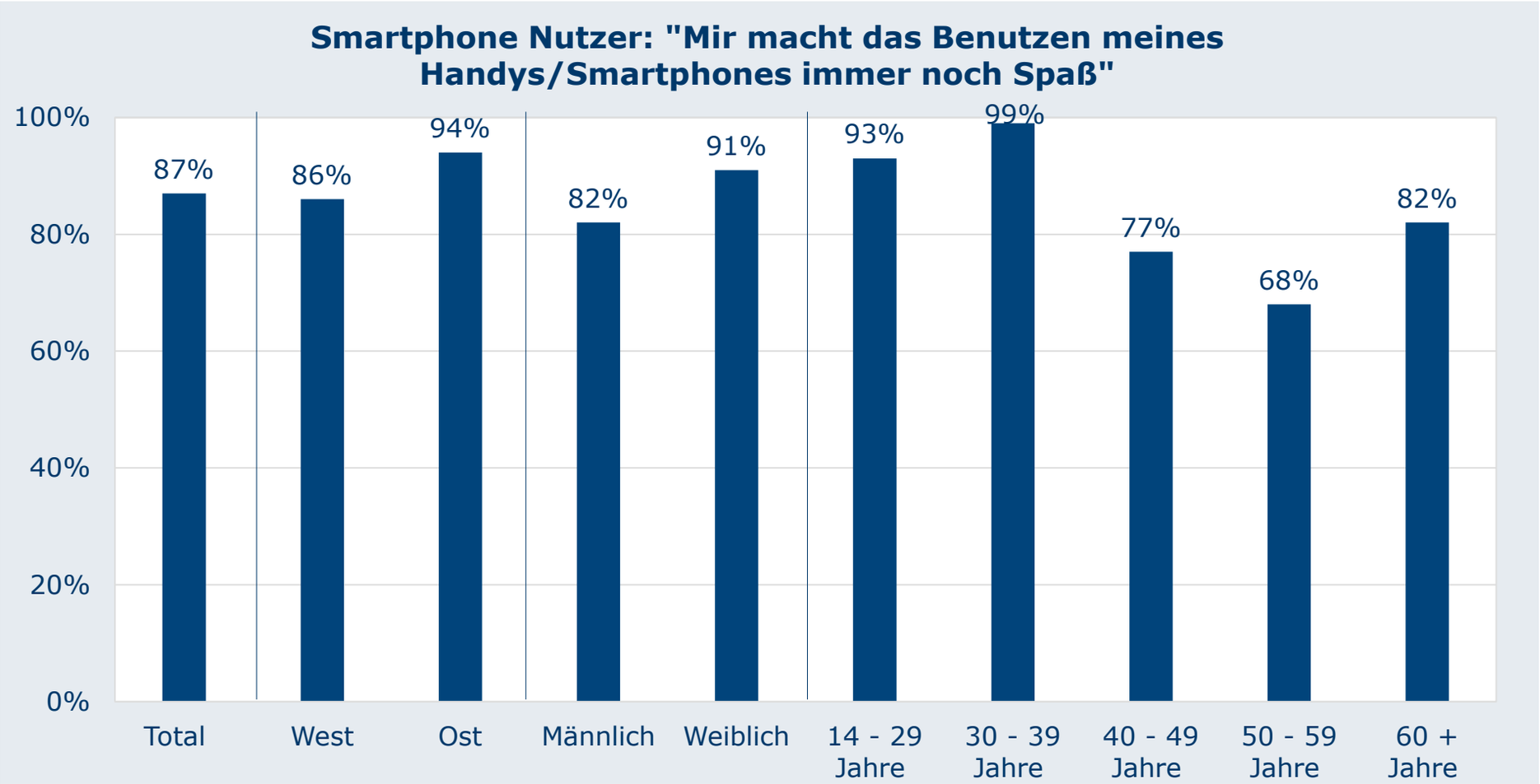
BVDW
Wir sind das Netz

Detailbetrachtung: *"Mir macht das Benutzen meines Handys/Smartphones immer noch Spaß"*

99 Prozent der 30-39-Jährigen Smartphone Nutzer sagen, dass die Smartphone Nutzung immer noch Spaß macht, bei den 14-29-Jährigen sind es 93 Prozent.

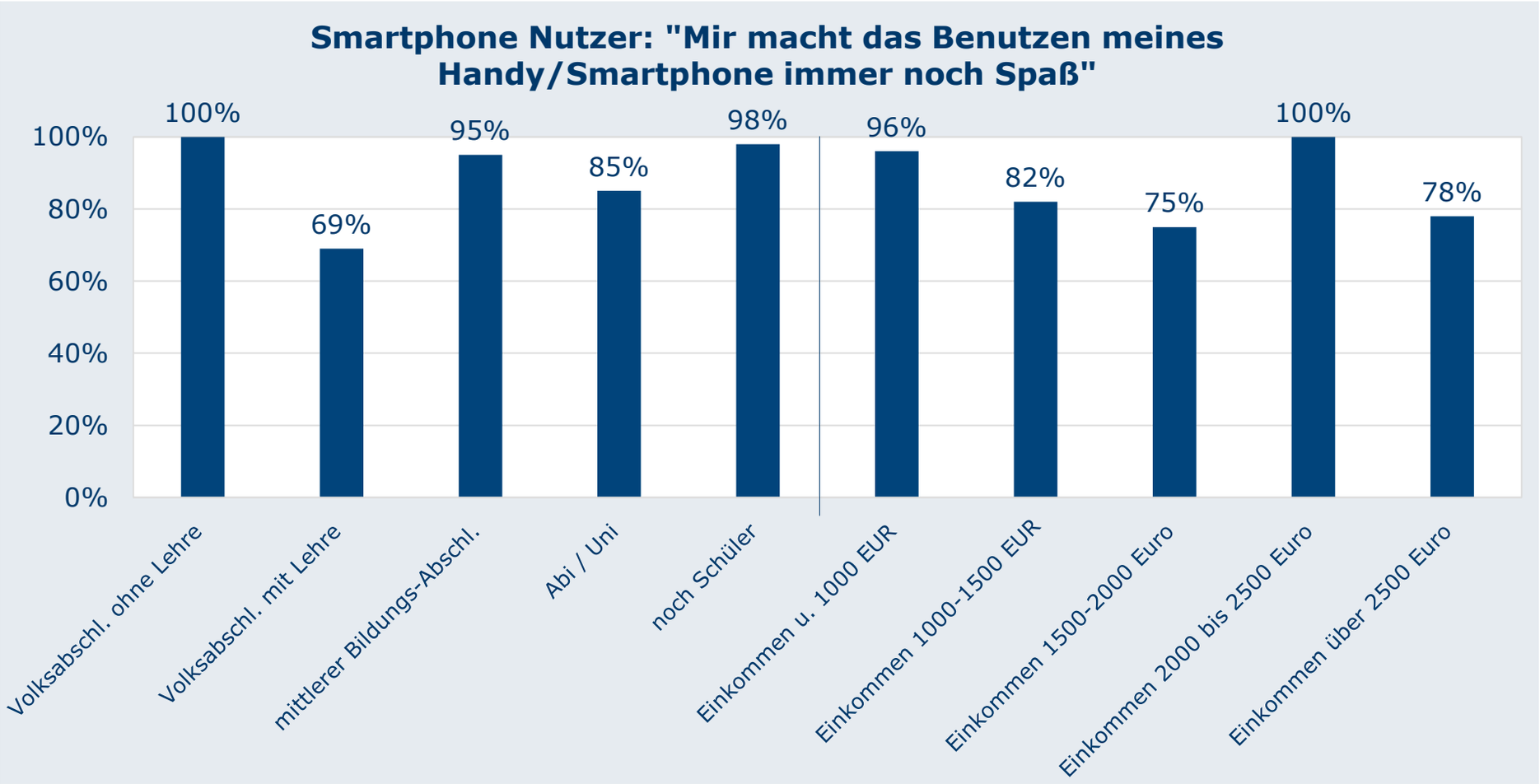
Frauen stimmen dem mit 91 Prozent deutlich stärker zu als Männer mit 82 Prozent.

99 Prozent der 30-39-Jährigen sagen, dass die Smartphone Nutzung immer noch Spaß macht, Frauen stimmen dem stärker zu als Männer.



Quelle: TNS Infratest (2014), CATI 100 Omnibus, Basis: N=228 (Besitzer eines Smartphones); Frage: „Ich lese Ihnen jetzt einige Aussagen zu Nutzung und Einstellungen rund ums Handy/Smartphone vor. Sagen Sie mir jeweils, ob die Aussagen auf Sie persönlich eher zutreffen oder eher nicht zutreffen."

Zwischen den einzelnen Bildungs- und Einkommensclustern zeigen sich zwar deutliche Schwankungen, jedoch ohne klaren Trend.



Quelle: TNS Infratest (2014), CATI 100 Omnibus, Basis: N=228 (Besitzer eines Smartphones); Frage: „Ich lese Ihnen jetzt einige Aussagen zu Nutzung und Einstellungen rund ums Handy/Smartphone vor. Sagen Sie mir jeweils, ob die Aussagen auf Sie persönlich eher zutreffen oder eher nicht zutreffen."

MOBILE
FOKUSGRUPPE IM BVDW

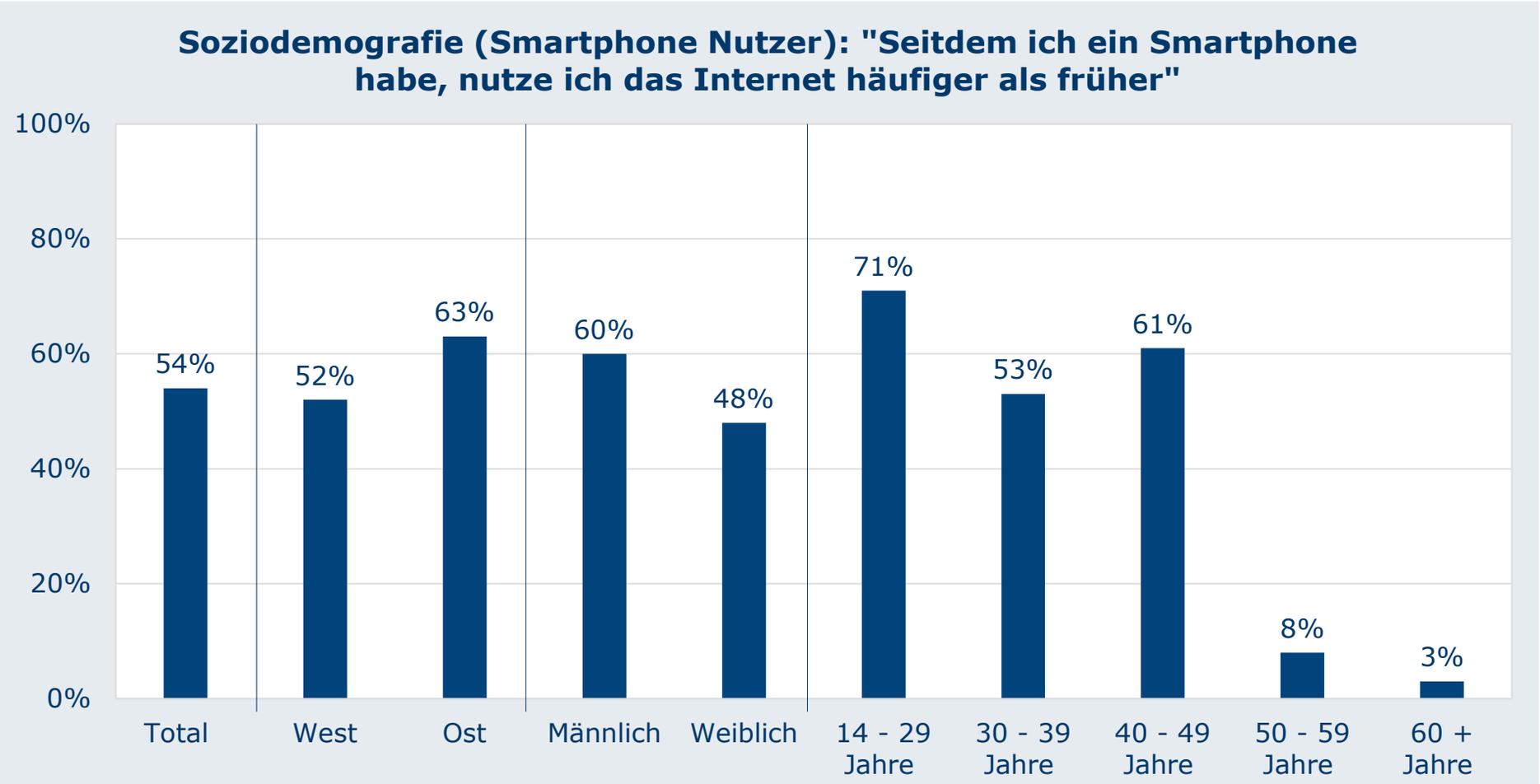
Google TNS TNS Infratest BVDW Wir sind das Netz

Detailbetrachtung: *"Seitdem ich ein Smartphone habe, nutze ich das Internet häufiger als früher"*

60 Prozent der Männer und 48 Prozent der Frauen geben an, dass sie durch das Smartphone häufiger online sind.

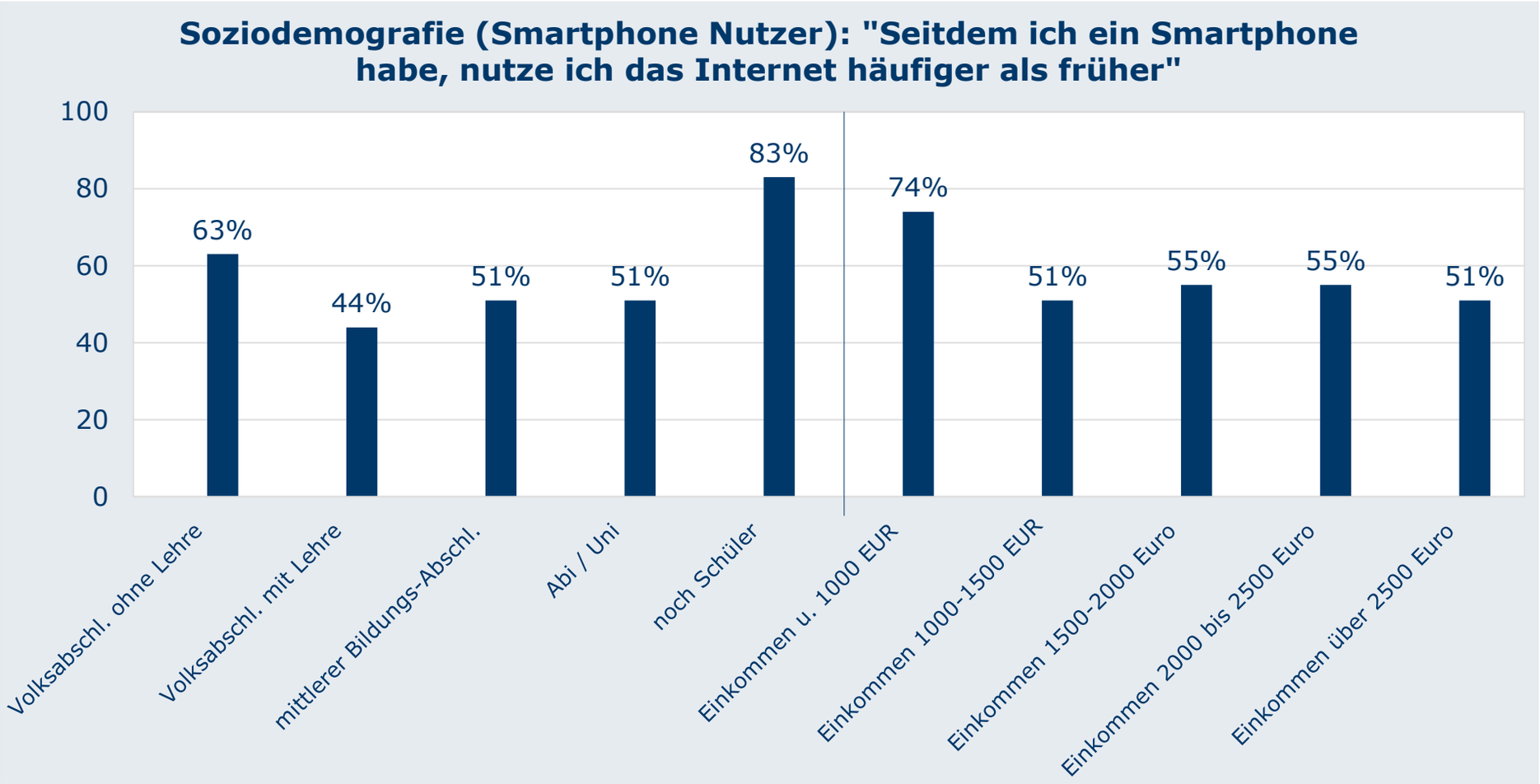
Von den befragten Schülern nutzen 83 Prozent das Internet häufiger als früher seitdem sie ein Smartphone besitzen.

60 Prozent der Männer und 48 Prozent der Frauen geben an, dass sie durch das Smartphone häufiger online sind.



Quelle: TNS Infratest (2014), CATI 100 Omnibus, Basis: N=228 (Besitzer eines Smartphones); Frage: „Ich lese Ihnen jetzt einige Aussagen zu Nutzung und Einstellungen rund ums Handy/Smartphone vor. Sagen Sie mir jeweils, ob die Aussagen auf Sie persönlich eher zutreffen oder eher nicht zutreffen."

Von den befragten Schülern nutzen 83 Prozent das Internet häufiger als früher seitdem sie ein Smartphone besitzen.



Quelle: TNS Infratest (2014), CATI 100 Omnibus, Basis: N=228 (Besitzer eines Smartphones); Frage: „Ich lese Ihnen jetzt einige Aussagen zu Nutzung und Einstellungen rund ums Handy/Smartphone vor. Sagen Sie mir jeweils, ob die Aussagen auf Sie persönlich eher zutreffen oder eher nicht zutreffen."

MOBILE
FOKUSGRUPPE IM BVDW

Google TNS

TNS Infratest

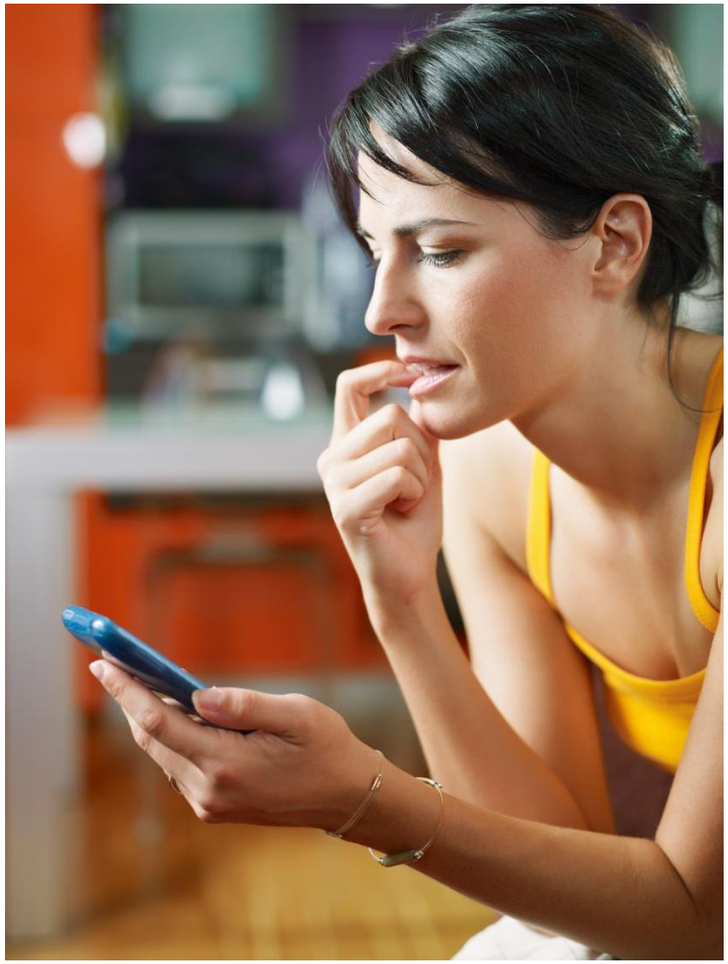
BVDW
Wir sind das Netz

Detailbetrachtung: *„Aufgrund von Datenschutz-Bedenken werde ich in Zukunft weniger Funktionen meines Smartphones nutzen"*

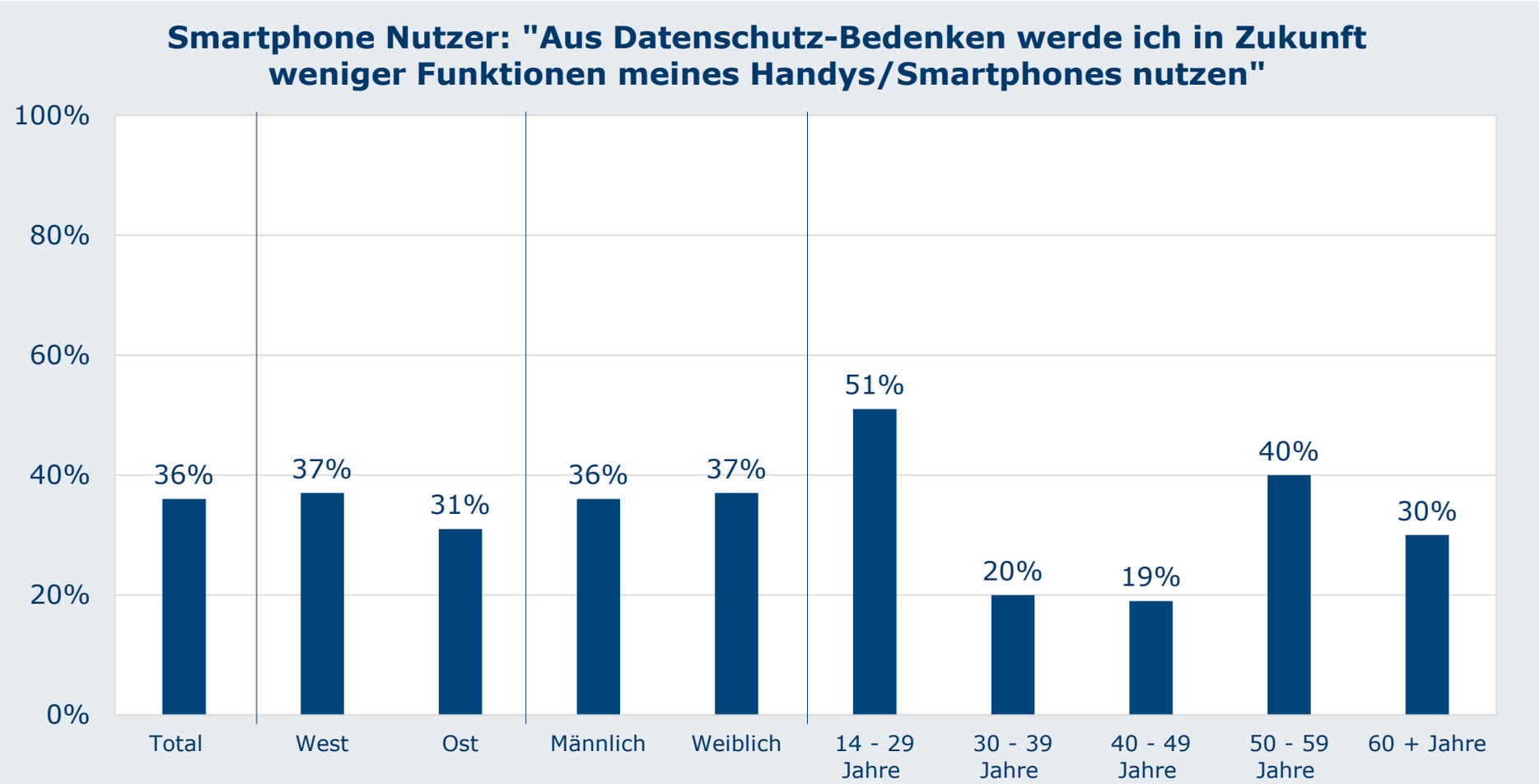
Mehr als jeder Zweite der 14-29-Jährigen Smartphone Nutzer will aus Datenschutz-Bedenken in Zukunft weniger Funktionen seines Handys nutzen. Bei den 50-59-Jährigen stimmen dem 40 Prozent zu.

Zwischen den Geschlechtern zeigen sich keine Unterschiede in der Einstellung.

Personen mit einem hohen Haushalts-Nettoeinkommen (über 2.500 Euro) weisen die geringste Zustimmung auf.



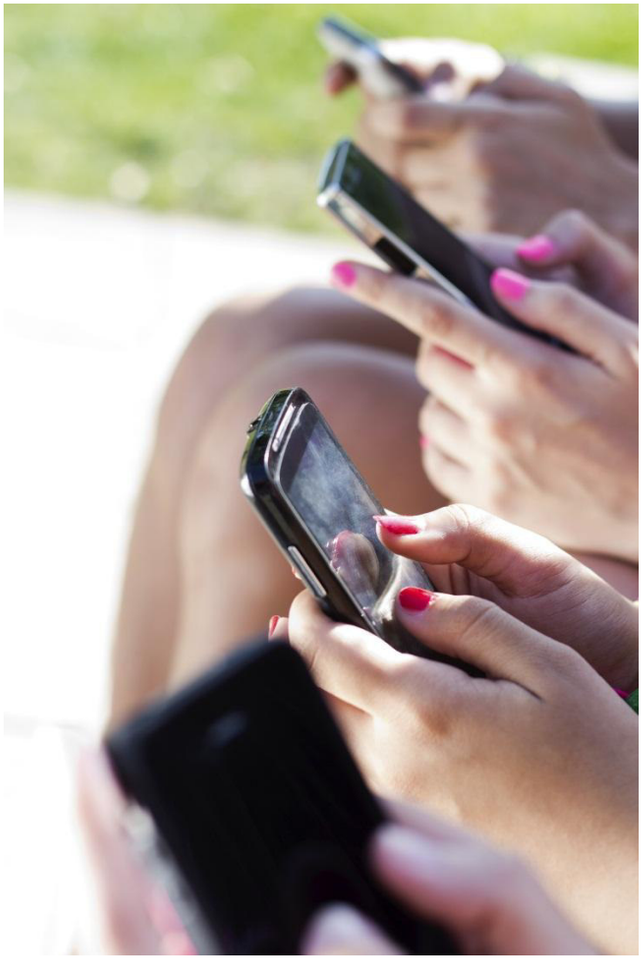
Mehr als jeder zweite der 14-29-Jährigen will aus Datenschutz-Bedenken in Zukunft weniger Funktionen seines Handys nutzen.



Quelle: TNS Infratest (2014), CATI 100 Omnibus, Basis: N=228 (Besitzer eines Smartphones); Frage: „Ich lese Ihnen jetzt einige Aussagen zu Nutzung und Einstellungen rund ums Handy/Smartphone vor. Sagen Sie mir jeweils, ob die Aussagen auf Sie persönlich eher zutreffen oder eher nicht zutreffen."

Executive Summary

- Mobile treibt die Online-Nutzung. 50 Prozent der Deutschen verwenden ein Smartphone (+25 Prozent 2014 zu 2013), 63 Prozent hiervon täglich (+21 Prozent 2014 zu 2013).
- Durchschnittlich werden mehr als zwei internetfähige Endgeräte genutzt. 14 Prozent nutzen ein Tablet, ein Smartphone und einen PC.
- Die Mehrheit der Smartphone-Nutzer (87 Prozent) hat noch immer Spaß an der Nutzung, hier zeigt sich besonders bei den Frauen eine hohe Zustimmung mit 91 Prozent (Männer: 82 Prozent). Mehr als die Hälfte (54 Prozent) der Befragten sind durch das Smartphone häufiger online als früher.



Studiendetails

1) TNS/Google Global Connected Consumer Study

- Die Global Connected Consumer Study liefert Basisdaten zur Marktpenetration von „connected devices" seit 2011, darunter auch in Deutschland. Speziell werden Internetpenetration & Zugangsquellen (Desktop, Smartphone, Tablet) analysiert.
- Methodik: Telefoninterviews (CATI) und Face-2-Face mit ca. 1.000 Befragten. Repräsentative Erhebung für die Gesamtbevölkerung ab 16 Jahren.
- Feldzeit der Studie: Januar/Februar 2014.

2) TNS Infratest – Dual-Frame Telefonbefragung

- Die Dual-Frame Telefonbefragung kombiniert Festnetz- und Mobilfunkstichproben und erfasst auf diese Weise auch (verbessert) Personengruppen, die nur oder leichter über Mobilfunk erreichbar sind. Dadurch wird die Qualität der Gesamtstichprobe in Richtung Repräsentativität und Ausschöpfung optimiert.
- Methodik: Dual-Frame Telefonbefragung von Festnetz- und Mobilfunknutzern im Rahmen des CATI 100 Omnibus von TNS Infratest mit ca. 1.000 Befragten pro Woche. Repräsentative Erhebung für die deutsche Bevölkerung ab 14 Jahren.
- Feldzeit der Studie: Januar 2014.

MOBILE
FOKUSGRUPPE IM BVDW

Google TNS

TNS Infratest

BVDW
Wir sind das Netz

Kontakt Google

Aline Breiter

Market Research DACH

Google Deutschland

Tel. +49 (0)40 80817-9228

Mail alineb@google.com

Dr. Ingo Knuth

Market Research DACH

Google Deutschland

Tel. +49 (0)40 80817-9459

Mail ingoknuth@google.com

MOBILE
FOKUSGRUPPE IM BVDW

Google TNS

TNS Infratest

BVDW
Wir sind das Netz

Kontaktinformationen TNS Infratest

Walter Freese

Head of Mobile,

TNS Infratest

Tel: 0521/ 9257 690
walter.freese@tns-infratest.com

Gabriele Herrmann

Director Tech & Media,

TNS Infratest

Tel. 040/ 44 119 380
gabriele.herrmann@tns-infratest.com

MOBILE
FOKUSGRUPPE IM BVDW

BVDW
Wir sind das Netz

Carola Lopez
Leiterin Marktforschung, Manger Digital Business

BVDW e.V.
Berliner Allee 57
40212 Düsseldorf
Fon +49 211 600456 - 26
Fax +49 211 600456 - 33
lopez@bvdw.org
www.bvdw.org

Barbara Kolocek
Projektmanager Digital Business

BVDW e.V.
Berliner Allee 57
40212 Düsseldorf
Fon +49 211 600456 - 17
Fax +49 211 600456 - 33
kolocek@bvdw.org
www.bvdw.org

© 2014 | Bundesverband Digitale Wirtschaft (BVDW) e.V.