BMI –IT4-644 004/14#5 2. Juli 2008

Einführung des elektronischen Personalausweises in Deutschland

---

Grobkonzept - Version 2.0

Bundesministerium des Innern

Referat IT 4 - Biometrie, Pass- und Ausweiswesen, Meldewesen

E-Mail: ePA@bmi.bund.de

INHALTSVERZEICHNIS

1 MANAGEMENTZUSAMMENFASSUNG

Der deutsche Personalausweis genießt als langjährig etabliertes, hoheitliches Identifizierungs- und Reisedokument großes Vertrauen. Sowohl im Bereich der Verwaltung als auch im privatwirtschaftlichen Bereich wird er für vielfältige Identifizierungszwecke und als Altersnachweis genutzt.

Ziel der Einführung des elektronischen Personalausweises (ePA) in Deutschland ist es, die bewährten Funktionen des „konventionellen" Personalausweises um elektronische Funktionen zu ergänzen und das Dokument damit den Herausforderungen und Möglichkeiten des 21. Jahrhunderts anzupassen.

Der neue Personalausweis dient vor allem der Identifizierung seines Inhabers im Geschäftsverkehr mit Verwaltung und Privatwirtschaft. Da diese ihre Geschäftsprozesse vermehrt auf elektronische Verfahren umstellen, werden sichere Identifizierungslösungen auch für den Einsatz in der elektronischen Welt des E-Government und E-Business benötigt.

Wesentliche Voraussetzung ist das gegenseitige Vertrauen und die Herstellung der erforderlichen Transparenz auf Seiten aller Beteiligten – Bürger, Wirtschaft, Verwaltung. Als in der realen Welt sicheres und anerkanntes Identifizierungsdokument ist der neuentwickelte elektronische Personalausweis geeignet, dieses Vertrauen herzustellen und wichtige Impulse für die Fortentwicklung im E-Government und E-Business zu geben.

Dazu müssen die auf dem Personalausweis aufgedruckten personenbezogenen Daten auch in elektronischer Form vorgehalten werden. Bei der Abwicklung von Online-Transaktionen können dann die jeweils erforderlichen Daten dem Geschäftspartner nach einer Berechtigungsprüfung in gesicherter Form elektronisch übermittelt werden. Über die Freigabe und Übermittlung der Daten entscheiden die Inhaber des Personalausweises selbst (PIN). Diese als „elektronischer Identitätsnachweis" bezeichnete Funktionalität (auch eID-Funktion oder Authentisierungsfunktion) ist neu und muss in Hinblick auf die eingesetzte Technik und die Prozessabläufe im Detail spezifiziert und gesetzlich verankert werden. Mit dem elektronischen Identitätsnachweis soll ein Mittel geschaffen werden, das die Anforderungen an Vertraulichkeit, Authentizität und Verfügbarkeit im E-Government und E-Business erfüllt und den Bürgerinnen und Bürgern in einfach zu handhabender und einheitlicher Weise zur Verfügung steht.

In der Regel reicht ein Identitätsnachweis, d. h. die Bestätigung der Identität einer Person zur

Abwicklung eines Geschäftsvorfalles aus. Ist jedoch in der realen Welt eine eigenhändige Unterschrift erforderlich, wird in der elektronischen Welt eine qualifizierte elektronische Signatur als Äquivalent verlangt. Die Funktion der elektronischen Signierung soll daher als Option ebenfalls in den elektronischen Personalausweis integriert werden. „Option“ heißt, dass der elektronische Personalausweis für die Aufnahme eines qualifizierten Signaturzertifikates gem. SigG vorbereitet ist, das Zertifikat selbst aber von den Inhabern des Personalausweises in den Chip nachgeladen werden muss. Diese Wahlfreiheit ermöglicht den Einsatz in Abhängigkeit von einem konkreten Bedarf.

Mehr Sicherheit bei der Verifikation der Identität von Personen wird zudem für behördliche Kontrollprozesse insbesondere durch die Integration biometrischer Merkmale in elektronischer Form erreicht. So wird der deutsche Reisepass bereits seit November 2005 mit einem kontaktlosen Chip, in dem u. a. biometrische Merkmale gespeichert werden, ausgerüstet. In Hinblick auf eine einheitliche Sicherheitsstrategie für Reisedokumente wird auch der elektronische Personalausweis biometrische Merkmale (das Gesichtsbild grundsätzlich und auf Antrag - also freiwillig - auch die Fingerabdrücke) enthalten, die ausschließlich zur Identifizierung gegenüber hoheitlichen Stellen genutzt werden. Um den Aufwand für die Ausstellung und die Kontrolle des elektronischen Personalausweises zu minimieren, wird er mit den gleichen biometrischen Merkmalen und der gleichen Technik wie der Reisepass ausgerüstet sein.

Die Integration biometrischer Informationen, einem elektronischen Identitätsnachweis und einer qualifizierten elektronischen Signaturfunktion vervollkommnet den künftigen elektronischen Personalausweis und macht ihn damit zum universellen, zukunftsfähigen und sicheren Schlüsselinstrument für E-Government und E-Business und zugleich zum zuverlässigen Identitätsnachweis zur Gewährleistung der Inneren Sicherheit Deutschlands.

2 EINFÜHRUNG

Der Personalausweis ist in Deutschland seit Jahrzehnten als staatliches Identifizierungsdokument etabliert. Als Passersatz dient er als Reisedokument in den Ländern der Europäischen Union und einigen weiteren Staaten. Neben dem hoheitlichen Bereich genießt der Personalausweis auch im privatwirtschaftlichen Umfeld hohes Vertrauen und wird dort zu Identifizierungszwecken, als Meldebescheinigung und als Altersnachweis eingesetzt. Damit die Bürger ihrer Ausweispflicht nachkommen können, besteht in Ausnahmefällen (z. B. nach Verlust des Personalausweises) auch die Möglichkeit, einen vorläufigen Personalausweis zu beantragen.

Bedingt durch den rasanten Fortschritt der Kommunikations- und Informationstechnik, insbesondere den Siegeszug des Internets als Plattform für die Abwicklung einer Vielzahl von Geschäften bzw. Verwaltungsverfahren auf elektronischem Wege (E-Business/E-Government), verändern sich auch die Anforderungen an eine sichere und zuverlässige Identifizierung der beteiligten Akteure untereinander: Da in der elektronischen Welt kein unmittelbarer Kontakt von Angesicht zu Angesicht zwischen den miteinander kommunizierenden Akteuren möglich ist, müssen neue Formen eines sicheren Identitätsnachweises an die Stelle der Sichtprüfung des Personalausweises treten.

Wesentliche Voraussetzung hierfür ist das gegenseitige Vertrauen und die Herstellung der erforderlichen Transparenz im Prozess der gegenseitigen Identifizierung zwischen den Akteuren – Bürgerinnen und Bürgern, Wirtschaft und Verwaltung.

Auch im Bereich der Inneren Sicherheit sind die Anforderungen an eine zweifelsfreie Identifizierung von Personen in den letzten Jahren stark gestiegen – nicht erst seit den Terroranschlägen von New York, Madrid und London sowie den versuchten Kofferbombenattentaten in Deutschland im Jahr 2006. Die zunehmende Mobilität der Gesellschaften innerhalb und außerhalb Europas erzeugt Wanderungsbewegungen, die an den Außengrenzen Deutschlands bzw. des Schengen-Raumes einer verstärkten Kontrolle bedürfen. Gleiches gilt für die Zunahme der grenzüberschreitenden organisierten Kriminalität (z. B. Drogen- und Menschenschmuggel, Geldwäsche, Proliferation). Die Wirksamkeit der Grenzsicherung, Gefahrenabwehr und Strafverfolgung im Inland ist in hohem Maße abhängig von den bestehenden Möglichkeiten zur sicheren, eindeutigen Personenfeststellung anhand vertrauenswürdiger (weil fälschungssicherer), zweifelsfrei einer natürlichen Person zuzuordnender Personaldokumente.

Angesichts der vorstehend genannten Anforderungen beabsichtigt der Bund, das bisherige Personalausweisdokument durch ein Ausweisdokument der „nächsten Generation“ abzulösen. Dieser **„elektronische Personalausweis“** soll - zusätzlich zu den bereits bewährten Sicherheitsmerkmalen des allgemein anerkannten konventionellen Personalausweises - um weitere elektronisch nutzbare Merkmale und Funktionen ergänzt werden. Das Ergebnis wird ein **kombiniertes Ausweissystem** (optischer und elektronischer Ausweis) sein, das universell einsetzbar ist, eine sichere und zuverlässige Identifizierung ermöglicht und sowohl den veränderten Nutzungsanforderungen von E-Government und E-Business als auch den Belangen der Inneren Sicherheit Rechnung trägt.

3 ZWECK UND AUFBAU DES DOKUMENTS

Das vorliegende Grobkonzept erörtert Erforderlichkeiten, Voraussetzungen, Nutzen und Gestaltungsmöglichkeiten für die Einführung eines elektronischen Personalausweises in Deutschland.

Ausgehend von einer Beschreibung des heutigen Verfahrens zur Identifizierung natürlicher Personen mit dem seit geraumer Zeit im Einsatz befindlichen Personalausweis in Deutschland werden zunächst die bestehenden Defizite und Handlungsfelder in Bezug auf die gegenwärtigen und zukünftig absehbaren Herausforderungen aufgezeigt (Stichworte: Sichere und zuverlässige Identifizierung, Transaktionssicherheit bei E-Government / E-Business im Internet). Anhand von Beispielen werden Beschaffenheit und Verwendung elektronischer Personaldokumente in anderen Ländern dargestellt und Schlussfolgerungen für die funktionale Auslegung eines zukünftigen elektronischen Personalausweises in Deutschland gezogen. Anhand konkreter (alltäglicher) Anwendungsszenarien werden die grundsätzlich mit der Einführung eines elektronischen Personalausweises verfolgten Ziele und Nutzen sowie die daraus ableitbaren Anforderungen und Gestaltungsoptionen für den elektronischen Personalausweis selbst und dessen Einsatzbedingungen im Zusammenhang mit Transaktionen im E-Government bzw. E-Business auf Seiten der Ausweisinhaber dargestellt. In Hinblick auf die Schaffung einer möglichst breiten Akzeptanz in der Bevölkerung und die gezielte Ansprache von Kreisen innovativer Pilotnutzer eines elektronischen Personalausweises werden auch Maßnahmen zur geeigneten Flankierung der Einführung vorgeschlagen. Den Abschluss bildet ein grober Umsetzungsplan, der einen Überblick über die kommenden Projektphasen und wesentlichen Meilensteine geben soll.

4 AUSGANGSLAGE

4.1 Zweck und Ausgestaltung des aktuellen Personalausweises

Jeder deutsche Staatsangehörige ist gem. § 1 Abs. 1 des Gesetzes über Personalausweise (PersAuswG) verpflichtet, nach Vollendung des 16. Lebensjahres und unter der Voraussetzung, dass er der Meldepflicht unterliegt, einen Personalausweis zu besitzen, sofern er sich nicht durch einen gültigen Reisepass ausweisen kann. Die neben dem Lichtbild und der Unterschrift des Ausweisinhabers auf dem Personalausweis aufzubringenden **personenbezogenen Informationen** regelt § 1 Abs. 2 PersAuswG abschließend:

1. Familienname und ggf. Geburtsname,
2. Vornamen,
3. Doktorgrad,
4. Tag und Ort der Geburt,
5. Größe,
6. Farbe der Augen,
7. gegenwärtige Anschrift,
8. Staatsangehörigkeit: deutsch.

Zusätzlich trägt der Personalausweis eine sog. **„maschinenlesbare Zone“** (MRZ), die nach §1 Abs. 3 PersAuswG folgende Informationen enthalten darf:

1. Die Abkürzung "IDD" für "Identitätskarte der Bundesrepublik Deutschland",
2. den Familiennamen,
3. den oder die Vornamen,
4. die Seriennummer des Personalausweises, die sich aus der Behördenkennzahl der Personalausweisbehörde und einer in der Regel fortlaufend zu vergebenden Ausweisnummer zusammensetzt,
5. die Abkürzung "D" für die Eigenschaft als Deutscher,
6. den Tag der Geburt,
7. die Gültigkeitsdauer des Personalausweises,
8. die Prüfziffern und
9. Leerstellen.

Aufgrund der terroristischen Ereignisse im September 2001 hat der Deutsche Bundestag mit dem im Jahr 2002 verabschiedeten Terrorismusbekämpfungsgesetz die Grundentscheidung getroffen, dass der Personalausweis neben dem Lichtbild und der Unterschrift grundsätzlich

auch weitere biometrische Merkmale von Fingern, Händen oder Gesicht des Personalausweisinhabers enthalten darf.[1]

Personalausweise werden für eine **Gültigkeitsdauer von 10 Jahren** ausgestellt; bei Personen unter 24 Jahren ist die Gültigkeit auf 6 Jahre beschränkt. Seit April 1987 wird der Personalausweis als laminiertes Papierdokument im sog. „ID2-Format“ (entspricht ungefähr der doppelten Scheckkartengröße) ausgegeben, da die bis zu diesem Zeitpunkt ausgegebenen Ausweise nicht mehr den Sicherheitsanforderungen an ein hoheitliches Identitätsdokument entsprachen. Verschiedene **optische Sicherheitsmerkmale** (z. B. Sicherheitsdruck, Laserbeschriftung) machen den aktuellen Personalausweis zu einem Hochsicherheitsdokument. Mit diesen Maßnahmen konnte die Fälschungssicherheit gegenüber seinem Vorgänger soweit erhöht werden, dass Totalfälschungen[2] schon heute praktisch nicht vorkommen.

4.2 Funktionen des aktuellen Personalausweises

Der in Deutschland z. Zt. ausgegebene Personalausweis dient in erster Linie als Dokument zum **Identitätsnachweis in hoheitlichen Verfahren**, d. h., zur eindeutigen Feststellung der Identität einer natürlichen Person durch berechtigte staatliche Stellen. Der Personalausweis ist dabei auf Verlangen der zur Prüfung der Personalien berechtigten Stelle vorzulegen. Die Identitätsprüfung – z. B. im Zuge einer Personenüberprüfung durch die Polizei, einer Anmeldung bei der zuständigen Meldebehörde oder der Beantragung von Sozialleistungen - erfolgt im direkten Kontakt durch Inaugenscheinnahme und Vergleich der im Personaldokument beschriebenen körperlichen Merkmale (z. B. Lichtbild, Größe, Augenfarbe, Alter) mit den tatsächlichen körperlichen Merkmalen der zu identifizierenden Person. Bei Übereinstimmung können die übrigen Daten des Dokuments (Identitätsmerkmale) der Person zugeordnet werden. Der Personalausweis dient gleichzeitig als **Passersatz- und damit als Reisedokument** zur Erfüllung der Passpflicht bei grenzüberschreitenden Reisen, sofern dies durch das Recht der Europäischen Union, internationale oder bilaterale Abkommen vorgesehen ist.

Neben der Identifizierung in hoheitlichen Verfahren werden Personalausweise auch im **privatwirtschaftlichen Bereich** seit langem für den Identitätsnachweis des Kunden gegenüber dem Händler oder Diensteanbieter genutzt. Analog zur Feststellung der Identität im hoheitlichen Verfahren (z. B. im Rahmen einer Polizei- oder Grenzkontrolle) übergibt der Personalausweisinhaber den Personalausweis im Geschäftverkehr dabei zur Prüfung an den Geschäftspartner, der die „behauptete“ Identität des Personalausweisinhabers mit der ihm ge-

[1] Siehe § 1 Abs. 4 PersAuswG

[2] zur missbräuchlichen Nutzung siehe Kapitel 5

genüberstehenden Person feststellt (Authentifizierung) und sich die für den Geschäftsvorgang erforderlichen Daten soweit erforderlich notiert. Dabei kann der Personalausweis als reiner Altersnachweis (z. B. für den Eintritt in eine Diskothek, beim Erwerb von Waren, deren Erwerb Altersbeschränkungen unterliegt) oder als Identitäts- bzw. Legitimationsnachweis beim Abschluss eines KFZ-Mietvertrages oder beim Check-in am Flugschalter verwendet werden.

Ist kein direkter Kontakt zwischen Geschäftspartnern und Personalausweisinhabern möglich, existieren in der Praxis auch Verfahren, bei denen eine Identitätsfeststellung auf Basis des Personalausweises über eine dritte, von beiden Partnern als vertrauenswürdig angesehene, Partei erfolgen kann.[3]

4.3 Lebenszyklus des aktuellen Personalausweises

Der Abschnitt beschreibt im Überblick die Prozesse von der Beantragung über ggf. von Amts wegen vorzunehmende Änderungen am ausgegebenen Dokument bis hin zur Vernichtung in Folge Einziehung/Ungültigwerdens des gegenwärtigen Personalausweises. Der Gesamtprozess gliedert sich in die sechs logisch und zeitlich aufeinander folgenden Prozessepisoden „Beantragung“, „Produktion“, „Ausgabe“, „Nutzung“, „Rücknahme / Einziehung“ und „Vernichtung“, die wiederum in Teilprozesse zerfallen. Im Folgenden werden die einzelnen Teilprozesse zur Veranschaulichung grafisch dargestellt und die darin enthaltenen Prozessschritte anhand standardisierter Prozesstabellen kommentiert.

Abbildung 1: Lifecycle des Personalausweises - Gesamtprozess (Ist)

4.3.1 Prozessepisode 1: Beantragung des Personalausweises (Ist)

Personalausweise werden auf förmlichen Antrag der Bürgerinnen und Bürger hin ausgestellt. Die Antragsteller müssen dafür grundsätzlich persönlich bei der für sie zuständigen Personalausweisbehörde ihres Hauptwohnortes erscheinen und dort ihre Identität nachweisen. Sind Bürgerinnen und Bürger jünger als 16 Jahre, müssen auch gesetzliche Vertreter des Antragstellers zugegen sein und dem Antrag zustimmen. Im Falle der Erstbeantragung bedarf es u. a.:

[3] z. B. Postalisches Identifizierungsverfahren

- des Nachweises der deutschen Staatsangehörigkeit (z.B. auf Basis einer Einbürgerungsurkunde oder deutscher Ausweisdokumente),
- des Nachweises der Namensführung (z.B. anhand einer nach deutschem Personenstandsrecht anerkannten Heiratsurkunde) sowie
- des Nachweises der Identität (vorläufiger oder endgültiger Personalausweis bzw. Reisepass, deutscher Führerschein, aber auch Zeugenerklärungen, wenn die Bescheinigung nach amtlicher Personenfeststellung durch das Bundeskriminalamt bzw. das zuständige Landeskriminalamt erfolgt).

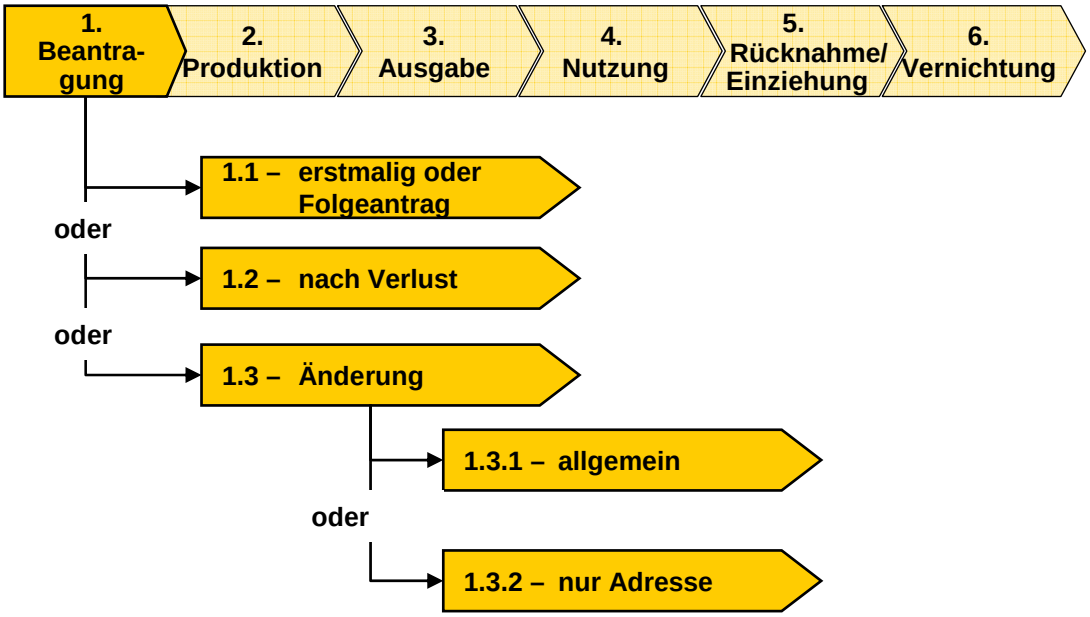

Abbildung 2: Prozessepisode 1 – Beantragung des Personalausweises (Ist)

Neben der Erstbeantragung ist das Antragsverfahren – in abgewandelter Form - auch **nach Ablauf der Gültigkeit** (Folgeantrag), bei **Verlust oder Änderung** des Inhalts von Personendaten zu durchlaufen. Hat sich beim Antragsteller nur die Adresse geändert, wird auf die Ausstellung eines neuen Dokuments verzichtet und die neue Adresse mittels eines auf dem Personalausweisdokument aufgebrachten, mit Dienstsiegel versehenen Aufklebers kenntlich gemacht.

4.3.1.1 Teilprozess 1.1: Erstmalige Beantragung oder Folgebeantragung (Ist)

Die Antragsdaten sind von der Personalausweisbehörde zu erfassen und elektronisch oder per Post an den – vom Bund bestimmten – Personalausweishersteller zu übermitteln

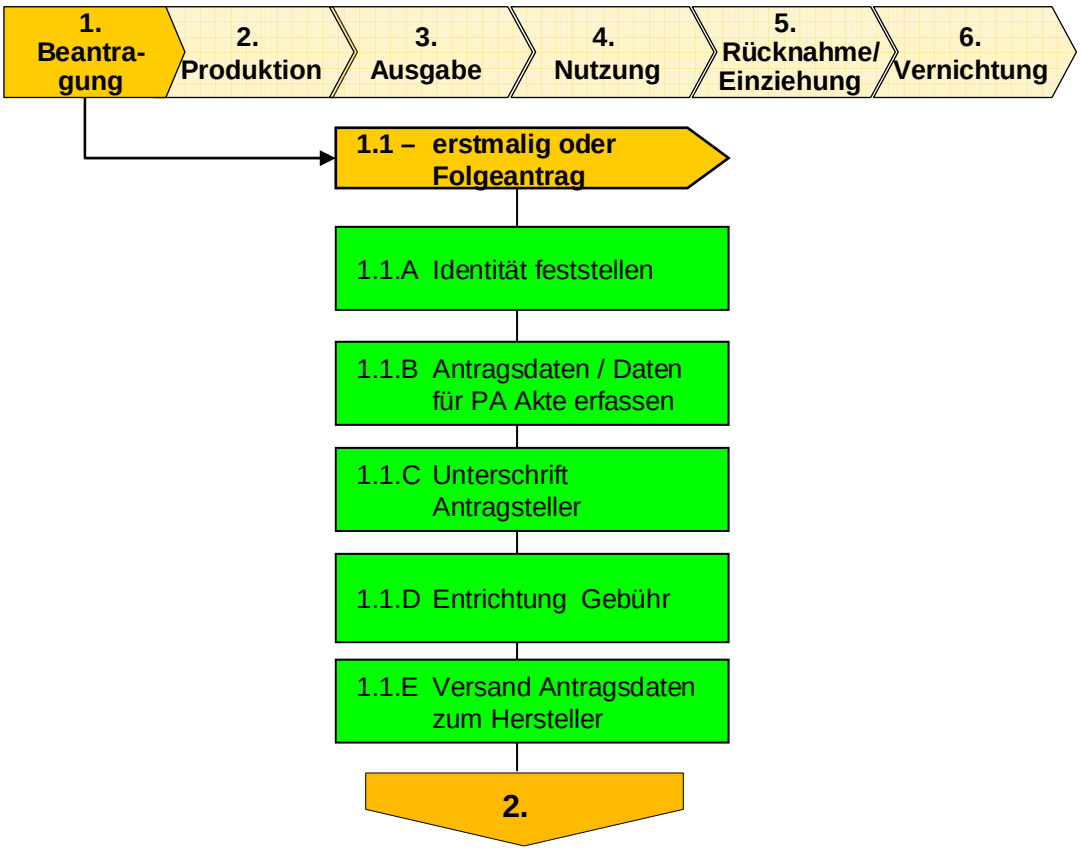

Abbildung 3: Teilprozess 1.1 – Erstmalige Beantragung oder Folgebeantragung (Ist)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
1.1.A	Identität feststellen	Bürgerinnen/Bürger, (ggf. gesetzlicher Vertreter), PA-Behörde	Sicherstellung Identifizierung nach Vorlage eines Identitätsnachweises	Identität ist festgestellt	

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
1.1.B	Antragsdaten / Daten für PA-Akte erfassen	PA-Behörde	Abgleich und ggf. Anpassung mit dem kommunalen Melderegister Anlegen / Anpassen elektronische PA-Akte Erfassung Personendaten für Antrag ggf. Erstellen eines vorläufigen PA Generierung und Ausdruck eines Antrags (mit automatisch generierter PA-Nummer) und Aufbringen Lichtbild	PA-Akte angelegt bzw. aktualisiert PA-Antrag ggf. vorläufiger PA	
1.1.C	Unterschrift Antragsteller	Bürgerinnen/ Bürger	Prüfung der Daten Unterzeichnung Antrag	PA-Antrag unterzeichnet	
1.1.D	Entrichtung Gebühr	Bürgerinnen/ Bürger, PA-Behörde	Einzahlung Ausweisgebühr	Gebühr bezahlt	Beim ersten Antrag entfällt die Gebühr
1.1.E	Versand Antragsdaten zum Hersteller	PA-Behörde	Scannen des Antrags und elektronischer Versand zum Hersteller oder Versand des Papierantrags zum Hersteller	Eingang PA-Antrag beim Hersteller	

Tabelle 1: Beschreibung TP 1.1 – Erstmalige Beantragung oder Folgebeantragung (Ist)

4.3.1.2 Teilprozess 1.2: Beantragung nach Verlust (Ist)

Gemäß den landesgesetzlichen Regelungen zum Personalausweisgesetz ist der Verlust eines Personalausweises von dessen Inhaber unverzüglich der zuständigen Personalausweisbehörde und Polizei anzuzeigen. Die Beantragung einer Ersatzausstellung nach Verlust zeigt der folgende Teilprozess.

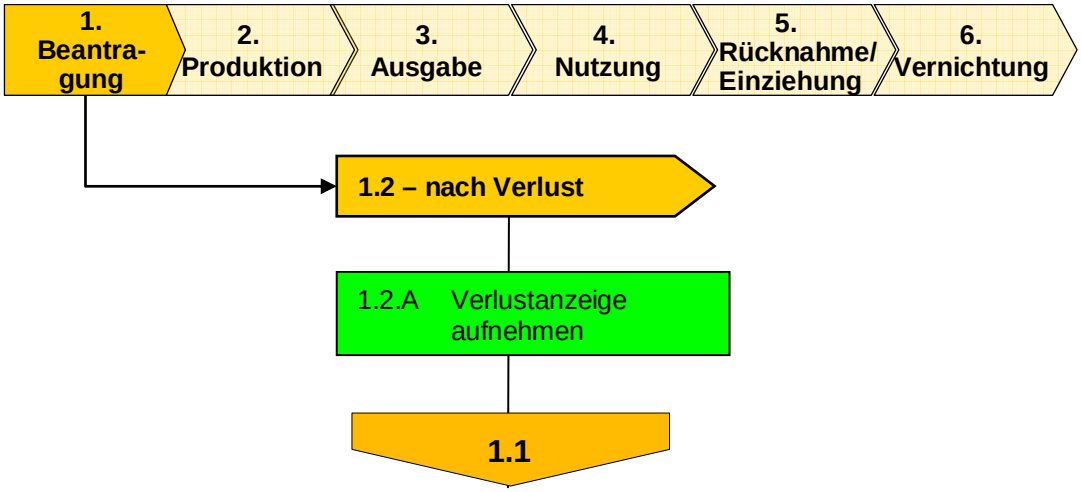

Abbildung 4: Teilprozess 1.2 – Beantragung nach Verlust (Ist)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
1.2.A	Verlustanzeige aufnehmen	Bürgerinnen/ Bürger, (ggf. gesetzlicher Vertreter), PA-Behörde	Prüfung der Identität des Antragstellers Aufnahme Verlustanzeige Aktualisierung PA-Akte	Verlustanzeige PA-Akte aktualisiert	
			weiter wie im Prozess 1.1		

Tabelle 2: Beschreibung TP 1.2 – Beantragung nach Verlust (Ist)

4.3.1.3 Teilprozess 1.3: Beantragung nach Änderung (Ist)

Änderungen im Personenstand oder der Hauptwohnung des Personalausweisinhabers ziehen auch Änderungen der auf dem Personalausweis vermerkten personenbezogenen Informationen nach sich. Dabei sind – je nach Anlass der Änderung – von der zuständigen Personalausweisbehörde bzw. dem Betroffenen unterschiedliche Maßnahmen einzuleiten.

Bei **Namensänderungen** z. B. in Folge Eheschließung, -scheidung oder Adoption ist die Ausstellung eines neuen Personalausweises erforderlich, der entsprechend zu beantragen ist.

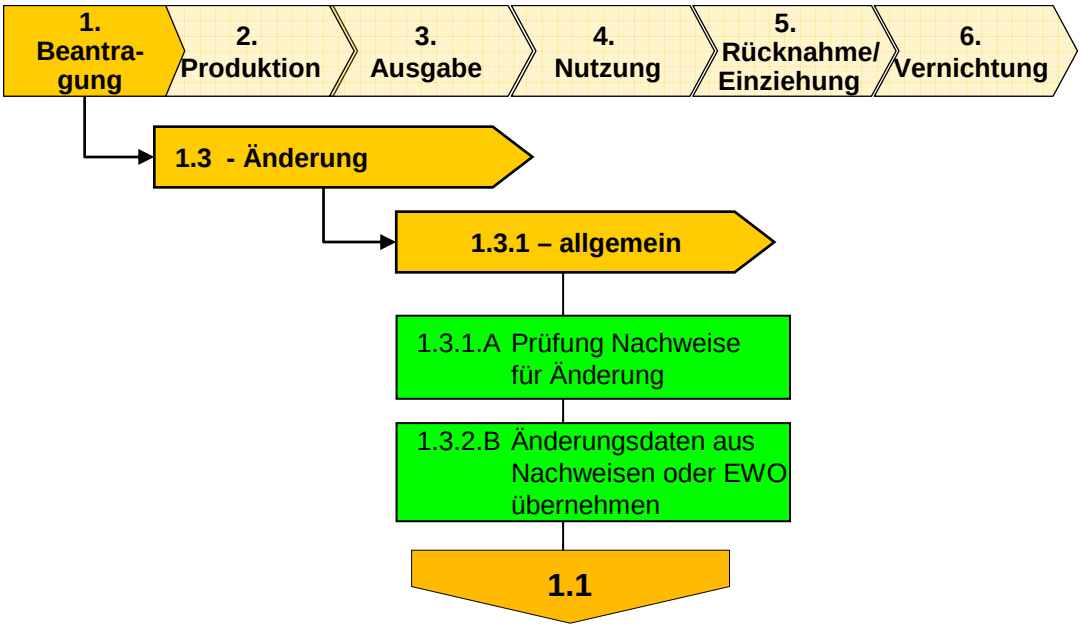

Abbildung 5: Teilprozess 1.3.1 – Beantragung nach Änderung allgemein (Ist)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
1.3.1.A	Prüfung Nachweise für Änderung	Bürgerinnen/ Bürger, (ggf. gesetzlicher Vertreter), PA-Behörde	Prüfung der Identität des Antragstellers Vorlage und Prüfung Nachweis für Änderung (z. B. Personenstandsurkunde, Antrag auf Ummeldung)	Prüfergebnisse, Nachweise	
1.3.1.B	Änderungsdaten aus Nachweisen oder EWO übernehmen	PA-Behörde	Aktualisierung PA-Akte Abgleich mit Melderegister-DB des EWO	PA-Akte aktualisiert	
			weiter wie im Prozess 1.1		

Tabelle 3: Beschreibung TP 1.3.1 – Beantragung nach Änderung allgemein (Ist)

Bei **Änderungen der Wohnanschrift der Hauptwohnung** i.V.m. der Ummeldung ist die Neubeantragung und -ausstellung eines Personalausweises i. d. R. nicht erforderlich. Stattdessen wird die neue Anschrift von der zuständigen Personalausweisbehörde auf dem Personalausweis vermerkt. Zu diesem Zweck wird gegenwärtig ein Aufkleber mit der neuen Anschrift angebracht und mit einem Dienstsiegel versehen.

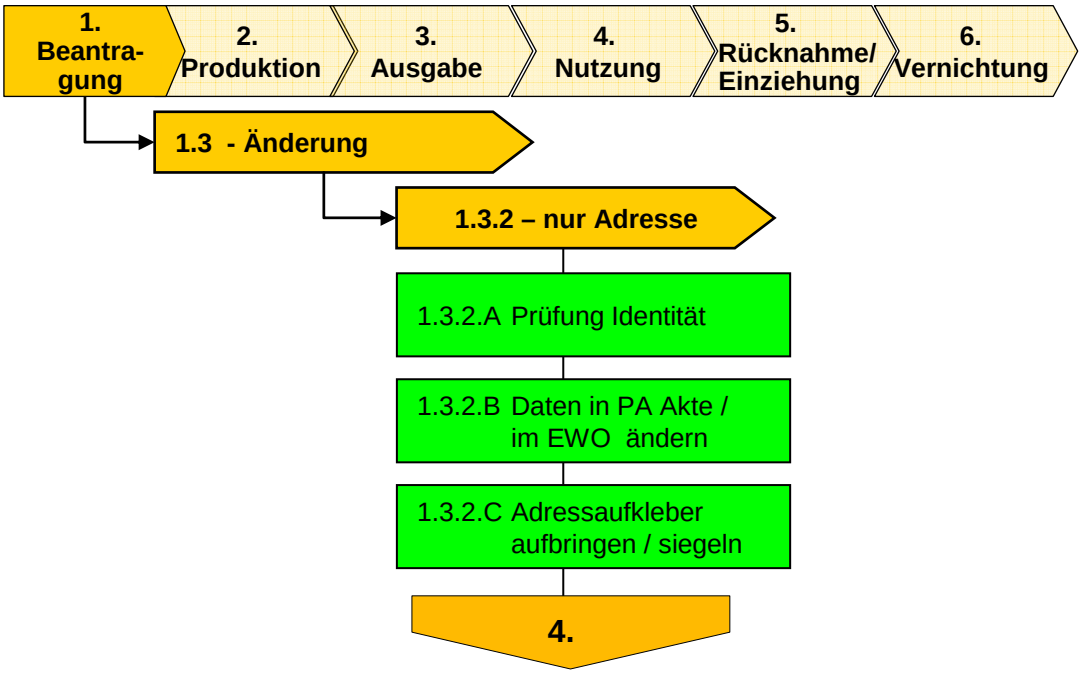

Abbildung 6: Teilprozess 1.3.2 – Beantragung nach Änderung – nur Adresse (Ist)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
1.3.2.A	Prüfung Identität	Bürgerinnen/ Bürger, PA-Behörde	Prüfung der Identität des Antragstellers und Vergleich mit Melderegisterdaten	Prüfergebnisse, Nachweise	
1.3.2.B	Daten in PA Akte/ im EWO-Verfahren ändern	PA-Behörde	Aktualisierung PA-Akte Aktualisierung PA-Daten	PA-Akte u. PA-Register aktuell	

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
1.3.2.C	Adressaufkleber aufbringen/ siegeln	PA-Behörde	Erzeugen Adressaufkleber Aufbringen und Siegeln auf dem Dokument	PA mit Aufkleber	In einigen Fällen versenden Personalausweisbehörden vollständig bedruckte Aufkleber an Antragsteller, die dann auf den Personalausweis geklebt werden.

Tabelle 4: Beschreibung TP 1.3.2 – Beantragung nach Änderung – nur Adresse (Ist)

4.3.2 Prozessepisode 2: Produktion des Personalausweises (Ist)

Die Produktion des Personalausweisdokumentes erfolgt in Deutschland zentral durch einen Hersteller (z. Zt. Bundesdruckerei GmbH). Der Herstellungsprozess wird erst nach Übermittlung einer Bestellung durch die berechtigte Stelle (Personalausweisbehörde) eingeleitet, d. h., eine Vorfertigung - z. B. unpersonalisierter Ausweisdokumente – findet nicht statt. Gemäß § 2 a Abs. 1 PersAuswG wird der Nachweis über beantragte und ausgegebene Personalausweise dezentral in der zuständigen Personalausweisbehörde in Form eines dort i. d. R. elektronisch geführten Personalausweisregisters geführt, das die personenbezogenen Daten der Personalausweisinhaber nebst digitalem Foto enthält. Dem Produzenten liegt zum Nachweis der Produktion eine Liste der Seriennummern und ein Hinweis zur ausstellenden Behörde aller produzierten Dokumente vor, ohne jedoch weitere personenbezogene Daten zu dieser Liste zu speichern. Eine zentrale Speicherung der Personalausweisdaten auf Landes- oder Bundesebene findet nicht statt.

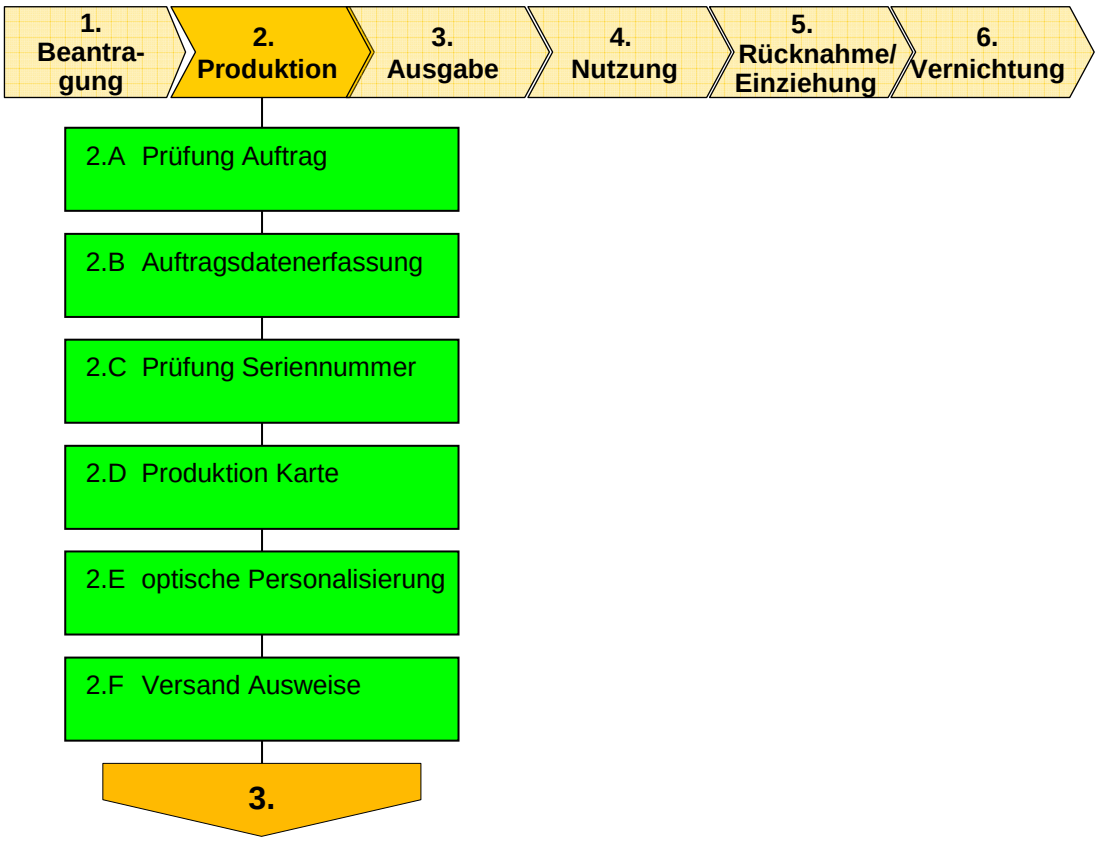

Abbildung 7: Prozessepisode 2 – Produktion des Personalausweises (Ist)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
2.A	Prüfung Auftrag	Hersteller, ggf. PA-Behörde	Prüfung des Auftrags (Bestellung von PA) auf Richtigkeit und Vollständigkeit Rücksprache zum Auftrag und ggf. Rücksendung bei Unstimmigkeiten	Auftrag geprüft	
2.B	Auftragsdatenerfassung	Hersteller	Einscannen der Papieranträge oder Qualitätsprüfung elektronisch übersandter Aufträge	Anträge elektronisch verfügbar	

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
2.C	Prüfung Seriennummer	Hersteller	Elektronische Prüfung der Richtigkeit und Eineindeutigkeit der Seriennummer	Seriennummer eineindeutig	Anträge mit nicht eineindeutiger Seriennummer werden nicht produziert und an die PA-Behörde zurückgesandt
2.D	Produktion Karte	Hersteller	Produktion des Kartenkörpers und Einbringung von Sicherheitsmerkmalen	Kartenkörper	
2.E	optische Personalisierung	Hersteller	Aufbringen der Personendaten, Lichtbild und Unterschrift sowie weiterer Sicherheitsmerkmale auf Kartenkörper	PA, produziert	
2.F	Versand Ausweise	Hersteller	Versand der Ausweise und Prüfergebnisse zu einer Bestellung an die PA-Behörde (mit Post oder Boten)	PA in PA-Behörde	

Tabelle 5: Beschreibung Prozessepisode 2 – Produktion des Personalausweises (Ist)

4.3.3 Prozessepisode 3: Ausgabe des Personalausweises an den Antragsteller (Ist)

Die von dem Ausweisproduzenten erstellten Personalausweise sind in der Personalausweisbehörde auf Richtigkeit und Vollständigkeit der Eintragungen zu prüfen und bei Mängeln ggf. erneut an den Ausweisproduzenten zu senden. Bei festgestellter Fehlerfreiheit wird der Ausweis von der Personalausweisbehörde dem jeweiligen Antragsteller persönlich oder auch einer bevollmächtigten Person nach Prüfung der Empfangsberechtigung ausgehändigt.

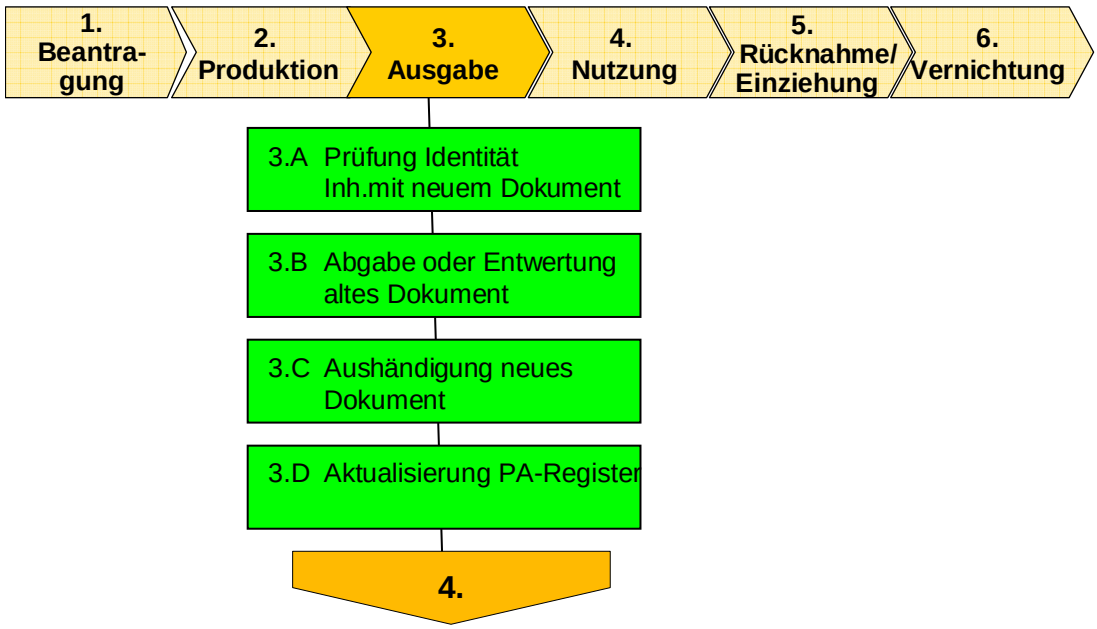

Abbildung 8: Prozessepisode 3 – Ausgabe des Personalausweises an den Antragsteller (Ist)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
3.A	Prüfung Identität Inh. mit neuem Dokument	Bürgerinnen/ Bürger, PA-Behörde	Prüfung Übereinstimmung Identitätsmerkmale des neuen Inhabers mit Dokument	Identität ist festgestellt	
3.B	Abgabe oder Entwertung altes Dokument	Bürgerinnen/ Bürger, PA-Behörde	ggf. Rückgabe altes Dokument oder Entwertung altes Dokument (bei Verbleib bei den Bürgerinnen und Bürgern)	altes Dokument eingezogen oder entwertet	
3.C	Aushändigung neues Dokument	PA-Behörde, Bürgerinnen/ Bürger	Übergabe neues Dokument an Bürgerinnen/ Bürger	neues Dokument übergeben	
3.D	Aktualisierung PA-Akte	PA-Behörde	Aktualisierung PA-Akte (Status PA)	PA-Akte aktualisiert	

Tabelle 6: Beschreibung Prozessepisode 3 – Ausgabe des Personalausweises an den Antragsteller (Ist)

4.3.4 Prozessepisode 4: Nutzung des Personalausweises (Ist)

Die Nutzung des gegenwärtigen Personalausweisdokumentes beschränkt sich im Wesentlichen auf die Verwendung als **Mittel zur Identitätsfeststellung in hoheitlichen Verfahren** (polizeiliche Personenfeststellung und Grenzkontrolle, Inanspruchnahme staatlicher Leistungen) oder als Nachweis der **Identität des Inhabers gegenüber privaten Dritten**, z. B. im Rahmen der Nutzung privatwirtschaftlicher Angebote wie bspw. einer Flugbuchung oder beim Erwerb altersbeschränkter Güter. Demzufolge sind zwei grundsätzliche, die anlassabhängige Nutzung beschreibende Teilprozesse zu unterscheiden.

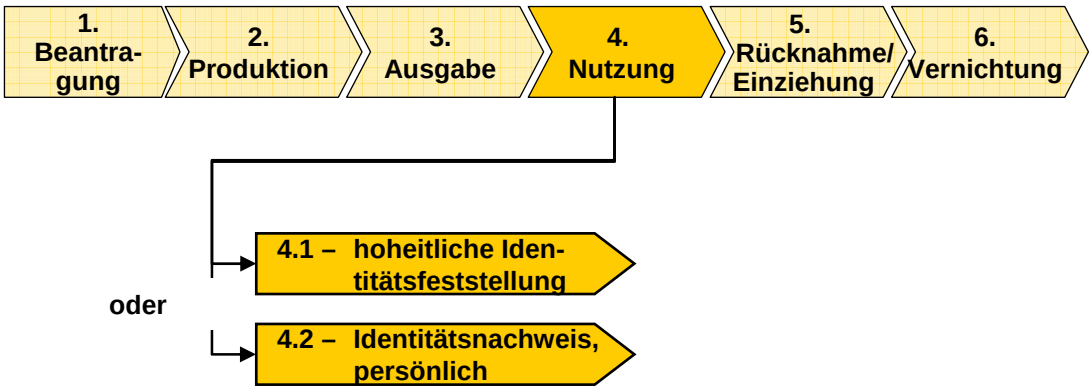

Abbildung 9: Prozessepisode 4 – Nutzung des Personalausweises (Ist)

4.3.4.1 Teilprozess 4.1: Nutzung zur hoheitlichen Identitätsfeststellung (Ist)

Auf Verlangen der zur Prüfung der Personalien berechtigten Stelle ist der Inhaber zur Vorlage des Personalausweises verpflichtet (§ 1 Abs. 1 PersAuswG). Die Identitätsprüfung erfolgt durch Inaugenscheinnahme und Vergleich der im Personaldokument beschriebenen körperlichen Merkmale (z. B. Lichtbild, Größe, Augenfarbe, Alter) mit den tatsächlichen körperlichen Merkmalen der zu identifizierenden Person. Bei Übereinstimmung können auch die übrigen Daten des Dokuments (Identitätsmerkmale) der Person zweifelsfrei zugeordnet werden. An diesen Prozessschritt kann sich eine maschinelle Überprüfung der Identitätsdaten und Sicherheitsmerkmale mit Abgleich gegen sicherheitsbehördliche Datensammlungen (z. B. Fahndung nach gestohlenen oder abhanden gekommenen Dokumenten) anschließen.

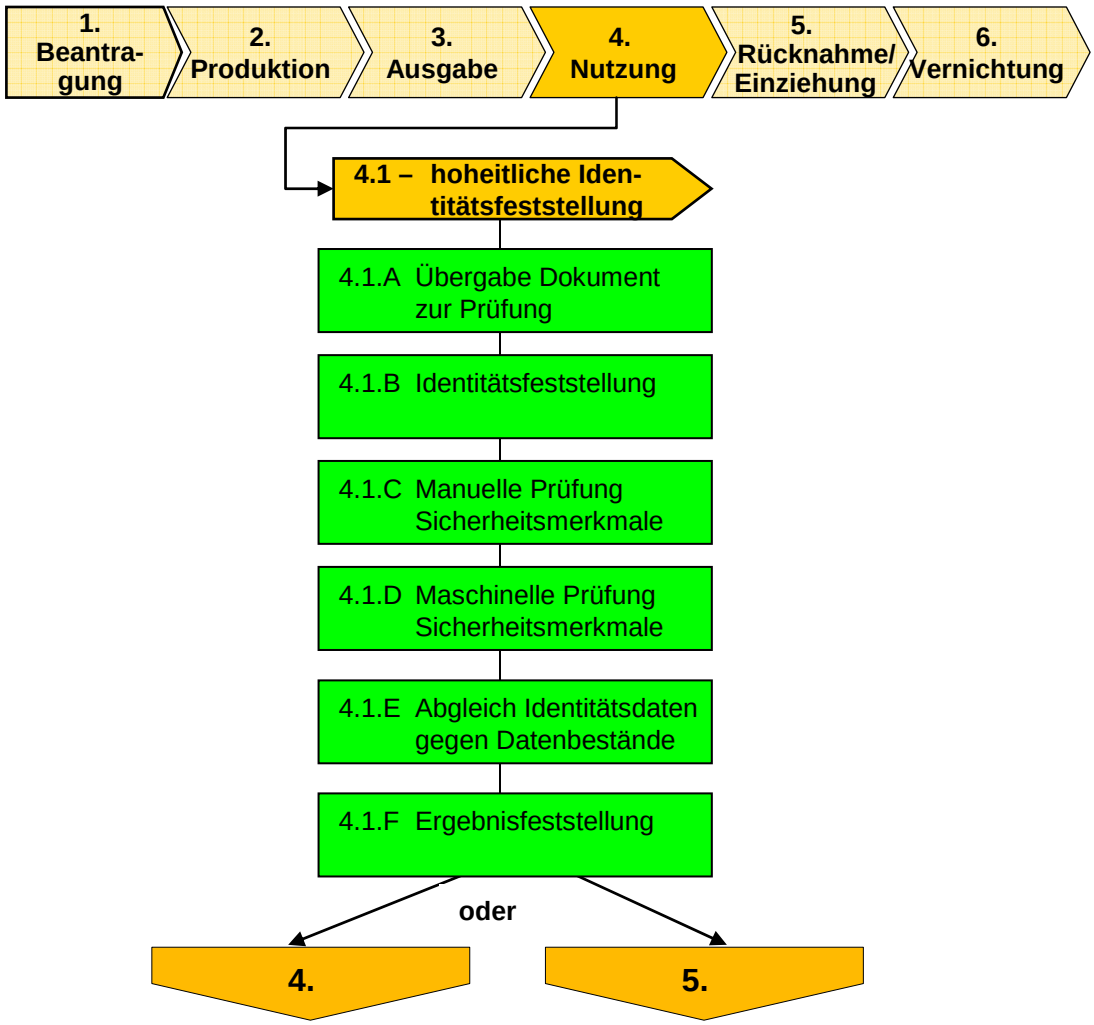

Abbildung 10: Teilprozess 4.1 – Nutzung zur hoheitlichen Identitätsfeststellung (Ist)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
4.1.A	Übergabe Dokument zur Prüfung	Bürgerinnen/ Bürger	Übergabe Dokument an Berechtigten nach Aufforderung	Dokument übergeben	
4.1.B	Identitäts-feststellung	Grenz- oder Vollzugspolizei, andere Behörde	Augenscheinliche Prüfung Lichtbild, Größe, Augenfarbe, Alter auf Übereinstimmung mit Inhaber	Identität festgestellt	
4.1.C	Manuelle Prüfung Sicherheits-merkmale	Grenz- oder Vollzugspolizei, andere Behörde	Prüfung der optisch kontrollierbaren Sicherheits-merkmale	Sicherheits-merkmale geprüft	

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
4.1.D	Maschinelle Prüfung von Sicherheitsmerkmalen	Grenz- oder Vollzugspolizei, andere Behörde	Maschinelle Prüfung von Sicherheitsmerkmalen	Sicherheitsmerkmale geprüft	
4.1.E	Abgleich Identitätsdaten gegen Datenbestände	Grenz- oder Vollzugspolizei, andere Behörde	Lesen der MRZ Abgleich der Identitätsdaten u. a. gegen INPOL-/ SIS-Personen- und Sachfahndung	Dokument oder Inhaber ausgeschrieben/ nicht ausgeschrieben	
4.1.F	Ergebnisfeststellung	Grenz- oder Vollzugspolizei, andere Behörde	Kontrolle der Ergebnisse	Identität und Dokument positiv überprüft oder weitere Untersuchungen notwendig	

Tabelle 7: Beschreibung TP 4.1 – Nutzung zur hoheitlichen Identitätsfeststellung (Ist)

4.3.4.2 Teilprozess 4.2: Nutzung zur Identifizierung und Autorisierung gegenüber privaten Dritten (Ist)

§ 4 Abs. 1 PersAuswG lässt die Verwendung des Personalausweises als Ausweis- und Legitimationspapier auch im nichtöffentlichen Bereich ausdrücklich zu. Im Unterschied zur Identifizierung in hoheitlichen Verfahren existiert aber bei der Identifizierung bzw. Autorisierung ggü. privaten Dritten wie bspw. Wirtschaftsunternehmen keine Ausweispflicht i. S. d. § 1 Abs. 1 PersAuswG; es liegt vielmehr im billigen Ermessen des Personalausweisinhabers, seine Identität dem Gegenüber – z. B. einem Händler oder Diensteanbieter - zu offenbaren. Analog zur Identitätsprüfung im Zuge der Beantragung staatlicher Leistungen stellt der Identitätsnachweis bzw. die Autorisierung aber auch hier i. d. R. das Zugangskriterium zur beanspruchten Leistung bzw. zum Erwerb der Ware dar. Wie im hoheitlichen Verfahren händigt der Personalausweisinhaber den Personalausweis dem Geschäftspartner zur Prüfung aus, damit dieser die „behauptete“ Identität des Personalausweisinhabers verifizieren kann (Authentifizierung). Für bestimmte Geschäftsvorfälle wie bspw. den Zugang zu Veranstaltungen oder die Ausleihe von Videofilmen ist dabei u. U. der Nachweis des Lebensalters hinreichend; die weiteren personenbezogenen Daten (Anschrift, Namen, ...) sind dann nicht von Bedeutung.

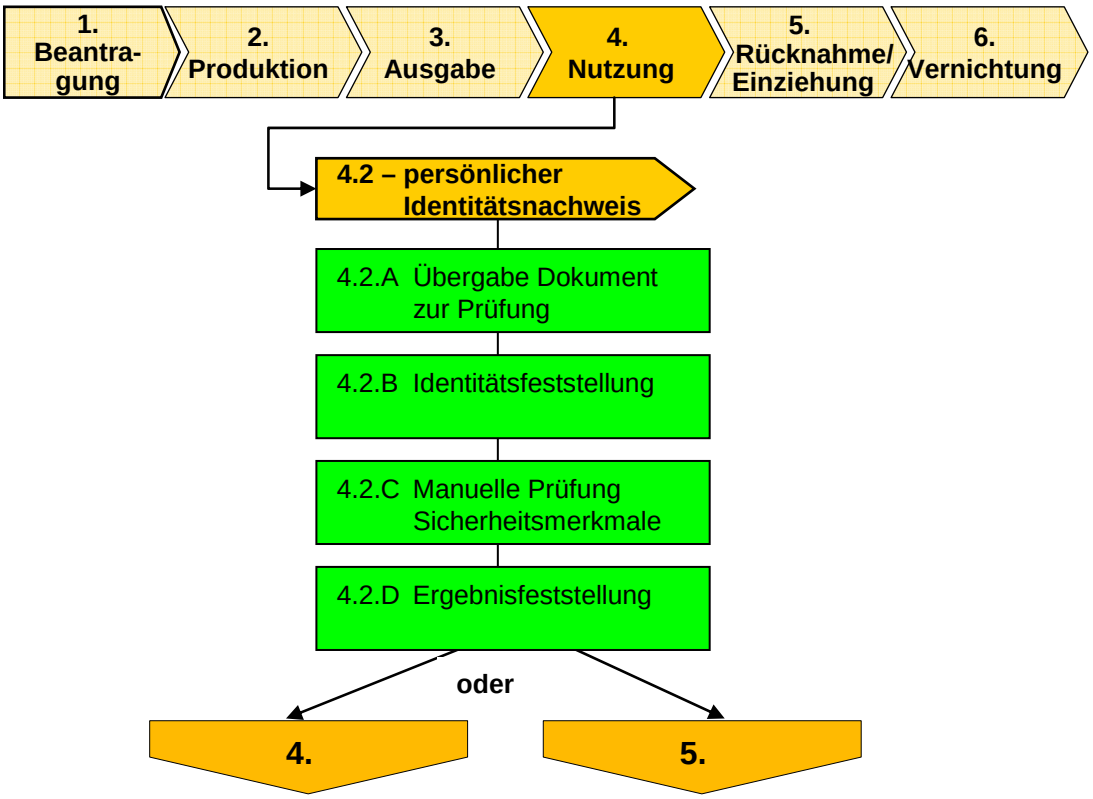

Abbildung 11: Teilprozess 4.2 – Nutzung zur Identifizierung und Autorisierung gegenüber privaten Dritten (Ist)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
4.2.A	Übergabe Dokument zur Prüfung	Bürgerinnen/ Bürger	Übergabe Dokument zur Erlangung eines Service/ zum Erwerb einer Ware	Dokument übergeben	
4.2.B	Identitäts-feststellung	Händler, Dienst-eanbieter	Augenscheinliche Prüfung Lichtbild, Größe, Augenfarbe, Alter auf Übereinstimmung mit Inhaber	Identität ist festgestellt	
4.2.C	Manuelle Prüfung Sicherheits-merkmale	Händler, Dienste-anbieter	Prüfung der optisch kontrollierbaren Sicherheits-merkmale	Sicherheits-merkmale geprüft	
4.2.D	Ergebnis-feststellung	Händler, Dienste-anbieter	Kontrolle der Ergebnisse und ggf. Übernahme notwendiger Daten für Leistungserbringung/ Verkauf bei Erkennung von Unregelmäßigkeiten erfolgt Zurückweisung oder ggf. Einschaltung der Ordnungsbehörden	Identität und Dokument positiv überprüft oder weitere Untersuchungen notwendig	

Tabelle 8: Beschreibung TP 4.2 – Nutzung zur Identifizierung und Autorisierung gegenüber

privaten Dritten (Ist)

4.3.5 Prozessepisode 5: Rücknahme / Einziehung des Personalausweises

Nach Ablauf der Gültigkeitsdauer werden Personalausweise ungültig, d. h. eine Verlängerung ist nicht möglich und es ist ein erneuter Antrag auf Ausstellung zu stellen. In diesem Fall wird der abgelaufene Personalausweis von der Personalausweisbehörde i. d. R. im Zuge der Ausgabe eines neuen Exemplars entwertet und dem Inhaber auf Wunsch überlassen oder wahlweise der Vernichtung zugeführt. Eine Ungültigkeit des Personalausweises tritt auch dann ein, wenn bspw. in Folge einer Überprüfung durch eine berechtigte Stelle Beschädigungen oder Manipulationen am Dokument festgestellt werden. Dann wird das Dokument eingezogen; bei Manipulationsversuchen sind von der zuständigen Stelle ggf. weitere strafrechtliche Maßnahmen einzuleiten.

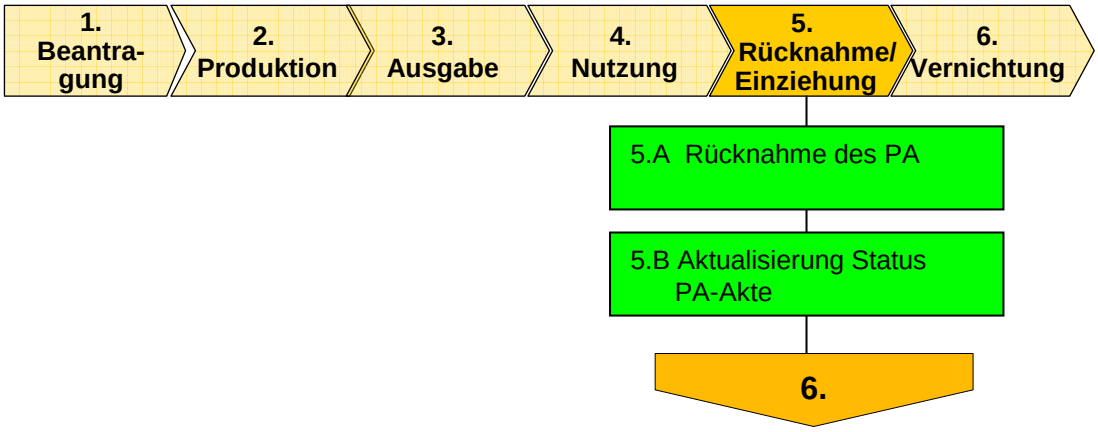

Abbildung 12: Prozessepisode 5 – Rücknahme/Einziehung des Personalausweises (Ist)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
5.A	Rücknahme des PA	PA-Behörde	Einziehen ungültiger Personalausweise zur Vernichtung oder Entwertung ungültiger Dokumente und Rückgabe an Bürgerinnen und Bürger	PA eingezogen oder entwertet	
5.B	Aktualisierung Status PA-Akte	PA-Behörde	Vermerk neuer Status in PA-Akte	Status PA-Akte aktualisiert	

Tabelle 9: Beschreibung Prozessepisode 5 – Rücknahme/Einziehung des Personalausweises (Ist)

4.3.6 Prozessepisode 6: Vernichtung des Personalausweises (Ist)

Nach Entwertung des ungültig gewordenen Ausweisdokumentes wird dieses von der Personalausweisbehörde dem Inhaber auf dessen Wunsch hin überlassen oder einbehalten. Bei Einbehaltung wird der Personalausweis der physischen Zerstörung und anschließenden fachgerechten Entsorgung durch einen autorisierten Dienstleister zugeführt.

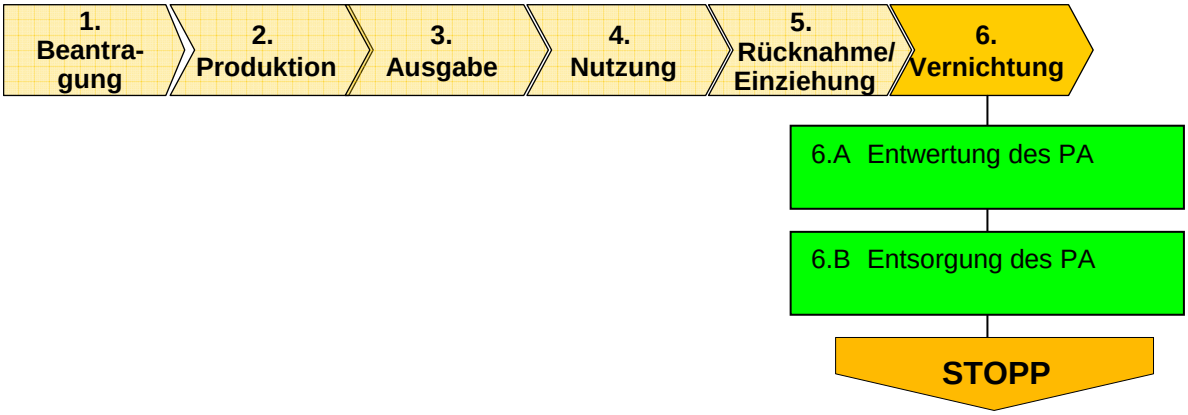

Abbildung 13: Prozessepisode 6 – Vernichtung des Personalausweises (Ist)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
6.A	Entwertung des PA	PA-Behörde	Entwertung des PA (z. B. durch Lochung, Abschneiden einer Ecke)	PA entwertet	
6.B	Entsorgung PA	PA-Behörde, Dienste-anbieter	Vernichtung durch Schredder und / oder Vernichtung erfolgt durch autorisierten Dienstean-bieter	PA vernichtet	

Tabelle 10: Beschreibung Prozessepisode 6 – Vernichtung des Personalausweises (Ist)

5 BESTEHENDE DEFIZITE UND HANDLUNGSFELDER

Mit dem derzeitigen, im Jahr 1987 eingeführten und in der Folge mit Sicherheitsmerkmalen nachgerüsteten, Personalausweis besitzt Deutschland eines der fälschungssichersten Personaldokumente der Welt. Bei näherer Betrachtung einschlägiger Anwendungsfälle des konventionellen Personalausweises im täglichen Kontakt der Bürgerinnen und Bürger mit staatlichen und privaten Stellen, werden jedoch bislang ungelöste und neu hinzutretende Probleme und Risiken deutlich. Diese ergeben sich vornehmlich in Folge sich wandelnder gesellschaftlicher Anforderungen an die Gewährleistung der Inneren Sicherheit und öffentlichen Ordnung sowie aus der zunehmenden Erschließung elektronischer Kanäle wie bspw. des Internets für die Abwicklung von Verwaltungsdienstleistungen und die Geschäftstätigkeit von Wirtschaftsunternehmen.

Im Rahmen des **Einsatzes des Personalausweises zur hoheitlichen Identifizierung** von Bürgerinnen und Bürgern durch den Staat (z. B. bei der Grenzkontrolle oder einer Polizeikontrolle im Inland) kommt es wesentlich auf einen sicheren Abgleich der Person mit den den Inhaber des Ausweises beschreibenden Merkmalen im Ausweis an. Hier musste bisher vor allem auf einen Vergleich des Lichtbildes mit der Person und die Überprüfung von Größe, Augenfarbe und - bei schriftlichen Verwaltungsverfahren - der geleisteten Unterschrift abgestellt werden. Angesichts der durchaus erheblichen Veränderung von Menschen im Laufe von 10 Jahren (Gültigkeit eines Personalausweises) ist **die zweifelsfreie Zuordnung in der Regel von Personen zu den von ihnen vorgelegten Ausweispapieren** oft erschwert. Fälschungsversuche führen aufgrund des hohen deutschen Sicherheitsstandards nicht zum Erfolg. Allerdings besteht die Gefahr, dass in einem nicht hinnehmbaren Umfang gestohlene oder verloren gegangene echte Dokumente von ähnlich aussehenden Personen verwendet werden. Dokumentenmissbräuche machen in der Kriminalitätsstatistik einen erheblich größeren Anteil als Dokumentenfälschungen aus. Während bei einer konventionellen – rein optischen – Kontrolle des Gesichtsbildes und der Person die Gefahr der Täuschung eines Kontrollbeamten besteht, können dagegen bei einer maschinellen biometriegestützten Kontrolle eindeutige Gesichts- bzw. Fingerabdruck-Daten anhand geeigneter Parameter geprüft werden, womit ein Dokumentenmissbrauch ausgeschlossen werden kann. Mit dieser Differenzierung in Dokumentenfälschung und -missbrauch müssen auch Statistiken interpretiert werden. Während Total- und Verfälschungen deutscher Dokumente aufgrund des hohen Sicherheitsniveaus i. d. R. schnell entdeckt werden, ist die Dunkelziffer für die Dokumentenmissbrauch und Täuschung naturgemäß hoch. Untersuchungen der Bundespolizei und aus

dem benachbarten europäischen Ausland ergeben erhebliche Anteile (zwischen 10% und 70% je nach Stichprobe und Ort) des Dokumentenmissbrauchs am Gesamtaufkommen urkundenbezogener Delikte. Wie hoch das Sicherheitsrisiko ohne biometrieunterstützte Kontrollen ausfällt, wird noch deutlicher, wenn man die Zahlen verloren bzw. gestohlen gemeldeter Dokumente heranzieht: Im INPOL-Gesamtbestand sind in Deutschland aktuell ca. 10,6 Millionen Gegenstände ausgeschrieben – darunter ca. 3,5 Millionen ausgestellte Dokumente, davon 2,26 Millionen Bundespersonalausweise. Praktisch bedeutet dies: Potentiell 2,26 Millionen deutsche Bürgerinnen und Bürger leben mit dem Risiko, dass mit ihrem Ausweis, d.h. ihrer Identität, Straftaten versucht werden. Was den Straftatbestand der unerlaubten Einreise anbelangt, haben Pass- und Ausweisdokumente ein vergleichbares Risikopotential, denn deutsche Personalausweise gelten als Passersatz und berechtigen damit nicht nur zur Reise in Länder wie Ägypten und Tunesien, sondern grundsätzlich zur Rückkehr in den Schengenraum. Bei statistischer Einbeziehung des gemeinsamen Schengenraumes erhöht sich die materielle Grundlage für Dokumentenmissbrauch erheblich: Im Schengener Informationssystem sind aktuell 21,7 Millionen Gegenstände zur Fahndung ausgeschrieben – darunter ca. 17,8 Millionen Personaldokumente.

Daher ist die Aufnahme biometrischer Merkmale in elektronischer Form im Personalausweis von wesentlicher Bedeutung, insbesondere zur stärkeren Bindung der Ausweisinhaber an das Dokument. Die Bürgerinnen und Bürger haben es damit in der Hand, sich durch die freiwillige Aufnahme ihrer Fingerabdrücke in den Personalausweis vor diesem Risiko zu schützen. Eine missbräuchliche Nutzung eines elektronischen Personalausweises mit gespeicherten Fingerabdrücken kann mit an Sicherheit grenzender Wahrscheinlichkeit aufgedeckt werden.

Im Rahmen der Verwaltungsmodernisierung und des Abbaus bürokratischer Hemmnisse bemühen sich viele Staaten in Europa um die **Umsetzung von Verwaltungsverfahren für die elektronische Welt (E-Government)**. Dies bietet sowohl den Bürgerinnen und Bürgern sowie der Wirtschaft Vorteile in Form größerer Flexibilität, Verfügbarkeit und Bequemlichkeit von Verwaltungsdienstleistungen als auch der Verwaltung die Möglichkeit zu schnelleren Verfahren mit geringeren Kosten. Grundlage für die Nutzung solcher Vorteile im E-Government ist allerdings die Möglichkeit einer hinreichenden elektronischen Authentisierung von Bürgerinnen und Bürgern, da Verwaltungsleistungen typischerweise nur für eindeutig bestimmte Personen erbracht werden dürfen und sollen. **Eine solche einheitliche Möglichkeit des Identitätsnachweises, wie sie der Personalausweis in der realen Welt bietet, fehlt bisher in der elektronischen Welt**. Dieser Problematik kann dadurch begegnet

werden, dass es den Bürgerinnen und Bürgern künftig möglich wird, sich in bewusster Entscheidung gegenüber Dritten, die sich zuvor selbst identifizieren müssen, zu authentisieren und für den Geschäftvorgang erforderliche verifizierbare personenbezogene Daten zu übermitteln.

Immer häufiger sind unbefugte Eingriffe Dritter in die elektronische Kommunikation zwischen den Anbietern von Online-Dienstleistungen und den Nutzern zu beobachten, in deren Folge die Betroffenen nicht selten wirtschaftliche Schäden erleiden. Immer wieder auftretende **IT-Sicherheitsprobleme im Internet** lassen echtes Vertrauen in online abgewickelte Transaktionen und in die potentiellen Partner – wenn überhaupt – nur langsam entstehen. Vertrauen in den Partner ist zugleich aber wesentliche Voraussetzung für den Willen zur Durchführung von Geschäften und damit das Wachstum des gesamten Marktes. Fehlende Mechanismen zur gegenseitigen Authentifizierung in der Online-Welt haben daher auch nachhaltige Folgen für die Wirtschaft. Umso dringender bedarf es der Einführung eines sicheren, vertrauenswürdigen Nachweises der Identität der Kommunikationspartner, der die aufgrund bisher **unzureichender Authentifizierungsmöglichkeiten** bestehenden Unsicherheiten bei Bürgerinnen und Bürgern mit privatwirtschaftlichen Anbietern im Internet zuverlässig beseitigt.

Darüber hinaus ist für bestimmte Transaktionen nicht nur die verlässliche Angabe von personenbezogenen Daten, sondern auch der verifizierbare **Akt einer bewussten Willenserklärung** erforderlich. In der realen Welt geschieht dies i. d. R. durch die eigenhändige Unterschrift. Da diese Möglichkeit in der elektronischen Welt in der Vergangenheit so nicht bestand, wurde als Pendant zur eigenhändigen Unterschrift die qualifizierte elektronische Signatur geschaffen, um auch online Rechtsverbindlichkeit herstellen zu können. Aufgrund der für eine alltägliche Nutzung sehr komplexen und schwerfälligen Umsetzung hat sich dieses Verfahren bislang jedoch noch nicht durchsetzen können. Um den Bürgerinnen und Bürgern ein möglichst praktisches und bequemes Verfahren bieten zu können, bedarf es der Bündelung der wichtigsten Online-Handlungsmöglichkeiten in einem einzigen Dokument.

6 EINSATZ ELEKTRONISCHER PERSONALAUSWEISE IN ANDEREN LÄNDERN

Das Kapitel gibt anhand einiger Beispiele europäischer Länder und der Sonderverwaltungsregion Hongkong der Volksrepublik China einen Überblick über unterschiedliche Gestaltungsformen elektronischer Personalausweisdokumente bzw. „ID-Cards“. Die Beispiele liefern erste Anhaltspunkte für die zu bestimmende Form und funktionale Ausstattung des zukünftigen deutschen elektronischen Personalausweises und lassen zugleich Rückschlüsse zu auf bewährte bzw. weniger bewährte Umsetzungsmodelle.

Belgien

In Belgien wurde mit dem Test neuer elektronischer Personalausweise im Jahr 2002 in 11 Testregionen begonnen. Ab April 2005 wurde der elektronische Personalausweis (Electronic Identity Card: eID) flächendeckend eingeführt, so dass Belgien auf diesem Feld eine Führungsrolle in Europa einnimmt. Bis zum Jahr 2009 soll jeder Belgier einen elektronischen Personalausweis besitzen.

Der neue Ausweis ist scheckkartengroß (sog. „ID1-Format“) und enthält einen kontaktbehafteten Chip (Chip mit Kontaktinterface) mit darauf gespeicherten personenbezogenen Daten. Die Wohnanschrift ist nur elektronisch gespeichert. Er hat eine Gültigkeitsdauer von fünf Jahren und wird zu einem Preis von EUR 10,00 zuzüglich einer gemeindeabhängigen Steuer abgegeben.

Abbildung 14: Personalausweis Belgien

Der Ausweis kann optional mit Zertifikaten zur Authentisierung und einer elektronischen Signaturfunktion ausgestattet werden. Er enthält keine automatisiert zu verarbeitenden biometrischen Merkmale und keinen Zugriffschutz für die auf dem Chip gespeicherten Daten. Diese sind folglich für jedes Lesegerät aus dem behördlichen wie privaten Bereich zugänglich.

Niederlande

Den niederländischen Personalausweis als Kunststoffkarte im ID1-Format gibt es bereits seit dem Jahr 2001. Seit August 2006 besitzt er – wie auch der elektronische Reisepass - einen kontaktlosen Speicherchip, in dem die Personendaten, das Gesichtsbild und eine persönliche Identifikationsnummer (die niederländische Steuer- und Sozialversicherungsnummer) gespeichert werden. Die Wohnanschrift befindet sich weder auf dem Dokument noch im Chip. Die Nutzung der im Chip gespeicherten Daten für E-Government-Anwendungen hat 2007 begonnen. Zertifikate für die elektronische Authentisierung und elektronische Signatur werden nicht gespeichert.

Der Personalausweis hat eine Gültigkeit von fünf Jahren und kostet etwa EUR 31,00.

Abbildung 15: Personalausweis Niederlande

Estland

Estland hat den elektronischen Personalausweis ab Januar 2002 eingeführt. Er ist ebenfalls scheckkartengroß (ID1-Format) und enthält einen kontaktbehafteten Chip. Der Personalausweis besitzt eine Gültigkeit von 10 Jahren und wird für eine Verwaltungsgebühr von EUR 10,00 an die Bürgerinnen und Bürger abgegeben.

Anders als in Deutschland, wo eine Personalausweispflicht nur dann besteht, wenn kein gültiger Reisepass vorhanden ist, gilt in Estland eine allgemeine Pflicht zum Besitz eines Personalausweises. Alle personenbezogenen Daten, die in optisch lesbarer Form auf der Ausweiskarte aufgebracht sind, werden zusätzlich - bis auf das Foto und die Unterschrift – in einem kontaktbehafteten Chip gespeichert. Ein besonderer Zugriffsschutz zu diesen Daten besteht auch hier nicht.

Die Wohnanschrift ist nicht Bestandteil der auf dem Ausweis aufgedruckten Personendaten

und wird auch nicht gespeichert. Eine zusätzliche elektronische Speicherung biometrischer Merkmale (Gesichtsbild, Fingerabdrücke o. ä.) findet bisher nicht statt.

Abbildung 16: Personalausweis Estland

Neben diesen Daten werden elektronische Zertifikate für elektronische Authentisierung und Signatur im kontaktbehafteten Chip gespeichert. Diese Anwendungen sind durch eine nur dem Inhaber bekannte PIN[4] vor missbräuchlicher Verwendung gesichert. Eine Besonderheit stellt die für E-Government -Zwecke dem Inhaber von staatlicher Seite zugewiesene, lebenslang gültige, im Authentisierungszertifikat enthaltene E-Mail-Adresse dar.

Die elektronischen Funktionen des Personalausweises können im Bereich E-Government und eingeschränkt auch im E-Business genutzt werden. Für die rechtsverbindliche elektronische Kommunikation mit staatlichen Stellen ist die Verwendung der elektronischen Signatur verpflichtend.

Italien

Der italienische elektronische Personalausweis wird im Scheckkartenformat (ID1) herausgegeben. Bei der Ausgabe durch die zuständige Stelle sind EUR 25,00 Verwaltungsgebühr zu entrichten. Ab Ausstelldatum ist er fünf Jahre gültig.

Der Ausweis enthält einen kontaktbehafteten Chip und als zusätzliches Speichermedium einen sog. Laserstreifen (optischer Speicher) auf der Rückseite der Karte.

[4] PIN = persönliche Identifikationsnummer („Geheimzahl“) zur Authentisierung ggü. einer Maschine und Freigabe geschützter Informationen.

Abbildung 17: Personalausweis Italien

Die Daten, die im Chip und im Laserstreifen gespeichert werden, sind identisch. Die Wohnanschrift des Inhabers wird nicht gespeichert, lediglich die Anschrift der zuständigen Einwohnerbehörde wird auf der Rückseite der Karte vermerkt. Als biometrische Daten werden Gesichtsbild und Fingerabdrücke verschlüsselt (als sog. Templates, beides nicht ICAO-konform) gespeichert. Die weiteren elektronisch gespeicherten Daten unterliegen keinem gesonderten Zugriffsschutz, sind daher mit jedem kompatiblen Lesegerät aus dem behördlichen wie privaten Bereich zugänglich und können sowohl für geschäftliche Transaktionen im E-Government als auch E-Business genutzt werden.

Zusätzlich enthält der Speicherchip ein Zertifikat für die elektronische Authentisierung und elektronische Signatur. Diese Funktion ist wie beim estnischen Ausweis mit einer PIN gesichert.

Spanien

Spanien führt ein nationales Register aller Personalausweisinhaber, in dem zu jeder Person die im elektronischen Personalausweis (eDNI) vorhandenen biometrischen Informationen (Gesichtsbild, Fingerabdrücke) gespeichert sind.

Der spanische Personalausweis selbst ist im ID1-Format gestaltet und besitzt einen kontaktbehafteten Speicherchip. Er wird für eine Gebühr von rd. EUR 7,00 an die Bürgerinnen und Bürger ausgegeben und hat eine Gültigkeit von fünf Jahren. Im Chip werden neben den Biometriedaten (Gesichtsbild, Fingerabdruck-Templates) personenbezogene Daten sowie das Zertifikat für die qualifizierte elektronische Signatur gespeichert. Die Konformität mit den einschlägigen Richtlinien der ICAO ist erst für die zukünftige Ausweisgeneration geplant. Die Wohnanschrift des Inhabers wird weder auf der Karte noch im Chip vermerkt.

Schweden

Der in Schweden seit dem Jahr 2005 ausgegebene elektronische Personalausweis ist scheckkartengroß (ID1-Format). Er ist ab Ausstellung fünf Jahre gültig und kostet rd. EUR 42,00. Im Unterschied zu den Ausweisen Belgiens, Italiens und Estlands enthält der Ausweis sowohl einen kontaktbehafteten als auch einen kontaktlosen Chip.

Abbildung 18: Personalausweis Schweden

Die Wohnanschrift wird auch in Schweden auf dem Personalausweis nicht gespeichert. Auf dem kontaktlosen Chip befindet sich als biometrisches Merkmal das Gesichtsbild des Inhabers in einem ICAO-konformen Speicherformat. Als Zugriffsschutz dient die sog. „Basic Access Control“ (BAC), die als Authentifizierungsverfahren den verschlüsselten Datenaustausch zwischen einem Inspektionssystem (Kartenlesegerät) und dem elektronischen Personalausweis sicherstellt.

Der kontaktbehaftete Chip ist bei der Ausgabe des Ausweises vorbereitet für die Verwendung in E-Government- und E-Business-Transaktionen, enthält jedoch zunächst noch keine Zertifikate. Diese müssen vom Inhaber in eigener Verantwortung nachgeladen werden.

Hongkong

Die Sonderverwaltungsregion Hongkong hat den elektronischen Personalausweis im Jahr 2003 eingeführt. Dieser hat Scheckartenformat (ID1) und besitzt einen kontaktbehafteten Chip. Die Karte ist bei Erstausgabe kostenlos und unbefristet gültig. Bei Ersatz nach Verlust wird eine Gebühr von umgerechnet etwa EUR 40,00 erhoben.

Neben personenbezogenen Daten wie Name, Geburtsdatum etc. werden auf dem Chip das Gesichtsbild und die Abdrücke beider Daumen als biometrische Daten gespeichert. Die Speicherung erfolgt wie beim italienischen Personalausweis in Form von Templates. Ein be-

sonderer Zugriffsschutz für die gespeicherten Daten besteht nicht.

Abbildung 19: Personalausweis Hongkong

Eine Besonderheit des Ausweises besteht darin, dass er eine eindeutige Personenkennzahl enthält, die dem Inhaber lebenslang zugeordnet ist. Eine Speicherung der Wohnanschrift des Inhabers auf dem Personalausweis findet nicht statt; diese wird in einem zentralen Adressregister gesondert geführt. Änderungen der Wohnanschrift müssen der für die Speicherung zuständigen Behörde gemeldet werden.

Als Kopierschutz besitzt jeder Chip eine eindeutige ID-Nummer, die in die gespeicherte PKI (Public Key Infrastruktur) eingebunden ist. Auf Wunsch des Inhabers können Signaturzertifikate integriert werden, die für die ersten zwei Jahre kostenfrei sind.

Formen und Ausstattungsmerkmale in der Übersicht

Nachfolgende Tabelle fasst die wesentlichen Ausstattungsmerkmale der vorgestellten elektronischen Personalausweise übersichtsartig zusammen.

Merkmal	Land						
	Belgien	Estland	Italien	Schweden	Hongkong	Spanien	Niederlande
Kosten f. Bürger (EUR)	10	10	25	42	keine (40 für Ersatzdokument)	7	31
Gültigkeit	5 Jahre	10 Jahre	5 Jahre	5 Jahre	unbefristet	10 Jahre	5 Jahre
Chip/ Interface	Kontaktchip	Kontaktchip	Kontaktchip und Laserstreifen	Kontaktchip und kontaktloser Chip	Kontaktchip	Kontaktchip	Kontaktloser Chip
Biometrie	nein	nein	ja (Gesichtsbild und Fingerabdrücke)	ja (Gesichtsbild)	ja (Gesichtsbild und Daumen)	ja (Gesichtsbild und Fingerabdruck-Templates)	ja (Gesichtsbild)
Zertifikate	Authentisierung/ elektron. Signatur	Authentisierung/ elektron. Signatur	Authentisierung/ elektron. Signatur	nein	Authentisierung/ elektron. Signatur	Authentisierung/ elektron. Signatur	nein
Zugriffsschutz für Biometrie- und Personendaten	kein	kein	kein	BAC	kein	kein	BAC
Speicherung Wohnanschrift	nur im Chip gespeichert	nein	nein	nein	nein	nein	nein

Tabelle 11: Merkmale der elektronischen Personalausweise anderer Länder

Aus dem Vergleich der verschiedenen landestypischen Lösungen lassen sich wichtige Erkenntnisse über die der spezifischen Umsetzung jeweils zugrunde liegenden Bedarfe und funktionalen Anforderungen gewinnen und gleichzeitig Rückschlüsse für die Ausgestaltung eines für Deutschland geeigneten Lösungsansatzes ziehen.

- Deutschland spielt mit der Einführung einer elektronischen Ausweiskarte keine Vorreiterrolle (Belgien hat diese z. B. schon 2002 eingeführt).

- Bis auf den niederländischen Personalausweis besitzen alle in den Beispielen beschriebenen Ausweise einen kontaktbehafteten Chip und sind im ID1-Format (Scheckkartenformat) realisiert. Dies entspricht den Anforderungen der bisher vorherrschenden Infrastruktur (Lesegeräte und Signaturverfahren).
- Schweden hat seit Oktober 2005 parallel mit dem elektronischen Pass auch in den elektronischen Personalausweis einen kontaktlosen Chip eingebunden. Die Niederlande sind Vorreiter bei der Implementierung eines ausschließlich kontaktlosen Interfaces in Analogie zum elektronischen Pass.
- Biometrische Merkmale werden bereits gespeichert, auch wenn diese nur im Beispiel Schweden und Niederlande der ICAO-Norm entsprechen (analog zu den ICAO-konformen elektronischen Reisepässen mit einer Basic Access Control versehen).
- Für die Authentisierung werden in allen Fällen Zertifikate von Public Key Infrastrukturen genutzt (in Schweden können diese nachgeladen werden).
- Als Zugriffsschutz auf im Chip gespeicherte Personendaten (die auch visuell auf der Karte sichtbar sind, Ausnahme: Foto und Signatur) wurde teilweise die Basic Access Control (BAC) vorgesehen. Weitergehende Schutzmechanismen bestehen nicht. Diese Daten sind mittels einschlägiger Lesevorrichtungen auslesbar. PKI-Funktionen werden in der Regel durch eine PIN geschützt.
- Die Nutzung eines kontaktbehafteten Chips limitiert die Nutzungs- und damit auch Gültigkeitsdauer im Regelfall auf fünf Jahre.
- Angaben zur Wohnanschrift sind auf keiner der Karten optisch sichtbar aufgebracht, in Belgien jedoch im Chip gespeichert.

7 SCHLUSSFOLGERUNGEN

Die Betrachtungen zum bisherigen, „konventionellen“ deutschen Personalausweis haben gezeigt, dass dieser sich – abgesehen von den in Kap. 4 beschriebenen Schwachstellen – im Grundsatz für die bisherigen Verwendungszwecke in der Praxis ausgezeichnet bewährt hat. Insbesondere in den Bereichen der polizeilichen Personenkontrolle im Inland, der Grenzkontrolle, der Identifizierung im privatwirtschaftlichen Umfeld bei Geschäften von Angesicht zu Angesicht sowie hinsichtlich seiner Fälschungssicherheit kann auf jahrelange positive Erfahrungen mit dem bisherigen Personalausweis zurückgeblickt werden. Diese positiven Erfahrungen müssen bei einer Neukonzeption des Personalausweises Berücksichtigung finden, um eine bedarfsgerechte funktionale Auslegung auch des zukünftigen Dokumentes sicherzustellen.

Im Interesse einer ausgewogenen und zukunftsorientierten Lösung müssen aber auch die bereits erkannten Optimierungsbedarfe, insbesondere bei der Identifizierung in hoheitlichen Verfahren bzw. der Bindung des Ausweisdokumentes an den Inhaber, sowie neu hinzugekommene Bedarfe, die sich aus der zunehmenden Elektronifizierung des Geschäftsverkehrs mit Behörden und Privatwirtschaft herleiten, bei der technischen Ausgestaltung des **zukünftigen „elektronischen“ Personalausweises** angemessen berücksichtigt werden:

- **Verbesserung der Zuverlässigkeit der Identifizierung in hoheitlichen Verfahren**
  In Ergänzung zum konventionell aufgebrachten Foto sollen elektronisch gespeicherte biometrische Merkmale im künftigen elektronischen Personalausweis aufgrund ihrer Maschinenlesbarkeit zu einer höheren Sicherheit der Identifizierung der überprüften Person und ihrer Zuordnung zu dem vorgelegten Personaldokument beitragen. Aus diesem Grund würde die Ausstattung des zukünftigen Personalausweises mit maschinenlesbaren biometrischen Merkmalen (Speicherung des Gesichtsbildes und freiwillig der Fingerabdrücke in einem Chip) zu einer Stärkung des Gesamtsystems der Identifizierung von Personen beitragen. Sie ergänzt damit das hohe Niveau der Fälschungssicherheit des Dokumentes selbst; u. a. auch durch die Verwendung elektronischer Signaturen als zusätzliches Sicherheitselement gegen Fälschungen und Verfälschungen.
- **Erhöhung der Transaktionssicherheit im elektronischen Geschäfts- bzw. Rechtsverkehr (E-Government / E-Business)**
  Der Bereich der elektronischen Geschäftsprozesse gewinnt immer weiter an Bedeutung, und den Bedürfnissen für eine sichere und datenschutzfreundliche elektroni-

sche Identifizierungslösung muss Rechnung getragen werden. Diesem Bedürfnis wird der elektronische Personalausweis gerecht, indem er es auf Basis des elektronischen Identitätsnachweises den Bürgerinnen und Bürgern ermöglicht, sich in bewusster Entscheidung gegenüber Dritten, die sich zuvor selbst identifizieren mussten, elektronisch zu authentisieren und für den Geschäftsvorgang erforderliche verifizierte personenbezogene Daten zu übermitteln. Dies versetzt die Bürgerinnen und Bürger in die Lage, Dienstleistungen der Verwaltung oder der Wirtschaft rund um die Uhr online abwickeln und so den Anforderungen einer immer mobileren und flexibleren Welt gerecht werden zu können. Die Steuerbarkeit der Preisgabe personenbezogener Informationen durch die Bürgerinnen und Bürger selbst und die Zuverlässigkeit der mittels elektronischem Personalausweis verifizierten Daten wird zu mehr Vertrauen in Online-Transaktionen auf beiden Seiten beitragen und so Unternehmen und Verbraucherinnen und Verbrauchern gleichermaßen Vorteile bringen. Zusätzlich soll der elektronische Personalausweis die Möglichkeit der Integration einer qualifizierten elektronischen Signatur bieten. Da elektronischer Identitätsnachweis und qualifizierte elektronische Signatur nicht zu jeder Zeit für jedermann erforderlich sind, soll die Entscheidung über die Integration und damit Nutzung dieser beiden Funktionen bei jedem Einzelnen liegen.

In einigen Ländern liegen bereits einschlägige Erfahrungen mit der Ausgestaltung und Anwendung elektronischer Identitätskarten (Personalausweise) vor. Die dort umgesetzten Lösungen adressieren die vorstehend beschriebenen Defizite und Handlungsfelder zumindest teilweise. So ist u. a. festzuhalten, dass in den meisten Ländern, in denen in den letzten Jahren neue Personalausweise ausgegeben wurden, diese auch für den Bereich der elektronischen Identifizierung vorgesehen sind. Wie die in Kap. 6 genannten Beispiele zeigen, wird zur Realisierung der elektronischen Identitätsfunktion jeweils mindestens ein Chip in die Ausweiskarte, die im Scheckkartenformat realisiert wird, integriert. Je nach Karte sind dabei Authentisierungs- bzw. Signaturzertifikate im Chip gespeichert, die z. B. für E-Government- oder E-Business-Zwecke ausgelesen werden können. Insbesondere in jenen Ländern, in denen Authentisierungszertifikate bzw. Signaturzertifikate standardmäßig in den Personalausweis integriert sind, ist eine gesteigerte Nutzung der darauf basierenden Identifizierungsfunktionen mit dem Personalausweis zu beobachten (z. B. Belgien). Werden die entsprechenden Funktionen hingegen nur auf ausdrücklichen Wunsch nachgerüstet, so ist eine geringere Nutzung der elektronischen Identifizierungsfunktionen zu beobachten (z. B. Hongkong).

Darüber hinaus zeigt sich bei aktuellen Karten (z. B. in Schweden), dass hier sowohl biometrische Merkmale kompatibel zu den ICAO-Standards gespeichert werden, als auch elektronische Identifizierungsdaten von der Karte abrufbar sind.

Aus den vorgenannten Erfahrungen mit neuen Identitätskarten anderer Länder ergeben sich folgende, für die Ausgestaltung eines elektronischen Personalausweises in Deutschland wesentliche Schlussfolgerungen:

1. **Die Aufnahme elektronischer biometrischer Merkmale ist sinnvoll und notwendig, insbesondere dann, wenn die Daten in einem Format gespeichert werden, das internationalen Standards genügt (ICAO).**
2. **Der elektronische Identitätsnachweis für elektronische Geschäftsprozesse soll standardmäßig für den elektronischen Personalausweis angeboten werden.**
3. **Die Aufnahme der qualifizierten elektronischen Signatur sollte als Option für rechtsverbindliche Online-Transaktionen vorgesehen werden.**

Diese Überlegungen und Schlussfolgerungen sind maßgeblich für die Formulierung der Ziele, die mit der Einführung eines elektronischen Personalausweises verfolgt werden, um letztlich die vorgenannten Handlungsfelder „Optimierung der Identifizierung in hoheitlichen Verfahren“, „Erhöhung der Sicherheit und Zuverlässigkeit bei der Nutzung von E-Government und E-Business“ und „Gewährleistung der Rechtsverbindlichkeit von Online-Transaktionen“ geeignet adressieren zu können.

Strategisches Ziel ist die weitere Verbesserung der bisherigen Funktionen und Eigenschaften des bestehenden Personalausweises bei gleichzeitiger Erschließung neuer Möglichkeiten des sicheren und für alle Beteiligten zuverlässigen Identitätsnachweises insbesondere in der Online-Welt, und die Schaffung eines größtmöglichen Nutzens für Bürgerinnen und Bürger, Wirtschaft und Verwaltung gleichermaßen.

8 EINFÜHRUNG DES ELEKTRONISCHEN PERSONALAUSWEISES

Aus der vorangehenden Analyse der Defizite beim Einsatz des aktuellen Personalausweises und der aufgezeigten Handlungsfelder (Kap. 5) sowie der aus den Beispielen anderer Länder gewonnenen Erkenntnisse hinsichtlich Zweckbindung und Ausgestaltung elektronischer Identitätsdokumente (Kap. 6) lassen sich nunmehr konkrete strategische Ziele für die Einführung eines elektronischen Personalausweises in Deutschland ableiten. Diese sollen zugleich als Leitlinien für die bedarfsgerechte Ausgestaltung des neuen Identitätsdokumentes entlang konkreter Anwendungsfälle des elektronischen Personalausweises sowohl im hoheitlichen wie auch privatwirtschaftlichen Kontext dienen.

Übergeordnete Aufgabe wird die weitere Modernisierung und Optimierung des bisherigen „konventionellen“ Personalausweises durch Überführung in einen sicheren, zukunftsfähigen, für eine Vielzahl von Anwendungen geeigneten und für die Inhaber komfortabel zu handhabenden Identitätsnachweis sein.

8.1 Zielformulierung

Mit der Einführung des elektronischen Personalausweises werden folgende primäre Ziele verfolgt:

- **Erhalt des bestehenden hohen Sicherheitsstandards des Dokuments**
  Unter Beibehaltung wesentlicher, bewährter Sicherheitsmerkmale des aktuell in Umlauf befindlichen Personalausweises soll auch weiterhin eine maximale Sicherheit gegen Manipulationen erreicht werden. Insbesondere sollen Total- und Verfälschungen des Dokuments soweit erschwert werden, dass diese – auch unter Einsatz moderner Technologien - nur mit kaum vertretbarem logistischen, technischen und finanziellen Aufwand vorgenommen werden könnten.
- **Vermeidung von Missbrauch echter Personalausweise i.V.m. Verbesserung der Sicherheit des Personalausweises als Reisedokument im Schengen-Raum und weiteren Staaten durch zusätzliche elektronische Funktionen**
  Eine stärkere Bindung des Dokuments an den Inhaber soll durch die Aufnahme biometrischer Merkmale in elektronischer Form (Fingerabdrücke auf Antrag und Gesichtsbild) geschaffen werden. Damit kann ein Missbrauch echter Personalausweise durch ähnlich aussehende Personen vermieden werden. Darüber hinaus findet eine Verbesserung der Fälschungssicherheit durch die Verwendung kryptographischer Mechanismen statt. Mangels entsprechender Vorgaben gibt es keine verpflichten-

den Mindestsicherheitsstandards und keine Verpflichtung zur Integration biometrischer Merkmale in elektronischer Form. Deutschland wird mit der Einführung des elektronischen Personalausweises ein Signal für Europa setzen und geht von einer sukzessiven Einführung dieser Technik auch in den anderen Mitgliedstaaten aus.

- **Garantie für ein hohes Sicherheitsniveau in der elektronischen Welt**
  Mit dem elektronischen Personalausweis soll eine Sicherheitsinfrastruktur bereitgestellt werden, die einen sicheren und zuverlässigen Identitätsnachweis in der elektronischen Welt ermöglicht. Für die Bürgerinnen und Bürger soll so die Sicherheit bei der Abwicklung von Transaktionen im E-Government und E-Business erhöht werden. Wirtschaftliche Schäden für Bürgerinnen und Bürger und Unternehmen sollen durch Einschränkung von Möglichkeiten zum Identitätsdiebstahl, z. B. durch Unterbindung von Phishing-Attacken (illegales Ausspähen von Passwörtern), vermieden werden.

- **Wirtschaft und Verwaltung durch die Identitätsinfrastruktur des elektronischen Personalausweises modernisieren**
  Mit dem elektronischen Personalausweis sollen innovative Sicherheitstechnologien eingeführt werden, auf deren Grundlage die Geschäftsprozesse der Informationsgesellschaft vertrauenswürdiger und effizienter gestaltet werden können. Der elektronische Personalausweis kann damit die Initialzündung zur vermehrten Bereitstellung innovativer Dienstleistungen im E-Government und im E-Business sein und zugleich die Bereitschaft zur Nutzung solcher Angebote auf Seiten der Bürgerinnen und Bürger spürbar erhöhen.

- **Den elektronischen Personalausweis als Komponente einer EU-weit harmonisierten Online-Authentisierung etablieren**

  - Grenzüberschreitender elektronischer Geschäftsverkehr soll sicher und komfortabel möglich sein.
  - Das hohe deutsche Sicherheitsniveau sollte auch als Grundlage für einen EU-weiten Standard für elektronische Personalausweise dienen.
  - Deutsche sollen ihren elektronischen Personalausweis auch in anderen EU-Staaten zur elektronischen Authentisierung nutzen können.
  - Bürgerinnen und Bürger anderer EU-Mitgliedstaaten sollen in Deutschland mit entsprechenden Identitätsdokumenten auch Dienstleistungen auf hohem Sicherheitsniveau in Anspruch nehmen können.

8.2 Der elektronische Identitätsnachweis mit dem Personalausweis im privatwirtschaftlichen und behördlichen Kontext

Kap. 8.2 beschreibt ausgewählte Vorschläge für den Einsatz des elektronischen Personalausweises durch Bürgerinnen und Bürger im privatwirtschaftlichen Kontext gegenüber Unternehmen (E-Business), in Behörden und öffentlicher Einrichtungen (E-Government) und zur Unterstützung medienbruchfreier Geschäftsprozesse.

Auf der Grundlage dieser Szenarien können Anforderungen und Entscheidungen für die funktionale und technische Ausgestaltung der elektronischen Funktionen des Ausweises abgeleitet werden. Das betrifft hauptsächlich seine Verwendung für den elektronischen Identitätsnachweis aber auch für die qualifizierte elektronische Signatur (QES).

8.2.1 Vorschläge für den elektronischen Identitätsnachweis im E-Business

Online-Banking	
aktuelle Situation	Gemäß einer repräsentativen Umfrage[5] wollen 55% der Internetnutzer den elektronischen Personalausweis künftig beim Online-Banking einsetzen. Im Online-Banking werden zur Anmeldung und Transaktion PIN-TAN-Verfahren eingesetzt. Diese sind in verschiedenen Varianten etabliert, schützen allerdings nicht vollständig vor bekannten Phishing-Attacken. Darüber hinaus bedarf es heute für eine Eröffnung eines Kontos bei einer Online-Bank der persönlichen Identitätsfeststellung mit einem gültigen Personalausweis.
künftiges Szenario	Die Sicherheit der PIN-TAN-Verfahren wird durch den zusätzlichen elektronischen Identitätsnachweis erhöht. Online-Banking kann mit dem elektronischen Identitätsnachweis des ePA sicherer werden. Phishing-Attacken können effektiv verhindert werden, indem sich Bankkunden mit dem ePA und die Online-Bank mit ihrem Berechtigungszertifikat gegenseitig ausweisen. Mit dem Berechtigungszertifikat kann der Bankkunde darauf vertrauen, dass er tatsächlich Transaktionen mit seiner Bank und nicht mit einem Dritten durchführt. Mit dem ePA und dem elektronischen Identitätsnachweis besteht ferner die Möglichkeit, die Konto-Eröffnung bei Online-Banken ggf. vollständig über das Internet anzubieten.

[5] BITKOM/ Webmonitor forsa 2008 – Anteil der deutschen Internetnutzer an 14 Jahre, die einen elektronischen Personalausweis zur Identifikation bei Online-Diensten nutzen würden

Versandhandel und Auktionen im Internet	
aktuelle Situation	Gemäß einer repräsentativen Umfrage[1] wollen 41% der Internetnutzer den elektronischen Personalausweis künftig bei Auktionen und 39% beim Shopping im Internet einsetzen. Beim Versand- und Auktionshandel im Internet erfolgt die Feststellung der Identität des privaten Käufers oder Verkäufers häufig nur durch die Zustellung der Zugangsdaten mit offener E-Mail. Die Seriosität des Händlers oder die Geschäftsfähigkeit des privaten Käufers oder Verkäufers können oft erst bei Störung nachträglich festgestellt werden.
künftiges Szenario	Mit dem ePA wird die Identität von Händlern bzw. privaten Käufern oder Verkäufern über das Internet nachgewiesen. Das Berechtigungszertifikat des Händlers bzw. der elektronischen Personalausweise privater Verkäufer und Käufer begründen ein **größeres Vertrauensverhältnis** zum Zeitpunkt der Online-Bestellung oder Gebotsabgabe. Der **Verbraucherschutz** im Online-Handel ist gestärkt. Der **Identitätsbetrug** bei Auktionen und Bestellungen wird erheblich erschwert. Bei Auktionen sind **Bietermaschinen oder Angebote der Verkäufer** ausgeschlossen.

Internetservice allgemein	
aktuelle Situation	Für private Zwecke nutzten 61,5 % der Bevölkerung das Internet im 1. Quartal 2007 täglich.[6] Bei der Einrichtung von Benutzerkonten auf Serviceportalen im Internet, einschl. E-Mail- und Hostingportalen, Webshops und Auktionsplattformen, aber auch für Tauschbörsen, Chats, Foren, Blogs, Computerspiele und vieles andere mehr werden personenbezogene Daten erhoben und Benutzernamen, Kennungen oder Spitznamen vergeben. Der personalisierte Zugang ist im Internet häufig nur mit einfachen Passwörtern geschützt. Die gleichen Kennungen oder Passwörter werden mehrfach verwendet. Aktive Internetnutzer verfügen darüber hinaus über verschiedene virtuelle Identitäten und müssen sich dafür eine Vielzahl von Benutzernamen und Passwörtern merken. Internetserviceanbieter erfragen bei der Anmeldung meist zusätzliche Personendaten zur Identitätsfeststellung, z.B. das Geburtsdatum oder die Hausnummer und nutzen diese – für die Anmeldung – häufig gar nicht erforderlichen Daten datenschutzrechtswidrig für andere gewerbliche Zwecke.

[6] Statistisches Bundesamt - Fachserie 15 Reihe 4 " Private Haushalte in der Informationsgesellschaft - Nutzung von Informations- und Kommunikationstechnologien (IKT)" mit Ergebnissen aus der IKT-Erhebung 2007

Internetservice allgemein	
künftiges Szenario	Die Identität des Inhabers eines Benutzerkontos wird bei der Einrichtung und bei jeder Anmeldung gegenüber dem Internetservice sicher nachgewiesen. Internetservices, die nur eine sichere Wiedererkennung des Nutzers fordern, nutzen den **pseudonymen Nachweis der Identität ohne Personendaten**. Durch die Vergabe von Berechtigungszertifikaten erfolgt der Zugriff auf ePA-Daten zweckbezogen und datensparsam. Zusätzlich kann der Ausweisinhaber das Auslesen erfragter Personendaten verweigern. Der Personalausweis mit PIN eröffnet die Möglichkeit, ein **sicheres „Single-Sign-On" für Internetservices** einzusetzen. Auf Basis **lokaler Identitätsverwaltungsprogramme** oder durch **eID-Provider** kann der Zugang zu Internetservices oder Netzwerkressourcen automatisiert werden. Der Daten- und Verbraucherschutz und die Sicherheit im Internet werden nachhaltig unterstützt.

Sichere E-Mail und Datensafe (Bürgerportale)	
aktuelle Situation	Mit dem Vorhaben „Bürgerportale" plant die Bundesregierung Internetserviceprovidern die gesicherte Erlaubnis für den Betrieb von manipulationssicheren und geschützten E-Mail- und Datenspeicherdiensten zu erteilen. Für die Einrichtung von Benutzerkonten und die personalisierte Anmeldung ist ein sicherer Identitätsnachweis erforderlich, um Missbrauch zu verhindern.
künftiges Szenario	Die Einrichtung von Benutzerkonten bei Bürgerportalen, der Zugang, Mailversand und die Speicherung elektronischer Dokumente erfolgt **sicher durch die elektronische Identifizierung mit dem Personalausweis.** Bürgerportal-Provider besitzen Zertifikate, die sie zur Erhebung der ePA-Daten im Rahmen des elektronischen Identitätsnachweises berechtigen.

Alterskontrolle	
aktuelle Situation	Gemäß einer repräsentativen Umfrage[1] wollen 36% der Internetnutzer den elektronischen Personalausweis künftig bei Internetspielen einsetzen. Der Zugang zu altersbeschränkten Internetangeboten oder Gütern über das Internet wird häufig nur durch eine bloße Alters- bzw. Identitätserklärung oder durch Angabe einer Bankverbindung geschützt. Zugangsbarrieren zu jugendgefährdenden Angeboten, Spielen oder Videos sind häufig leicht zu umgehen. Auch der Zugang zu alterbeschränkten Waren und Dienstleistungen, wie z.B. Genussmitteln an Automaten und Kassensystemen oder Spielautomaten, bedarf einer verbesserten Zugangkontrolle

Alterskontrolle	
künftiges Szenario	Die **Identität oder die Erreichung einer bestimmten Altersgrenze** kann zuverlässig über das Internet, an Automaten oder Kassensystemen festgestellt werden. Das Erreichen einer Altersgrenze kann sich ein Diensteanbieter durch die Verwendung entsprechender Berechtigungszertifikate (siehe Kapitel 9.3.4.3) durch den ePA bestätigen lassen. **Wesentlich ist hierbei, dass keine Geburtsdaten oder andere Personendaten übermittelt werden müssen**. Jugendliche sind damit sowohl vor gefährdenden Angeboten und der Preisgabe Ihrer Personendaten, die Anbieter vor den Folgen einer nicht rechtmäßigen Zugangsgewährung bzw. Abgabe wirksam geschützt.

Elektronischer Autoschlüssel	
aktuelle Situation	Kraftfahrzeuge sind heute regelmäßig mit einer Wegfahrsperre ausgestattet, die üblicherweise mit dem Autoschlüssel deaktiviert werden kann. Damit wird die Benutzung des Fahrzeugs durch den Besitz des Schlüssels geschützt. Die Autoindustrie hat gemeinsam mit der Versicherungswirtschaft damit begonnen, weitere Techniken für Wegfahrsperren zu entwickeln.
künftiges Szenario	Der elektronische Personalausweis kann dem zusätzlichen **Schutz von Kraftfahrzeugen gegen Missbrauch oder Diebstahl** dienen. Mit dem elektronischen Identitätsnachweis des ePA können das Führen des Fahrzeugs oder technische Funktionen des Fahrzeugs für einzelne Personen oder Personengruppen gespeichert und mit dem Personalausweis aktiviert werden.

QES - Antrag	
aktuelle Situation	Die Beantragung einer qualifizierten elektronischen Signatur erfordert gemäß Signaturgesetz eine eindeutige Identitätsprüfung des Antragstellers. Dafür ist heute die Vorlage eines Personalausweises und das persönliche Erscheinen erforderlich.
künftiges Szenario	Mit dem elektronischen Personalausweis erfolgt die Identitätsüberprüfung des Antragstellers bei **Beantragung einer qualifizierten elektronischen Signatur künftig über das Internet**. Die Zertifizierungsdiensteanbieter besitzen die dafür erforderlichen Berechtigungszertifikate.

8.2.2 Vorschläge für den elektronischen Identitätsnachweis im E-Government

Online-Ummeldung	
aktuelle Situation	Bürgerinnen und Bürger, die der Meldepflicht unterliegen, müssen nach einem Umzug oder in Folge einer Namensänderung der für sie örtlich zuständigen Meldebehörde die neue Wohnanschrift bzw. den angenommenen Namen mitteilen. Hierfür ist bislang im Regelfall das persönliche Erscheinen der Betroffenen bei der Behörde notwendig, nicht selten verbunden mit erheblichen Anfahrt- und Wartezeiten.
künftiges Szenario	Mit dem ePA könnte künftig das althergebrachte Meldeverfahren durch ein Online-Verfahren abgelöst werden. Dazu würde für die An- bzw. Ummeldung oder die Fortschreibung der Meldedaten nach der elektronischen Identifizierung ein bereits weitgehend vorausgefülltes Meldeformular zur Verfügung gestellt und von den Meldepflichtigen online ausgefüllt, ggf. elektronisch signiert und über eine gesicherte Verbindung an das Melderegister übermittelt werden. Über eine geplante „Transparenzfunktion“ könnten sich meldepflichtige Bürgerinnen und Bürger ggf. nach Identifizierung mittels ePA über sie betreffende, an berechtigte Dritte erteilte Auskünfte aus dem Melderegister informieren.

ELSTER-Online	
aktuelle Situation	Jährlich werden rund fünf Millionen Einkommensteuererklärungen über das Internet bei den Finanzämtern eingereicht. Um auf die eigenhändige Unterschrift und Einsendung des Papierformulars zu verzichten und damit eine schnellere Bearbeitung im Finanzamt zu erwirken, ist ein gesondertes elektronisches Elster-Online-Zertifikat erforderlich, das zuvor einmalig beantragt werden muss.
künftiges Szenario	Mit dem elektronischen Identitätsnachweis des elektronischen Personalausweises werden die gesondert zu beantragenden **Elster-Online-Zertifikate abgelöst**. Die Anzahl der ausschließlich über das Internet abgegebenen Einkommensteuererklärungen steigt signifikant. Mit dem Belegverzicht sparen die Finanzämter Ressourcen, werden Übertragungsfehler in das elektronische System vermieden und Bearbeitungszeiten verringert. Die Finanzämter erhalten die erforderlichen Berechtigungszertifikate.

Internetauskunft aus Registern, Datenbanken und Verfahren	
aktuelle Situation	Die Beantragung von Auskünften über Eintragungen in öffentlichen Registern oder Datenbanken ist heute vielfach bereits online möglich. Sie erfordert entweder die persönliche Vorlage des Personalausweises, die Einsendung einer Personalausweiskopie oder eine elektronische Signatur - so z.B. für die Einsicht in Personen- und Adressdaten im Melderegister, zur Erlangung eines Führungszeugnisses aus dem Bundeszentralregister, zur Abfrage des Punktestands im Verkehrszentralregister, zum Stand des Rentenkontos oder zu Eintragungen bei der Schufa u. a. m.

Internetauskunft aus Registern, Datenbanken und Verfahren	
künftiges Szenario	Mit dem elektronischen Identitätsnachweis erfolgt der **sichere Zugriff auf Registereinträge und Datenbanken im Internet** soweit für den Personalausweisinhaber zulässig. **Behörden-Bescheinigungen und Dokumente können online beantragt werden.** Wartezeiten sowie Versand- und Kopierkosten senken den Aufwand beidseitig. Die Fachbehörden und Einrichtungen erhalten die erforderlichen Berechtigungszertifikate für den Zugriff auf die ePA-Daten. Ein so personalisierter transparenter Internetzugang zu den von öffentlichen Stellen gespeicherten Personendaten, z.B. zum eigenen Melderegistereintrag, wird das Vertrauensverhältnis der Bürgerinnen und Bürger zum Staat verbessern. Die Online-Verfolgung des Bearbeitungsstandes eines Vorgangs, z.B. eines Leistungsantrags, stellt einen Teil der Serviceorientierung der Verwaltung dar.

Kfz- An- und Ummeldung	
aktuelle Situation	Jährlich finden in Deutschland rund 40 Millionen Meldevorgänge im Kfz-Wesen statt. Ausgenommen die Terminvereinbarung oder Wunschkennzeichenbestellung ist dabei bisher immer auch das persönliche Vorsprechen bei der Kfz-Zulassungsbehörde der zuständigen Kommune bzw. des Landkreises für die An- oder Abmeldung, Stilllegung etc. erforderlich. Bei der Kfz- An- oder Ummeldung ist zudem der Nachweis der Versicherung erforderlich.
künftiges Szenario	Der elektronische Personalausweis wird im Internet für den elektronischen Identitätsnachweis gegenüber einem Fachverfahren eingesetzt werden, das Kfz-Zulassungsbehörden und Versicherungen integriert. Das Verfahren wird zunächst durch den postalischen Versand von Zulassungspapieren und ggf. Kfz-Kennzeichen ergänzt werden. So könnten gegenüber dem bisherigen Verfahren bereits Verwaltungskosten eingespart, der Zeitaufwand für Behördengänge auf Seiten der Bürgerinnen und Bürger verringert und der Zeitpunkt der Abwicklung flexibilisiert werden.

Überprüfung gewerblich Beschäftigter	
aktuelle Situation	Zur Aufdeckung von Schwarzarbeit und illegaler Beschäftigung nehmen Bundesagentur für Arbeit und die Bundesfinanzverwaltung bundesweit regelmäßig stichprobenartig Kontrollen z.B. von Bauunternehmen und Gaststätten vor. Für die Prüfung der Ordnungsmäßigkeit der Beschäftigungsverhältnisse ist die zweifelsfreie Feststellung der Identität der Angetroffenen durch Personendokumente erforderlich. Zusätzlich werden Daten weiterer Behörden abgefragt. Bislang ist diese Überprüfung sehr zeitaufwendig.
künftiges Szenario	Mit dem elektronischen Personalausweis ist die **Identitätsfeststellung bei Kontrollen vor Ort** deutlich beschleunigt. Über mobile Endgeräte mit Berechtigungszertifikaten und Kartenleserfunktion könnten die elektronischen Identitätsdaten ausgelesen und über Datenfunkverbindungen an die anzufragenden Stellen übermittelt werden.

8.2.3 Vorschläge für die Automatisierung von Geschäftsprozessen

Elektronische Prozessabwicklung in der Wirtschaft	
aktuelle Situation	Eine elektronische Prozessabwicklung ist heutzutage – insbesondere in der Wirtschaft – weit fortgeschritten. Dies betrifft z. B. Materialfluss, Produktion oder Lagerhaltung und Auslieferung. Allerdings werden aufgrund fehlender Prozessintegration von externen Lieferanten-, Kunden- oder auch Produktionsprozessen sowie medienbruchbehafteter interner Geschäftsprozesse häufig Daten doppelt erfasst bzw. manuell erhoben. In vielen Fällen fehlt zur Automatisierung der Geschäftsprozesse die Möglichkeit, eine elektronische Datenübernahme aus Personalausweisen vorzunehmen.
künftiges Szenario	Der elektronische Identitätsnachweis ermöglicht es, den ePA auch zur Erfassung von **Personen, Mitarbeitern, Lieferanten oder Kunden in Geschäftsprozesse elektronisch zu erfassen** und so den Prozess vollständig medienbruchfrei abzuwickeln ohne weitere Personenidentifikationssysteme einführen zu müssen. Die Unternehmen beantragen dazu die erforderlichen Berechtigungszertifikate. Bei gleichzeitiger Anwendung der optionalen QES wird die Beteiligung von Personen in kritischen Prozessen oder Rechtsgeschäften rechtsicher beweisbar.

Elektronische Prozessabwicklung in der Verwaltung	
aktuelle Situation	Bürgerinnen und Bürger müssen zur Beantragung von Leistungen im Regelfall persönlich bei der jeweils zuständigen Behörde erscheinen und den Personalausweis zur Identifizierung vorlegen. Darüber hinaus müssen die Bürgerinnen und Bürger händisch Formulare ausfüllen und dabei lange Wartezeiten in Kauf nehmen.
künftiges Szenario	Der elektronische Identitätsnachweis ermöglicht es, diese Prozessschritte zu automatisieren, indem zukünftig die Bürgerinnen und Bürger – ihr Einverständnis vorausgesetzt – mit dem in der Behörde vorhandenen Lese- und Schreibgerät die ePA-Daten ausgelesen und direkt im System verarbeitet werden können. Damit werden Doppeleingaben und -arbeiten verhindert und langwierige administrative Prozesse beschleunigt.

Zugangskontrollen	
aktuelle Situation	Zur Wahrung von Betriebsgeheimnissen oder aus anderen Schutzgründen erfolgt beim Zugang zu Unternehmen, Werkstätten, Labors, Rechenzentrum, Ministerien usw. eine Personenkontrolle mit Personendokumenten oder Betriebsausweisen. Die Personendaten von Besucher werden häufig am Eingang manuell erfasst.

Zugangskontrollen	
künftiges Szenario	Mit dem elektronischen Personalausweis werden **manuelle Zugangskontrollen automatisiert** oder verschiedene Zugangssysteme für Personal und Betriebsfremde effizient auf eine sichere technische Basis zusammengeführt. Investitionen in eine moderne Kartentechnologie für Betriebsausweise können reduziert werden. Der elektronische Identitätsnachweis könnte somit künftig auch innerbetrieblich für weitere Anwendung als Multifunktionskarte (Kantine, Disposition, Intranet usw.) verfügbar gemacht werden

Einloggen in IT-Systeme und Mitarbeiterportale	
aktuelle Situation	In der heutigen Berufswelt sind Arbeitsplatzcomputer in der Firma, Telearbeit und mobiles IT-Arbeiten gängige Praxis. Die Arbeitsplatzcomputer, Internet- und Intranetzugänge, Datenbanken und andere IT-Systeme im Unternehmen sind häufig durch verschiedene Passwörter oder Schlüssel geschützt. Telearbeit oder mobiles Arbeiten erfordert meist den verschlüsselten Zugang ins Firmennetz über einen VPN-Client. Das Zugangsverfahren mit Passwörtern, Schlüsseln, zeitlichen Begrenzungen oder Token erschwert die Handhabbarkeit für die Mitarbeiter häufig. Vergisst der Arbeitnehmer seine vielen Zugangsdaten oder den Token führt dies schnell dazu, dass ein Weiterarbeiten nicht möglich ist.
künftiges Szenario	Mit dem elektronischen Identitätsnachweis werden aufwendige betriebliche Identifizierungsverfahren beim **Einloggen in IT-Systeme deutlich vereinfacht** und verschiedene Zugangsverfahren als „**Single-Sign-On“** in einem personalisierten Mitarbeiterportal zusammengeführt. Die Bedienbarkeit der wachsenden Zahl von IT-Systemen und Anwendungen wird nutzerfreundlich vereinfacht, die **Produktivität** verbessert. Investitions- und Betriebskosten für verschiedene Identifizierungssysteme werden im Unternehmen reduziert. Beispielsweise kann der ePA für den betrieblichen Zugang zu öffentlichen Ausschreibungsplattformen genutzt werden.

8.2.4 Vorschläge für die QES mit dem elektronischen Personalausweis

ELENA (Jobcard)	
aktuelle Situation	Rund 3 Millionen Arbeitgeber in Deutschland stellen jedes Jahr etwa 60 Millionen Bescheinigungen, Einkommensnachweise und Auskünfte für ihre Angestellten in Papierform aus. Mit einem Gesetzentwurf plant die Bundesregierung diese Bescheinigungen zur Entbürokratisierung für die Unternehmen automatisiert elektronisch in einer zentralen Speicherstelle zu erfassen. Dabei sind die informationelle Selbstbestimmung der Angestellten zu wahren und die Einkommens- und Beschäftigungsdaten vor Missbrauch zu schützen.
künftiges Szenario	Die Bereitstellung der Beschäftigtendaten soll in der zentralen Speicherstelle über ein Registraturfachverfahren erfolgen. Die **datenschutzgerechte Speicherung und der Abruf der Daten aus der zentralen Speicherstelle** erfolgt auf der Grundlage elektronischer Signaturzertifikate der Antragsteller. Die abrufberechtigen Mitarbeiter der Arbeitsagenturen oder Kommunalbehörden müssen zusätzlich den **Datenabruf mit ihrer QES** unterschreiben. Durch das ELENA-Verfahren kann auf die Ausstellung von papiergebundenen Einkommensnachweisen verzichtet werden. Dieses Verwaltungsverfahren ist medienbruchfrei, zeit- und ressourcensparend und kann damit die Bearbeitungszeiten für die Bürgerinnen und Bürger verkürzen. Behördengänge entfallen und werden auch unabhängig von Öffnungszeiten über das Internet erledigt.

Elektronisches Handels- und Unternehmensregister	
aktuelle Situation	Am 1. Januar 2007 wurde das zentrale elektronische Unternehmensregister eingeführt. Alle deutschen Kapitalgesellschaften müssen gemäß EHUG ihre Jahresabschlüsse beim Bundesanzeiger auf elektronischem Wege einreichen. Bereits 800.000 Registeranmeldungen wurde so elektronisch vollzogen. Die elektronische Auskunft aus dem EHU erfolgt über ein gemeinsames Registerportal der Länder Nur noch bis Ende 2009 können Meldungen – gegen eine höhere Gebühr – in Papierform eingereicht werden.
künftiges Szenario	**Meldungen für die Handels- und Unternehmensregister** sind ab 2010 ausschließlich elektronisch **mit der QES** über das Internet zu erbringen. Die Verwendung des Personalausweises als optionaler Träger für QES-Zertifikate kann die Handhabung erleichtern.

Elektronische Rechnungen	
aktuelle Situation	Elektronische Rechnungen im Geschäftsverkehr erfordern die Unterzeichnung mit QES, wenn der Rechnungsempfänger einen Vorsteuerabzug geltend machen möchte. Demgegenüber können papiergebundene Rechnungen formfrei erstellt werden. Das führt mangels Verbreitung und Akzeptanz der qualifizierten elektronischen Signatur meist zu Medienbrüchen in der Rechnungsstellung von Unternehmen.
künftiges Szenario	**Elektronische Rechnungen können mit dem elektronischen Personalausweis unterschrieben werden**, der zusätzlich ein QES-Zertifikat enthält. Verfügt der die Rechnung ausstellende Unternehmer oder sein beauftragter Mitarbeiter über einen elektronischen Personalausweis, kann die optionale Signaturfunktion des ePA genutzt werden und die Ausstellung zusätzlicher Signaturkarten entfallen.

9 ANFORDERUNGEN AN DEN ELEKTRONISCHEN PERSONALAUSWEIS

Ausgehend von den mit der Einführung des elektronischen Personalausweises verfolgten Zielen und dem erwarteten Beitrag des elektronischen Personalausweises zur Gewährleistung einer sicheren, vertrauensvollen und komfortablen Identifizierung und Authentifizierung in den vorstehend beschriebenen Anwendungsfällen im E-Government und E-Business, lassen sich drei grundsätzliche funktionale Anforderungen an das Dokument ableiten. Diese ziehen wiederum klar abgrenzbare organisatorische, technische, rechtliche und wirtschaftliche Anforderungen nach sich.

9.1 Funktionale Anforderungen

Zusammenfassend soll der künftige elektronische Personalausweis

- weiterhin als **Mittel der körperlichen Identitätsprüfung** in der realen Welt durch Sichtkontrolle insbesondere auf Basis des Gesichtsbildes und Prüfung anderer biometrischer Merkmale erhalten bleiben,
- als **biometriegestütztes, elektronisches Reisedokument** verwendbar sein sowie
- ein **elektronischer Identitätsnachweis und (optional) eine qualifizierte elektronische Signatur** für die Nutzung von E-Government- und E-Business- Angeboten vorhalten.

Daraus ergeben sich folgende funktionale Anforderungen:

Lfd. Nr.	Anforderung
Der elektronische Personalausweis als Mittel der körperlichen Identitätsprüfung	
FU.1	Der elektronische Personalausweis enthält alle notwendigen Daten und Sicherheitsmerkmale, damit der Inhaber im Reiseverkehr eindeutig identifiziert werden kann und das Dokument selbst durch hochwertige Sicherheitsmerkmale geschützt ist.
FU.2	Es muss auch ohne Hilfsmittel und unter schlechten Sichtverhältnissen (Nacht, Regen) möglich sein, zum einen die Identität des Inhabers und zum anderen die Echtheit des Dokumentes selbst feststellen zu können. Hierzu soll das Ausweisbild in Farbe und in mit dem gegenwärtigen Personalausweis vergleichbarer Größe aufgebracht werden.
FU.3	Eine wesentliche Verlängerung des Prüfprozesses soll nach Möglichkeit vermieden werden.

Lfd. Nr.	Anforderung
FU.4	Die Prüfbarkeit des Personalausweises im privatwirtschaftlichen und hoheitlichen Umfeld ist unter Beibehaltung der bisher aufgedruckten, personenbezogenen Daten zu gewährleisten.
FU.5	Die für die Reisedokumentenfunktion gemeinschaftsrechtlichen Vorgaben stellen Minimalanforderungen dar und sind bindend. Dies schließt die Spezifikationen der International Civil Aviation Organization (ICAO) für maschinell lesbare Reisedokumente ein. (*EU-Vorgaben: Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. L 385 vom 29.12.2004, S. 1-6*)
Der elektronische Personalausweis als biometriegestütztes elektronisches Reisedokument	
FU.6	Der elektronische Personalausweis wird die gleichen biometrischen Merkmale und die gleiche Technik wie der ePass erhalten, so dass auch Ausstellung und Kontrolle analog zum ePass erfolgen können. Einschränkend ist festzuhalten, dass die Fingerabdrücke auf freiwilliger Basis nur auf Antrag der Bürgerinnen und Bürger in den ePA aufgenommen werden.
FU.7	Die Kompatibilität zum ePass mit Biometrie ist herzustellen, damit der elektronische Personalausweis auch in Zukunft im Rahmen einer einheitlichen Sicherheitsstrategie für den grenzüberschreitenden Personenverkehr als sicheres Reisedokument und vollwertiges Passersatzdokument genutzt werden kann.
FU.8	Die geplante Verwendung der elektronisch vorgehaltenen biometrischen Merkmale bleibt ausschließlich dem hoheitlichen Bereich vorbehalten.
Der elektronische Personalausweis mit dem elektronischen Identitätsnachweis und (optionaler) qualifizierter elektronischer Signatur	
FU.9	Die Ausweisinhaber sollen selbst über die Nutzung des elektronischen Identitätsnachweises entscheiden, indem sie bei der Aushändigung des Personalausweises schriftlich gegenüber der Personalausweisbehörde erklären, ob sie den elektronischen Identitätsnachweis nutzen wollen oder nicht.
FU.10	Die elektronische Authentisierung wird durch Nutzung der elektronischen Ausprägung der bereits bisher auf den Personalausweis aufgedruckten personenbezogenen Daten in elektronischer Form gewährleistet.
FU.11	Zur Authentisierung werden die für den jeweiligen Einsatzzweck erforderlichen personenbezogenen Daten dem Kommunikationspartner in gesicherter Form übermittelt.
FU.12	Die Authentisierung soll sowohl offline an dafür ausgerüsteten Geräten lokal vor Ort als auch online über eine Netzverbindung erfolgen können.
FU.13	Die Bindung zwischen dem elektronischen Personalausweis und seinem Inhaber wird bei der Nutzung der elektronischen Authentisierung durch Besitz des Ausweises selbst und das Wissen um ein zugehöriges Geheimnis (PIN) hergestellt.

Lfd. Nr.	Anforderung
FU.14	Der Zugriff auf Daten wird über Berechtigungszertifikate des Diensteanbieters abgesichert und gesteuert. Das Berechtigungszertifikat muss u. a. Angaben über den Diensteanbieter und dessen Datenschutzaufsichtsbehörde, Angaben zu dessen Berechtigungen für den Zugriff auf einzelne Datenfelder (z. B. Name, Alter, Adresse) und den Erhebungs- und Verarbeitungszweck enthalten. Ohne Übermittlung eines solchen gültigen Berechtigungszertifikats werden keine personenbezogenen Daten aus dem Dokument übertragen.
FU.15	Der elektronische Personalausweis muss funktional so vorbereitet werden, dass Bürgerinnen und Bürger die qualifizierte elektronische Signaturfunktion in eigener Verantwortung mit Hilfe eines privaten Zertifizierungsdiensteanbieters in den elektronischen Personalausweis integrieren können. Der Personalausweis dient damit als sichere Signaturerstellungseinheit.

Tabelle 12: Funktionale Anforderungen an den elektronischen Personalausweis

9.2 Technische Anforderungen

Das Kapitel beschreibt die technischen Anforderungen, die zur Realisierung der in Kap. 9.1 formulierten funktionalen Anforderungen an den elektronischen Personalausweis zu stellen sind. Dies umfasst die Anforderungen an das Ausweisdokument selbst und die zur Nutzung der Funktionen erforderlichen IT-Verfahren (Anwendungen). Sofern mehrere grundsätzliche Alternativen zur Realisierung der Anforderungen existieren, werden diese hinsichtlich ihrer Vor- und Nachteile diskutiert und – wo möglich und sinnvoll – mit einem Votum versehen.

9.2.1 Anforderungen an das Ausweisdokument

9.2.1.1 Elektronische Schnittstelle (Chip)

Aus Gründen der Kompatibilität zur Kontrollinfrastruktur des ePasses wird der elektronische Personalausweis für die biometrischen Merkmale mit kontaktloser elektronischer Schnittstelle für den integrierten Chip nach ISO 14443 (vgl. [8]) ausgestattet. Für den elektronischen Identitätsnachweis und die qualifizierte elektronische Signatur wird derselbe Chip genutzt. Bei dieser Ein-Chip-Lösung mit kontaktloser Schnittstelle wird in den Ausweis lediglich ein einziger Chip mit einer kontaktlosen Schnittstelle nach ISO 14443 eingebracht. Eine solche Lösung hat insbesondere die folgenden Vorteile:

- Geringer Verschleiß, da das Auslesen berührungslos erfolgt.
- Unempfindlich gegen Verschmutzung, Feuchtigkeit etc., da keine elektrischen Kontakte an der Oberfläche vorhanden sind.
- Kostengünstig, da nur ein Chip benötigt wird.

- Kann auch mit mobilen Geräten genutzt werden (Handy, Organizer), die zunehmend mit kontaktlosen Schnittstellen ausgestattet werden.

Die Anforderungen des beschriebenen elektronischen Personalausweises an Langlebigkeit, Ausfallsicherheit, Zukunftssicherheit und Kosten erfüllt die kontaktlose Ein-Chip-Lösung daher besser als andere denkbare Varianten (kontaktbehaftet, zwei Chips, etc.). Mit dem rein kontaktlosen elektronischen Personalausweis im Scheckkartenformat der Niederlande und der kontaktlosen Multifunktionskarte des Verkehrsverbundes Rhein-Ruhr sind erfolgreiche Referenzprojekte verfügbar.

Darüber hinaus ist zu berücksichtigen, dass der Chip, der die Signaturfunktion enthält, die Anforderungen einer sicheren Signaturerstellungseinheit (SSE) erfüllen muss (vgl. [12]). Dies kann für die kontaktlose Ein-Chip-Lösung sichergestellt werden.

9.2.1.2 Physisches Kartenformat (Kartenkörper)

Das physische Format des elektronischen Personalausweises wird in der Größe ID1 (Scheckkartenformat) ausgestaltet. Das Scheckkartenformat wurde bisher bei allen neueren Identitätskarten mit integriertem Chip verwendet. Als Beispiele sind hier die Identitätskarten in Belgien, Schweden und Hongkong (siehe auch Kapitel 6) zu nennen. Auch viele EU-Mitgliedsstaaten, mit deren Personalausweisen die Einreise auch nach Deutschland möglich ist, haben Personalausweise in diesem Format eingeführt. Die deutschen Sicherheitsbehörden müssen also generell in der Lage sein, Personalausweise im Scheckartenformat zu kontrollieren. Auch Fälschungen können im neuen Format mit der gleichen Zuverlässigkeit wie bisher erkannt werden. Für das ID1-Format beim zukünftigen elektronischen Personalausweis spricht insbesondere auch das handliche Format, das das Mitführen des Personalausweises erleichtert und damit höhere Akzeptanz als das größere ID2-Format bei den Bürgerinnen und Bürgern genießt.

9.2.1.3 Gültigkeitsdauer

Die Gültigkeit des bisherigen deutschen Personalausweises beträgt 10 Jahre (für Personen ab Vollendung des 24. Lebensjahres). Elektronische Personalausweise in anderen Ländern sind zumeist entweder 10 oder 5 Jahre gültig.

Aufgrund der Entscheidung für eine Chiplösung mit ausschließlich kontaktloser Schnittstelle kann diese Gültigkeitsdauer im Hinblick auf die technische Haltbarkeit des Dokuments aufrechterhalten werden. Für eine Gültigkeitsdauer von 10 Jahren sprechen darüber hinaus die folgenden Argumente:

- Das Mengengerüst hinsichtlich Beantragung und Produktion bleibt im Vergleich zum bisherigen Zustand gleich.
- Geringere Kosten und Aufwand für die Bürgerinnen und Bürger bezogen auf die Lebensdauer von 10 Jahren als bei 5-jähriger Gültigkeit, da regelmäßig nur ein Dokument beantragt, produziert und ausgegeben werden muss.
- Geringere Kosten bei den Ausgabestellen gegenüber 5-jähriger Gültigkeitsdauer, da im gleichen Zeitraum nur halb so viele Anträge bearbeitet werden müssen.

9.2.1.4 Anforderungen an das Ausweisdokument – Zusammenfassung

Lfd. Nr.	Anforderung
Elektronische Schnittstelle (Chip)	
TE.1	Der elektronische Personalausweis wird mit einem Chip ausgestattet, der eine kontaktlose Schnittstelle aufweist.
TE.2	Der Speicherchip ist so auszulegen, dass er die biometrischen Merkmale in elektronischer Form (Gesichtsbild und Fingerabdrücke des Inhabers) und eID-Daten sowie ein qualifiziertes Signaturzertifikat und die entsprechenden kryptographischen Schlüssel aufnehmen kann.
Physisches Kartenformat	
TE.3	Als Format für den Kartenkörper des elektronischen Personalausweises wird das Scheckkartenformat (ID1) vorgesehen.
TE.4	Der Ausweis muss einen Schichtenverbund aufweisen, der eine Separierung der echtheitssichernden Elemente von den datentragenden Schichten wirksam verhindert.
TE.5	Soweit möglich ist das Material selbst mit Sicherheitsmerkmalen auszustatten. Falls der Kartenaufbau kein Sicherheitspapier entsprechend dem bisherigen Personalausweis aufweist, ist eine Kompensation der Sicherheitsmerkmale des Papiers über die Mindestanforderungen in den übrigen Bereichen der sicherungstechnischen Ausstattung hinaus vorzusehen.
TE.6	Die Kartenoberfläche ist mit einer Sicherheitsprägung mit Mikroschrift- und Kippeffektmerkmalen auszustatten, nach Möglichkeit spezielle Formgebung des Kartenkörpers zur Unterscheidung von handelsüblichen Rohlingen.

Lfd. Nr.	Anforderung
Gültigkeitsdauer	
TE.7	Gültigkeitsdauer des Dokuments ab Ausstellungsdatum: 10 Jahre, bei Personen unter 24 Jahren 6 Jahre Gültigkeit.
Haltbarkeit	
TE.8	Der elektronische Personalausweis muss hohen Anforderungen an Haltbarkeit und Gebrauchstauglichkeit genügen. Er muss die in einschlägigen Normen festgelegten Anforderungen zur Beständigkeit unter extremen klimatischen Bedingungen, Haltbarkeit unter mechanischer Belastung und Resistenz gegen Strahlung und chemische Einwirkungen erfüllen. Als Leitlinie sind die von ICAO im Technical Report on Durability of Machine Readable Passports[7] publizierten Anforderungen zu berücksichtigen.
Kopierschutz	
TE.9	Der elektronische Personalausweis ist mit hochgradig gegen digitale Reproduktions- und Kopiertechniken schützenden, optisch variablen Elementen als Sicherheitsmerkmalen auszustatten (z. B. durch vollflächige Integration eines individualisierten, optisch variablen Sicherheitselements auf der Kartenvorderseite, das mindestens die im bisherigen PA realisierten Sicherheitsfunktionen umfasst). Darüber sind kryptographische Vorkehrungen gegen das Kopieren bzw. Verifizieren des Chips zu etablieren (Chip Authentication).
Schutz gegen Manipulation/ Erkennung von Fälschungen	
TE.10	Zum Schutz der inhaltlichen Angaben sind Personenmerkmale, wie Lichtbild und Inhaberunterschrift durch sichere Verfahren in das Dokumentenmaterial zu integrieren.
TE.11	Die spezielle Ausstellungstechnik muss eine hochgradige Absicherung gegen Verfälschungsmanipulationen bewirken und von allgemein zugänglichen digitalen Drucktechniken eindeutig unterscheidbar sein.
TE.12	Es sind geeignete physikalische Sicherheitsmerkmale für eine maschinelle Echtheitsprüfung zu integrieren, die mindestens das technologische Niveau der in den bisherigen deutschen Ausweisdokumenten enthaltenen Maschinenprüfmerkmale aufweisen.
TE.13	Die auf dem Chip des ePA gespeicherten Daten sind mittels elektronischer Signaturen gegen Manipulationen zu schützen (Passive Authentication).

Tabelle 13: Anforderungen an das Ausweisdokument

Detaillierte Anforderungen an die Ausgestaltung des elektronischen Personalausweises bzgl. Materialtechnik, Sicherheitsdruck, Kopierschutztechnik, Ausstellungstechnik und Sicherheitsfunktionen für maschinelle Echtheits- und Identitätsprüfungen werden im Rahmen einer Leistungsbeschreibung spezifiziert.

[7] ICAO, Technical Report on Durability of Machine Readable Passports, Version 3.2 vom 30.08.2006

9.2.2 Anforderungen an die elektronischen Anwendungen

Die beiden in Kap. 9.1 beschriebenen elektronischen Funktionen des elektronischen Personalausweises – zum einen der elektronische Personalausweis als biometriegestütztes, elektronisches Reisedokument und zum anderen als Träger eines elektronischen Identitätsnachweises und einer (optionalen) qualifizierten elektronischen Signatur für die Nutzung von E-Government und E-Business – sollen in vollständig getrennten Anwendungen realisiert werden. Daraus ergeben sich folgende anwendungsspezifische Anforderungen:

Lfd. Nr.	Anforderung
Anwendung „biometriegestütztes Reisedokument“	
EA.1	Die Anwendung als biometriegestütztes Reisedokument entspricht im Wesentlichen der Realisierung im neuen Reisepass (ePass) und soll mindestens den Anforderungen der ICAO (vgl. [5]) und der europäischen Spezifikation für den Zugriff auf die freiwillig im Chip gespeicherten Fingerabdrücke (vgl. [1]) entsprechen.
EA.2	Im Chip des elektronischen Personalausweises sollen für diese Anwendung neben den alphanumerischen personenbezogenen Daten zur Identifizierung das Gesichtsbild und auf Wunsch des Antragstellers auch die Fingerabdrücke für die biometrische Auswertung gespeichert werden.
EA.3	Der Zugriff auf die im Chip gespeicherten Daten (wie z. B. Fingerabdruck oder Gesichtsbild) werden vor unberechtigtem Auslesen geschützt.
EA.4	Im Gegensatz zum ePass ist beim elektronischen Personalausweis zu berücksichtigen, dass auf dem PA keine Angaben zum Geschlecht enthalten sind.
EA.5	Bei der Realisierung des elektronischen Personalausweises im ID1-Format ist zu berücksichtigen, dass sich eine 3-zeilige MRZ auf der Rückseite befinden muss, damit die Kompatibilität zu den Anforderungen der ICAO gewahrt bleibt.
Anwendung „elektronischer Identitätsnachweis“	
EA.6	Für die Nutzung des elektronischen Identitätsnachweises muss sich zunächst der Daten anfragende Diensteanbieter (Behörde oder privater Dritter) gegenüber dem elektronischen Personalausweis authentisieren und die Berechtigung zum Zugriff auf bestimmte Datenfelder des elektronischen Personalausweises nachweisen.
EA.7	Auf dem elektronischen Personalausweis dürfen nur behördlich überprüfte Daten gespeichert werden.
EA.8	Die Identifizierung des Ausweisinhabers muss anhand der auf dem elektronischen Personalausweis gespeicherten Daten erfolgen. Ausschließlich die folgenden Datenfelder können im Wege des elektronischen Identitätsnachweises übermittelt werden: Vornamen, Familienname, Doktorgrad, Tag und Ort der Geburt, gegenwärtige Anschrift, Dokumentenart, Abkürzung „D“ für Bundesrepublik Deutschland, Angabe, ob Personalausweis gültig ist, Angabe, ob ein bestimmtes Alter über- oder unterschritten wird (Alterskontrolle), Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht, ein diensteanbieter- und kartenspezifisches Kennzeichen.

Lfd. Nr.	Anforderung
EA.9	Es werden maximal die für den Geschäftsprozess notwendigen Daten übertragen, für die der Diensteanbieter ein Berechtigungszertifikat zuvor übermittelt hat.
EA.10	Ein elektronischer Identitätsnachweis darf nur mit Einwilligung der Ausweisinhaber möglich sein. Nach Anzeige der Daten, auf die ein Diensteanbieter gemäß Berechtigungszertifikat zugreifen darf, kann der Personalausweisinhaber die Übertragung einzelner Daten durch Auskreuzen ablehnen. Die Übermittlung der freigegebenen personenbezogenen Daten erfolgt in jedem Einzelfall explizit durch die Eingabe einer persönlichen geheimen PIN des Ausweisinhabers.
EA.11	Der Ausweisinhaber muss während der gesamten Gültigkeit des ePA die Möglichkeit haben, den elektronischen Identitätsnachweis bei der Personalausweisbehörde ein- oder ausschalten sowie Adresse und PIN ändern zu lassen.
EA.12a	Auf den ePA soll eine Karten-Zugangsnummer aufgedruckt werden. Diese sollte insbesondere für Prozesse in der Personalausweisbehörde und im hoheitlichen Bereich zum Einsatz kommt. Mit entsprechenden Zugriffszertifikaten und der Karten-Zugangsnummer sollen hoheitliche Stellen und Behörden • Zugriff auf eID-Daten im Chip haben, ohne dass der ePA-Inhaber seine geheime PIN verwenden muss, • Ein- und Ausschalten des elektronischen Identitätsnachweises, • Änderungen von Adressen und PINs durchführen.
EA.12b	Aus Sicherheitsgründen wird die geheime PIN gesperrt, wenn der ePA-Inhaber diese zweimal von drei möglichen Versuchen falsch eingibt. Um den dritten Eingabeversuch zu ermöglichen, kann diese Sperrung durch Eingabe der aufgedruckten Zugangsnummer aufgehoben werden. Dies bedeutet, dass der Inhaber seine geheime PIN noch einmal für den dritten Eingabeversuch freischalten kann. Schlägt auch der dritte Eingabeversuch fehl, ist die geheime PIN vollständig gesperrt. Eine Entsperrung ist dann nur noch mit Eingabe der PUK oder in der Personalausweisbehörde möglich (siehe Kapitel 9.3.4.4). Aufgrund der kontaktlosen Schnittstelle besteht die latente Gefahr von Denial-of-Service (DoS)-Attacken durch fremde Personen auf den elektronischen Identitätsnachweis. Derartige Attacken können z.B. durch vorsätzliches Senden falscher PINs zum ePA umgesetzt werden. Um den ePA-Inhaber vor solchen Missbräuchen zu schützen, kann eine Freischaltung nur mit der oben beschriebenen Zugangsnummer vorgenommen werden.
EA.13	Der Diensteanbieter prüft regelmäßig anhand einer Sperrliste, ob ein elektronischer Personalausweis verloren oder gestohlen gemeldet wurde.
EA.14	Während der Durchführung der gegenseitigen Authentisierung wird zwischen dem ePA und dem Diensteanbieter ein verschlüsselter Kanal aufgebaut, so dass die zu übertragenden personenbezogenen Daten von Dritten nicht mitgelesen werden können.
EA.15	Es werden die Daten übermittelt, die der Diensteanbieter auf Grundlage seines Berechtigungszertifikats angefordert hat und die nicht vom Personalausweisinhaber ausgekreuzt bzw. abgelehnt wurden.

Lfd. Nr.	Anforderung
Anwendung „qualifizierte elektronische Signatur“	
EA.16	Die elektronische Signatur-Anwendung soll eine sichere, rechtsverbindliche und signaturgesetzkonforme elektronische Unterschrift ermöglichen.
EA.17	Die Anwendung muss im Rahmen der Produktion des ePA technisch für die nachträgliche Aufbringung einer QES vorbereitet werden und die gesetzlichen Regelungen (SigG und SigV) berücksichtigen. (vgl.[10])
EA.18	Für die Erzeugung einer qualifizierten elektronischen Signatur muss der elektronische Personalausweis die Anforderungen an eine sichere Signaturerstellungseinheit gemäß Signaturgesetz erfüllen. Hierfür muss der geheime Schlüssel in sicherer Weise auf dem ePA erzeugt oder auf ihn geladen werden. Er darf nicht ausgelesen werden können.
EA.19	Die Anwendungen sind von einander sicher abzuschotten und mit einer eigenen PIN zu sichern. Die Signaturanwendung soll dabei so ausgestaltet werden, dass das mehrmalige nachträgliche Nachladen eines qualifizierten Signaturzertifikates möglich ist. Damit bleibt es dem Inhaber des Personalausweises überlassen, zu welchem Zeitpunkt die Funktion der qualifizierten elektronischen Signatur auf dem Personalausweis aktiviert wird.
EA.20	Die Nachlademöglichkeit eines qualifizierten Signaturzertifikates ermöglicht es dem Inhaber des Personalausweises ein Trustcenter seiner Wahl auszusuchen, das ihm den privaten Schlüssel des qualifizierten Signaturzertifikats auf seinen Personalausweis lädt. Die Kosten für dieses qualifizierte Signaturzertifikat sind vom Inhaber des Personalausweises zu tragen.
Anwendungen allgemein	
EA.21	Es darf keine Möglichkeit bestehen, ausführbaren Programmcode nachträglich in den elektronischen Personalausweis zu laden. Die Anwendungen des elektronischen Personalausweises sind daher nicht updatefähig. Dies bedeutet auch, dass weitere Anwendungen nicht nachgeladen werden können.

Tabelle 14: Anforderungen an die Anwendungen des elektronischen Personalausweises

9.3 Organisatorische Anforderungen

Die Implementierung der neuen elektronischen Funktionen wirkt sich auch auf die gegenwärtigen Prozesse im Lifecycle des elektronischen Personalausweises aus. Die Veränderungen betreffen die Prozessepisoden Beantragung, Produktion, Ausgabe und Nutzung und erfordern dort Anpassungen im Ablauf.

Im Folgenden werden die Änderungen oder Erweiterungen der betroffenen Ist-Prozesse (vgl. Kap. 4.3) skizziert und daraus Anforderungen abgeleitet, die in Zusammenarbeit mit dem zukünftigen Hersteller des elektronischen Personalausweises, den Personalausweis- und sonstigen beteiligten Behörden der Länder im Zuge der Einführung des elektronischen Personalausweises umzusetzen sind. Aus Gründen der Übersichtlichkeit werden die unverändert gebliebenen Prozessschritte in den Prozesstabellen nicht erneut beschrieben.

9.3.1 Prozessepisode 1: Beantragung des elektronischen Personalausweises (Soll)

9.3.1.1 Teilprozess 1.1: Erstmalige Beantragung oder Folgebeantragung (Soll)

Wie bisher können die Bürgerinnen und Bürger einen neuen elektronischen Personalausweis bei ihrer zuständigen Personalausweisbehörde beantragen. Zukünftig wird es die Möglichkeit geben, einen Personalausweis auch im Ausland bei den vom Auswärtigen Amt bestimmten deutschen Auslandsvertretungen zu beantragen.

Bei den einzelnen Schritten der Beantragung ergeben sich aus der geplanten Speicherung biometrischer Merkmale (Gesichtsbild, Fingerabdrücke auf Wunsch) auf dem Chip des elektronischen Personalausweises Veränderungen bei der Datenerfassung und der Versendung der Produktionsdaten an den Dokumentenhersteller. Weiterhin werden den Bürgerinnen und Bürgern bei der Beantragung Informationen rund um den neuen Personalausweis zur Verfügung gestellt.

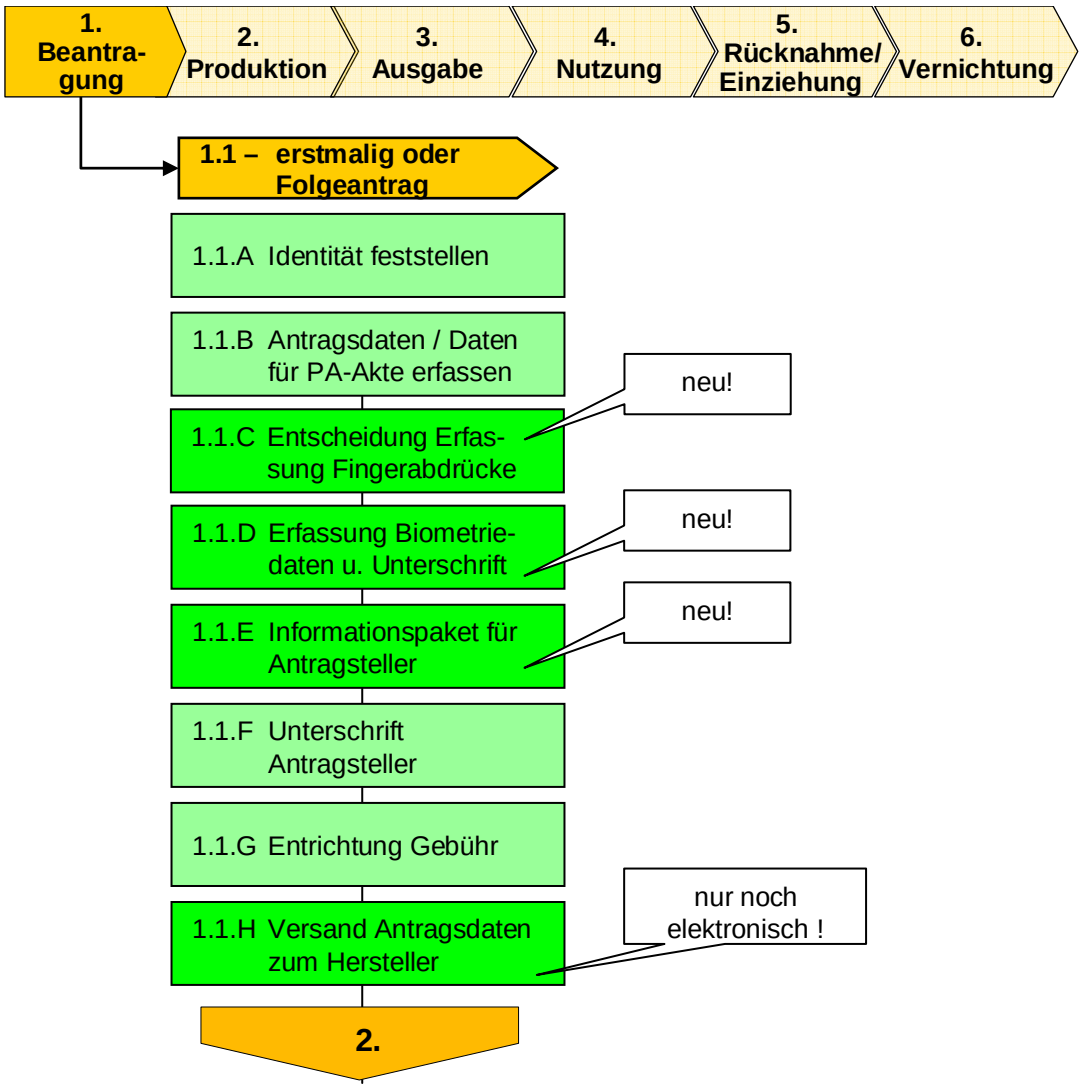

Abbildung 20: Teilprozess 1.1 – Erstmalige Beantragung oder Folgebeantragung (Soll)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
			(…)		
1.1.C	Entscheidung Erfassung Fingerabdrücke	Bürgerin/ Bürger	Die Bürgerin/ der Bürger entscheidet sich, ob seine Fingerabdrücke im Chip des ePA gespeichert werden sollen. Die PA-Behörde hält die Entscheidung der Bürgerin/ des Bürgers schriftlich fest.	Entscheidung der Bürgerin/ des Bürgers ist dokumentiert	
1.1.D	Erfassung Biometriedaten und Unterschrift	PA-Behörde	Scannen des Lichtbildes und Prüfung auf Biometrietauglichkeit In Abhängigkeit der Entscheidung der Bürgerin/ des Bürgers Erfassung von Fingerabdrücken und Prüfung der Biometrietauglichkeit Erfassung der Unterschrift z. B. mit Hilfe eines Grafik-Pads	Biometriedaten und Unterschrift elektronisch erfasst	
1.1.E	Informationspaket für Antragsteller	PA-Behörde	Übergeben eines Informationspaketes zu den neuen Funktionen des Personalausweises inkl. Information des Antragstellers über den elektronischen Identitätsnachweis	Antragsteller erhält Informationen über den neuen PA	Grundlage für die Entscheidung zur Nutzung des elektronischen Identitätsnachweises bei Abholung des neuen PA oder später
			(…)		
1.1.H	Versand Antragsdaten zum Hersteller	PA-Behörde	Zusammenstellen Antragsdaten und elektronischer Versand	Eingang PA-Antrag beim Hersteller	

Tabelle 15: Beschreibung TP 1.1 – Erstmalige Beantragung oder Folgebeantragung (Soll)

Anforderungen aus dem Prozess

Lfd. Nr.	Anforderung
O.1	Die Aufnahme biometrischer Daten im Beantragungsprozess erfordert in allen PA-Behörden die entsprechende Geräte-Infrastruktur (z. B. Scanner für elektronische Bereitstellung des Fotos; Fingerabdruck-Scanner; Lesegeräte zur Verifikation der Daten) und ein elektronisches Antragsverfahren.
O.2	In den meisten Kommunen sind die Pass-Behörden bzw. Bürgerämter auch für Personalausweise zuständig. Durch die angestrebte, zum ePass kompatible Ausgestaltung des elektronischen Personalausweises als biometriegestütztes Reisedokument werden Synergieeffekte hinsichtlich gemeinsam zu nutzender Infrastruktur zur Geltung kommen.
O.3	Das Personal in den PA-Behörden ist entsprechend zu schulen, um die geforderten Qualitätsanforderungen an die Erfassung biometrischer Merkmale sicherzustellen und dem Antragsteller im Erfassungsprozess der Fingerabdrücke Hilfestellung zu geben, soweit nicht im Rahmen der ePass-Einführung geschehen.
O.4	Das Personal der PA-Behörde muss die Antragsteller ausführlich zur Freiwilligkeit der Speicherung der Fingerabdrücke aufklären und die anschließende Entscheidung der Bürgerinnen und Bürger dokumentieren.
O.5	Das Personal der PA-Behörde muss den Antragstellern ausführliche Informationen zum neuen Personalausweis, insbesondere zur freiwilligen Erfassung der Fingerabdrücke und zum elektronischen Identitätsnachweis zur Verfügung stellen. Zu diesem Zweck ist ein Informationspaket auszuhändigen, welches u. a. die neuen Funktionen des PA, die Voraussetzungen zur Nutzung des elektronischen Identitätsnachweises, den Umgang mit PIN und PUK[8], die Möglichkeit des Ein- und Ausschaltens des elektronischen Identitätsnachweises, Anlaufstellen für Verlustmeldungen und Sorgfaltspflichten erläutert.
O.6	In das Verfahren ist ein softwarebasiertes Qualitätssicherungstool einzubetten. Dieses prüft das von der Bürgerin oder dem Bürger bereitgestellte Lichtbild und ggf. die Qualität der von der Bürgerin oder dem Bürger in der Behörde aufgenommenen Fingerabdrücke auf die geforderte Biometrietauglichkeit.
O.7	Die Übertragung der Antragsdaten zum Hersteller des ePA erfolgt verschlüsselt und signiert auf elektronischem Weg. Damit wird u. a. ein Abhören und unbemerktes Verfälschen von Daten ausgeschlossen.

Tabelle 16: Anforderungen TP 1.1 – Erstmalige Beantragung oder Folgebeantragung (Soll)

[8] PUK = Personal Unblocking Key, ein persönlicher Entsperrungsschlüssel, mit dem bei mehrmaliger Fehleingabe der PIN die Karte wieder freigeschaltet werden kann.

9.3.1.2 Teilprozess 1.3: Beantragung nach Änderung (Soll)

Die Bürgerinnen und Bürger haben die Möglichkeit, bestimmte Daten des ePA im Laufe des Lebenszyklus des ePA zu ändern. Dies betrifft insbesondere die Adressdaten. Diese Teilprozesse werden nachfolgend dargestellt.

9.3.1.3 Teilprozess 1.3.2: Beantragung nach Änderung – nur Adresse (Soll)

Ein wichtiges Datum des bisherigen Personalausweises ist die Wohnanschrift des Personalausweisinhabers. Diese wird für vielfältige Geschäftsvorfälle benötigt wie z. B. bei der Paketabholung im Postamt oder der Kontoeröffnung bei einer Bank. Bei der **Adressänderung** wird wie bisher ein Adressaufkleber mit der neuen Adresse aufgebracht und gesiegelt. Zusätzlich wird die neue Adresse auch im Chip des ePA gespeichert.

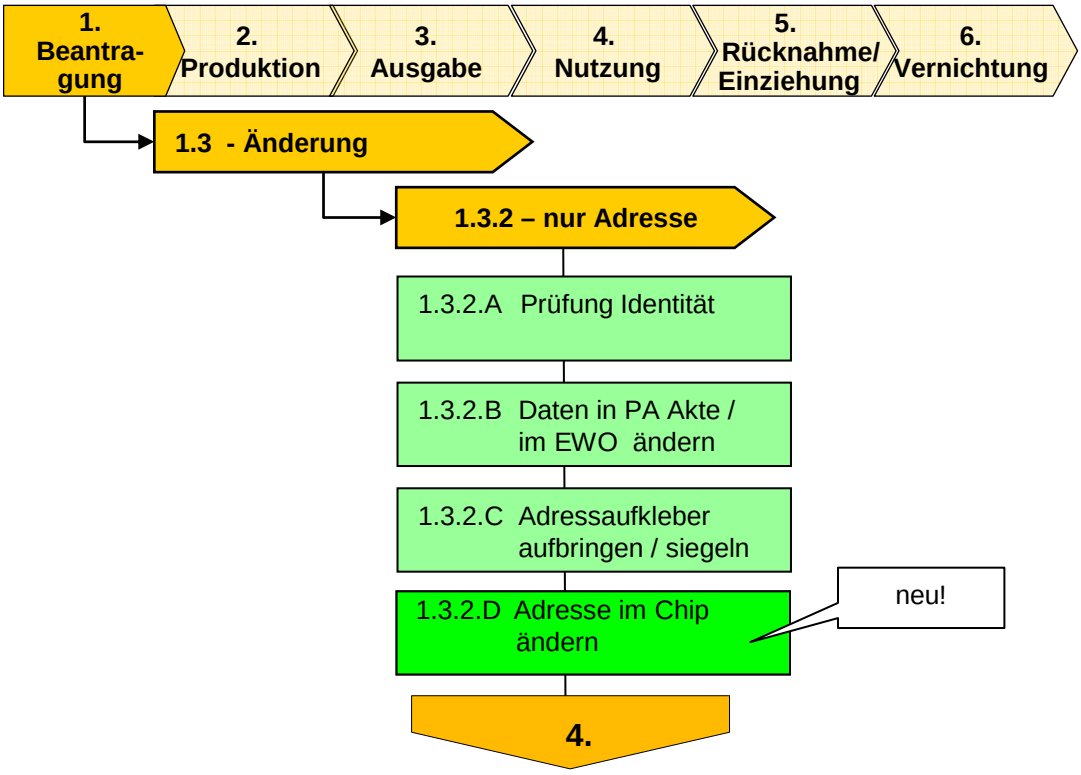

Abbildung 21: Teilprozess 1.3.2 – Beantragung nach Änderung – nur Adresse (Soll)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
			(…)		
1.3.2.D	Adresse im Chip ändern	PA-Behörde/ Meldebehörde	Elektronische Änderung der Adressdaten im Chip gemäß neuer Anschrift mit Berechtigungszertifikat	Adressdaten im Chip aktuell	

Tabelle 17: Beschreibung TP 1.3.2 – Beantragung nach Änderung – nur Adresse (Soll)

Anforderungen aus dem Prozess

Lfd. Nr.	Anforderung
O.8	Die Adressänderung kann ausschließlich von der PA-Behörde vorgenommen werden. Entsprechende Sicherheitsmechanismen (z. B. Zertifikate) sind vorzusehen.
O.9	Bei Änderung der Wohnanschrift des Ausweisinhabers ist die Adresse auf dem elektronischen Personalausweis im Chip zu ändern und ein Adressaufkleber mit geänderter Adresse anzubringen und zu siegeln.

Tabelle 18: Anforderungen TP 1.3.2 – Beantragung nach Änderung – nur Adresse (Soll)

9.3.2 Prozessepisode 2: Produktion des elektronischen Personalausweises (Soll)

Bei der Produktion des elektronischen Personalausweisdokumentes ergeben sich Anpassungen in den Prozessschritten Auftragsdatenerfassung, Produktion der Ausweiskarte sowie der elektronischen Personalisierung (Zuspeicherung der personenbezogenen Merkmale in den im Ausweis integrierten Chip), die Erzeugung und die Versendung eines ePA-Inhaber-spezifischen PIN/PUK-Briefes.

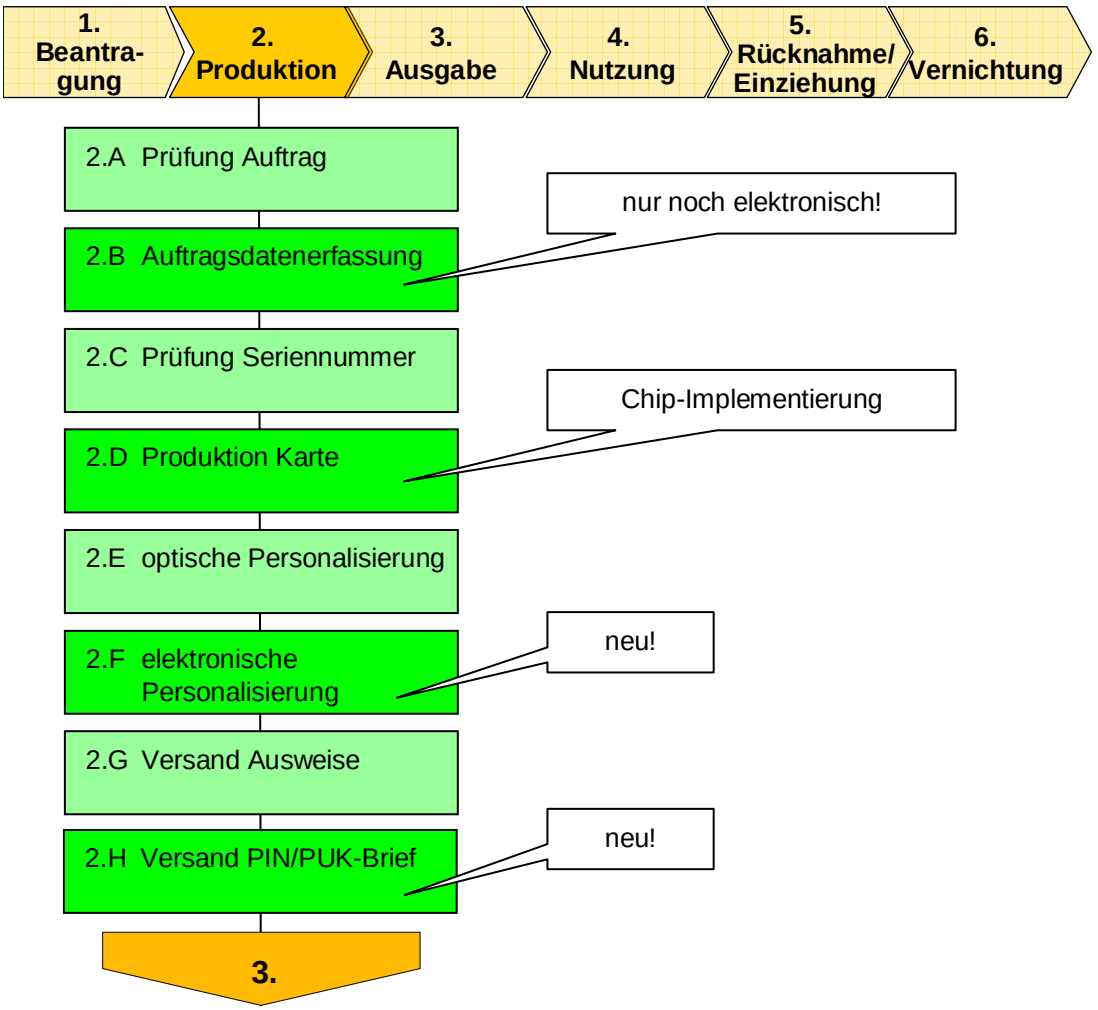

Abbildung 22: Prozessepisode 2 – Produktion des elektronischen Personalausweises (Soll)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
			(…)		
2.B	Auftragsdatenerfassung	Hersteller	Qualitätsprüfung elektronisch übersandter Aufträge	Anträge elektronisch verfügbar	
			(…)		
2.D	Produktion Karte	Hersteller	Produktion des Kartenkörpers und Einbringung von Sicherheitsmerkmalen Implementierung eines Chips in den Kartenkörper	Kartenkörper mit Chip	
			(…)		

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
2.F	Elektronische Personalisierung	Hersteller	Implementierung des Kartenprofils Schreiben der Daten der Biometriefunktion (Personendaten, Gesichtsbild, ggf. Fingerabdrücke) Erzeugung eines Schlüsselpaars (PKI) für den Chip und eines Zertifikats Schreiben der Daten für den elektronischen Identitätsnachweis Erzeugung einer PIN / PUK und des zugehörigen Briefes, Versendung des Briefes nach Auslieferung Aufdruck der Karten-Zugangsnummer, mit der hoheitliche Stellen auf alle Daten im Chip zugreifen können	Daten im Chip gespeichert	
2.H	Versand des PIN / PUK Briefes	Hersteller, Bürgerinnen/ Bürger	Übersendung des Briefes durch den Produzenten erfolgt gemeinsam mit der Information, dass der Ausweis ausgeliefert wurde und in der Ausweisstelle abgeholt werden kann. Der PIN / PUK-Brief enthält zudem das sog. ePA-spezifische „Sperrkennwort“, mit dem die Bürgerin/ der Bürger die eID-Funktion beim Abhandenkommen des Dokuments sperren lassen kann.	PIN/PUK versandt.	
			(…)		

Tabelle 19: Beschreibung Prozessepisode 2 – Produktion des elektronischen Personalausweises (Soll)

Anforderungen aus dem Prozess

Lfd. Nr.	Anforderung
O.10	Im Herstellungsprozess des elektronischen Personalausweises erfolgt zusätzlich die Einbringung des Speicherchips in das Dokument.
O.11	Zur Absicherung gegen unrechtmäßige Ausstellung von Blanko-Dokumenten ist die Herstellung - wie auch heute schon - zentral umzusetzen.
O.12	Neben der optischen Personalisierung erfolgt in einem gesonderten Schritt auch eine elektronische Personalisierung des Ausweisdokuments. Die Gewährleistung der Integrität der Daten und des Zugriffsschutzes erfordern die Anwendung von kryptographischen Verfahren und den Aufbau einer PKI.
O.13	Während der elektronischen Personalisierung muss die Generierung einer/eines zufälligen PIN/PUK zur Nutzung des elektronischen Identitätsnachweises erfolgen.
O.14	Dem Antragsteller wird im Standardfall vom Produzenten ein PIN/PUK-Brief für den elektronischen Identitätsnachweis übersandt. Dieser verbleibt auch dann bei den Bürgerinnen und Bürgern, wenn sie den elektronischen Identitätsnachweis nicht nutzen möchten. Eine Abschaltung kann bei der PA-Behörde während der gesamten Gültigkeitsdauer des Personalausweises beantragt werden.
O.15	Der Ausweisproduzent schaltet automatisch den elektronischen Identitätsnachweis vor Ausgabe des Personalausweises aus, wenn der Antragsteller das 16. Lebensjahr noch nicht vollendet hat. Nach Vollendung des 16. Lebensjahres kann diese auf Antrag durch eine PA-Behörde wieder eingeschaltet werden.

Tabelle 20: Anforderungen Prozessepisode 2 – Produktion des elektronischen Personalausweises (Soll)

9.3.3 Prozessepisode 3: Ausgabe des elektronischen Personalausweises an den Antragsteller (Soll)

Die Prozessepisode zur Ausgabe des elektronischen Personalausweises an den Antragsteller durch die Personalausweisbehörde wird um zwei Schritte – Entscheidung über das Aus- oder Einschalten des elektronischen Identitätsnachweises sowie die optionale Sichtprüfung der im Chip gespeicherten personenbezogenen Daten – erweitert.

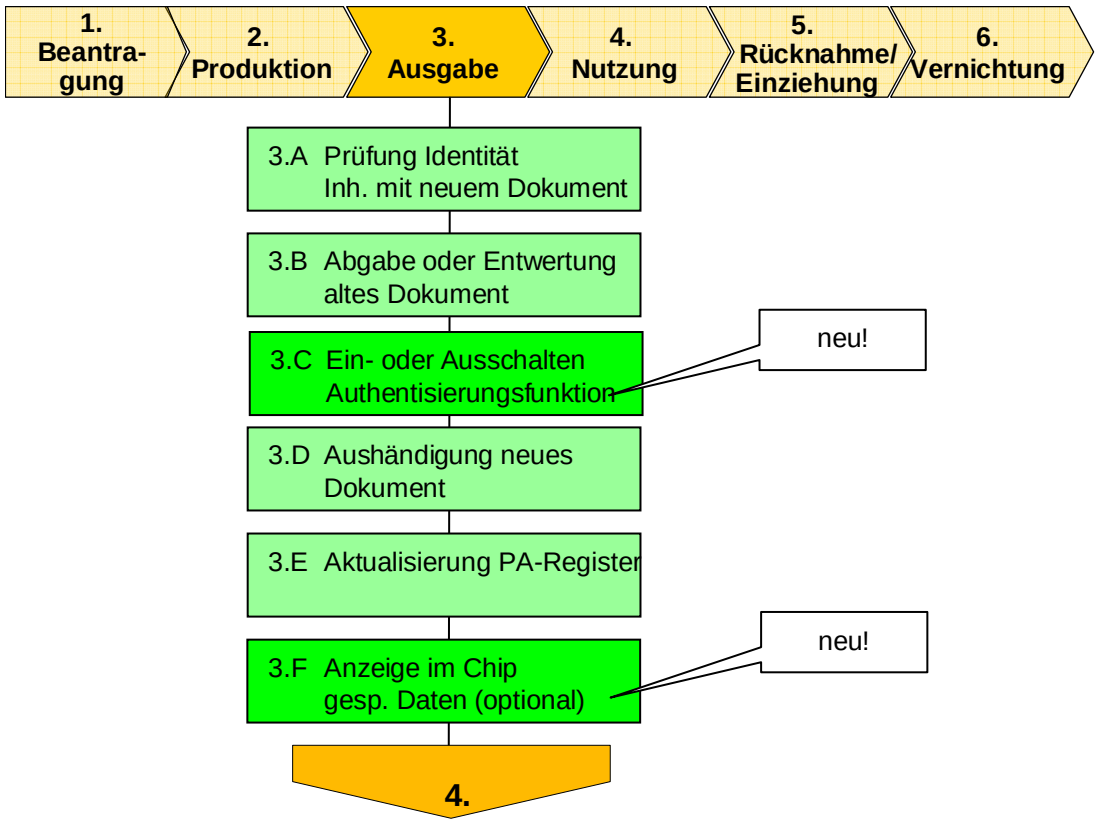

Abbildung 23: Prozessepisode 3 – Ausgabe des elektronischen Personalausweises an den Antragsteller (Soll)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
			(…)		
3.C	Entscheidung Ein- oder Ausschalten des elektronischen Identitätsnachweises	Bürgerinnen/ Bürger/PA-Behörde	Aufgrund des mit Beantragung übergebenen ausführlichen Informationspaketes durch die PA-Behörde an die Bürgerinnen und Bürger weist die PA-Behörde vor Ausgabe des ePA aktiv auf die Entscheidungsmöglichkeit über die Nutzung des elektronischen Identitätsnachweises hin. Entscheidung der Bürgerin oder des Bürgers, ob sie/er den elektronischen Identitätsnachweis nutzen möchte oder aber die Ausschaltung der Funktion auf der Karte verlangt.	Ausschalten des elektronischen Identitätsnachweises	Die Bürgerinnen oder Bürger sollen die letzte Entscheidung über den Nutzungsgrad seines Ausweisdokumentes haben.
3.F	Anzeige im Chip gespeicherter Daten	PA-Behörde, Bürgerinnen/ Bürger	Auflegen des elektronische Personalausweises auf ein spezielles Terminal unter Nutzung der Zugriffskontrollfunktionen Anzeige der Chipdaten am Display des Gerätes	Anzeige der Daten	Nur auf Wunsch der Bürgerin oder des Bürgers

Tabelle 21: Beschreibung Prozessepisode 3 – Ausgabe des elektronischen Personalausweises an den Antragsteller (Soll)

Anforderungen aus dem Prozess

Lfd. Nr.	Anforderung
O.16	Dem Antragsteller ist bei Übergabe seines neuen Ausweises die Möglichkeit zu geben, die im Chip gespeicherten Daten zu prüfen. Dafür sind in den PA-Behörden entsprechende Lesegeräte bereitzustellen, soweit nicht auf die vorhandene Infrastruktur des ePasses zurückgegriffen werden kann.

Tabelle 22: Anforderungen Prozessepisode 3 – Ausgabe des elektronischen Personalausweises an den Antragsteller (Soll)

9.3.4 Prozessepisode 4: Nutzung des elektronischen Personalausweises (Soll)

Der elektronische Personalausweis wird auch weiterhin als Dokument zur Identitätsfeststellung in hoheitlichen Verfahren oder zur Identifizierung des Inhabers gegenüber privaten Dritten verwendet werden können. Durch die Speicherung von Biometriedaten werden im hoheitlichen Bereich die Prüfmöglichkeiten erweitert. Mit der Einführung weiterer elektronischer Funktionalitäten (Identitätsnachweis in elektronischen Transaktionen und elektronische Signatur) erweitert sich auch der Anwendungsbereich bzw. Nutzungsprozess.

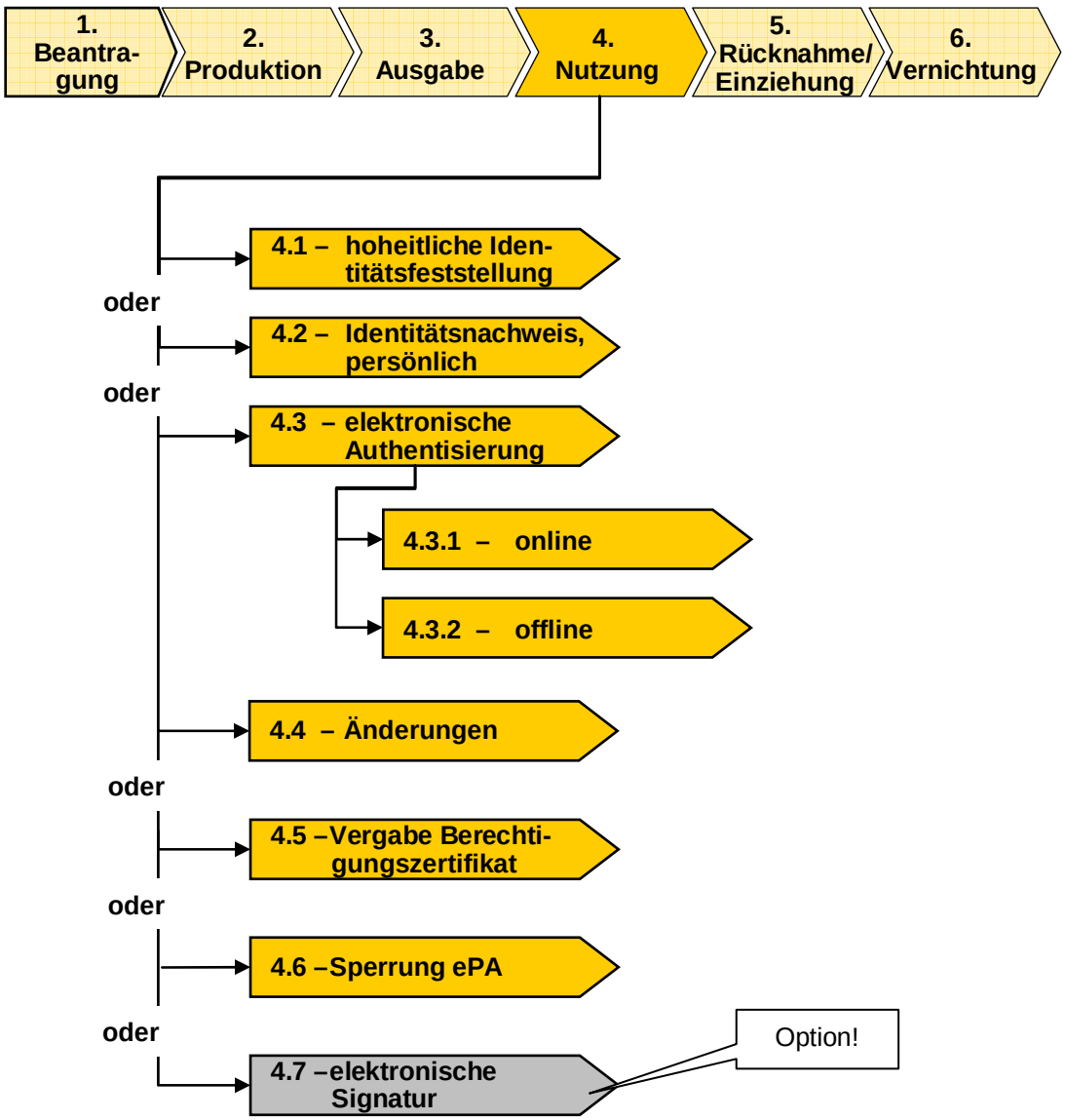

Abbildung 24: Prozessepisode 4 – Nutzung des elektronischen Personalausweises (Soll)

9.3.4.1 Teilprozess 4.1: Nutzung zur hoheitlichen Identitätsfeststellung (Soll)

Die Identitätsprüfung erfolgt nach wie vor durch Inaugenscheinnahme und Vergleich der auf dem Personaldokument optisch sichtbar aufgebrachten körperlichen Merkmale (z. B. Lichtbild, Größe, Augenfarbe, Alter) mit den tatsächlichen körperlichen Merkmalen der zu identifizierenden Person. Hinzu kommt durch die Möglichkeit der elektronischen Erfassung von auf dem Chip speicherbaren Biometriedaten (Gesichtsbild, ggf. der Fingerabdrücke) eine eindeutige Zuordnung des Ausweisdokumentes zu seinem Inhaber.

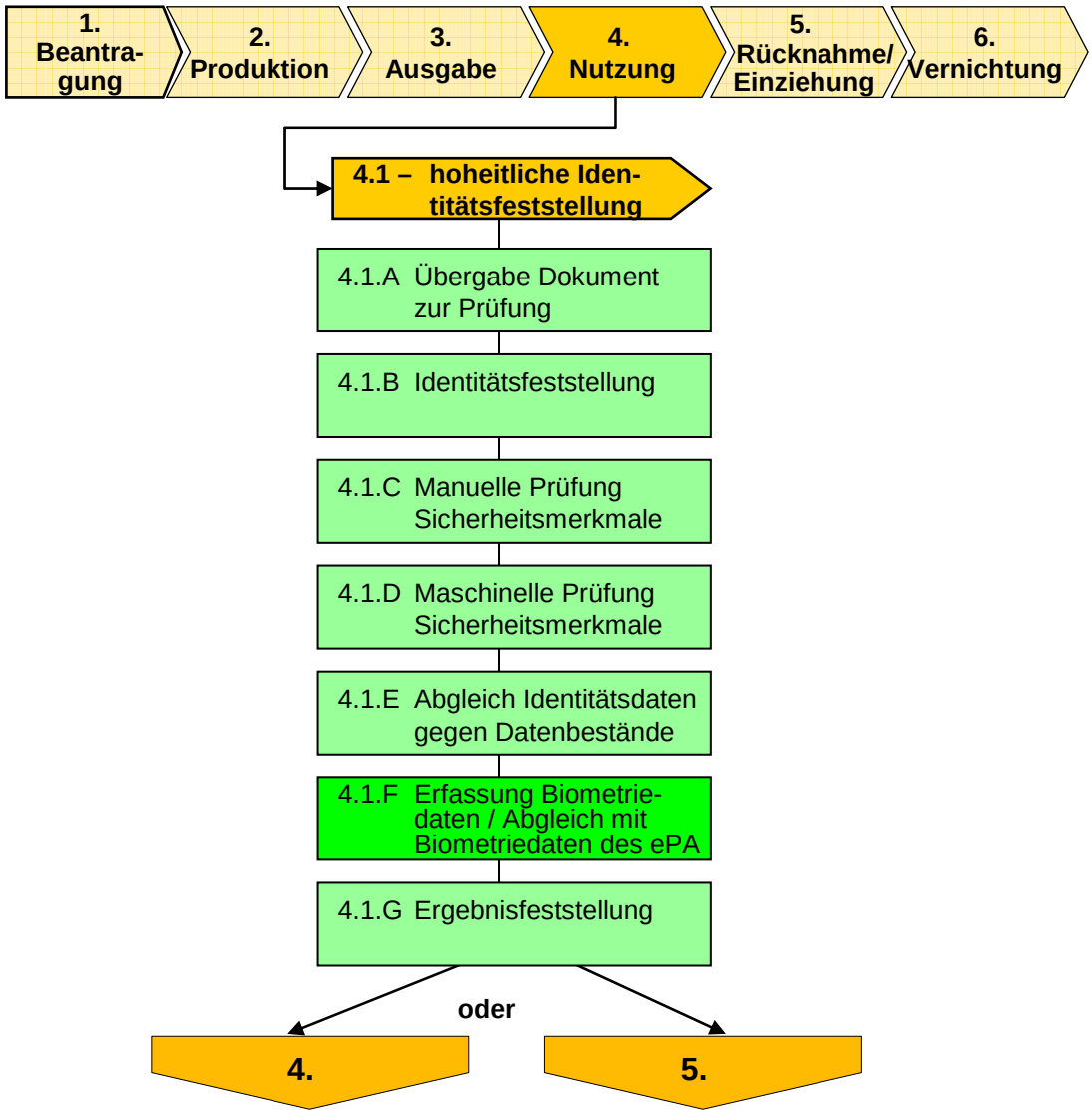

Abbildung 25: Teilprozess 4.1 – Nutzung zur hoheitlichen Identitätsfeststellung (Soll)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
			(…)		
4.1.F	Erfassung Biometriedaten	Grenz- oder Vollzugspolizei, andere Behörde	Aufnahme des Gesichtsbilds und /oder der Fingerabdrücke der Bürgerinnen/ Bürger am Kontrollort Prüfung des Chips des elektronischen Personalausweises auf Authentizität Durchführung der Basic und Extended Access Control Auslesen des Gesichtsbildes und der Fingerabdrücke aus dem Chip Biometrische Berechnung und Abgleich der Ergebnisse der Daten vor Ort mit denen des Chips Anzeige der Ergebnisse	Biometriedaten sind abgeglichen	Die Zugriffskontrolle auf die gespeicherten Daten entspricht den Vorgaben der ICAO und ist Grundlage, um sensible Daten (Fingerabdrücke) aus dem Chip lesen zu können.

Tabelle 23: Beschreibung TP 4.1 – Nutzung zur hoheitlichen Identitätsfeststellung (Soll)

Anforderungen aus dem Prozess

Lfd. Nr.	Anforderung
O.17	Die zusätzliche Nutzung der Biometrie erfordert den Aufbau einer entsprechenden Infrastruktur (Kamera, Fingerprint-Scanner, IT-Verfahren) und deren optimale Einbindung in die bisherigen Prozesse für die maschinelle Prüfung der Sicherheitsmerkmale.
O.18	Auf Grund der Analogie der Biometriefunktion zum ePass sind Synergieeffekte zwischen ePass und ePA weitmöglichst zu nutzen.

Tabelle 24: Anforderungen TP 4.1 – Nutzung zur hoheitlichen Identitätsfeststellung (Soll)

9.3.4.2 Teilprozess 4.3: Nutzung zur elektronischen Authentisierung (Soll)

Das Verfahren zur Authentisierung, d. h., zum zweifelsfreien Nachweis der Identität des Inhabers gegenüber staatlichen Stellen und privaten Dritten, wird mit der Einführung des elektronischen Identitätsnachweises wesentlich erweitert. Es entsteht ein neuer Teilprozess, der den herkömmlichen Prozess des Identitätsnachweises ergänzt. Die elektronische Authentisierung kann sowohl online (z. B. Authentisierung über das Internet) als auch offline erfolgen. Die folgenden Tabellen beschreiben die Prozessabläufe, die im Kern des Verfahrens identisch sind.

Teilprozess 4.3.1: Elektronische Authentisierung – online (Soll)

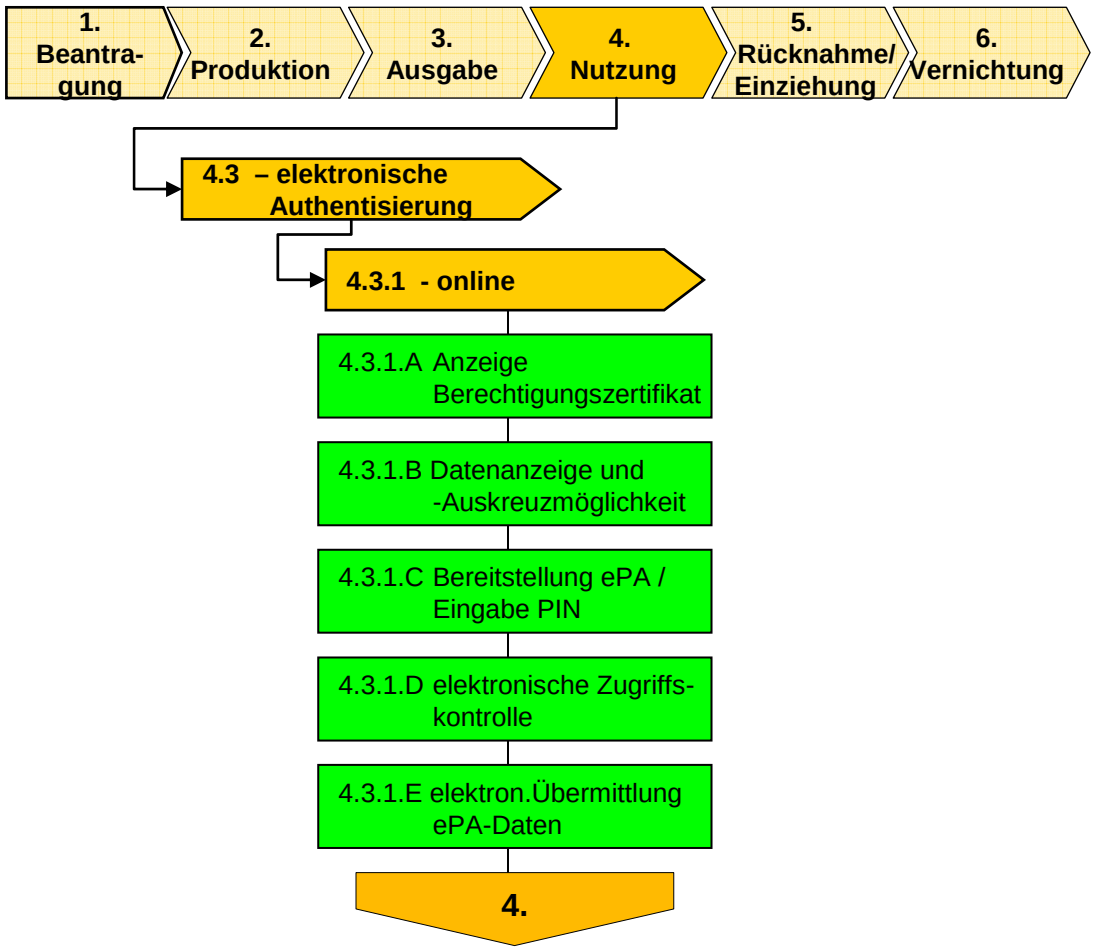

Abbildung 26: Teilprozess 4.3.1 – Elektronische Authentisierung – online (Soll)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
4.3.1.A	Anzeige Berechtigungszertifikat	IT-Verfahren	Anzeige der Daten des Berechtigungszertifikats des Diensteanbieters am Bildschirm	Zertifikatsdaten angezeigt	
4.3.1.B	Datenanzeige/ Auskreuzmöglichkeit	Bürgerinnen/ Bürger	Anzeige der zu übertragenden Daten gemäß des Berechtigungszertifikats des Diensteanbieters Bürgerinnen/Bürger können die Übertragung einzelner Daten durch Auskreuzen ablehnen	Zum Diensteanbieter im Zuge der Authentisierung zu übertragende Daten	

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
4.3.1.C	Bereitstellung elektronischer Personalausweis/ Eingabe PIN	Bürgerinnen/ Bürger	Bereitstellung des elektronischen Personalausweises zum Lesen der Chip-Daten Eingabe PIN als Bestätigung zur Datenfreigabe	PIN-Daten eingegeben	Die Bürgerinnen und Bürger sind mit Übermittlung der nicht abgelehnten Daten einverstanden und machen dies durch PIN-Eingabe deutlich.
4.3.1.D	Elektronische Zugriffskontrolle	IT-Verfahren	Das anfragende IT-Verfahren (z. B. Online-Bestellung) des Diensteanbieters authentisiert sich gegenüber dem Chip (Berechtigung) Chip authentisiert sich gegenüber dem IT-Verfahren als elektronischer Personalausweis Prüfung, ob elektronischer Personalausweis als gestohlen oder verloren gegangen in der Sperrliste vermerkt ist Aufbau einer stark gesicherten Verbindung zwischen Chip und IT-Verfahren des Dienstean-bieters	Chip und IT-Verfahren sind authentisch Stark gesicherte Verbindung (nur wenn elektronischer Personalausweis nicht in Sperrliste), sonst Abbruch und Hinweis	
4.3.1.E	Elektronische Übermittlung der Daten des elektronischen Personalausweises gemäß Berechtigung	IT-Verfahren	Lesen der Daten gemäß Berechtigung und Übertragung zum Dienstean-bieter	Daten werden gemäß Berechtigung und Freigabe zum Diensteanbieters übertragen	Nur Daten des elektronischen Identitätsnachweises, für die eine Berechtigung vorliegt und keine Auskreuzung vorgenommen wurde, können übertragen werden!

Tabelle 25: Beschreibung TP 4.3.1 – Elektronische Authentisierung – online (Soll)

Teilprozess 4.3.2: Elektronische Authentisierung – offline (Soll)

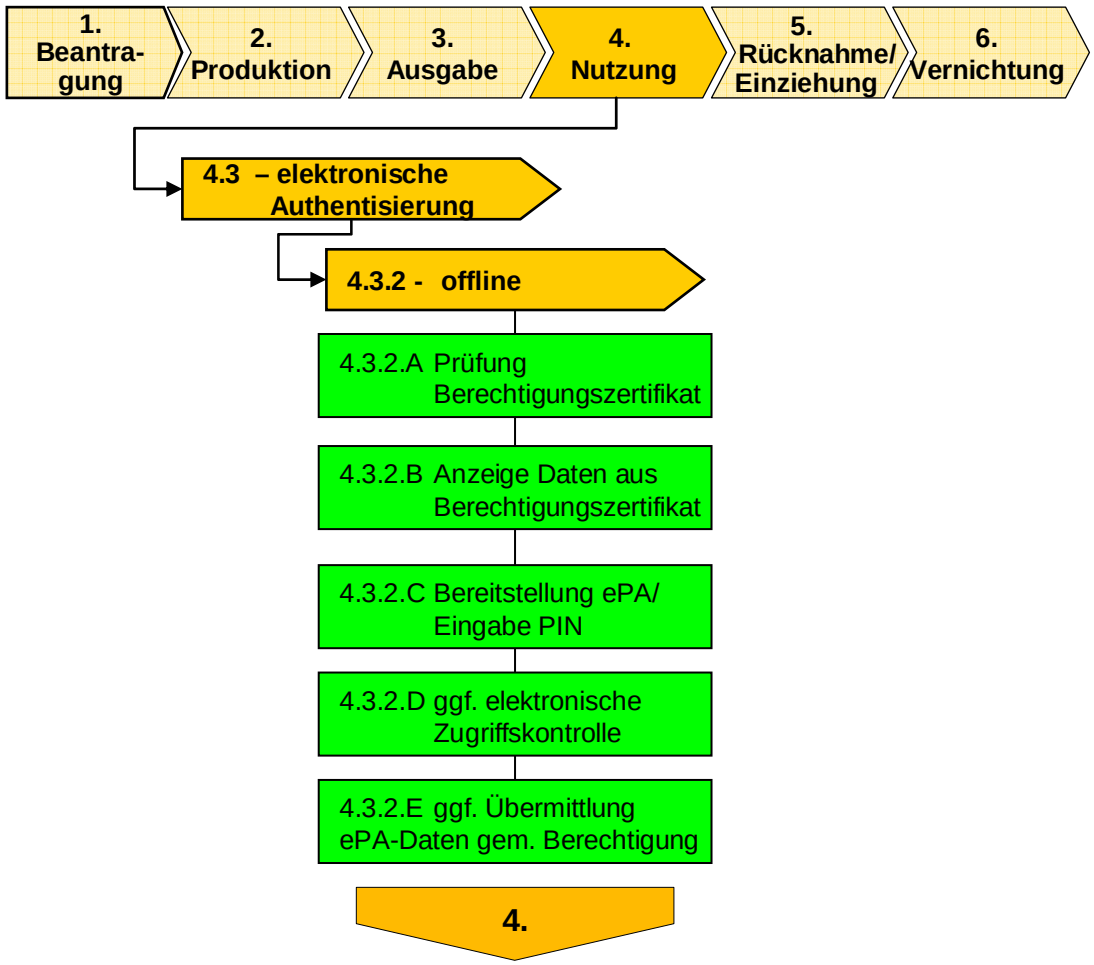

Abbildung 27: Teilprozess 4.3.2 – Elektronische Authentisierung – offline (Soll)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
4.3.2.A	Prüfung Berechtigungszertifikat	Bürgerin/Bürger	Prüfung des Berechtigungszertifikats	Zertifikat geprüft	Voraussetzung: Das Offline-Gerät muss für die Bürgerinnen und Bürger als zertifiziertes Gerät für die Berechtigung zum Auslesen von Daten (z. B. Altersgrenze „über 18“) kenntlich sein.
4.3.2.B	Anzeige Daten aus Berechtigungszertifikat	Bürgerin/ Bürger	Anzeige der Daten aus dem Berechtigungszertifikat des Diensteanbieters	Datenübergabe oder Anzeige der Daten ggf. geschützt durch Siegel	
4.3.2.C	Bereitstellung des e-PA/ Eingabe PIN	Bürgerin/ Bürger	Im Falle des Einsatzes eines Terminals wird der ePA zum Auslesen der Daten übergeben. In diesem Falle wird die PIN des elektronischen Identitätsnachweises eingegeben.	PIN-Daten eingegeben	Bürgerinnen und Bürger sind mit der Übermittlung der Daten gemäß Berechtigungszertifikat einverstanden
4.3.2.D	Ggf. Elektronische Zugriffskontrolle	Offline-Gerät (z.B. Terminal)	Das Offline-Gerät des Diensteanbieters authentisiert sich gegenüber dem Chip (Berechtigung) Chip authentisiert sich gegenüber dem Automat als elektronischer Personalausweis Aufbau einer stark gesicherten Verbindung zwischen Chip und Automat	Chip und Offline-Gerät sind authentisch Stark gesicherte Verbindung	
4.3.2.E	Ggf. Übermittlung der Daten des elektronischen Personalausweises gemäß Berechtigung	IT-Verfahren	Senden der Daten gemäß Berechtigung	Daten gemäß Berechtigung übertragen	Nur Daten des elektronischen Identitätsnachweises (z. B. Altersgrenze „über 16“) können übertragen werden!

Tabelle 26: Beschreibung TP 4.3.2 – Elektronische Authentisierung – offline (Soll)

Anforderungen aus dem Prozess

Lfd. Nr.	Anforderung
O.19	Schaffung von Transparenz für die Beteiligten (Bürgerinnen und Bürger und Diensteanbieter) über Status, Ereignisse und Ergebnisse während des gesamten Authentisierungsprozesses, um eine hohe Akzeptanz für die Funktion zu erreichen.
O.20	Leichte Handhabbarkeit der Funktionen und eine übersichtliche Darstellung der Prozessschritte, deren Folgen und Ergebnisse.
O.21	Bürgerinnen und Bürger haben die vollständige Kontrolle über die zu übertragenden Daten (Auskreuzen) und den Ablauf mit der jederzeitigen Möglichkeit zur Beendigung des Vorgangs.
O.22	Bereitstellung der Softwarevoraussetzungen (Middleware) für eine leichte Installation und sichere Nutzung der Funktion durch Bürgerinnen, Bürger und den Diensteanbieter (z. B. eCard-API, Plugins für Web-Browser).
O.23	Unterstützung der Bürgerinnen und Bürger durch die Bereitstellung von Supportfunktionen (Help Desk, Web Sites, Informationsmaterial).
O.24	Hohe Integrität und Manipulationssicherheit des Prozesses durch starke Verschlüsselung der Kommunikation zwischen ePA und Diensteanbietern.

Tabelle 27: Anforderungen TP 4.3 – Nutzung zur elektronischen Authentisierung (Soll)

9.3.4.3 Teilprozess 4.4: Änderungen während der ePA-Nutzung (Soll)

Während der Nutzungsdauer des ePA sind Änderungen der Authentisierungs-PIN sowie des Status des elektronischen Identitätsnachweises (Ein-/Ausschalten) möglich.

9.3.4.4 Teilprozess 4.4.1: Änderung der PIN (Soll)

Die **Authentisierungs-PIN** dient der Einwilligung zur Übertragung personenbezogener ePA-Daten durch den Inhaber an einen Diensteanbieter. Damit stellt die PIN ein Schlüsselelement des Personalausweises dar. Aus diesem Grund ist es wesentlich, dass der Inhaber seine PIN ändern kann. Die nachfolgenden Möglichkeiten bestehen:

PIN-Änderung bei Vergessen der PIN	Hat die Bürgerin oder der Bürger die PIN vergessen, kann eine PIN-Änderung ausschließlich in der Personalausweisbehörde nach einer eindeutigen Identifizierung durch die Behörde vorgenommen werden. Die Behörde benötigt ein Berechtigungszertifikat.
PIN-Änderung bei Kenntnis der alten PIN	Ist der Bürgerin oder dem Bürger die PIN noch bekannt und sie/er möchte diese ändern, kann dies unter Verwendung der bisherigen PIN am heimischen PC getan werden.
Keine PIN-Änderung durch den PUK	Der PUK dient ausschließlich zum Zurücksetzen des Fehlbedienungszählers. Eine Änderung der PIN ist durch den PUK ausgeschlossen.

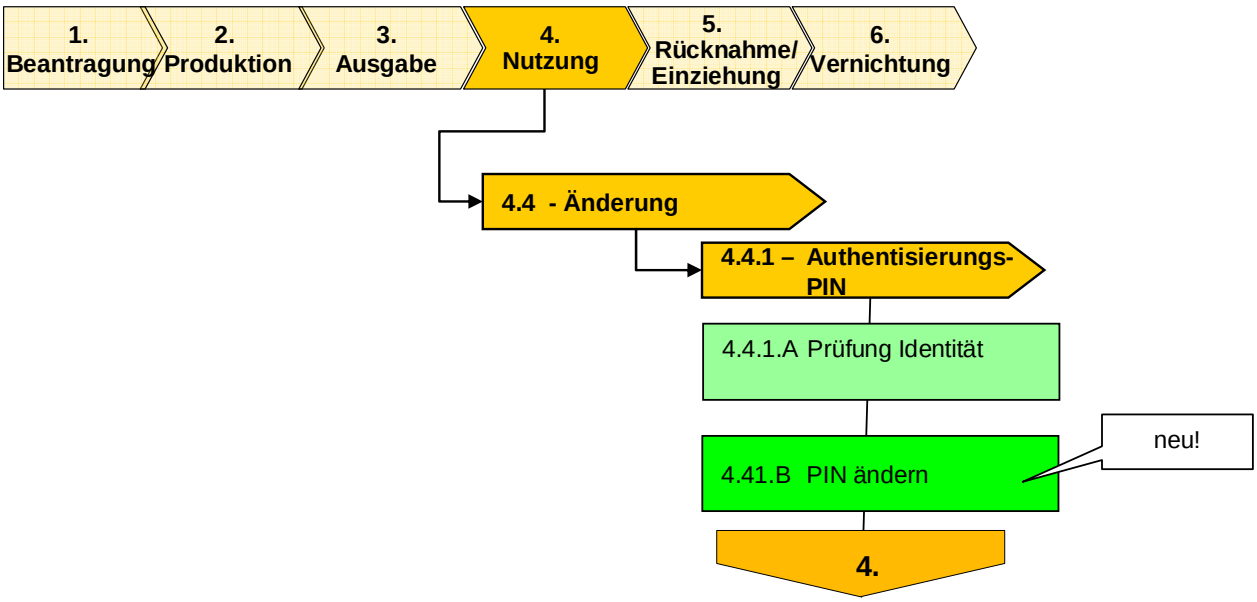

Abbildung 28: Teilprozess 4.4.1 – Änderung der PIN (Soll)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
			(…)		
4.4.1.B	PIN ändern	PA-Behörde / Meldebehörde	Elektronische Änderung PIN im Chip mit Berechtigungszertifikat	Neue PIN	

Tabelle 28: Beschreibung TP 4.4.1 –Änderung der PIN (Soll)

Anforderungen aus dem Prozess

Lfd. Nr.	Anforderung
O.25	Eine vergessene PIN kann ausschließlich von der PA-Behörde neu gesetzt werden. Entsprechende Sicherheitsmechanismen (z. B. Zertifikate) sind vorzusehen.

Tabelle 29: Anforderungen TP 4.4.1 – Änderung der PIN (Soll)

9.3.4.5 Teilprozess 4.4.2: Änderung des Identitätsnachweises (Authentisierungsfunktion) (Soll)

Der Ausweisinhaber kann bei Ausgabe, aber auch während der gesamten Gültigkeitsdauer des Personalausweises entscheiden, ob er den elektronischen Identitätsnachweis nutzen oder ausschalten lassen möchte.

Je nach Entscheidung kann die Funktion durch die PA-Behörde aus- oder eingeschaltet werden. Für Jugendliche, die das 16. Lebensjahr noch nicht erreicht haben, hat der Produ-

zent den elektronischen Identitätsnachweis automatisch vor Ausgabe auszuschalten. Mit Erreichung des 16. Lebensjahres kann der ePA-Inhaber die Funktion wieder einschalten lassen. Nachfolgend wird der Prozess dargestellt:

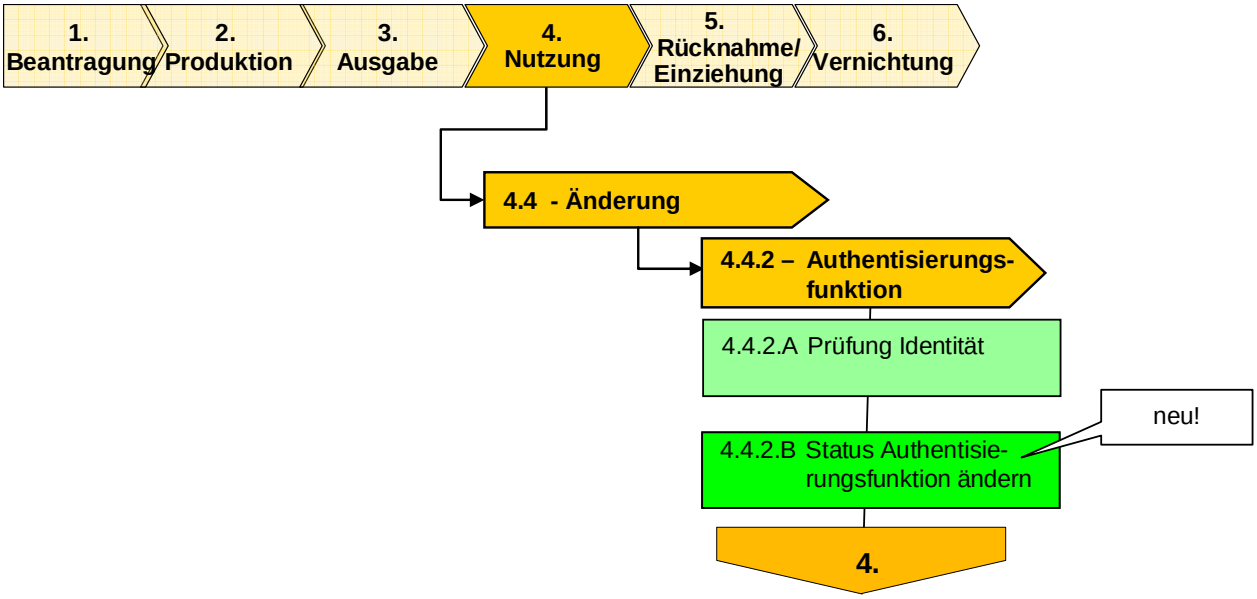

Abbildung 29: Teilprozess 4.4.2 – Änderung der Authentisierungsfunktion (Soll)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
			(…)		
4.4.2.B	Status des elektronischen Identitätsnachweises im Chip ändern	PA-Behörde / Meldebehörde	Elektronische Änderung des Status des elektronischen Identitätsnachweises mit Berechtigungszertifikat	Ein- oder Ausschalten des elektronischen Identitätsnachweises	

Tabelle 30: Beschreibung TP 4.4.2 – Änderung der Authentisierungsfunktion (Soll)

Anforderungen aus dem Prozess

Lfd. Nr.	Anforderung
O.26	Der elektronische Identitätsnachweis kann ausschließlich von der PA-Behörde unter Nutzung eines Berechtigungszertifikats ein- oder ausgeschaltet werden. Entsprechende Sicherheitsmechanismen (z. B. Zertifikate) sind vorzusehen.

Tabelle 31: Anforderungen TP 4.4.2 – Beantragung nach Änderung – Authentisierung (Soll)

9.3.4.6 Teilprozess 4.5: Vergabe Berechtigungszertifikate (Soll)

Bei dem elektronischen Identitätsnachweis handelt es sich um eine neue Funktion des ePA für die sichere Online-Identifizierung. Hierbei sollen potentiellen Geschäftspartnern z. B. im Internet personenbezogene Daten zur Verfügung gestellt werden können. Der Zugriff auf die Daten des ePA wird dabei über sog. „Berechtigungszertifikate“ geregelt, die der Geschäftspartner im Authentisierungsprozess vorweisen muss, um auf bestimmte Datenfelder zugreifen zu können. Die Entscheidung über den Umfang der zu übermittelnden Daten und die endgültige Datenfreigabe selbst liegt in jedem Einzelfall beim Inhaber des elektronischen Personalausweises. Das Berechtigungszertifikat wird über folgende Inhalte verfügen:

1. Name, Anschrift und E-Mail-Adresse des Diensteanbieters
2. Kategorien der angefragten Daten
3. Zweck der Übermittlung
4. Verweis auf die Datenschutzerklärung des Diensteanbieters
5. Hinweis auf die zuständige Datenschutzaufsichtsbehörde
6. Gültigkeitsdauer des Berechtigungszertifikats

Die Prüfung der Zuverlässigkeit des Diensteanbieters erfolgt durch eine staatliche Stelle (Zulassung). Die Einhaltung der datenschutzrechtlichen und sicherheitstechnischen Vorgaben wird durch die zuständigen Aufsichtsbehörden (z. B. Datenschutzbeauftragte der Länder) im Rahmen ihrer regulären Aufgabenerfüllung übernommen.

Erfolgt die Zulassung, werden dem Diensteanbieter die Berechtigungszertifikate ausgestellt.

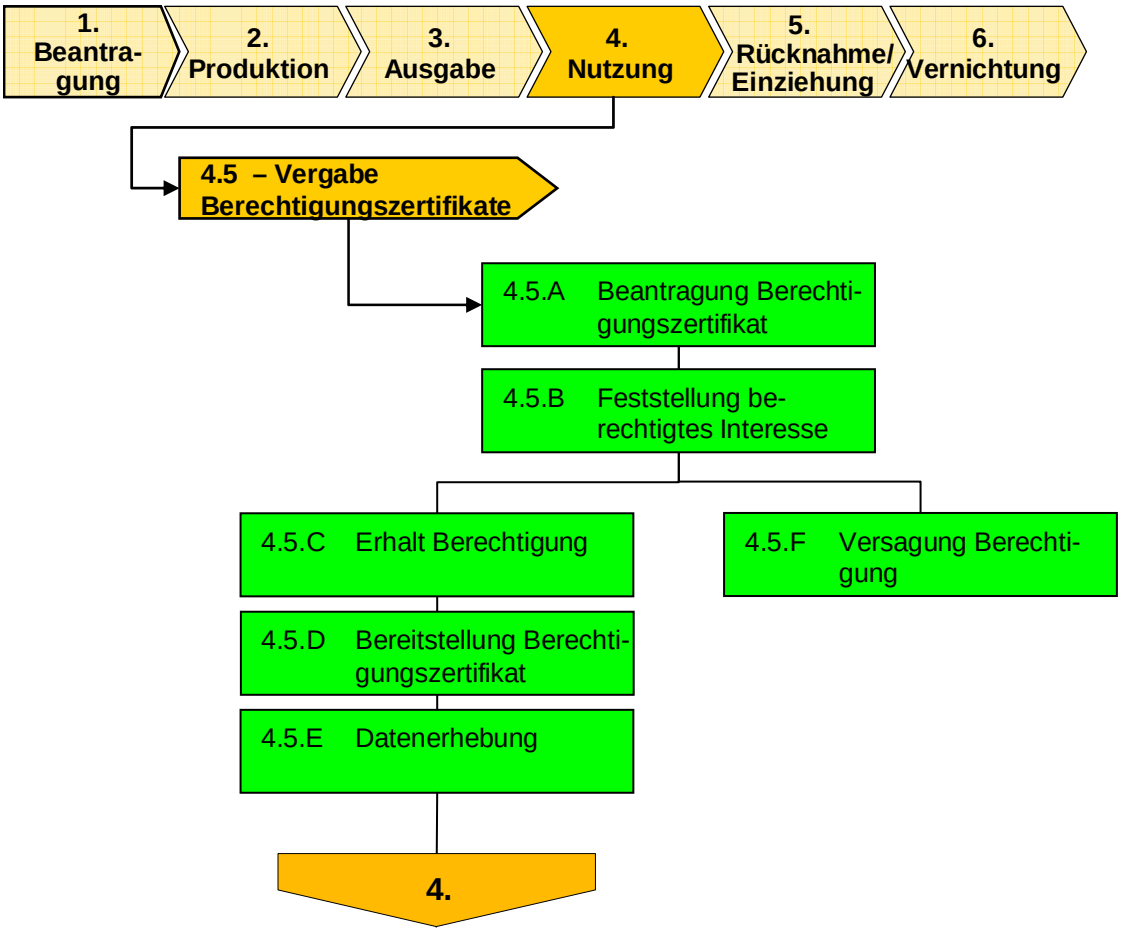

Abbildung 30: Teilprozess 4.5: – Vergabe Berechtigungszertifikate (Soll)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
4.5.A	Beantragung Berechtigung	Dienstean-bieter	Beantragung Berechtigung mit u. a. folgende Daten: Name, Anschrift, E-Mail, Zweck der Übermittlung, Datenschutzerklärung zuständige Datenschutzaufsichtsbehörde, Angaben über die eingesetzte Hard- und Software und Herstellererklärung Es ist darzulegen, dass geeignete (zertifizierte) Software zum Einsatz kommt.	Antrag gestellt	Antragsberechtigt ist jede natürliche oder juristische Person, die im Rahmen von E-Business bzw. E-Government Dienstleistungen erbringen und hierfür die Authentisierungsdaten von Bürgerinnen und Bürgern erheben wollen. Diese müssen ein berechtigtes Interesse für die Nutzung personenbezogenen Daten nachweisen.
4.5.B	Feststellung berechtigtes Interesse	staatliche Stelle	Erforderlichkeitsprüfung über Zweck und Umfang der Authentisierungs-Datenerhebung und -verarbeitung	Erteilung oder Versagung	Die Überprüfung der Erforderlichkeit ist Teil des Verwaltungsverfahrens Die Erteilung der Berechtigung ist ausgeschlossen, wenn der Zweck offensichtlich rechtswidrig ist oder in der geschäftsmäßigen Übermittlung der Daten besteht.

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
4.5.C	Erhalt Berechtigung	Diensteanbieter /staatliche Stelle	Diensteanbieter erhält Berechtigung und wird aufgefordert, ein Schlüsselpaar (geheimer und öffentlicher Schlüssel) mit zertifizierter Crypto-Soft- und Hardware zu erstellen. Den öffentlichen Schlüssel sowie ein https-Zertifikat für die sichere Verbindung zwischen PC des Ausweisinhabers und des Diensteanbieters übergibt der Diensteanbieter auf sicherem Wege an die staatliche Stelle Hieraus generiert die staatliche Stelle das Berechtigungszertifikat und überreicht dieses dem Diensteanbieter.	Zulassung	
4.5.D	Bereitstellung Berechtigungszertifikat	Staatliche Stelle	Das Zertifikat wird mit den festgelegten Inhalten erstellt und signiert.	Erhalt Berechtigungszertifikat	
4.5.E	Datenerhebung	Diensteanbieter	Der Diensteanbieter kann nunmehr ePA-Daten erheben.	Datenerhebung möglich	
4.5.F	Versagung Berechtigung	Diensteanbieter/ staatliche Stelle	Durch Verwaltungsakt wird die Versagung der Zertifikatsausgabe ausgesprochen. Die staatliche Stelle teilt entsprechend die Versagungsgründe mit. Der Diensteanbieter hat die Möglichkeit, Widerspruch einzulegen und ggf. Klage einzureichen.	Versagung	Gründe für Versagung können sein: - Unzulässige Nutzung des Berechtigungszertifikates - Erteilung aufgrund falscher Angaben - Veranlassung der Rücknahme durch die Datenschutzaufsichtsbehörde

Tabelle 32: Teilprozess 4.5: Vergabe Berechtigungszertifikate (Soll)

Berechtigungen für die Erhebung von Authentisierungsdaten werden für einen Zeitraum von drei Jahren vergeben. Berechtigungszertifikate laufen nach ein bis drei Tagen ab. Folgezertifikate sind bei der staatlichen Stelle online abrufbar. Es ist geplant, Berechtigungszertifikate für Offline-Geschäfte über einen längeren Zeitraum auszustellen.

Da der Hardware-Token ePA als Prüfinstanz der Zertifikate keine Sperrlisten herunterladen und speichern kann, wird dieser Prozess über sehr kurze Laufzeiten der Zertifikate abgebildet.

Pseudonyme Authentisierung: Bereichsspezifisches Kennzeichen

Um die in Artikel 5 Grundgesetz garantierte Meinungs- und Informationsfreiheit zu gewährleisten, ist u. a. in § 13 Abs.6 Telemediengesetz (TMG) geregelt, dass ein Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren. Das Bundesdatenschutzgesetz versteht unter **Pseudonymisierung** das "... Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren."

Mit Hilfe des zukünftigen Personalausweises wird diese Forderung für die Diensteanbieter leicht umsetzbar sein. Es wird jedem Diensteanbieter bei der Erteilung eines Berechtigungszertifikates eine eindeutige (zufällig vergebene) Kennnummer zugewiesen. Diese Nummer ist Bestandteil des Berechtigungszertifikats. Bei der Authentisierung eines ePA-Inhabers mittels Pseudonym wird aus dieser Kennummer unter Verwendung eines personalausweisindividuellen Geheimnisses ein sog. bereichsspezifisches Kennzeichen berechnet. Dieses wird als Pseudonym dem Diensteanbieter übermittelt.

Aufgrund der Kopplung von Kennnummer des Diensteanbieters mit dem zusätzlichen Geheimnis des Personalausweises kann der Diensteanbieter den Personalausweis immer eindeutig identifizieren. Da unterschiedliche Diensteanbieter verschiedene Kennnummern besitzen, ist das so berechnete bereichsspezifische Kennzeichen – das Pseudonym – auch für jeden Diensteanbieter unterschiedlich, so dass sich auf diese Weise keine diensteanbieterübergreifenden Nutzerprofile erstellen lassen. Auch ein Raten der Kennnummer ist nicht möglich, da der private Schlüssel des Dienstanbieters bekannt sein müsste.

Anforderungen aus dem Prozess

Lfd. Nr.	Anforderung
O.27	Die Vergabe von Berechtigungszertifikaten an Diensteanbieter zur Nutzung des elektronischen Identitätsnachweises muss über eine Zertifikatsausgabestelle erfolgen.
O.28	Die Berechtigungen werden unter bestimmten Voraussetzungen erteilt. Neben der Angabe der für die Zertifikatserstellung erforderlichen Daten ist hier auch eine Prüfung der datenschutzrechtlichen Erforderlichkeit der Datenabfrage aus elektronischen Personalausweisen für den im Zertifikat genannten Zweck vorzusehen.
O.29	Es ist zu gewährleisten, dass die Diensteanbieter über gültige Zertifikate verfügen.
O.30	Das bereichsspezifische Kennzeichen erlaubt keine Rückrechnung auf die Ursprungsdaten.

Tabelle 33: Anforderungen an den Prozess zur Vergabe von Berechtigungszertifikaten

Zusammenfassend können folgende berechtigte Stellen mit entsprechenden Berechtigungszertifikaten und der auf dem ePA aufgedruckten Zugangsnummer bzw. der geheimen PIN des ePA-Inhabers auf folgende Daten zugreifen:

	Hoheitliche Stellen (ermächtigte Behörden wie im PassG)			**Öffentliche Stellen** (E-Government)		**Nicht-öffentliche Stellen** (E-Business)	
	Berechtigungszertifikat für Biometriedaten + Zugangsnummer	Berechtigungszertifikat für elektronischen Identitätsnachweis + Zugangsnummer	Ohne Berechtigungszertifikat	Berechtigungszertifikat für elektronischen Identitätsnachweis + PIN des Inhabers	Ohne Berechtigungszertifikat	Mit Berechtigungszertifikat für elektronischen Identitätsnachweis + PIN des Inhabers	Ohne Berechtigungszertifikat
Biometriedaten	ja	nein	nein	nein	nein	nein	nein
elektronischer Identitätsnachweis	ja	ja	nein	ja	nein	ja	nein

Tabelle 34: Anforderungen an den Prozess zur Vergabe von Berechtigungszertifikaten

9.3.4.7 Teilprozess 4.6: Sperrliste für verloren gegangene und gestohlene Ausweise (Soll)

Das derzeitige Verfahren für die Anzeige verloren gegangener Personalausweise wird zukünftig um eine Sperrliste für gestohlene und verloren gegangene Personalausweise erweitert. Diese Sperrliste wird in einer zentralen Stelle (Sperrlistenbetreiber) zur Verfügung gestellt. Der Verlust des ePA wird somit weiterhin der Personalausweisbehörde gemeldet. Die Personalausweisbehörde wiederum informiert durch Übermittlung eines Sperrmerkmals (z.B. Öffentlicher Schlüssel) den Sperrlistenbetreiber.

Zusätzlich zum Sperrmerkmal übermittelt die Behörde das Ablaufdatum, damit das Sperrmerkmal nur so lange in der Sperrliste verbleibt, wie das Dokument noch gültig gewesen wäre. Das Ablaufdatum ist lediglich für den Sperrlistenbetreiber bestimmt, der die Liste verwaltet.

Zur Absicherung des Diensteanbieters ist dieser verpflichtet, sich regelmäßig die aktuelle Sperrliste mit den verlorenen oder gestohlenen (und noch gültigen) ePA von den Seiten des Sperrlistenbetreibers herunterzuladen.

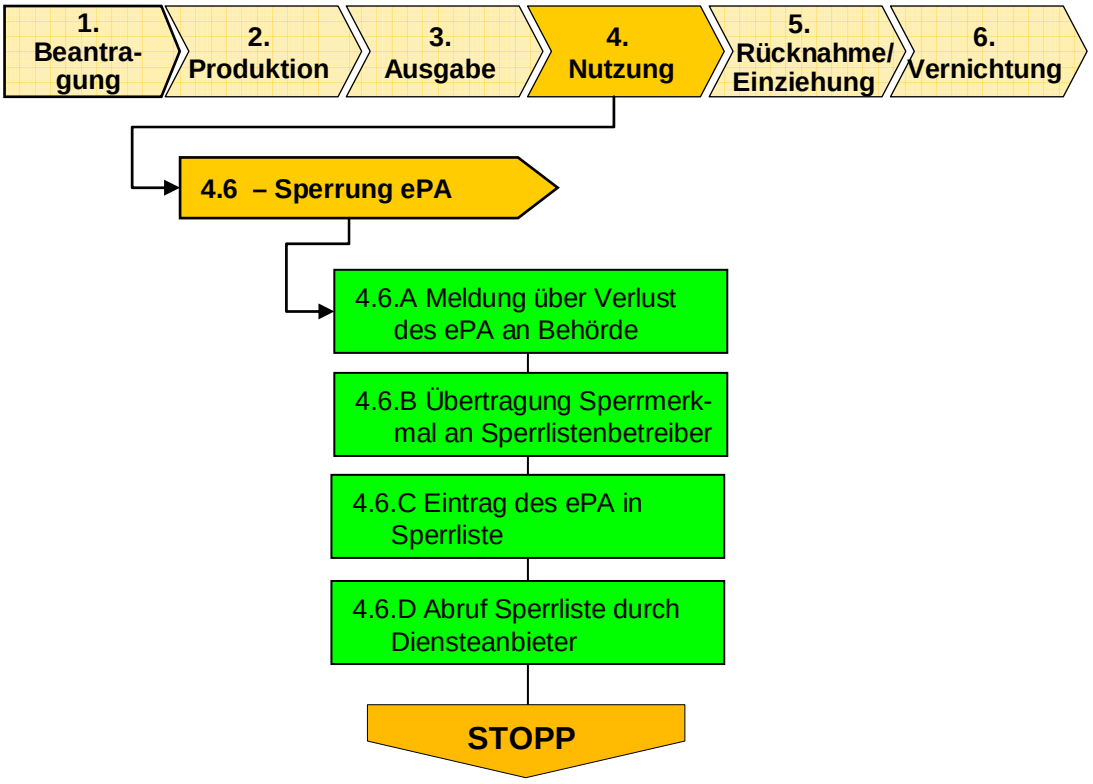

Abbildung 31: Teilprozess 4.6: – Sperrung ePA (Soll)

Lfd. Nr.	Aktivität	Ausführende(r)	Handlung	Ergebnis	Anmerkung
4.6.A	Meldung über Verlust des ePA an Behörde	Bürgerin/ Bürger	Meldung des Verlustes bei Behörde	Meldung	Zukünftig soll die Möglichkeit bestehen, jederzeit über öffentlich verfügbare Kommunikationsverbindungen einen ePA sperren lassen zu können.
4.6.B	Übertragung Sperrmerkmal an Sperrlistenbetreiber	Behörde	Automatische Übertragung des Sperrmerkmals an Sperrlistenbetreiber	Übertragung	
4.6.C	Eintrag des ePA in Sperrliste	Sperrlistenbetreiber	Eintrag in Sperrliste	Sperrung vorgenommen	
4.6.D	Abruf Sperrliste durch Diensteanbieter	Unternehmen	Regelmäßiger Abruf der Sperrliste	Abruf	

Tabelle 355: Teilprozess 4.6: – Sperrung ePA (Soll)

Anforderungen aus dem Prozess

Lfd. Nr.	Anforderung
O.31	Der Inhaber eines Personalausweises ist verpflichtet, der Personalausweisbehörde unverzüglich den Verlust des Ausweises anzuzeigen. Um Missbrauch des elektronischen Identitätsnachweises abhanden gekommener Personalausweise zu verhindern, wird eine Sperrliste eingerichtet.
O.32	Es muss möglich sein, dass Bürgerinnen und Bürger für die Sperrung eine zentrale Rufnummer nutzen können (z.B. D115, 116 116)
O.33	Für die elektronische Übermittlung des Sperrmerkmals muss ein sicherer https-Kanal vom Sperrlistenbetreiber zur Verfügung gestellt werden.
O.34	Der Sperrlistenbetreiber muss eine redundante Infrastruktur zur Verfügung stellen, damit Diensteanbieter die regelmäßige Möglichkeit haben, Sperrlisten abzurufen.
O.35	Der Sperrlistenbetreiber muss einen 365x24x7-Support zur Verfügung stellen.

Tabelle 36: Anforderungen an den Prozess zur Sperrung bei Verlust des ePA

9.3.4.8 Teilprozess 4.7: Elektronische Signatur

Der ePA-Inhaber wird von der PA-Behörde darüber informiert, dass der ePA auch für die optionale Nutzung einer qualifizierten elektronischen Signatur vorbereitet ist. Sollte der Inhaber eine qualifizierte elektronische Signatur nutzen wollen, kann er von einem Zertifizierungsdiensteanbieter (ZDA) ein Signaturzertifikat aufbringen lassen. Weitere Details hierzu werden den Bürgerinnen und Bürgern in Form einer Informationsbroschüre zur QES überlassen.

9.4 Anforderungen an die IT-Sicherheit

Die Sicherheitsanforderungen an die Anwendungen des elektronischen Personalausweises müssen sowohl den Vorgaben des Datenschutzes Rechnung tragen als auch dem Schutz vor Verfälschung dienen. Die bisherigen Erfahrungen zeigen diverse Bedrohungen wie z. B.

- **Diebstahl**,
- **Manipulation des Ausweisdokumentes**,
- **Manipulation an Ausweis-Lesegeräten**,
- **Abhören der Datenkommunikation**,
- **Diebstahl der PIN**,
- **„Man in the Middle“-Attacke**,
- **Skimming** und
- **Phishing**

gegen die auch der elektronische Personalausweis geschützt werden muss.

Die grundsätzlichen Anforderungen an ein umfassendes Sicherheitskonzept für den elektronischen Personalausweis entlang seines Lebenszyklusses von der Beantragung bis zur Vernichtung sind in einem Sicherheitsrahmenkonzept definiert. Es enthält sowohl Vorgaben für die Ausweishersteller als auch Empfehlungen für die Personalausweisbehörden. Bei der Sicherheitskonzeption sind u. a. die folgenden Anforderungen zu berücksichtigen:

Lfd. Nr.	Anforderung
S.1	Es muss ausgeschlossen werden, dass der PA physisch so manipuliert wird, dass eine andere Person die Identität des Ausweisinhabers annehmen kann. Darüber hinaus muss auch eine elektronische Manipulation des Chips ausgeschlossen werden, damit eine andere Person nicht auf elektronischem Weg die Identität des Inhabers annehmen kann.

Lfd. Nr.	Anforderung
S.2	Jede Form von gefälschten oder manipulierten elektronischen Personalausweisen bzw. Teilen davon müssen erkannt werden können.
S.3	Ein elektronischer Personalausweis oder Teile davon dürfen nicht unbemerkt und unberechtigt auf einen anderen ePA kopiert werden können. Einem Missbrauch durch „biometrisch ähnliche“ Personen ist entsprechend vorzubeugen. Dies gilt auch für Authentisierung und Signatur, die kryptographisch an den elektronischen Personalausweis gebunden werden müssen.
S.4	Lesegeräte für den PA müssen so sicher sein, dass ein Eingriff durch Dritte in den Kommunikationsprozess mit dem PA ausgeschlossen werden kann (z. B. durch zertifizierte Leser).
S.5	Der Zugriff auf die personenbezogenen Daten im elektronischen Personalausweis darf nur mit Einwilligung des Benutzers möglich sein (z. B. Freischaltung durch PIN-Eingabe) oder über hoheitliche Berechtigungszertifikate. Zudem darf der elektronische PA oder Teile davon nur von mit Berechtigungszertifikaten versehenen elektronischen Anwendungen gelesen werden können.
S.6	Nach einem Diebstahl der PIN muss es möglich sein, diese zu ändern.
S.7	Die Angreifbarkeit des PA durch eine „Man-in-the-Middle“-Attacke muss ausgeschlossen werden (z. B. durch Chip- und Terminal-Authentisierung).
S.8	Das Abhören der Kommunikation zwischen Diensteanbieter und PA muss ausgeschlossen werden können (z. B. durch Verschlüsselung). Die Verschlüsselung muss auf geeignete kryptographische Verfahren zurückgreifen, die ausreichende Schlüssellängen aufweisen.
S.9	Um sicherzustellen, dass ein elektronischer Personalausweis vertrauenswürdige Sicherheitsmechanismen zur Verfügung stellt, muss der elektronische Personalausweis einer Common Criteria Evaluierung nach angemessenen Schutzprofilen (vgl u. a. [3]) unterzogen werden.

Tabelle 37: Anforderungen an die IT-Sicherheit

9.5 Rechtliche Anforderungen

Die Einführung eines um elektronische Funktionalitäten ergänzten Personalausweises schafft neue Anwendungsfelder, die sowohl Chancen als auch Risiken für die Beteiligten bergen. Dementsprechend sind die rechtlichen Rahmenbedingungen neu zu gestalten.

Das folgende Kapitel stellt zunächst das Gerüst der bestehenden Regelungen dar. In der Folge wird der projektspezifische Anpassungsbedarf erläutert. Das Kapitel schließt mit einem Überblick zu berücksichtigender Regulierungen auf europäischer Ebene.

9.5.1 Nationales Recht

9.5.1.1 Personalausweisrecht des Bundes und der Länder

Der bisherige Personalausweis ist ein nationales Dokument zum Identitätsnachweis, das in hoheitlichen und privaten Zusammenhängen verwendet wird. Ausgehend von dieser Funktionalität regelt das Gesetz über Personalausweise und zugehöriges Verordnungsrecht im Wesentlichen den Inhalt, das Aussehen, die verbundenen Prozesse, die zugehörige Registerstruktur und die Verwendungsmöglichkeiten des Dokuments und der enthaltenen personenbezogenen Daten sowie mit dem Dokument verbundene Rechte und Pflichten.

Lfd. Nr.	Anforderung
R.1	Das Personalausweisrecht wird insbesondere in Hinblick auf die nunmehr auch elektronisch vorgehaltenen personenbezogenen Daten, einen vollständigen elektronischen Antragsprozess, die visuell sichtbaren Datenkategorien und die neue Form und Optik des Personalausweises zu überarbeiten sein. Weitere Anpassungen betreffen die nachfolgend behandelten Themenbereiche, gleichwohl dürften spezialgesetzliche Regelungen - soweit diese erforderlich werden – i. d. R. im Personalausweisrecht zu verorten sein.

Tabelle 38: Änderungsanforderungen Personalausweisrecht des Bundes

Aufgrund der bis 2006 ausgestalteten Kompetenz im Ausweisrecht existieren Ausführungsgesetze der Länder zum Personalausweisgesetz, die insbesondere zuständigkeitsrechtliche Fragen, aber auch Verfahren bei Verlust und andere praktisch relevante Konstellationen regeln. Mit Verabschiedung der Föderalismusreform ist die ausschließliche Gesetzgebungskompetenz für das Personalausweisrecht im September 2006 auf den Bund übergegangen, so dass hier eine Vereinheitlichung durch Übernahme von landesrechtlichen Regelungen in das Personalausweisgesetz möglich geworden ist.

Lfd. Nr.	Anforderung
R.2	Durch den Übergang der ausschließlichen Gesetzgebungskompetenz für das nationale Personalausweisrecht im Rahmen der Föderalismusreform auf den Bund sind die bisher landesrechtlich getroffenen Regelungen zu vereinheitlichen und in das nationale PersAuswG zu überführen, soweit sie nicht die Kompetenzzuweisung für Aufgaben nach dem PersAuswG an Landesbehörden die ausschließliche Organisationskompetenz der Länder betreffen.

Tabelle 39: Änderungsanforderungen Personalausweisrecht der Länder

9.5.1.2 Spezialgesetzliche Vorschriften

Eine Vielzahl von spezialgesetzlichen Vorschriften enthalten Regelungen zur Identifizierung von Personen, die den Personalausweis ausdrücklich als anerkannte oder vorgeschriebene Form der Identifizierung vorsehen. Der Bereich, den diese Vorschriften abdecken, ist stark heterogen und reicht von diversen Wahlordnungen über Prüfungsvorschriften für staatliche Führerscheine bis hin zu kreditwirtschaftlichen Vorgaben zur Verhinderung von Geldwäsche.

Lfd. Nr.	Anforderung
R.3	Mit der Einführung neuer Funktionalitäten ist zu prüfen, inwieweit die jeweiligen spezialgesetzlich vorgesehenen Identifizierungen auch mittels der neuen Identifizierungsmöglichkeiten, insbesondere des elektronischen Identitätsnachweises wahrgenommen werden können. Je nach Ergebnis ist hier entweder eine Erstreckung der gesetzlich vorgesehenen „Identifizierung mittels Personalausweis“ auf die elektronische Authentisierung zu regeln oder aber die Authentisierung ist für bestimmte Verfahren explizit zuzulassen.

Tabelle 40: Änderungsanforderungen spezialgesetzliche Vorschriften

9.5.1.3 Integration biometrischer Merkmale

Nach dem terroristischen Anschlag vom 11. September 2001 in den USA wurde im Rahmen der Anti-Terror-Gesetzgebung in Deutschland auch das PersAuswG angepasst. Seitdem können in Folge des Terrorismusbekämpfungsgesetzes bei Vorhandensein eines entsprechenden Bundesgesetzes neben den vorhandenen personenbezogenen Daten zur Identifizierung auch weitere biometrische Merkmale gespeichert und zur Identitätsfeststellung genutzt werden. Die konkrete Ausgestaltung dieser Merkmale und ihrer Nutzung muss in einem entsprechenden Bundesgesetz geregelt werden. In Hinblick auf die geplante Einführung auf einem Chip vorgehaltener biometrischer Merkmale für den elektronischen Personalausweis soll zum Erhalt der Einsatzmöglichkeit als Reisedokument eine weitgehende Kompatibilität zum ePass erreicht werden. Rechtliche Rahmenbedingungen für die Einbeziehung biometrischer Merkmale sind mit dem neuen Passgesetz und dem zugehörigen Verordnungsrecht erarbeitet worden und können insofern als Vorlage für personalausweisrechtliche Regelun-

gen dienen.

Lfd. Nr.	Anforderung
R.4	Für die Integration elektronisch vorgehaltener biometrischer Merkmale ist die Verweisstruktur der Regelungen des Passgesetzes zu übernehmen. Inhaltlich sind die Regelungen auf den Personalausweis anzupassen, dies betrifft insbesondere das Verordnungsrecht (Anpassung der TR PDÜ auf Format und Funktionen des elektronischen Personalausweises).

Tabelle 41: Änderungsanforderungen aus der Integration biometrischer Merkmale

9.5.1.4 Elektronische Authentisierung und qualifizierte elektronische Signatur

Gänzlich neue rechtliche Rahmenbedingungen werden für den elektronischen Identitätsnachweis des elektronischen Personalausweises erarbeitet. Hierzu wird der Bund eine Infrastruktur zur elektronischen Authentisierung der Bürgerinnen und Bürger gegenüber privaten und öffentlichen Stellen schaffen. Um das Vertrauen in das Dokument zu sichern, ist ein klarer Rechtsrahmen für die Einsatzmöglichkeiten und -grenzen der elektronischen Authentisierung zu schaffen. Außerdem sind die Rechte und Pflichten der Beteiligten bei der Verwendung des elektronischen Identitätsnachweises zu definieren. Bei der Vertrauensbildung werden Berechtigungszertifikate für Stellen, die verifizierte Daten aus elektronischen Personalausweisen abrufen möchten, eine wesentliche Rolle spielen. Dafür ist eine Infrastruktur zur Vergabe von Berechtigungszertifikaten zu etablieren, die das Sicherheitsinteresse der Bürgerinnen und Bürger und des Staates berücksichtigt und einen effektiven Vergabe- und Nutzungsprozess für die Zertifikatsempfänger sicherstellt.

In den elektronischen Personalausweis soll von den Bürgerinnen und Bürgern auch eine qualifizierte elektronische Signatur integriert werden können. Das Signaturrecht regelt im Signaturgesetz und in der Signaturverordnung Anforderungen an Signaturanbieter und die Arten verfügbarer elektronischer Signaturen. Auf dieser Infrastruktur können und sollen optional auf dem elektronischen Personalausweis speicherbare Signaturen grundsätzlich aufsetzen.

Lfd. Nr.	Anforderung
Künftiger elektronischer Identitätsnachweis	
R.5	Neue rechtliche Rahmenbedingungen für den elektronischen Identitätsnachweis des elektronischen Personalausweises müssen erarbeitet werden. Dazu gehört ein klarer Rechtsrahmen für die Einsatzmöglichkeiten und -grenzen und die Rechte und Pflichten der Beteiligten beim Einsatz des elektronischen Identitätsnachweises. Außerdem ist eine Infrastruktur zur Vergabe von Berechtigungszertifikaten aufzubauen. Hier sind neben den Zertifikatsausstellern insbesondere die zu prüfenden Anforderungen für den Erhalt einer Berechtigung und die Kontrolle des Fortbestehens der Ausstellungsvoraussetzungen festzulegen.
Künftige Verwendung des Personalausweises als Träger einer qualifizierten elektronischen Signatur	
R.6	In Hinblick auf die Integration von qualifizierten elektronischen Signaturen in den elektronischen Personalausweis soll grundsätzlich auf die Anforderungen und Wirkungen gem. Signaturgesetz verwiesen werden. Gleichwohl ist zu regeln, von wem in welcher Form und zu welcher Zeit Signaturen auf das Dokument aufgebracht werden können. Die Gültigkeitsdauern von elektronischen Personalausweisen und elektronischen Signaturzertifikaten sind zu harmonisieren (SigG Zertifikate z. B. 2x5 Jahre). Das bedeutet, dass ein mehrmaliges Nachladen eines Signaturzertifikats möglich sein muss. Außerdem können bestimmte Ausgestaltungsformen des Personalausweises weitere Anpassungen des Signaturrechts erforderlich machen. So ist bisher die qualifizierte elektronische Signatur auf Basis kontaktloser Signaturkarten nicht zulässig. Da der elektronische Personalausweis ausschließlich mit kontaktlosen Schnittstellen produziert werden soll, wird eine Anpassung erforderlich.

Tabelle 42: Änderungsanforderungen aus dem elektronischen Identitätsnachweis und der elektronischen Signaturfunktion

9.5.1.5 Datenschutz und IT-Sicherheit

Bereits bisher gingen mit dem Personalausweis eine Reihe sensitiver datenschutzrechtlicher Fragestellungen einher, die durch allgemeines Datenschutzrecht, insbesondere das Bundesdatenschutzgesetz, grundsätzlich geregelt werden. Diese Regelungen werden um personalausweisspezifische Regelungen im Personalausweisrecht – insbesondere der Umfang mit personenbezogenen Daten, dem Personalausweisregister, die Verwendung der Seriennummer sowie Zertifikatsschlüssel – spezifiziert und ergänzt.

Lfd. Nr.	Anforderung
Datenschutz und IT-Sicherheit	
R.7	Durch die Einbindung elektronischer Funktionalitäten sind künftig auch Fragestellungen im Kontext der IT-Sicherheit und daraus resultierender Verantwortlichkeiten rechtlich zu klären. Über grundsätzliche Regelungen im Datenschutzrecht hinaus werden hier auch bereichsspezifische Regelungen z. B. zum Umgang mit PINs etc. zu treffen sein. Aufgrund der Integration von Zertifikaten und Schlüsseln, die als eindeutige Personenkennzeichen für die Gültigkeitsdauer des Personalausweises verwendet werden können, sind den Regelungen zur Seriennummer äquivalente Vorkehrungen zum Schutz des allgemeinen Persönlichkeitsrechts zu treffen. Darüber hinaus wird eine klare Trennung der unterschiedlichen Nutzergruppen für unterschiedliche Funktionalitäten vorzunehmen sein (so ist z. B. die Nutzung biometrischer Daten ausschließlich der hoheitlichen Identifizierung vorzubehalten).

Tabelle 43: Änderungsanforderungen Datenschutz, IT-Sicherheit und Haftungsrecht

9.5.1.6 Weitere Regelungen (insbes. Verordnungsrecht)

Mit Einführung des ePasses mit Fingerabdruckdaten in Deutschland hat das Bundesamt für Sicherheit in der Informationstechnik eine technische Richtlinie zur Produktionsdatenerfassung, Produktionsdatenqualitätsprüfung und -übermittlung für Pässe (TR PDÜ) erstellt. Die TR PDÜ beinhaltet Anforderungen an die Passdatenerfassungs- und Kommunikationssoftware sowie an die Hardware zur Erfassung biometrischer Daten.

Für den ePA ist analog zu der TR PDÜ für Pässe eine TR für elektronische Personalausweise zu erstellen. Diese Richtlinie wird die Inhalte der TR PDÜ für den ePass weitgehend übernehmen, da Datenerfassung und -übermittlung im Wesentlichen den Anforderungen des ePasses entsprechen. Eine eigenständige TR PDÜ „elektronischer Personalausweis“ erscheint notwendig, da in der TR PDÜ ePass z. B. gesetzliche Grundlagen referenziert werden, die nur für den ePass gelten. Darüber hinaus werden absehbar weitere technische Richtlinien erforderlich (z. B. TR EAC, TR eID, TR QES). Die konkrete Ausprägung und inhaltliche Gestaltung erfolgt im Rahmen des Verordnungsgebungsverfahrens.

9.5.2 Rechtliche Bezüge innerhalb Europas

9.5.2.1 Zuständigkeit

Die Ausgabe von Personalausweisen befindet sich derzeit in der Verantwortung der einzelnen Mitgliedsstaaten. Zwar sieht der Entwurf der neuen Europäischen Verfassung eine Zuständigkeitsregelung der Europäischen Union zur Einführung eines europäischen Identitätsdokuments vor, doch ist ein Inkrafttreten der Verfassung zum jetzigen Zeitpunkt nicht absehbar, so dass ein nationaler Handlungsbedarf der Fortentwicklung bestehen bleibt.

Auch wenn eigene Regelungen zu nationalen ID-Karten zuständigkeitsbedingt nicht bestehen, wird die Ausgestaltung des Personalausweises durch andere EU-Vorgaben doch zumindest mittelbar gleichwohl faktisch bindend beeinflusst.

9.5.2.2 Vorgaben der EU

Der Erhalt der Eigenschaft des elektronischen Personalausweises als Passersatz macht eine kompatible Ausgestaltung zum ePass erforderlich. Daher werden die in der Verordnung des Rates über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger (VO des Rates (EG) Nr. 2252/2004 (vgl. [2])) enthaltenen Anforderungen insbesondere in Bezug auf die ICAO entsprechend berücksichtigt. Eine Verpflichtung zur Aufnahme der Fingerabdrücke in Personalausweisen besteht nach den Regularien der EU und der ICAO nicht.

Im EU-Ratsdokument 14390/05 werden gemeinsame Standards für nationale Ausweissysteme der Mitgliedsländer der Europäischen Union festgelegt. Hierdurch erfolgt eine Bindung an die ePass-Vorgaben der ICAO, sowohl bezüglich der minimalen Sicherheitsstandards, als auch bezüglich der weiteren Vorgehensweise im Hinblick auf die Anwendung biometrischer Verfahren.

Weitere Vorgaben insbesondere im Hinblick auf den Einsatz des elektronischen Personalausweises als Identitätsdokument bei der Grenzkontrolle ergeben sich auch aus VO (EG) Nr. 2133/2004 (Schengener Informationssystem).

9.6 Wirtschaftliche Anforderungen

Die neuen Funktionen des elektronischen Personalausweises und die damit verbundenen Vorteile sind mit möglichst geringem Aufwand für die Bürgerinnen und Bürger, die Wirtschaft und den Staat nutzbar zu machen.

Generell ist zu berücksichtigen, dass das deutsche Personalausweisrecht eine Ausweispflicht vorschreibt. Es ist daher darauf zu achten, dass für den elektronischen Personalausweis keine unverhältnismäßig hohen Gebühren verlangt werden und die Prozesse entlang des gesamten Lifecycle des elektronischen Personalausweises (vgl. Kap. 4.3 und 9.3) im Sinne einer möglichst kostengünstigen Abwicklung gestaltet werden.

Der elektronische Personalausweis wird die Abwicklung elektronischer Geschäftsprozesse revolutionieren. Unternehmen werden zukünftig in der Lage sein, elektronische Dienste anzubieten, die der Identitätsprüfung einer Bürgerin bzw. eines Bürgers bedürfen und bisher nicht vertrauenswürdig online durchgeführt werden können.

Darüber hinaus wird das Beantragungsverfahren dem des elektronischen Reisepasses angeglichen, so dass zukünftig ausschließlich **eine** elektronische Antragsdatenübermittlung möglich ist. Verfahrensvereinfachungen sind die Folge.

Die Diensteanbieter erhalten durch den elektronischen Identitätsnachweis – unter Verwendung von Berechtigungszertifikaten – personenbezogene Daten und können so auf alternative und kostenträchtige Identifizierungsverfahren, verzichten.

Ein Teil dieses Einsparungspotentials könnte zur Finanzierung der für den elektronischen Identitätsnachweis notwendigen Infrastruktur genutzt werden. Die Diensteanbieter werden für die Berechtigungszertifikate eine Gebühr entrichten müssen.

Die Höhe der Gebühr könnte sich bspw. an der Anzahl der Transaktionen oder an der Nutzungsdauer orientieren.

Lfd. Nr.	Anforderung
Allgemein	
W.1	Funktionen jenseits des Identitätsnachweises werden nicht über die Personalausweisgebühr finanziert, sondern werden optional umgesetzt, wobei die Finanzierung den Nutzern auferlegt wird (z. B. qualifizierte elektronische Signatur).
W.2	Infrastrukturen, die für Ausstellung und Kontrolle anderer Personaldokumente geschaffen wurden (z. B. ePass), sollen zur Kostenersparnis auch für den elektronischen Personalausweis genutzt werden.

Lfd. Nr.	Anforderung
W.3	Mittelfristig sollen für eine anteilige Finanzierung des elektronischen Identitätsnachweises jene Marktteilnehmer verstärkt herangezogen werden, für die sich gegenüber bisherigen Authentisierungsmethoden erhebliche Einsparungen ergeben. Ziel ist eine Kostenverteilung, die den jeweils entstehenden Vorteilen (Kosteneinsparung, Komfortgewinn) der Marktteilnehmer Rechnung trägt.

Tabelle 44: Wirtschaftliche Anforderungen

9.7 Mögliche Ausprägung des neuen elektronischen Personalausweises

Vor dem Hintergrund der vorgenannten Anforderungen zeigen die folgenden Abbildungen eine denkbare Umsetzung des elektronischen Personalausweises einschließlich der gemäß PersAuswG aufzudruckenden Informationen.

Abbildung 32: Gestaltungsbeispiel für den elektronischen Personalausweis – Vorderseite

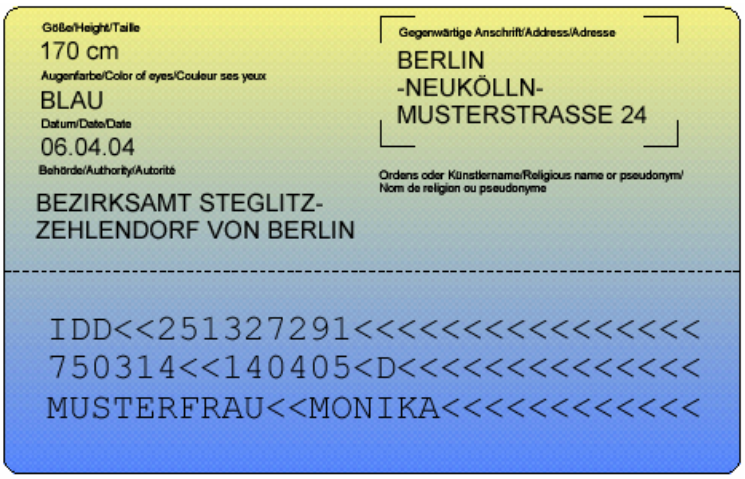

Abbildung 33: Gestaltungsbeispiel für den ePA - Rückseite

Der Personalausweis wird somit neben den hoheitlichen Symbolen des Herkunftslandes Bundesrepublik Deutschland folgende Daten enthalten:

1. Familienname und. Geburtsname,
2. Vornamen,
3. Doktorgrad,
4. Tag und Ort der Geburt,
5. Lichtbild,
6. Unterschrift,
7. Größe,
8. Farbe der Augen,
9. Anschrift, bei Anschrift im Ausland die Angabe „ohne Wohnanschrift im Inland“,
10. Staatsangehörigkeit,
11. Seriennummer und
12. Ordensname, Künstlername.

Zusätzlich enthält der elektronische Personalausweis (wie auch der bisherige Personalausweis) eine maschinenlesbare Zone (MRZ), die folgende Informationen enthalten darf:

13. Die Abkürzung "IDD" für "Identitätskarte der Bundesrepublik Deutschland",
14. die Seriennummer des Personalausweises,
15. den Tag der Geburt,
16. die Gültigkeitsdauer des Personalausweises,
17. die Abkürzung "D" für die Eigenschaft als Deutscher,
18. den Familiennamen,
19. den oder die Vornamen.

10 EINORDNUNG DES ELEKTRONISCHEN PERSONALAUSWEISES IN ANDERE NATIONALE UND INTERNATIONALE VORHABEN

10.1 Interoperabilität mit dem Vorhaben “Elektronische Aufenthaltstitel in Deutschland“

Die EU-Kommission hat eine Verordnung des Rates zur Änderung der Verordnung (EG) Nr. 1030/2002 (vgl. [14]) verabschiedet, die die Integration und Nutzung biometrischer Merkmale in Aufenthaltstiteln vorsieht. Gründe zur Vergabe von Aufenthaltstiteln können in der Ausbildung oder Erwerbstätigkeit von Drittstaatsangehörigen liegen. Möglich sind auch völkerrechtliche, humanitäre, familiäre oder politische Gründe.

Der Vorschlag der Kommission beinhaltet, zukünftig das Gesichtsbild sowie die Fingerabdrücke digital in einem Chip auf einer Aufenthaltskarte zu speichern. Diese Aufenthaltstitel sind als eigenständige Dokumente auszustellen. Der Vorschlag der Kommission überlässt es den Mitgliedstaaten zu entscheiden, ob die Dokumente noch mit zusätzlichen Funktionen ausgestattet werden. Deutschland plant auf dieser Grundlage die elektronischen Aufenthaltstitel mit dem elektronischen Identitätsnachweis und (optional) einer elektronischen Signatur auszustatten (analog zum elektronischen Personalausweis).

Die Projekte zur Einführung des elektronischen Personalausweises und der elektronischen Aufenthaltstitel werden so koordiniert, dass eine weitgehende technische Kompatibilität erreicht wird, so dass

- mit dem biometrischen Dokument eAT ein einheitliches Sicherheitsniveau erreicht wird und
- auch den ausländischen Bürgerinnen und Bürgern eine elektronische Authentisierung mit diesem Dokument ermöglicht wird.

10.2 Interoperabilität mit den Infrastrukturen des elektronischen Reisepasses (ePass)

Auf Grundlage der Festlegungen der EU führte Deutschland als einer der ersten EU-Mitgliedsstaaten den biometriegestützten Reisepass (ePass) ein. Unabhängig von der zukünftigen Ausgestaltung des elektronischen Personalausweises soll seine Funktion als biometriegestütztes Reisedokument weitgehend kompatibel zu der des ePasses sein, um einheitliche Verfahren und die technische Infrastruktur im Erfassungs- und Prüfungsprozess für beide Dokumenttypen nutzen zu können (s. Kap. 9.1).

10.3 Bezüge zur Initiative „Europäische Informationsgesellschaft 2010“ (i2010)

Die EU Kommission verabschiedete im Jahr 2005 die Initiative „i2010: Europäische Informationsgesellschaft 2010“. Im Rahmen dieser Initiative wird ein Aktionsplan erarbeitet, um elektronische, bürgernahe Informationsdienste zu schaffen, die transparenter, leichter zugänglich und kostengünstiger sind. Dabei nehmen elektronische Identitäten (eID) eine zentrale Stellung ein.

Im November 2005 haben die zuständigen EU-Minister auf einer Konferenz in Manchester eine Deklaration verabschiedet mit dem Ziel, bis zum Jahr 2010 für alle EU-Bürger und die Wirtschaft die Voraussetzungen für eine sichere, datenschutzkonforme und allgemein akzeptierte elektronische Identifizierung zu schaffen. Elektronische Identitätskarten werden weiterhin in nationaler Verantwortung ausgegeben, sie sollen aber interoperabel sein und einem gemeinsamen technischen Sicherheitsstandard genügen (vgl. Kap. 9.5.2.2), insbesondere hinsichtlich des Vertrauensniveaus in die Daten und den Authentisierungsprozessen.

Die Spezifikation des elektronischen Personalausweises in Deutschland wird diesen Anforderungen entsprechen. Durch Mitarbeit in den entsprechenden Gremien nimmt Deutschland aktiv Einfluss auf die Erstellung entsprechender europäischer Standards für Identitätskarten und elektronische Identitäten.

10.4 Programm „E-Government 2.0“ der Bundesregierung

Mit dem Programm „E-Government 2.0 - zukunftsorientierte Verwaltung durch Innovationen“ hat die Bundesregierung im September 2006 eine übergreifende Strategie für die Modernisierung der Bundesverwaltung vorgelegt. Ziel des Programms ist es, die Bundesverwaltung effizienter und deren Leistungen und Verfahren einfacher, schneller und kundenfreundlicher zu gestalten. Gleichzeitig kommt dem Staat noch eine weitere Rolle zu: Er wird zum Nachfrager und Förderer von Zukunftstechnologien und sichert die erforderlichen Infrastrukturen der Informationstechnik. Durch den Einsatz innovativer und neuer Techniken wird er zum Impulsgeber und zum Partner der Wirtschaft.

Im Handlungsfeld Identifikation sollen die Infrastrukturvoraussetzungen geschaffen werden, um im elektronischen Raum eine sichere Identifizierung zwischen Bürgerinnen und Bürgern, Wirtschaft und Verwaltung zu ermöglichen. Durch Bereitstellung zuverlässiger, sicherer Verfahren der wechselseitigen Identitätsfeststellung von Kommunikationspartnern sollen die Risiken der Nutzung falscher Identitäten im E-Business und E-Government wesentlich verringert werden.

Der elektronische Personalausweis als Kernvorhaben des Programms „E-Government 2.0“ der Bundesregierung wird dafür eine wichtige Infrastrukturvoraussetzung bilden. Durch enge Abstimmung der Maßnahmen-Konzepte des E-Government 2.0 Programms (z. B. das Angebot von Bürgerportalen) und der Spezifizierung des elektronischen Personalausweises wird eine optimale Einbindung gesichert.

11 UMSETZUNGSPLANUNG

Zur Umsetzung des Vorhabens zur Einführung des elektronischen Personalausweises wurde im Bundesministerium des Innern ein Projekt initiiert, das folgende wesentliche Teilprojekte enthält:

1. **Leistungsbeschreibung zum elektronischen Personalausweis**
   Ausgehend von den Aussagen des Grobkonzepts sollen in einem Feinkonzept die Architektur und Eckpunkte der Lösung weiter spezifiziert werden. Sie bilden die Vorgabe an den Hersteller zur Ausgestaltung der technischen Umsetzung.

2. **Rechtsgrundlagen**
   Die Änderung der technischen Grundlagen sowie die Implementierung neuer Funktionen für den elektronischen Personalausweis erfordern die Schaffung der notwendigen rechtlichen Rahmenbedingungen im Personalausweisgesetz und weiteren Rechtsvorschriften. Wichtige Meilensteine auf dem Weg zu einem novellierten Personalausweisgesetz sind:

   - **Referentenentwurf,**
   - **Kabinettsbeschluss und**
   - **Verabschiedung durch den Bundestag und den Bundesrat.**

3. **Vorbereitung der Herstellung des elektronischen Personalausweises**
   Auf Basis der Vorgaben der Leistungsbeschreibung soll durch den Hersteller ein produktions- und sicherheitstechnisches Konzept erarbeitet werden, das die endgültige technische Lösung des elektronischen Personalausweises beschreibt. Auf dieser Basis wird der Hersteller einen **Prototypen** entwickeln und produzieren. Dieser soll bereits alle wesentlichen Sicherheitsmerkmale und Funktionen enthalten und Grundlage für einen nachfolgenden Feldtest sein.

4. **Vorbereitung des neuen Lifecycle-Management (LCM) für den elektronischen Personalausweis**
   Parallel zur Vorbereitung der Produktion des Dokuments sollen alle notwendigen Maßnahmen zur Abwicklung der Beantragung, Bestellung beim Hersteller, Ausgabe, Rücknahme und Vernichtung des elektronischen Personalausweises erfolgen. Dazu zählen auch denkbare Maßnahmen zur Nutzungsbegleitung für die Bürgerinnen und

Bürger wie u. a. die Bereitstellung notwendiger Software oder die Einrichtung eines Callcenters als Ansprechpartner und Hilfestellung für die sichere Nutzung der neuen elektronischen Funktionen.

5. Pilotierung und Feldtest zur Nutzung des elektronischen Personalausweises

Zur Sicherstellung einer erfolgreichen und erprobten Einführung des elektronischen Personalausweises sind sowohl Technologieerprobungen im Rahmen von Pilotierungsprojekten als auch ein Feldtest vorgesehen. Im Rahmen der Pilotierungen sind insbesondere die Anwendungen zu erproben, die zukünftig für die Nutzung des elektronischen Identitätsnachweises relevant sind. Hierbei werden u. a. die geplanten Chipkarten, Lesegeräte, Software, eCard-API, E-Government- und E-Business-Dienste sowie deren Kompatibilität untereinander getestet.

Der Erprobung schließen sich zwei Feldtests an. Zum einen werden in den PA-Behörden die zum Einsatz gelangenden Technologien (Lesegeräte) und Fachverfahren (EWO-Verfahren) sowie Bearbeitungsprozesse (u. a. Änderung der PIN) getestet. Zum anderen findet ein zweiter Feldtest statt, der die Erprobung des elektronischen Identitätsnachweises im Kontext spezieller Anwendungen zwischen Bürgerinnen und Bürger, Verwaltung und Wirtschaft im Rahmen von E-Business und E-Government vorsieht.

Erfahrungen aus dem ePass-Projekt werden an dieser Stelle zu Grunde gelegt.

6. Rollout

Nach einem erfolgreichen Systemtest soll die Umstellung der Produktion, des Lifecycle-Management und der Beginn der Produktion des elektronischen Personalausweises erfolgen.

Die technischen und organisatorischen Voraussetzungen sollen nach gegenwärtiger Planung bis Ende 2009 geschaffen werden. Die Durchführung der erforderlichen Pilotierungs- und Feldtestmaßnahmen ist von Mitte 2008 bis voraussichtlich Mitte 2009 geplant.

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

Abs.	Absatz
Access Verifier	Stelle zur Ausgabe von Berechtigungszertifikaten zum Zugriff auf Identitätsmerkmale im Rahmen des elektronischen Identitätsnachweises des ePA
Art.	Artikel
Authentisierung	Glaubhaftmachen einer Identität (aktiv)
Authentifizierung	Beglaubigung, Bestätigung der Echtheit einer behaupteten Identität
BKA	Bundeskriminalamt
bspw.	beispielsweise
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
bzw.	beziehungsweise
ca.	circa
DB	Datenbank
d. h.	das heißt
eID (Card)	electronic Identity (Card); Dokument zum elektronischen Identitätsnachweis
eID-Funktion	Elektronischer Identitätsnachweis, Authentisierungsfunktion
ePA	Elektronischer Personalausweis
ePass	Reisepass mit Speicherung von biometrischen Personenmerkmalen in einem Chip
EU	Europäische Union
EUR	Euro
gem.	gemäß
ggf.	gegebenenfalls
ggü.	gegenüber
ICAO	International Civil Aviation Organization
ID1	genormtes Format für Identitätsdokumente, entspricht dem Scheckkartenformat
ID2	genormtes Format für Identitätsdokumente, entspricht dem Format des aktuellen Personalausweises
ID-Card	Identitäts-Karte
Identität	Dynamische Sammlung verschiedener Merkmale einer Person
Identitätsfeststellung	Prozess der Überprüfung der Identität einer Person, in der Regel verbunden mit der Authentifizierung

i. d. R.	in der Regel
INPOL	Informationssystem der Polizeien des Bundes und der Länder
i. S.	im Sinne
IT	Informationstechnik/-technologie
Kryptographie	Schutz von Daten durch Verschlüsselung
Mio.	Million(en)
Mrd.	Milliarde(n)
MRZ	Machine Readable Zone; maschinenlesbarer Bereich; Bereich auf einem Personalausweis oder Pass mit Daten, die optisch lesbar sind und automatisiert ausgewertet werden können
o. ä.	oder ähnlich
PA	Personalausweis
PDÜ	Passdaten-Übermittlung
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PUK	Personal (PIN) Unblocking Key
QES	Qualifizierte elektronische Signatur
rd.	rund
s.	siehe
SIS	Schengen-Informationssystem
TAN	Transaktionsnummer
TR	Technische Richtlinie
u. a.	unter anderem
u. U.	unter Umständen
vgl.	vergleiche
z. B.	zum Beispiel
z. T.	zum Teil
z. Zt.	zur Zeit

REFERENZEN

[1] BSI; *Advanced Security Mechanisms for Machine Readable Travel Documents*, Technical Report, Version 0.90, 2005

[2] Europäische Kommission, Verordnung des Rates über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger, KOM(2004) 116, 15152/04

[3] Common Criteria Protection Profile, Machine Readable Travel Document with „ICAO Application“, Basic Access Control, BSI-PP-0017

[4] ICAO; *Machine Readable Travel Documents, Development of a Logical Data Structure (LDS) for Optional Capacity Expansion Technologies*, Technical Report, Revision 1.7, 2004

[5] ICAO; *PKI for Machine Readable Travel Documents Offering ICC Read-Only Access*, Technical Report, Version 1.1, 2004

[6] ICAO; Supplement 9303; Version 2005-4 V3.0; June 12, 2005

[7] ISO/IEC 7816-x: *Identification Cards – Integrated Circuit Cards*, 2004/2005

[8] ISO/IEC 14443: *Identification Cards – Contacless Integrated Circuit Cards – Proximity Cards*

[9] Rankl, Wolfgang; Effing, Wolfgang; *Handbuch der Chipkarten*, Carl Hanser Verlag, ISBN 3-446-22036-4, 2002

[10] Signaturbündnis/SRC GmbH; *SigAll-API – Specification of the Application Programming Interface to the Signature Card,* Version 1

[11] Gesetz über Rahmenbedingungen für elektronische Signaturen vom 16. Mai 2001; BGBl I 2001, 876; zuletzt geändert am 07.07.2005

[12] Verordnung zur elektronischen Signatur vom 16. November 2001; BGBl I 2001, 3074; zuletzt geändert am 04.01.2005

[13] Gesetz über die Bundespolizei vom 19. Oktober 1994; BGBl I 1994, 2978,2979; zuletzt geändert am 21.06.2005

[14] Verordnung (EG) Nr. 1030/2002 des Rates vom 13. Juni 2002 zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatsangehörige, ABl. EU Nr. L 157, S. 1.

[15] Gesetz über Personalausweise vom 19. Dezember 1950; BGBl 1950, 807, zuletzt geändert am 25.03.2002