Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie TR-03127
eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control

Personalausweis, elektronischer Aufenthaltstitel und eID-Karte für Unionsbürger

Version 1.30 draft

15. Mai 2020

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

Der Personalausweis (PA) und der Aufenthaltstitel (eAT) enthalten seit 2010 bzw. 2011 einen kontaktlosen Chip als Sicherheitsmerkmal. Damit wurde – zusammen mit dem elektronischen Reisepass seit 2007 – eine Familie hoheitlicher elektronischer Dokumente geschaffen. Ergänzt wird diese Familie ab dem 01.11.2020 um eine eID-Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums (kurz eID-UB). Im Gegensatz zu Personalausweis oder Aufenthaltstitel handelt es sich bei der eID-Karte für Unionsbürger um eine Karte rein für die elektronische Verwendung, nicht um ein physisches Ausweisdokument.

Diese Dokumente werden – soweit möglich – technisch identisch ausgestaltet, mit dem Ziel, eine gemeinsame Infrastruktur sowohl für die hoheitliche Anwendung als auch für die sichere Identifizierung für eGovernment/eBusiness als Grundlage für die Digitalisierung von Geschäftsprozessen zu schaffen. Die drei Dokumententypen (PA, eAT und eID-UB) werden im Folgenden vereinfachend zusammengefasst als *Dokument* oder *Ausweis* bezeichnet[1].

Grundlage für die Ausgestaltung sind dabei

- für den Personalausweis das Personalausweisgesetz ([PAuswG]) und die Personalausweisverordnung,
- für den Aufenthaltstitel die Vorgaben der EU ([EU-RP]), das Aufenthaltsgesetz ([AufenthG]) und die Aufenthaltsverordnung,
- für die eID-Karte für Unionsbürger das eID-Karte-Gesetz ([eIDKG])
- sowie das „Sicherheitsrahmenkonzept für das Gesamtsystem des elektronischen Personalausweises“ ([SiKo]), welches analog auch auf den Aufenthaltstitel und die eID-Karte für Unionsbürger Anwendung findet.

Der im Dokument integrierte Chip ist ein Sicherheitsmerkmal zur Erhöhung der Fälschungssicherheit und bietet die Möglichkeit der Aufnahme biometrischer Merkmale zur Erhöhung der Bindung zwischen Ausweis und Inhaber.

Darüber hinaus eröffnet er die Möglichkeit, das Dokument um eine Funktion zu erweitern, die dem Dokumenteninhaber einerseits und eBusiness- oder eGovernment-Dienstleistern andererseits eine sichere gegenseitige Authentisierung u.a. über eine Internet-Verbindung auf hohem Vertrauensniveau nach [TR-03107], Teil 1, ermöglicht. Der elektronische Identitätsnachweis ist nach [eIDAS] für die grenzüberschreitende elektronische Identifizierung auf Vertrauensniveau *hoch* notifiziert und kann somit im gesamten europäischen Wirtschaftsraum zur sicheren Identifizierung eingesetzt werden[2]. Aus dieser Funktion ergibt sich eine Vielzahl von Anwendungsmöglichkeiten.

Eine zusätzliche Anwendung des Dokuments ist eine Signaturanwendung zur Erzeugung qualifizierter Signaturen. Diese Anwendung wird erst vom Karteninhaber nachträglich bei Bedarf aktiviert.

In dieser Technischen Richtlinie werden die für den elektronischen Personalausweis, den elektronischen Aufenthaltstitel und die eID-Karte für Unionsbürger verwendeten Verfahren vorgestellt und auf die entsprechenden Spezifikationen verwiesen. Soweit nicht explizit anders angegeben, beziehen sich alle Angaben auf alle Dokumententypen.

1 Dabei ist zu beachten, dass die eID-Karte für Unionsbürger kein Ausweisdokument im engeren Sinne ist.

2 Die Notifizierung der eID-Karte für Unionsbürger als Bestandteil des Systems zum elektronischen Identitätsnachweis ist zur Einführung der eID-Karte vorgesehen.

2. Datenerfassung und -übertragung

Bei Antragstellung für das Dokument werden in der Personalausweisbehörde, der Ausländerbehörde bzw. der eID-Karte-Behörde (im Folgenden generisch *Ausweisbehörde*) die notwendigen persönlichen Daten des Antragstellers erfasst und anschließend an den Ausweishersteller übertragen. Die zu erfassenden Daten ergeben sich aus dem Personalausweisgesetz, dem Aufenthaltsgesetz bzw. dem eID-Karte-Gesetz sowie den zugehörigen Verordnungen. Die notwendigen Verfahren und Datenformate werden in [TR-03104], [TR-03121] und [TR-03123] festgelegt.

2.1 Persönliche Daten

Für den Ausweis werden folgende personenbezogenen Daten erfasst:

- Vorname(n), Familienname, gegebenenfalls Geburtsname
- Doktorgrad
- Tag und Ort der Geburt
- Anschrift (inkl. Postleitzahl) und – bei Adressen in Deutschland – der amtliche Gemeindeschlüssel des Wohnortes

Daneben werden für den Personalausweis und den Aufenthaltstitel biometrische Daten (Gesichtsbild, Fingerabdrücke (Personalausweis: optional, Aufenthaltstitel: verpflichtend), Unterschrift, Augenfarbe und Größe) erfasst. Für die eID-Karte für Unionsbürger werden keine biometrische Daten erfasst.

Für den Personalausweis und die eID-Karte für Unionsbürger wird zusätzlich – soweit vorhanden – der Ordens- oder Künstlername erfasst, für den Aufenthaltstitel das Geschlecht sowie gegebenenfalls aufenthaltsrechtliche Nebenbestimmungen.

2.2 Gesichtsbild

Zur Erfassung des Gesichtsbildes für Personalausweis und Aufenthaltstitel, sowohl für den Aufdruck auf den Kartenkörper als auch zur elektronischen Speicherung im Chip, legt der Antragsteller ein Lichtbild vor. Die Anforderungen an das Lichtbild werden in [TR-03121] festgelegt.

Das vorgelegte Lichtbild wird in der Ausweisbehörde mit einer zertifizierten Erfassungs- und Qualitätssicherungssoftware (vgl. Anhang A) erfasst und in das für den Ausweis verwendete JPEG2000-Format [ISO 15444] konvertiert.

Alternativ besteht auch die Möglichkeit, das Gesichtsbild vor Ort in der Ausweisbehörde zu erfassen oder der digitalen Übermittlung vom Fotografen zur Ausweisbehörde. Die Qualitätssicherung und Konvertierung erfolgt analog zu der Erfassung über ein mitgebrachtes Lichtbild. Die Vorgaben in [TR-03104] und [TR-03121] sind zu beachten.

2.3 Fingerabdrücke

Optional (Personalausweis) bzw. verpflichtend (Aufenthaltstitel) werden im Chip zwei Fingerabdruckbilder gespeichert. Die Bilder werden mit Hilfe von zertifizierten Fingerabdruckscannern sowie zertifizierter Erfassungs- und Qualitätssicherungssoftware erfasst (vgl. Anhang A). Die Anforderungen an die Erfassungskomponenten und an den Erfassungsprozess – sowohl Anforderungen an die Qualität der erfassten Daten als auch Verfahrensweisen in besonderen Fällen wie z.B. bei Vorliegen einer Behinderung – werden in [TR-03104] und [TR-03121] festgelegt.

2.4 Unterschrift

Ebenfalls erfasst wird für Personalausweis und Aufenthaltstitel die Unterschrift des Antragstellers. Die Unterschrift wird nur auf dem jeweiligen Ausweis aufgedruckt und nicht im Chip gespeichert.

2.5 Datenübertragung

Die Datenübertragung zwischen den Ausweisbehörden und dem Ausweishersteller wird in entsprechenden Profilen gemäß [TR-03104] und [TR-03123] spezifiziert. Die Datenübertragung erfolgt ausschließlich elektronisch.

Die [TR-03104] beschreibt grundsätzliche Prozesse und organisatorische Regelungen, die im Zusammenhang mit der Datenerfassung, Beantragung und Auslieferung des Ausweises gelten. Das XML-basierte Datenmodell für die Antragsdaten wird in [TR-03123] spezifiziert. Die Spezifikation der Sicherheitsmechanismen (Verschlüsselung und Signatur) zur Sicherung der Vertraulichkeit und Authentizität der Antragsdaten findet sich in [TR-03132].

Die verschlüsselten und signierten Daten werden mit Hilfe eines dafür im Deutschen Verwaltungsdiensteverzeichnis [DVDV] eingerichteten Dienstes über OSCI-Transport [OSCI] übertragen, dessen Funktionsweise in einer Dienstbeschreibung (Bestandteil von [TR-03132]) dargelegt wird.

2.6 Kommunikation zwischen Ausweisbehörden

In bestimmten Fällen müssen verschiedene Ausweisbehörden Informationen untereinander austauschen, z.B. bei

- Beantragung eines Ausweises bei einer nicht zuständigen Behörde
- Umzug
- Ausweissperre bei einer Ausweisbehörde, die nicht den zugehörigen Eintrag im Ausweisregister führt.

Diese Kommunikation ist nicht Bestandteil dieser Richtlinie.

2.7 Dokumentennummer

Die Dokumentennummern der Ausweise setzen sich aus einer vierstelligen alphanumerischen Behördenkennziffer und einer fünfstelligen alphanumerischen, pseudozufälligen Nummer zusammen. Die Bildung des pseudozufälligen Teils erfolgt nach den Vorgaben in [TR-03116], Teil 2.

Werden die Nummern durch den Ausweishersteller zur Verfügung gestellt, wird die Übertragung zu den Ausweisbehörden in [TR-03104] spezifiziert. Jeder Ausweis erhält eine neue Nummer.

3. Dokument

Kartenkörper

Das Dokument ist im TD1-Format gemäß [ICAO 9303], Part 5, ausgestaltet. Das Design der Karte und die physikalischen Sicherheitsmerkmale (z.B. Hologramme) sind nicht Gegenstand dieser Richtlinie.

Chip

In den Ausweis ist ein kontaktloser Chip integriert. Der Chip kommuniziert mit einem passenden Kartenterminal, welches als Lese- oder Schreibgerät fungiert. Die Datenübertragung zwischen Chip und Terminal erfolgt mittels induktiver Kopplung nach [ISO 14443]. Der Unique Identifier (UID, [ISO 14443] Typ A) bzw. der Pseudo-Unique PICC Identifier (PUPI, [ISO 14443] Typ B) des Chips wird bei jeder Aktivierung des Chips zufällig erzeugt.

Die Kommunikation zwischen Chip und Terminal erfolgt nach [ISO 7816].

Der Chip speichert personen- und dokumentenbezogene Daten wie in Abschnitt 3.2 beschrieben. Die zugehörigen Zugriffsprotokolle finden sich in Kapitel 3.1.Ferner ist der Ausweis eine nach eIDAS-Verordnung [eIDAS] zertifizierte qualifizierte Signaturerstellungseinheit[3].

Der Chip basiert auf dem Profil „Identity Card with Protected MRTD Application“ (Personalausweis und eID-Karte für Unionsbürger) bzw. dem Profil „Identity Card with optional EU-compliant MRTD Application“ (Aufenthaltstitel) nach [TR-03110], Teil 4. Soweit möglich folgen die Anwendungen dem Profil 1 “*eID Application with mandatory ICAO functionality and conditional digital signature functionality*” der European Citizen Card ([CEN 15480], Teil 4).

3.1 Authentisierungsverfahren

Für die Zugriffskontrolle und die Authentisierung des Chips sowie des Terminals werden folgende kryptographischen Protokolle genutzt und müssen durch Chip bzw. Terminal implementiert werden (siehe auch [TR-03116], Teil 2):

- Password Authenticated Connection Establishment – PACE ([TR-03110], Teil 2),
- Terminalauthentisierung Version 2 – TA2 ([TR-03110], Teil 2);
- Passive Authentisierung – PA ([ICAO 9303], Part 11, und [TR-03110], Teil 2);
- Chipauthentisierung Version 2 und Version 3 – CA2 / CA3 ([TR-03110], Teil 2);
- nur Aufenthaltstitel: Basic Access Control[4] und PACE ([ICAO 9303], Part 11) sowie Terminalauthentisierung Version 1 und Chipauthentisierung Version 1 gemäß [TR-03110], Teil 1.

Mit diesen kryptographischen Protokollen ist der Zugriff auf Daten des Ausweises mittels der *General Authentication Procedure* nach [TR-03110], Teil 2, möglich. Für den Aufenthaltstitel ist entsprechend den Vorgaben der EU ([EU-RP]) zusätzlich der Zugriff auf die Daten der Biometriefunktion (Abschnitt 3.2.2) mittels *Standard ePassport Inspection Procedure* und *Advanced ePassport Inspection Procedure* gemäß [TR-03110], Teil 1, möglich.

Die Aktive Authentisierung nach [ICAO 9303], Part 11, wird aus Datenschutzgründen nicht implementiert (siehe [TR-03110], Teil 1, Anhang B „Challenge Semantics“).

[3] Vor Inkrafttreten von [eIDAS] ausgegebene Karten sind gemäß dem mittlerweile durch das Vertrauensdienstegesetz (VDG) abgelösten Signaturgesetz (SigG) bestätigte sichere Signaturerstellungseinheiten.

[4] Nur für vor dem 01.11.2019 ausgegebene Dokumente.

Die Anforderungen an die zugrunde liegenden Algorithmen und an die zu verwendenden Schlüssellängen werden in [TR-03116], Teil 2, in der jeweils aktuellen Fassung festgelegt. Zu den Verfahren der Kryptographie auf elliptischen Kurven ist [TR-03111] verbindlich.

3.1.1 PACE

Das PACE-Protokoll dient dem Aufbau eines verschlüsselten und integritätsgesicherten Kanals zwischen Terminal und Chip und dem gleichzeitigen Nachweis, dass sich Chip und Terminal im Besitz des gleichen Passwortes befinden. Das zu verwendende Passwort unterscheidet sich je nach Anwendungsfall, siehe Abschnitt 3.3.

Sofern im Folgenden Rechte durch die *General Authentication Procedure* nachgewiesen werden sollen, so teilt das Terminal bereits durch PACE dem Chip seinen Terminaltyp sowie die angestrebten Rechte mit.

3.1.2 Terminalauthentisierung

Die Terminalauthentisierung dient dem Nachweis der Zugriffsrechte eines Terminals bzw. eines Diensteanbieters gegenüber dem Chip.

Der Nachweis der Zugriffsrechte über die Terminalauthentisierung im Rahmen der *General Authentication Procedure* ist bei Personalausweis und eID-Karte für Unionsbürger für alle in den Anwendungen des Chips gespeicherten personen- und dokumentenbezogenen Daten notwendig. Beim Aufenthaltstitel ist für den Zugriff auf DG1 und DG2 der Biometriefunktion (Abschnitt 3.2.2) mittels *Standard ePassport Inspection Procedure* keine Terminalauthentisierung notwendig.

Die Zugriffsrechte des Terminals werden an die in der Chipauthentisierung ausgehandelten Sitzungsschlüssel gebunden, d.h. die Rechte des Terminals können nur innerhalb des durch die Chipauthentisierung aufgebauten verschlüsselten Kanals ausgeübt werden. Die Terminalauthentisierung kann pro Sitzung nur einmal durchgeführt werden. Eine neue Sitzung wird durch den Abbau des verschlüsselten Kanals (und damit verbunden Löschen der Sitzungsschlüssel und Zurücksetzen aller Zugriffsrechte) und Selektieren des Master Files gestartet.

Die Rechte des Terminals werden über Zertifikate der Berechtigungs-PKI vergeben. Die Berechtigungs-PKI (auch EAC-PKI, siehe Abschnitt 5.2) ist eine dreistufige PKI, bestehend aus:

- der Wurzelinstanz (CVCA, Country Verifying Certification Authority), betrieben vom BSI;
- mehreren Document Verifier (DV);
- den Zertifikaten der Terminals bzw. Diensteanbieter.

Durch die Zertifikate werden die maximalen Zugriffsrechte eines Terminals festgelegt und verschiedene Terminaltypen unterschieden (Abschnitt 4):

- *hoheitliches nationales Inspektionssystem*
- *hoheitliches ausländisches Inspektionssystem*
- *hoheitliches nationales Authentisierungsterminal*
- *nicht-hoheitliches/ausländisches Authentisierungsterminal*
- *Signaturterminal* für qualifizierte elektronische Signaturen.

In der *General Authentication Procedure* ist die Terminalauthentisierung nur erfolgreich, wenn der Terminaltyp aus dem Zertifikat mit dem in PACE angekündigten übereinstimmt und das für PACE benutzte Passwort für den Terminaltyp zulässig ist (vgl. Tabelle 4). Zugriffsrechte werden dann nur erteilt, wenn sie sowohl in PACE angestrebt als auch durch die Zertifikatskette und Terminalauthentisierung nachgewiesen wurden.

3.1.3 Passive Authentisierung

Die Passive Authentisierung dient dem Echtheitsnachweis der auf dem Chip gespeicherten Daten. Dazu werden die in der Biometrieanwendung (Abschnitt 3.2.2) gespeicherten Daten und die öffentlichen Schlüssel des Chips vom Ausweishersteller mit seinem Document Signer aus der Dokumenten-PKI (Abschnitt 5.1) signiert. Die Dokumenten-PKI ist eine zweistufige PKI bestehend aus:

- der Wurzelinstanz (CSCA, Country Signing Certification Authority), betrieben vom BSI;
- dem Document Signer (DS), betrieben vom Ausweishersteller.

Die Datengruppen der nicht-hoheitlichen eID-Anwendung werden nicht signiert.

Authentisierungs- und *Signaturterminals* führen die Passive Authentisierung nur für die Datei EF.CardSecurity (die u.a. den öffentlichen Schlüssel des Chips enthält, siehe Abschnitt 3.2.5) durch. *Inspektionssysteme* führen die Passive Authentisierung zusätzlich für die Datei EF.SOD der Biometrieanwendung durch, um die Daten dieser Anwendung explizit zu authentisieren.

Die Passive Authentisierung weist nur die Echtheit der Daten nach, nicht die des Chips selbst. Dies leistet erst die Chipauthentisierung in Verbindung mit der Passiven Authentisierung.

Das Zertifikat des Document Signer ist auf dem Chip selbst gespeichert (DS-Zertifikat), während das Zertifikat der Wurzel-Instanz (CSCA-Zertifikat) beim BSI bzw. einem nachgelagerten Public Key Directory (PKD) erhältlich ist. Somit kann sich jeder Zugriffsberechtigte über die Dokumenten-PKI von der Echtheit der signierten Daten und (in Verbindung mit der Chipauthentisierung) des Chips und der darauf gespeicherten Daten überzeugen.

3.1.4 Chipauthentisierung

Die Chipauthentisierung (spezifiziert in [TR-03110]) dient dem Nachweis, dass der Chip in Besitz des privaten Schlüssels ist, der zum in der Datei EF.CardSecurity/EF.ChipSecurity im Master File (bzw. beim Aufenthaltstitel zusätzlich in der DG14 der Biometrieanwendung) gespeicherten öffentlichen Schlüssel gehört. In Verbindung mit der Passiven Authentisierung wird damit die Echtheit des Chips und damit auch der auf dem Chip gespeicherten Daten nachgewiesen.

Weiter dient die Chipauthentisierung dem Aufbau eines sicheren Kanals zwischen Terminal bzw. Diensteanbieter und Chip. Chipauthentisierung Version 3 beinhaltet darüber hinaus eine Pseudonyme Signatur (PSA), welche eine pseudonyme Identifizierung ermöglicht.

Im Rahmen der *General Authentication Procedure* kann das Terminal nach Aufbau des verschlüsselten Kanals gemäß den in der Terminalauthentisierung nachgewiesenen Zugriffsrechten auf den Chip zugreifen.

3.2 Gespeicherte Daten

Die Daten auf dem Ausweis sind in drei Anwendungen organisiert, und zwar

- die Biometrieanwendung (Datenformat analog zum elektronischen Reisepass),
- die eID-Anwendung,
- die Signaturanwendung zur Erzeugung qualifizierter elektronischer Signaturen.

Auf alle in den Anwendungen des Personalausweises und der eID-Karte für Unionsbürger gespeicherten Daten kann nur nach erfolgreicher Authentisierung des Terminals mittels PACE, Terminalauthentisierung und Chipauthentisierung (*General Authentication Procedure*) zugegriffen werden (Abschnitt 4). Beim Aufenthaltstitel ist zusätzlich der Zugriff auf bestimmte Daten der Biometrieanwendung (Abschnitt 3.2.2) mittels *Standard/Advanced ePassport Inspection Procedure* möglich.

3.2.1 Karten-/Anwendungserkennung

Die auf den Ausweisen vorhandenen Anwendungen werden durch korrespondierende Application Identifier in der Datei EF.DIR im Master File erkannt (Reisepässe enthalten meist keine Datei EF.DIR):

- Biometrieanwendung: Application Identifier `0xA0000002471001` (siehe [ICAO 9303], Part 10);
- eID-Anwendung: Application Identifier `0xE80704007F0007030` (siehe [TR-03110]);
- eSign-Anwendung nach [TR-03117]: Application Identifier `0xA000000167455349474E`.

3.2.2 Biometrieanwendung

In der Biometrieanwendung werden die in Tabelle 1 aufgeführten von der ICAO in [ICAO 9303], Part 10, definierten Datengruppen gespeichert. Die weiteren von der ICAO definierten Datengruppen (DG4 bis DG16) werden nicht belegt, abgesehen von DG14 beim Aufenthaltstitel.

Datei	Inhalt	Zugriffsrecht Lesen
EF.COM (nur eAT)	Liste der vorhandenen Datengruppen und Versionsinformation gemäß [ICAO 9303] (Von der Nutzung dieser Datengruppe wird abgeraten, da diese nicht signiert ist.)	nur eAT: BIS/EIS
EF.SOD	Hashwerte der Datengruppen DG1, DG2, DG3; Signatur über diese Hashwerte sowie das DS-Zertifikat (gemäß [ICAO 9303])	IS; nur eAT: BIS/EIS
EF.CVCA (nur eAT)	Trustpoints für Zertifikatskette der Rolle *Inspektionssystem* der Terminalauthentisierung	nur eAT: BIS/EIS
DG1	PA, eAT: Daten der maschinenlesbaren Zone (MRZ), wie auf dem Ausweiskörper aufgedruckt eID-UB: MRZ mit DocumentType „UB“, ausgebendem Land „D“ und Platzhalter „<“ für alle weiteren Felder der MRZ	IS; nur eAT: BIS/EIS
DG2	PA, eAT: Digitales Gesichtsbild, identisch mit dem aufgedruckten Bild eID-UB: statisches eID-Logo	IS; nur eAT: BIS/EIS
DG3	PA, eAT: Zwei Fingerabdrücke (im Personalausweis optional, im Aufenthaltstitel verpflichtend). Werden keine Fingerabdrücke gespeichert, enthält diese Datengruppe einen zufälligen Wert eID-UB: Zufälliger Wert für „keine Fingerabdrücke“	IS + *Read DG3;* nur eAT: EIS + *Read DG3*

DG14 (nur eAT)	Enthält folgende `SecurityInfos` nach [TR-03110]:
	`ChipAuthenticationInfo`
	`ChipAuthenticationPublicKeyInfo`
	`TerminalAuthenticationInfo`
	sowie `PACEInfo` nach [ICAO 9303], Part 11.
	Der enthaltene öffentliche Schlüssel für die Chipauthentisierung ist identisch mit dem Schlüssel aus EF.ChipSecurity.
		nur eAT: BIS/EIS

IS: mit General Auhentication Procedure authentisiertes *Inspektionssystem* (PACE mit CAN / MRZ, TA2, CA2/3); BIS: *Basic Inspection System* mit Standard Inspection Procedure (BAC/PACE); CA1 sofern vom BIS unterstützt; EIS: *Extended Inspection System* mit Advanced Inspection Procedure (BAC/PACE; CA1; TA1)		

Tabelle 1: Dateien der Biometrieanwendung

Datei	Inhalt	Zugriffsrecht		
		Lesen	**Schreiben**	**Interne Verwendung**
DG1	Dokumententyp	IS; AT + *Read DG1*	-	-
DG2	Ausgebender Staat („D“ für Deutschland)	IS; AT + *Read DG2*	-	-
DG3	Ablaufdatum im Format JJJJMMTT	IS; AT + *Read DG3*	-	AT
DG4	Vorname(n)	IS; AT + *Read DG4*	-	-
DG5	Familienname	IS; AT + *Read DG5*	-	-
DG6	PA, eID-UB: Ordensname/Künstlername eAT: unbenutzt	IS; AT + *Read DG6*	-	-
DG7	Doktorgrad	IS; AT + *Read DG7*	-	-
DG8	Geburtsdatum im Format JJJJMMTT	IS; AT + *Read DG8*	-	-
DG9	Geburtsort als unformatierter Text	IS; AT + *Read DG9*	-	-
DG10	Staatsangehörigkeit	IS; AT + *Read DG10*	-	-
DG11 - DG12	unbenutzt	-	-	-
DG13	Geburtsname	IS; AT + *Read DG13*	-	-
DG14 - DG16	unbenutzt	-	-	-
DG17	Adresse	IS; AT + *Read DG17*	AT + *Write DG17*	-
DG18	Wohnort-ID	IS; AT + *Read DG18*	AT + *Write DG18*	AT + *Community ID Verification*
DG19	eAT: Nebenbestimmungen I PA, eID-UB: unbenutzt	IS; AT + *Read DG19*	AT + *Write DG19*	-
DG20	eAT: Nebenbestimmungen II PA, eID-UB: unbenutzt	IS; AT + *Read DG20*	AT + *Write DG20*	-
DG21	unbenutzt	-	-	-
	Vergleichsgeburtsdatum für Altersverifikation	-	-	AT + *Age Verification*
	Schlüssel für anbieterspezifisches Sperrmerkmal (Abschnitt 4.4.2.1)	-	-	AT
	Schlüssel für anbieter- und kartenspezifische Kennung (Abschnitt 4.4.2.2)	-	-	AT + *Restricted Identification* (für CA2 / RI) AT + *PSA* (für CA3)
IS: authentisiertes *Inspektionssystem* (PACE mit CAN o. MRZ, TA2, CA2/3); AT: authentisiertes *Authentisierungsterminal* (PACE mit eID-PIN o. CAN (mit Recht *CAN allowed*), TA2, CA2/3);				

Tabelle 2: Dateien der eID-Anwendung

Zugriff auf die Biometrieanwendung erhalten

- beim Personalausweis und bei der eID-Karte für Unionsbürger ausschließlich mit der General Authentication Procedure authentisierte *Inspektionssysteme*, dabei enthält die Anwendung bei der eID-Karte für Unionsbürger keine personenbezogenen Daten;
- beim Aufenthaltstitel ist zusätzlich die Standard/Advanced Inspection Procedure möglich.

Für den Zugriff auf alle Datengruppen (Personalausweis und eID-Karte für Unionsbürger) bzw. DG3 (Aufenthaltstitel) ist der Nachweis der entsprechenden Rechte über die Terminalauthentisierung notwendig.

Schreiben von Daten in der Biometrieanwendung ist nach der Produktion des Ausweises nicht mehr möglich.

3.2.3 eID-Anwendung

Mit Hilfe der eID-Anwendung des Ausweises ist es dem Ausweisinhaber möglich, sich gegenüber einer dritten Person zu identifizieren und zu authentisieren. Dies ist auch über eine Internet-Verbindung (d.h. gegenüber eGovernment- und eBusiness-Diensten) möglich. Die eID-Anwendung ist die Basis für den *elektronischen Identitätsnachweis* (siehe Abschnitt 4.7) und für das *Vor-Ort-Auslesen* (siehe Abschnitt 4.8).

Die Datengruppen der eID-Anwendung werden in Tabelle 2 dargestellt. Die weiteren in [TR-03110], Teil 4, definierten Datengruppen werden nicht belegt.

Anmerkungen zu einzelnen Datengruppen:

- **DG1**: Der Dokumententyp ist „ID“ beim Personalausweis, „AR“, „AS“ oder „AF“ beim Aufenthaltstitel, und „UB“ für die eID-Karte für Unionsbürger.
- **DG8**: Nicht bei allen Ausweisinhabern ist das Geburtsdatum vollständig bekannt. In der Datengruppe DG8 wird das Geburtsdatum im Format `JJJJMMTT` gespeichert, soweit es bekannt ist, unbekannte Teile werden durch Leerzeichen aufgefüllt. Für die spezielle Funktion *Altersverifikation* (Abschnitt 4.4.5) wird zusätzlich das gemäß der bekannten Teildaten spätestmögliche Datum als Vergleichsdatum intern gespeichert (z.B. falls vom Geburtsdatum nur das Jahr bekannt ist, der 31.12. des Jahres). So wird sichergestellt, dass auch im Falle unvollständiger Geburtsdaten eine Altersverifikation nur dann positiv ist, wenn der Inhaber sicher das nachzuweisende Alter hat.
- **DG10**: In Personalausweisen, die vor dem 01.11.2019 ausgegeben wurden, ist diese Datengruppe leer. Siehe auch Anhang D.
- **DG13**: Siehe auch Anhang D.
- **DG17**: Im Allgemeinen wird der Wohnort als strukturierte Adresse (`structuredPlace` gemäß [TR-03110], Teil 4, bestehend aus Länderkennung, Straße mit Hausnummer, Wohnort, Region und Postleitzahl) gespeichert.

  Wohnt der Ausweisinhaber im Ausland, so wurde stattdessen in Personalausweisen, die vor dem 01.11.2019 ausgegeben wurden, der Text „keine Wohnung in Deutschland“[5] (`noPlaceInfo` gemäß [TR-03110], Teil 4) gespeichert. Gleiches gilt in Fällen, in denen die ausländische Adresse durch die ausgebende Behörde nicht verifiziert werden konnte.
- **DG18**: Im Feld *Wohnort-ID* wird der zum Wohnort gehörige Gemeindeschlüssel gespeichert, um eine Abfrage auf den Wohnort mit der speziellen Funktion Wohnortabfrage (Abschnitt 4.4.6) zu ermöglichen. Der Inhalt der Datengruppe besteht im Allgemeinen aus einer Folge von 14 dezimalen Ziffern:

[5] Bei Ausweisen, die vor dem 15.05.2018 ausgegeben / geändert wurden, lautet der Text „keine Hauptwohnung in Deutschland“.

1. Drei Ziffern für den Ländercode gemäß ISO 3166-1 numeric, ergänzt um eine führende „0“ (z.B. „0276“ für Deutschland)
2. Zwei Ziffern für das Bundesland gemäß amtlichem Gemeindeschlüssel (AGS)
3. Eine Ziffer für den Regierungsbezirk gemäß AGS, ergänzt um eine führende „0“
4. Zwei Ziffern für Stadtkreis (kreisfreie Stadt) bzw. den Landkreis (Kreis) gemäß AGS
5. Drei Ziffern für die Gemeinde, ergänzt um führende „0“.

Die Angaben 2.-5. entsprechen dabei dem amtlichen Gemeindeschlüssel (AGS) des Statistischen Bundesamtes, und werden nur für Adressen in Deutschland gespeichert. Aufgrund der abgestuften Nutzungsmöglichkeit der Wohnortabfrage ist eine Speicherung als Binary Coded Decimal (BCD) mit zwei Ziffern pro Byte vorgesehen, die gegebenenfalls das Auffüllen mit einer führenden „0“ erforderlich macht.
Für Adressen im Ausland wird die Datengruppe nach dem Ländercode mit „0“ aufgefüllt[6].
Für das Auslesen dieser Datengruppe werden keine nicht-hoheitlichen Berechtigungszertifikate ausgegeben.

Zugriff auf die Dateien erhalten nach erfolgreicher Authentisierung

- *Authentisierungsterminals* mit Schreib- und Leserechten entsprechend der Authentisierung;
- *Inspektionssysteme*.

Die Daten werden nicht signiert. Dadurch wird verhindert, dass ein Diensteanbieter aus der eID-Anwendung ausgelesene Daten mit einem kryptographischen Echtheitsnachweis an Dritte weitergeben kann. Stattdessen wird die Integrität und Authentizität der Daten implizit über den durch die Chipauthentisierung ausgehandelten verschlüsselten und integritätsgesicherten Kanal gesichert.

Der Inhalt der Datengruppen *Adresse* und *Amtlicher Gemeindeschlüssel* sowie der Datengruppen *Nebenbestimmungen I/II* beim Aufenthaltstitel sind nachträglich, d.h. nach Ausgabe des Ausweises, unter Nachweis eines entsprechenden Zertifikates änderbar. Dies wird durch den Änderungsdienst der Ausweisbehörden umgesetzt, siehe Abschnitt 7.

Zur Vergabe der Zugriffsberechtigungen auf die Datengruppen siehe [CP-eID].

3.2.4 Signaturanwendung

Die Signaturanwendung dient zur Erstellung qualifizierter elektronischer Signaturen nach [eIDAS]. Vor Nutzung der Signaturanwendung muss durch den Inhaber ein Signaturschlüsselpaar erzeugt werden. Die Signaturanwendung erlaubt das Anlegen eines Schlüsselpaares für qualifizierte elektronische Signaturen (QES).

Vor Anlegen eines Schlüsselpaares für qualifizierte elektronische Signaturen muss durch den Inhaber zunächst eine Signatur-PIN (Abschnitt 3.3.4) angelegt werden. Das Anlegen eines Signaturschlüsselpaares und die Ausstellung des zugehörigen qualifizierten Zertifikats erfolgt durch einen qualifizierten Zertifizierungsdiensteanbieter (Abschnitt 4.4.3).

Die Signaturanwendung einschließlich der Prozesse zur Erzeugung von Schlüsselpaaren und von Signaturen wird in [TR-03117] beschrieben. Zur Beschreibung eines vorhandenen Signaturschlüsselpaares und eines Signaturzertifikates enthält der Ausweis eine *Cryptographic Information Application* nach [ISO 7816] Teil 15 und [EN 419212].

6 Für Ausweise ohne Adresse in Deutschland, die vor dem 01.11.2019 ausgegeben wurden, oder bei nicht verifizierter Adresse, ist diese Datengruppe leer.

3.2.5 Master File

Neben den oben beschriebenen personen- und dokumentenbezogenen Daten werden auf dem Chip Systemdaten (wie z.B. Domain-Parameter), die zur Abwicklung der Zugriffsprotokolle notwendig sind, sowie die Passwörter für PACE im Master File (MF) des Chips gespeichert (vgl. Tabelle 3).

Um eine Identifizierung des Ausweises (und damit das Auflösen des Pseudonyms, Abschnitt 4.4.2.2) über den in der Datei EF.CardSecurity gespeicherten öffentlichen Schlüssel für die Chipauthentisierung zu verhindern, ist dieser Schlüssel nicht chipindividuell. Stattdessen wird für jede Generation von Ausweisen jeweils der gleiche Schlüssel verwendet, so dass über diesen Schlüssel ein eindeutiges

Datei	**Inhalt**	**Zugriffsrecht**		
		Lesen	**Schreiben**	**Interne Verwendung**
EF.ATR/INFO	Nach [CEN 15480] Teil 2, enthält Minimal Card Capabilities Descriptor (CCD) nach [CEN 15480] Teil 3	immer	-	-
EF.DIR	Liste der Kartenapplikationen ([CEN 15480] Teil 2)	immer	-	-
EF.CardAccess	Siehe Abschnitt 3.2.5.	immer	-	-
EF.CardSecurity	Siehe Abschnitt 3.2.5.	PACE	-	-
EF.ChipSecurity	Siehe Abschnitt 3.2.5.	PACE+TA2 als IS oder AT mit Recht *Privileged Terminal*	-	-
	MRZ-Passwort	-	-	Für PACE
	CAN	-	-	Für PACE
	eID-PIN	-	PACE mit eID-PIN; AT + *PIN Management*	Für PACE
	PUK	-	-	Für PACE
	Trustpoints für die Terminalauthentisierung	Rückgabe durch PACE	Bei Import eines Link-Zertifikates	-
	Private Schlüssel für Chipauthentisierung Version 2 und 3, deren öffentliche Schlüssel in EF.CardSecurity angegeben sind.	-	-	Für CA nach PACE + TA2
	Private Schlüssel für Chipauthentisierung Version 2 und 3, deren öffentliche Schlüssel in EF.ChipSecurity angegeben sind.	-	-	Für CA nach PACE + TA2 als IS oder AT mit Recht *Privileged Terminal*
AT: authentisiertes *Authentisierungsterminal* (PACE mit eID-PIN o. CAN (mit Recht *CAN allowed*), TA2, CA2/3);				

Tabelle 3: Dateien im Master File

Identifizieren eines Ausweises nicht möglich ist. Ebenso ist die Signatur über die Datei EF.CardSecurity für die Ausweise einer Generation statisch.

Die Dateien EF.CardAccess, EF.CardSecurity und EF.ChipSecurity enthalten jeweils die folgenden `SecurityInfo`s nach [TR-03110] (die Elemente können z.T. auch mehrfach vorkommen):

- EF.CardAccess
  - `PACEInfo`
  - `ChipAuthenticationInfo`
  - `ChipAuthenticationDomainParameterInfo`
  - `PSAInfo`[7,8]
  - `PrivilegedTerminalInfo`[9]
  - `TerminalAuthenticationInfo`
  - `CardInfo`
- EF.CardSecurity
  - Alle Elemente aus EF.CardAccess
  - `ChipAuthenticationPublicKeyInfo`
  - `PSPublicKeyInfo`
  - `RestrictedIdentificationInfo`[10]
  - `RestrictedIdentificationDomainParameterInfo`

  sowie die Signatur über diese Daten einschließlich des zugehörigen DS-Zertifikats.
- EF.ChipSecurity
  - Alle Elemente aus EF.CardAccess[11]
  - `ChipAuthenticationPublicKeyInfo`
  - `PSPublicKeyInfo`
  - `RestrictedIdentificationInfo`
  - `RestrictedIdentificationDomainParameterInfo`
  - `EIDSecurityInfo` mit Hashwerten der Datengruppen DG4, DG5, DG8 und DG9 der eID-Anwendung[13]

  sowie die Signatur über diese Daten einschließlich des zugehörigen DS-Zertifikats.

3.3 Passwörter

Das Passwort für das PACE-Protokoll (Abschnitt 3.1.1) differiert je nach Anwendungsfall:

- eine auf dem Kartenkörper aufgedruckte sechsstellige Nummer (CAN – *Card Access Number*);

7 Siehe auch Anhang D.

8 Das Protokoll Pseudonymous Signature Authentication erzeugt zwei Identifier, die für das Sperrmerkmal und das Pseudonym genutzt werden (siehe Abschnitt 4.4.2). Entsprechend sind die Authentisierungsbedingungen für die beiden Identifier auf `ps1-authinfo = 0` und `ps2-authinfo = 1` gesetzt.

9 Siehe auch Anhang D.

10 Dieses Element ist zweimal enthalten, zum einen für den Schlüssel zur Berechnung des Sperrmerkmals, zum anderen zur Berechnung des Pseudonyms (siehe Abschnitt 4.4.2). Für das Sperrmerkmal ist das Feld `authorizedOnly` in diesem Element auf `FALSE` gesetzt, für das Pseudonym auf `TRUE`; vgl. auch Tabelle 2.

11 Gemäß [TR-03110] enthält das Element `PrivilegedTerminalInfo` im Vergleich zu EF.CardAccess zusätzlich für jeden chipindividuellen CA-Schlüssel ein Element `ChipAuthenticationPublicKeyInfo`.

13 Siehe auch Anhang D.

- Hash über Dokumentennummer, Geburtsdatum und Ablaufdatum aus der maschinenlesbaren Zone (MRZ);
- die eID-PIN: dies ist entweder eine dem Karteninhaber im PIN-Brief (Abschnitt 6.2) mitgeteilte fünfstellige eID-Transport-PIN oder eine nur dem Karteninhaber bekannte operationelle sechsstellige eID-PIN;
- ein dem Karteninhaber im PIN-Brief (Abschnitt 6.2) mitgeteilter zehnstelliger PUK.

3.3.1 CAN - Card Access Number

Bei der CAN handelt es sich um eine auf der Vorderseite des Ausweises aufgedruckte sechsstellige dezimale zufällige Nummer, die sich nicht aus anderen personen- oder dokumentenbezogenen Daten (wie z.B. Dokumentennummer) berechnen lässt. Diese Nummer wird als Passwort für PACE verwendet, wenn der Aufbau eines sicheren Kanals zwischen Ausweis und Terminal notwendig ist, aber keine Bindung an den Ausweisinhaber durch die Eingabe der geheimen eID-PIN erforderlich ist:

- Hoheitliche Kontrolle (Abschnitt 4.3);
- Vor-Ort-Auslesen (Abschnitt 4.8);
- Änderungsdienst/Visualisierung in den Ausweisbehörden (Abschnitt 7);
- Verbindungsaufbau zur Signaturanwendung (Abschnitt 4.5).

Weiter wird die CAN genutzt, um den dritten Eingabeversuch der eID-PIN freizuschalten (s.u.).

Die CAN besitzt keinen Fehlbedienungszähler.

3.3.2 MRZ

Für *Inspektionssysteme* kann statt der CAN auch die MRZ (genauer: SHA-1-Hashwert von Dokumentennummer, Geburtsdatum und Ablaufdatum) als PACE-Passwort verwendet werden, damit die für den Reisepass eingesetzten Lesegeräte auch für den Personalausweis und Aufenthaltstitel verwendet werden können.

3.3.3 eID-PIN

Die eID-PIN ist eine nur dem Ausweisinhaber bekannte sechsstellige dezimale Nummer. Sie dient der Freigabe der in der eID-Anwendung gespeicherten Daten für die Benutzung außerhalb der hoheitlichen Kontrolle sowie der Bindung dieser Funktionen an den Inhaber des Ausweises (Authentisierung durch Besitz und Wissen).

Die beim Herstellungsprozess gesetzte initiale, zufällig erzeugte PIN ist eine fünfstellige Transport-PIN, d.h. sie kann nur zum Setzen einer operationellen eID-PIN durch den Inhaber (Abschnitt 4.6.1), aber nicht zur Authentisierung genutzt werden. Dadurch ist sichergestellt, dass die operationelle eID-PIN ausschließlich dem Ausweisinhaber bekannt ist. Die Transport-PIN wird dem Inhaber durch den PIN-Brief mitgeteilt (Abschnitt 6.2).

Um ein Erraten der eID-PIN durch Ausprobieren zu verhindern, enthält die Karte einen Fehlbedienungszähler (FBZ), der nach drei falschen PIN-Eingaben die eID-PIN sperrt. Dadurch ergibt sich die Gefahr eines Denial of Service-Angriffs (DoS) über die kontaktlose Schnittstelle auf die eID-PIN durch mehrmaliges Falscheingeben der eID-PIN ohne Kenntnis des Inhabers. Um dies zu verhindern, wird der dritte Eingabeversuch erst nach erfolgreicher Eingabe der auf der Karte aufgedruckten CAN ermöglicht. Die Freigabe des dritten Versuchs gilt nur im aktuellen Secure Messaging-Kanal, d.h. die Freigabe verfällt bei einem Schließen des Kanals z.B. durch einen Reset des Chips. Dieses PIN-Schema ist in Abbildung 1 dargestellt.

Der oben beschriebene Ablauf der PIN-Eingaben kann prinzipiell vor dem Benutzer des Ausweises weitestgehend verborgen bleiben. Es ist z.B. vorstellbar, dass die lokal auf dem eigenen Rechner des Benutzers installierte Software (eID-Client) während der Installation die aufgedruckte CAN abfragt und später während der Anwendung einen gegebenenfalls notwendigen dritten Eingabe-Versuch automatisch (mit entsprechender Information des Nutzers) mit der CAN „freischaltet".

Zum Wechsel der eID-PIN gibt es zwei Möglichkeiten:

- Nach Eingabe der aktuellen eID-PIN kann der Inhaber eine neue eID-PIN setzen (Abschnitt 4.6);
- Um ein Neusetzen der eID-PIN auch dann zu ermöglichen, wenn der Ausweisinhaber seine aktuelle eID-PIN vergessen hat, gibt es zusätzlich die Möglichkeit, in einer Ausweisbehörde eine neue eID-PIN ohne Kenntnis der alten zu setzen. Das Recht, eine neue eID-PIN zu setzen, weist die Ausweisbehörde dabei über die Terminalauthentisierung nach (Abschnitt 7).

Die weiteren in [TR-03110] definierten Möglichkeiten zum Neusetzen der eID-PIN sind nicht implementiert.

3.3.4 Signatur-PIN

Für die Erzeugung qualifizierter elektronischer Signaturen verwaltet der Chip eine Signatur-PIN. Dabei handelt es sich nicht um ein PACE-Passwort, sondern sie wird, wie bei Signaturanwendungen üblich, mit dem VERIFY-Kommando an die Karte übertragen, vgl. [TR-03117]. Die Signatur-PIN ist

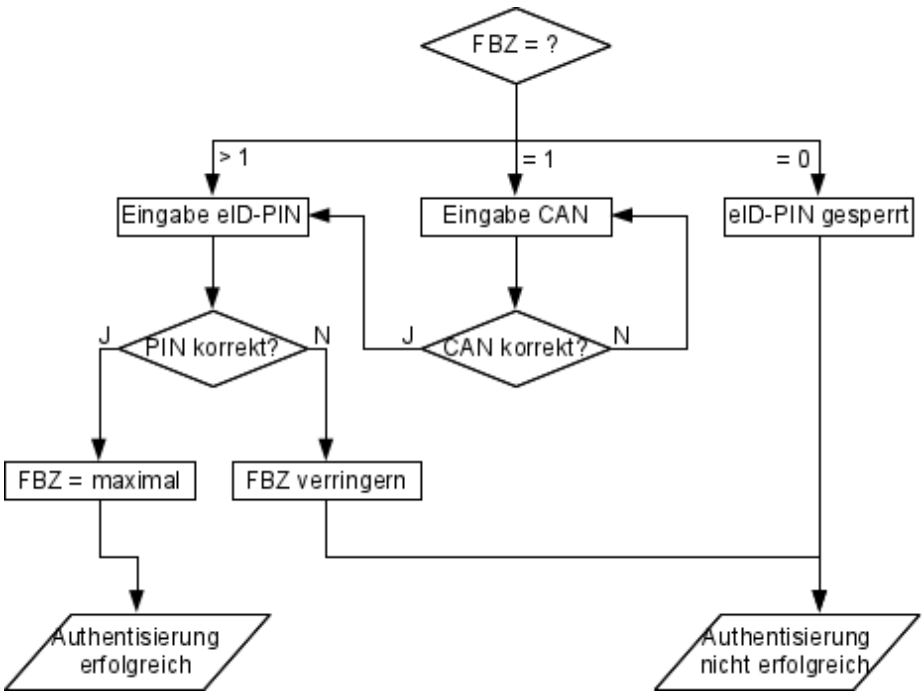

Abbildung 1: Eingabe der eID-PIN

eine sechsstellige dezimale Nummer und besitzt einen Fehlbedienungszähler, der die Signatur-PIN nach drei Falscheingaben sperrt.

Die Signatur-PIN kann

- nach Eingabe der aktuellen Signatur-PIN neu gesetzt werden;
- nach Authentisierung als *Signaturterminal* mit dem Recht *Generate qualified electronic signature*, sofern kein Signaturschlüsselpaar für qualifizierte elektronische Signaturen vorhanden ist bzw. dieses terminiert ist, mit der eID-PIN als PACE-Passwort terminiert und neu gesetzt werden.

Im Auslieferungszustand der Karte ist keine Signatur-PIN gesetzt, d.h. vor dem Erzeugen eines qualifizierten Schlüsselpaares muss der Inhaber eine Signatur-PIN setzen.

3.3.5 Pin Unblocking Key (PUK)

Das Entsperren der eID-PIN und der Signatur-PIN nach dreimaliger Falscheingabe erfolgt über einen zehnstelligen PUK (Abschnitt 4.6). Die eID-PIN und die Signatur-PIN sind jeweils mit einem Rücksetzzähler ausgestattet, die ein jeweils maximal zehnmaliges Zurücksetzen des Fehlbedienungszählers der eID- bzw. Signatur-PIN mit Hilfe des PUK erlauben. Der PUK selbst hat keinen Fehlbedienungszähler.

Der PUK ist ebenfalls zufällig erzeugt und Bestandteil des PIN-Briefes.

4. Zugriff auf Ausweisdaten

4.1 *General Authentication Procedure*

Ein Zugriff auf in dem Ausweis gespeicherte Daten erfolgt im Allgemeinen durch folgende Schritte:

Chip	Terminal
Lesen der Datei EF.CardAccess	
	Eingabe/Lesen PACE-Passwort (eID-PIN/CAN/MRZ)
PACE (Abschnitt 3.1.1)	
Übertragen der Zertifikatskette Terminalauthentisierung (Abschnitt 3.1.2)	
Lesen der Datei EF.CardSecurity	
	Passive Authentisierung EF.CardSecurity (Abschnitt 3.1.3)
Chipauthentisierung (Abschnitt 3.1.4)	
Authentisierungsterminal (optional): Abfrage der Dokumentengültigkeit (Abschnitt 4.4.1) *Authentisierungsterminal* (optional): Lesen des Sperrmerkmals (Abschnitt 4.4.2.1)	
	Authentisierungsterminal (optional): Sperrlistenabfrage – nur möglich, wenn Ausweis noch gültig (Abschnitt 5.3)
Inspektionssystem: Lesen des EF.SOD	
	Inspektionssystem: Signaturprüfung EF.SOD (Passive Authentisierung)
Optional: Auslesen der freigegebenen Daten (Abschnitt 3.2.3), Ausüben der speziellen Rechte (Abschnitt 4.4)	
	Inspektionssystem: Vergleichen der Hashwerte der ausgelesenen Datengruppen mit den in der Datei EF.SOD gespeicherten Werten

Nicht für alle technisch möglichen Rechtekombinationen werden entsprechende Zertifikate ausgegeben, so werden z.B. keine Rechte zur Installation der Signaturanwendung an *hoheitliche nationale Authentisierungsterminals* ausgegeben.

4.2 *Standard/Advanced ePassport Inspection Procedure*

Beim Aufenthaltstitel ist der Zugriff auf die Biometrieanwendung zusätzlich über die *Standard ePassport Inspection Procedure* bzw. die *Advanced ePassport Inspection Procedure* gemäß [TR-03110], Teil 1, möglich.

4.3 Inspektionssystem

Ein *Inspektionssystem* ist ein Terminal zur hoheitlichen Kontrolle, z.B. durch Polizei oder im Rahmen der Grenzkontrolle. Ein *Inspektionssystem* hat Lesezugriff auf die in der Biometrieanwendung gespeicherten MRZ-Daten (DG1) und das Gesichtsbild (DG2). Werden durch die Terminalauthentisierung die entsprechenden Rechte nachgewiesen, so hat ein *Inspektionssystem* auch Lesezugriff auf die Fingerabdrücke (DG3) und die Daten der eID-Anwendung.

In keinem Fall hat ein *Inspektionssystem* Zugriff auf die Signaturanwendung oder Schreibzugriff auf den Chip.

Terminaltyp		**PACE-Passwort**	**Mögliche Terminalrechte**
Inspektionssystem (hoheitlich national bzw. hoheitlich ausländisch)	*General Authentication Procedure*	CAN; MRZ	• Lesezugriff auf DG1 (MRZ), DG2 (Gesichtsbild) der Biometrieanwendung • Lesezugriff auf Daten der eID-Anwendung • Lesezugriff auf DG3 (Fingerabdrücke) der Biometrieanwendung je nach nachgewiesenen Rechten
	Nur eAT: *Standard ePassport Inspection Procedure*	CAN; MRZ	Lesezugriff auf DG1 (MRZ), DG2 (Gesichtsbild) der Biometrieanwendung
	Nur eAT: *Advanced ePassport Inspection Procedure*	CAN; MRZ	Lesezugriff auf DG1 (MRZ), DG2 (Gesichtsbild), DG3 (Fingerabdrücke) der Biometrieanwendung
Authentisierungsterminal (hoheitlich national bzw. nicht-hoheitlich/ausländisch)		eID-PIN; CAN falls Recht *CAN allowed* nachgewiesen	Lese-/Schreibzugriff auf die Datengruppen der eID-Anwendung gemäß authentisierten Rechten Spezielle Rechte: • Erzeugung eines Signaturschlüsselpaares • eID-PIN setzen, eID-Anwendung An-/Ausschalten • Pseudonym • Altersverifikation • Wohnortabfrage
Signaturterminal		CAN	• Erzeugung qualifizierter Signaturen mit zusätzlicher Eingabe der Signatur-PIN • Setzen einer neuen Signatur-PIN mit zusätzlicher Eingabe der alten Signatur-PIN
		eID-PIN	• Anlegen der Signatur-PIN • Terminieren des Schlüssels für qualifizierte Signaturen und der Signatur-PIN
Nicht authentisiertes Terminal		eID-PIN	Setzen einer neuen eID-PIN
		PUK	Zurücksetzen der Fehlbedienungszähler von eID-PIN/Signatur-PIN

Tabelle 4: Teminaltypen

4.4 Authentisierungsterminal

Ein *Authentisierungsterminal* ist berechtigt, auf die eID-Anwendung zuzugreifen. Dabei wird durch die in der Authentisierung vergebenen Rechte festgelegt, welche Daten/Funktionen freigegeben werden. Die Datenfelder werden in Abschnitt 3.2.3 aufgelistet. Zusätzlich kann einem *Authentisierungsterminal* das Recht zugeteilt werden, bestimmte Daten auf dem Chip (z.B. die aktuelle Adresse) zu ändern.

Unterschieden wird zwischen *hoheitlichen nationalen Authentisierungsterminals* und *nicht-hoheitlichen/ausländischen Authentisierungsterminals*.

Für *hoheitliche nationale Authentisierungsterminals* wird im Allgemeinen das Recht *CAN allowed* gesetzt, d.h. es kann die CAN als PACE-Passwort genutzt werden. Bei Verwendung der CAN ist keine Personenbindung möglich, d.h. die Personenbindung muss z.B. durch die Identifizierung des Inhabers über das Ausweisbild erfolgen. Genutzt werden *hoheitliche nationale Authentisierungsterminals* z.B. für den Änderungsdienst in den Ausweisbehörden, vgl. Abschnitt 7.

Nicht-hoheitliche/ausländische Authentisierungsterminals benötigen je nach Anwendungsfall und Berechtigung entweder die Eingabe der geheimen eID-PIN oder der CAN. Verwendet werden *nicht-hoheitliche/ausländische Authentisierungsterminals* z.B. für den elektronischen Identitätsnachweis (mit eID-PIN), siehe Abschnitt 4.7, und das Vor-Ort-Auslesen (mit CAN), siehe Abschnitt 4.8.

Neben dem Lesen personenbezogener Daten bietet die eID-Anwendung einige spezielle Funktionen (siehe die folgenden Abschnitte), für die das *Authentisierungsterminal* nach Durchführung der *General Authentication Procedure* berechtigt ist bzw. spezielle über die Terminalauthentisierung nachgewiesene Zugriffsrechte benötigt. Die genaue Umsetzung dieser Funktionen wird in [TR-03110] spezifiziert.

4.4.1 Abfrage der Dokumentengültigkeit

Ein Diensteanbieter muss im Rahmen einer Authentisierung sicherstellen können, dass der Ausweis noch nicht abgelaufen ist. Dies kann prinzipiell durch das Auslesen des Ablaufdatums realisiert werden. Aus Gründen der Datensparsamkeit wird die Überprüfung der Dokumentengültigkeit aber durch eine Anfrage an den Ausweis durchgeführt, d.h. der Diensteanbieter sendet ein Testdatum (im Allgemeinen das aktuelle Datum) zum Ausweis und erhält als Antwort, ob zu diesem Zeitpunkt der Ausweis noch gültig ist. Dadurch ist ein Auslesen des Ablaufdatums nicht notwendig.

Das Testdatum wird als Teil der Terminalauthentisierung übergeben, um ein gezieltes Eingrenzen des Ablaufdatums durch wiederholtes Anfragen mit verschiedenen Testdaten zu verhindern.

4.4.2 Pseudonyme Merkmale

Der Ausweis bietet die Möglichkeit der pseudonymen Authentisierung, d.h. der Ausweisinhaber kann sich gegenüber einem Diensteanbieter authentisieren, ohne persönliche Daten freizugeben. Insbesondere bildet der Ausweis für jeden Diensteanbieter ein anderes Pseudonym, so dass das Verbinden von Pseudonymen über Diensteanbietergrenzen hinweg nicht möglich ist.

Auf der anderen Seite wird für den Eintrag in eine Sperrliste (z.B. für gestohlene Ausweise) prinzipiell eine Ausweiskennung bzw. ein anderes Sperrmerkmal notwendig, um die Sperrliste abfragen zu können. Um nun zu verhindern, dass über das Sperrmerkmal die Pseudonymität aufgehoben wird, ist auch das Sperrmerkmal anbieterspezifisch. Für die Abfrage der Sperrliste werden dem Diensteanbieter anbieterspezifische Sperrlisten zur Verfügung gestellt (Abschnitt 5.3).

Die pseudonymen Merkmale können mittels der Protokolle Restricted Identification oder Pseudonymous Signature Authentication (PSA) als Bestandteil der Chipauthentisierung Version 3 erzeugt werden (siehe [TR-03110]).

Um sicherzustellen, dass jeder Diensteanbieter nur seine pseudonyme Merkmale erzeugen kann, ist die jeweilige Kennung des Diensteanbieters (*Terminal Sector*) Bestandteil des Zugriffszertifikats des Diensteanbieters, das vom Chip überprüft wird. Aus dieser Kennung und einem auf dem Chip gespeicherten Geheimnis erzeugt der Chip das jeweilige pseudonyme Merkmal. Dabei kann von dem Merkmal für einen Diensteanbieter nicht auf das Merkmal eines anderen Anbieters geschlossen werden.

Chipseitig wird für pseudonymen Sperrmerkmale das gleiche Geheimnis für die Erzeugung mittels Restricted Identification und Pseudonymous Signature Authentication genutzt, so dass bei gleichem Terminal Sector die beiden Protokolle i.W. das gleiche Sperrmerkmal liefern, für Detail siehe [TR-03110], Part 2).

4.4.2.1 Lesen des Sperrmerkmals

Der Diensteanbieter kann nach erfolgreicher Authentisierung mit der *General Authentication Procedure* sein spezifisches Sperrmerkmal erzeugen.

4.4.2.2 Anbieter- und kartenspezifische Kennung (Pseudonym)

Zur Pseudonymerzeugung muss durch das Terminal das Recht *Restricted Identification* bzw. *PSA* nachgewiesen werden.

4.4.3 Erzeugung eines Signaturschlüsselpaares

Zur Installation der Signaturanwendung muss das Terminal das Recht *Install Qualified Certificate* nachweisen.[14]

Über diese Funktion kann der Ausweisinhaber mit Hilfe eines qualifizierten Vertrauensdiensteanbieters Schlüsselpaare für die Signaturanwendung erzeugen und entsprechende Zertifikate nachladen. Voraussetzung für die Erzeugung eines Schlüsselpaares für qualifizierte elektronische Signaturen ist das Setzen einer Signatur-PIN durch den Ausweisinhaber (Abschnitt 3.3.4).

Der qualifizierte Vertrauensdiensteanbieter (qVDA) authentisiert sich gegenüber dem Ausweis als *nicht-hoheitliches/ausländisches Authentisierungsterminal* und stellt die Identität des Inhabers durch Auslesen geeigneter Datengruppen (entsprechend der authentisierten Leserechte) der eID-Anwendung fest. Anschließend wird durch den qVDA die Schlüsselerzeugung auf dem Chip gestartet, der so erzeugte öffentliche Schlüssel ausgelesen und ein qualifiziertes Zertifikat auf dem Chip gespeichert.

Der qVDA darf ein qualifiziertes Zertifikat maximal für die Gültigkeitsdauer des Ausweises ausstellen.

Der genaue Ablauf ist in [TR-03117] definiert.

4.4.4 eID-PIN setzen, eID-Anwendung anschalten

Benötigt den Nachweis des Rechtes *PIN Management* durch das Terminal.

Mit dieser Funktion kann der Ausweisinhaber an einem *Authentisierungsterminal* eine neue eID-PIN setzen. Dies ist für den Fall gedacht, dass der Ausweisinhaber seine eID-PIN vergessen hat und somit nicht in der Lage ist, selbst mittels Eingabe der alten eID-PIN eine neue zu setzen, vgl. Abschnitt 3.3.3. Umgesetzt wird dies über den Änderungsdienst, vgl. Abschnitt 7.

Zusätzlich wird über dieses Recht das Anschalten der eID-Anwendung im Änderungsdienst (Abschnitt 7) realisiert. Bei abgeschalteter eID-Anwendung ist hierbei nur die Benutzung mit der eID-PIN als Passwort deaktiviert, d.h. *Authentisierungsterminals* ohne Recht *CAN allowed* können nicht mehr auf die eID-Anwendung zugreifen. *Inspektionssysteme* und *Authentisierungsterminals* mit Recht *CAN allowed* können weiterhin auf die eID-Anwendung zugreifen.

14 Hinweis: Zur Zeit wird dieser Dienst durch keinen Vertrauensdiensteanbieter angeboten.

4.4.5 Altersverifikation

Benötigt den Nachweis des Rechtes *Age Verification* durch das Terminal.

Ein wichtiger Anwendungsfall für die eID-Anwendung ist die sichere Altersverifikation eines Ausweisinhabers. Um die Freigabe des Geburtsdatums zu vermeiden, wird sie nicht über einen Zugriff auf das Geburtsdatum realisiert, sondern mittels einer „Anfrage" an den Ausweis, ob der Inhaber vor einem bestimmten Testdatum geboren ist.

Das Testdatum wird als Teil der Terminalauthentisierung übergeben und vom Chip verifiziert, um ein gezieltes Eingrenzen des Alters des Inhabers durch wiederholtes Anfragen mit verschiedenen Testdaten zu verhindern.

4.4.6 Wohnortabfrage

Zur Wohnortabfrage benötigt das Terminal das Recht *Community ID Verification*.

Um lokalisierte Dienste zu ermöglichen, bietet die eID-Anwendung analog zur Altersverifikation die Verifikation eines bestimmten Wohnortes. Genutzt wird für diese Überprüfung für Adressen in Deutschland der amtliche Gemeindeschlüssel des Wohnortes, der während der Personalisierung auf dem Ausweis gespeichert wird und im Falle einer Adressänderung, ebenso wie die Adresse, elektronisch aktualisiert wird (Abschnitt 7).

Der amtliche Gemeindeschlüssel enthält Angaben über das Bundesland, den Regierungsbezirk, die Stadt bzw. den Kreis und die Gemeinde. Die Wohnortabfrage ermöglicht neben einer Anfrage auf einen bestimmten Wohnort (Gemeinde) auch eine Anfrage entsprechend der anderen Gliederungsebenen (Bundesland, Regierungsbezirk, Kreis), siehe Abschnitt 3.2.3. Dadurch ist es einem Diensteanbieter z.B. möglich, Dienste nur für Einwohner eines bestimmten Bundeslandes anzubieten.

Für Adressen im Ausland ist nur eine Prüfung auf das Land möglich.

Analog zur Altersverifikation wird der abgefragte Ort als Teil der Terminalauthentisierung übergeben, so dass ein Diensteanbieter den Wohnort nicht durch wiederholtes Abfragen eingrenzen kann.

4.5 Signaturterminal

An einem *Signaturterminal* kann bei Nutzung der CAN als Passwort und zusätzlicher Eingabe/Verifikation der Signatur-PIN

- eine qualifizierte Signatur ausgelöst werden, sofern ein Schlüsselpaar für qualifizierte Signaturen erzeugt wurde (vgl. Abschnitt 4.4.3);
- eine neue Signatur-PIN gesetzt werden.

Bei Nutzung der eID-PIN als PACE-Passwort kann eine vorhandene Signatur-PIN und das Schlüsselpaar für qualifizierte Signaturen gelöscht werden.

Die genauen Abläufe werden in [TR-03117] spezifiziert.

4.6 Nicht authentisiertes Terminal

Für bestimmte, durch den Ausweisinhaber lokal durchgeführte administrative Vorgänge wird keine Terminal- und Chipauthentisierung benötigt.

4.6.1 Setzen einer neuen eID-PIN mit der aktuellen eID-PIN

Zum Setzen einer neuen eID-PIN authentisiert sich der Ausweisinhaber zunächst durch die Eingabe der aktuellen geheimen eID-PIN. Diese eID-PIN wird dem Chip gegenüber durch das PACE-Protokoll nachgewiesen. Anschließend wird die neue eID-PIN an den Chip übertragen und vom Chip aktiviert.

Der genaue Ablauf ist in [TR-03110] spezifiziert.

4.6.2 Rücksetzen des Fehlbedienungszählers der eID-PIN/Signatur-PIN mit PUK

Zum Zurücksetzen des Fehlbedienungszählers der eID-PIN oder der Signatur-PIN wird PACE mit dem PUK als Passwort durchgeführt und anschließend der oder die Fehlbedienungszähler zurückgesetzt. Jeder PIN (eID-PIN/Signatur-PIN) ist ein Rücksetzzähler zugeordnet, der ein maximal zehnmaliges Zurücksetzen mittels des PUK des zugehörigen Fehlbedienungszählers erlaubt.

Der genaue Ablauf ist in [TR-03110] für die eID-PIN bzw. [TR-03117] für die Signatur-PIN spezifiziert.

4.7 Elektronischer Identitätsnachweis

Der elektronische Identitätsnachweis (oder Online-Authentisierung / Online-Ausweisfunktion), d.h. die Authentisierung gegenüber einem Diensteanbieter (Diensteanbieter nach § 21 [PAuswG] bzw. Identifizierungsdiensteanbieter nach § 21b [PAuswG]) über ein Netzwerk (Internet), ist ein Spezialfall eines Zugriffs durch ein *Authentisierungsterminal* mit der *General Authentication Procedure*. Hier wird die Rolle des *Authentisierungsterminals* aufgeteilt auf das lokale Terminal (bestehend aus Lesegerät und lokalem Rechner einschließlich der benötigten Software) und auf den Diensteanbieter als entferntem Terminal. Voraussetzung für die eigentliche Online-Authentisierung ist eine bestehende Verbindung zwischen lokalem Terminal und entferntem Terminal (Diensteanbieter), beispielsweise in Form einer SSL/TLS-Verbindung.

Der elektronische Identitätsnachweis läuft in folgenden Schritten ab:

<table>
<tr><th>Chip</th><th>Lokales Terminal</th><th>Diensteanbieter</th></tr>
<tr><td></td><td colspan="2">Übertragen des Diensteanbieterzertifikats</td></tr>
<tr><td></td><td>Präsentation des Zertifikats
Einschränken der Zugriffsrechte durch Benutzer
Zustimmung Nutzer durch Eingabe der eID-PIN</td><td></td></tr>
<tr><td colspan="2">Lesen der Datei EF.CardAccess
PACE mit eID-PIN als Passwort (Abschnitt 3.1.1)</td><td></td></tr>
<tr><td colspan="3">Übertragen der vollständigen Zertifikatskette
Terminalauthentisierung (Abschnitt 3.1.2)</td></tr>
<tr><td colspan="3">Lesen der Datei EF.CardSecurity</td></tr>
<tr><td></td><td></td><td>Passive Authentisierung
(Abschnitt 3.1.3)</td></tr>
<tr><td colspan="3">Chipauthentisierung (Abschnitt 3.1.4)</td></tr>
<tr><td colspan="3">Lesen des Sperrmerkmals (Abschnitt 4.4.2.1), Abfrage der Dokumentengültigkeit (Abschnitt 4.4.1)</td></tr>
<tr><td></td><td></td><td>Sperrlistenabfrage
(Abschnitt 5.3)</td></tr>
<tr><td colspan="3">Auslesen der freigegebenen Daten (Abschnitt 3.2.3),
Ausüben der speziellen Rechte[15] (Abschnitt 4.4)</td></tr>
</table>

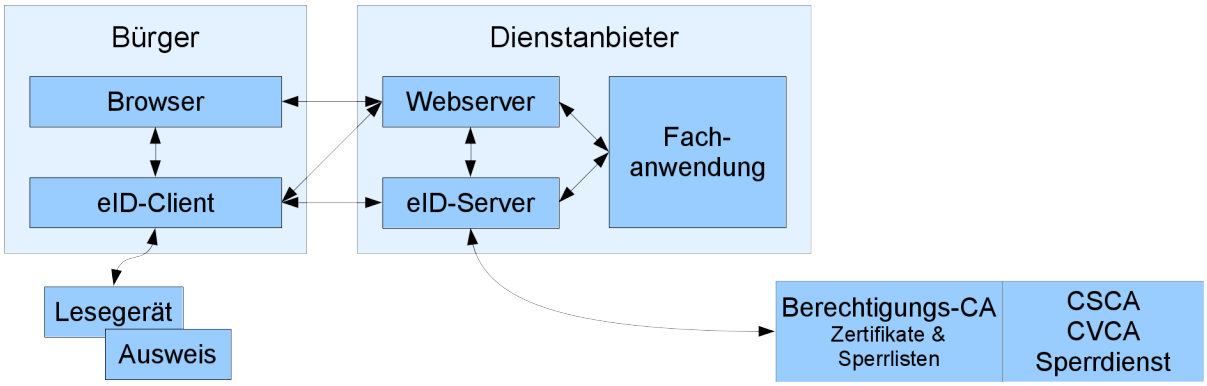

Abbildung 2: Kommunikationsbeziehungen elektronischer Identitätsnachweis

Im zweiten Schritt wird das Berechtigungs-Zertifikat des Diensteanbieters einschließlich der Informationen über den Diensteanbieter (siehe Abschnitt 5.2.1) dem Benutzer durch die lokale Software (eID-Client) präsentiert.

Gemäß § 18 (4) [PAuswG] muss der Benutzer die Gelegenheit haben, die folgenden Daten einzusehen:

- Name, Anschrift und Email-Adresse des Diensteanbieters;
- Erwünschte Zugriffsrechte; Abfragedatum für Altersverifikation, falls eine Altersverifikation durchgeführt werden soll;
- Hinweis auf die für den Diensteanbieter zuständige Datenschutzbehörde;
- Gültigkeitszeitraum des Zertifikats.

Der Benutzer hat die Möglichkeit, die vom Diensteanbieter durch das Zertifikat erbetenen Zugriffsrechte weiter einzuschränken. Die eingeschränkten Rechte werden als Bestandteil des nachfolgenden PACE-Protokolls an den Chip übertragen. Durch Eingabe der eID-PIN wird das Auslesen der Daten an das Einverständnis des Inhabers und gleichzeitig der Ausweis an den Inhaber gebunden.

Da PACE einen sicheren Kanal zwischen Chip und lokalem Terminal aufbaut, wird die Kommunikation zwischen Diensteanbieter und Chip in den nachfolgenden Authentisierungsschritten (Terminalauthentisierung, Passive Authentisierung, Chipauthentisierung) durch das lokale Terminal verschlüsselt und integritätsgesichert bzw. die Antworten des Chips entschlüsselt und auf Integrität geprüft. Als Bestandteil der Chipauthentisierung wird ein durchgehender gesicherter Kanal zwischen Chip und Diensteanbieter aufgebaut, so dass das lokale Terminal ab jetzt die Kommandos und die Antworten nur noch unverändert weiterreicht.

Zur Umsetzung des elektronischen Identitätsnachweises (vgl. Abbildung 2) empfiehlt das BSI die Verwendung geeigneter Komponenten, vgl. auch Anhang A:

- Kartenleser gemäß [TR-03119];
- Lokale Client-Software (eID-Client) gemäß [TR-03124], Teil 1;
- Komponente (eID-Server) auf Seiten des Diensteanbieters für die Kommunikation mit dem eID-Client und der Berechtigungs-PKI (Abschnitt 5.2) gemäß [TR-03130]. Der eID-Server kann durch den Diensteanbieter selbst oder durch einen beauftragten eID-Service (Auftragsdatenverarbeitung) betrieben werden.

Vorgaben für den Diensteanbieter bzw. für die Integration des elektronischen Identitätsnachweises in Webanwendungen finden sich in [TR-03128], Teil 1.

15 Bei Chip Authentisierung Version 3 wird das Pseudonym bei Vorliegen der entsprechenden Berechtigung bereits in Rahmen der Chip Authentisierung zurückgegeben.

4.8 Vor-Ort-Auslesen

Das Vor-Ort-Auslesen ist ebenfalls ein Spezialfall eines Zugriffs durch ein *Authentisierungsterminal* mit der *General Authentication Procedure*. Das Vor-Ort-Auslesen dient nicht der Authentisierung des Ausweisinhabers, sondern der medienbruchfreien und automatisierten Übernahme der Ausweisdaten in eine Anwendung, etwa ein Formular.

Die Identifizierung des Ausweisinhabers muss vor dem Auslesen der Daten auf anderem Wege erfolgen, z.B. über eine Identifizierung über das aufgedruckte Lichtbild.

Nach erfolgter Identifizierung und nach Zustimmung des Ausweisinhabers erfolgt das Vor-Ort-Auslesen in folgenden Schritten:

Chip	**Terminal**
	Erfassen der CAN
Lesen der Datei EF.CardAccess PACE mit CAN als Passwort (Abschnitt 3.1.1)	
Übertragen der Zertifikatskette; Terminalauthentisierung (Abschnitt 3.1.2)	
Lesen der Datei EF.CardSecurity	
	Passive Authentisierung (Abschnitt 3.1.3)
Chipauthentisierung (Abschnitt 3.1.4)	
Lesen des Sperrmerkmals (Abschnitt 4.4.2.1), Abfrage der Dokumentengültigkeit (Abschnitt 4.4.1)	
	Sperrlistenabfrage (Abschnitt 5.3)
Auslesen der freigegebenen Daten (Abschnitt 3.2.3), Ausüben der speziellen Rechte (Abschnitt 4.4)	

Vorgaben für den Vor-Ort-Auslese-Anbieter bzw. für die Integration des Vor-Ort-Auslesens in Anwendungen finden sich in [TR-03128], Teil 1.

5. Hintergrundsysteme

5.1 Dokumenten-PKI

Bestimmte auf dem Chip gespeicherte Daten (Daten der Biometrieanwendung, die Dateien EF.CardSecurity/EF.ChipSecurity, die u.a. die öffentlichen Schlüssel der Chipauthentisierung enthalten) werden während der Personalisierung beim Ausweishersteller digital signiert. Die Authentizität der Signatur wird über die Dokumenten-PKI nach [ICAO 9303] nachgewiesen.

Die Dokumenten-PKI besteht aus zwei Stufen:

- die Wurzelinstanz (CSCA, Country Signing Certification Authority), betrieben vom BSI;
- dem Document Signer (DS), betrieben vom Ausweishersteller.

Die Zertifikate über die öffentlichen Schlüssel des Document Signers sind auf dem Chip in der Datei EF.CardSecurity gespeichert.

Die Zertifikate der Dokumenten-PKI sind X.509-Zertifikate. Das genaue Zertifikats-Profil wird in [ICAO 9303] und in der Certificate Policy [CP-CSCA] der Wurzelinstanz der Dokumenten-PKI (CSCA) definiert.

Das Zertifikat über den öffentlichen Schlüssel der Wurzelinstanz sowie Rückruflisten (Certificate Revocation Lists – CRLs) sind von der Wurzelinstanz erhältlich. Für die Diensteanbieter des eBusiness/eGovernment werden diese Zertifikate und Sperrlisten durch die jeweiligen Berechtigungs-CAs zur Verfügung gestellt.

5.2 Berechtigungs-PKI

Im Rahmen der Terminalauthentisierung (Abschnitt 3.1.2) wird eine Zertifikatskette an den Chip übermittelt. Durch diese Kette werden der Typ des Terminals (*Inspektionssystem, Authentisierungsterminal, Signaturterminal*, Abschnitt 4) sowie die maximalen Rechte des Terminals festgelegt. Diese Zertifikatskette wird durch die Berechtigungs-PKI erzeugt.

Die Berechtigungs-PKI besteht aus drei Stufen:

- die Wurzelinstanz (CVCA, Country Verifying Certification Authority), betrieben vom BSI;
- mehrere Document Verifier (DV);
- die *Inspektionssysteme*, *Authentisierungsterminals* und *Signaturterminals*.

Für verschiedene Anwendungsbereiche werden separate Document Verifier betrieben:

- Qualitätssicherung beim Ausweishersteller und im BSI;
- Anwendungen in den Ausweisbehörden – Änderungsdienst/Visualisierung (Abschnitt 7);
- Berechtigungs-CAs für eBusiness/eGovernment-Diensteanbieter (elektronischer Identitätsnachweis, Vor-Ort-Auslesen unter Anwesenden – siehe Abschnitt 5.2.1);
- hoheitliches Kontrollwesen – Polizei und Grenzkontrolle;
- *Signaturterminals* erhalten ein Zertifikat für den Zugriff auf die Signaturfunktion (Abschnitt 5.2.2).

Die Zertifikate der Berechtigungs-PKI sind CV-Zertifikate (Card Verifiable Certificates) nach [ISO 7816], Teil 6 und [TR-03110]. Da der Chip keine Rückruflisten für die Zertifikate verarbeiten kann,

werden stattdessen die Terminalzertifikate – ausgenommen Zertifikate für *Signaturterminals* – mit einer kurzen Laufzeit ausgestellt.

Da der Ausweis keine eigene Stromversorgung (Batterie) enthält, enthält der Chip keine Uhr. Um dennoch eine Kontrolle der Gültigkeit der Zertifikate durch den Chip zu ermöglichen, speichert der Chip ein angenähertes aktuelles Datum, das dieser aus den Ausstellungsdaten bestimmter vorgelegter Zertifikate ableitet. Berücksichtigt werden hier

- CVCA- und DV-Zertifikate
- Terminalzertifikate von *hoheitlichen nationalen Inspektionssystemen* und *hoheitlichen nationalen Authentisierungsterminals*.

Grundlage für die Berechtigungs-PKI sind die Certificate Policies der CVCA ([CP-ePass], [CP-eID], [CP-eSign]). Auf dieser Grundlage erstellen die verschiedenen CA-Betreiber dieser PKI ihre Umsetzungskonzepte und Certificate Policies. Die Protokolle zur Kommunikation der Instanzen der Berechtigung-PKI untereinander werden in [TR-03129] spezifiziert.

5.2.1 Zertifikatsvergabe für eBusiness/eGovernment

Die Zugriffszertifikate für *nicht-hoheitliche/ausländische Authentisierungsterminals* (d.h. für den elektronischen Identitätsnachweis und das Vor-Ort-Auslesen) werden durch Berechtigungs-CAs vergeben. Voraussetzung ist hierfür die Erteilung einer Berechtigung durch die Vergabestelle für Berechtigungszertifikate (VfB). Ausgenommen sind Anbieter des öffentlichen Sektors in EU-Mitgliedstaaten, die gemäß [eIDAS] / § 21 (7) [PAuswG] ohne Verwaltungsverfahren für den elektronischen Identitätsnachweis berechtigt sind.

Ein Diensteanbieter, der den elektronischen Identitätsnachweis oder das Vor-Ort-Auslesen für seine Geschäftsprozesse nutzen möchte, wendet sich an die VfB, um eine Berechtigung zu erhalten. Zu Details zu notwendigen Unterlagen siehe die Verfahrensbeschreibung der Vergabestelle [VfB].

Es wird empfohlen, für die Einbindung des elektronischen Identitätsnachweises bzw. des Vor-Ort-Auslesens ein Sicherheitskonzept zur erstellen oder, wenn vorhanden, ein bestehendes Sicherheitskonzept entsprechend zu erweitern. Für Identifizierungsdiensteanbieter ist ein Sicherheitskonzept und dessen Zertifizierung verbindlich, siehe auch [TR-03128], Teil 2.

Auf Basis der Berechtigung kann der Diensteanbieter bei einer Berechtigungs-CA die Ausstellung des benötigten Zugriffszertifikats beantragen.

Durch das Zugriffszertifikat werden zusätzlich zu den üblichen Angaben in Zertifikaten der Berechtigungs-PKI (wie z.B. Terminaltyp, Zugriffsrechte, Gültigkeitszeitraum) durch *Certificate Extensions* weitere Angaben zertifiziert:

- `TerminalSector`, jeweils für die Protokolle *Restricted Identification* und *Pseudonymous Signature Authentication*, des Diensteanbieters für die anbieter- und kartenspezifischen Kennungen und das Sperrmerkmal;
- die `CertificateDescription` mit Angaben, die dem Benutzer bei der Nutzung des elektronischen Identitätsnachweises (Abschnitt 4.7) angezeigt werden können (siehe auch [CP-eID]):
  - Name des Diensteanbieters (`subjectName`);
  - Name der ausstellenden Berechtigungs-CA (`issuerName`);
  - Anschrift und Email-Adresse des Diensteanbieters, Zweck der Anfrage des Dienstanbieters[16], Typ des Diensteanbieters[17] und die zuständige Datenschutzbehörde (`termsOfUsage`);

16 Nur für vor dem 15.07.2017 erteilte Berechtigungen.

17 Im Falle von Identifizierungsdiensteanbietern oder Vor-Ort-Diensteanbietern

- Im Falle von Zertifikaten, die für den elektronischen Identitätsnachweis ausgestellt werden, sind weiter die Hash-Werte der TLS-Zertifikate des Diensteanbieters (und ggfs. eines eID-Servers) zur Überprüfung durch den eID-Client des Bürgers enthalten (`commCertificates`).

Die *Extensions* werden in [TR-03110], Teil 4, spezifiziert.

Die genauen technischen und organisatorischen Abläufe werden in den Certificate Policies (CP) der Berechtigungs-CAs festgelegt, die diese basierend auf der Certificate Policy [CP-eID] der Wurzel-Instanz der Berechtigungs-PKI erstellen. Die Kommunikationsprotokolle werden in [TR-03129] festgelegt.

5.2.2 *Signaturterminals*

Signaturterminals sind mit eigenen Berechtigungszertifikaten ausgestattet, die durch den Ausweis im Rahmen der Terminalauthentisierung überprüft werden. Dazu wird ein Zertifikat für eine bestimmte Leserbauart ausgestellt. Die Zertifikate sind längere Zeit gültig, um ein häufiges Erneuern des Zertifikates zu vermeiden. Details sind in [TR-03119] und [CP-eSign] beschrieben.

5.3 Ausweis-Sperrlisten

Verschiedene Funktionen des Ausweises können über verschiedene Methoden gesperrt werden:

- Sperre der eID-PIN durch dreimalige Falscheingabe der eID-PIN (Abschnitt 3.3.3);
- Sperrmeldung an die Ausweisbehörde oder Sperrhotline (vgl. Abbildung 3):

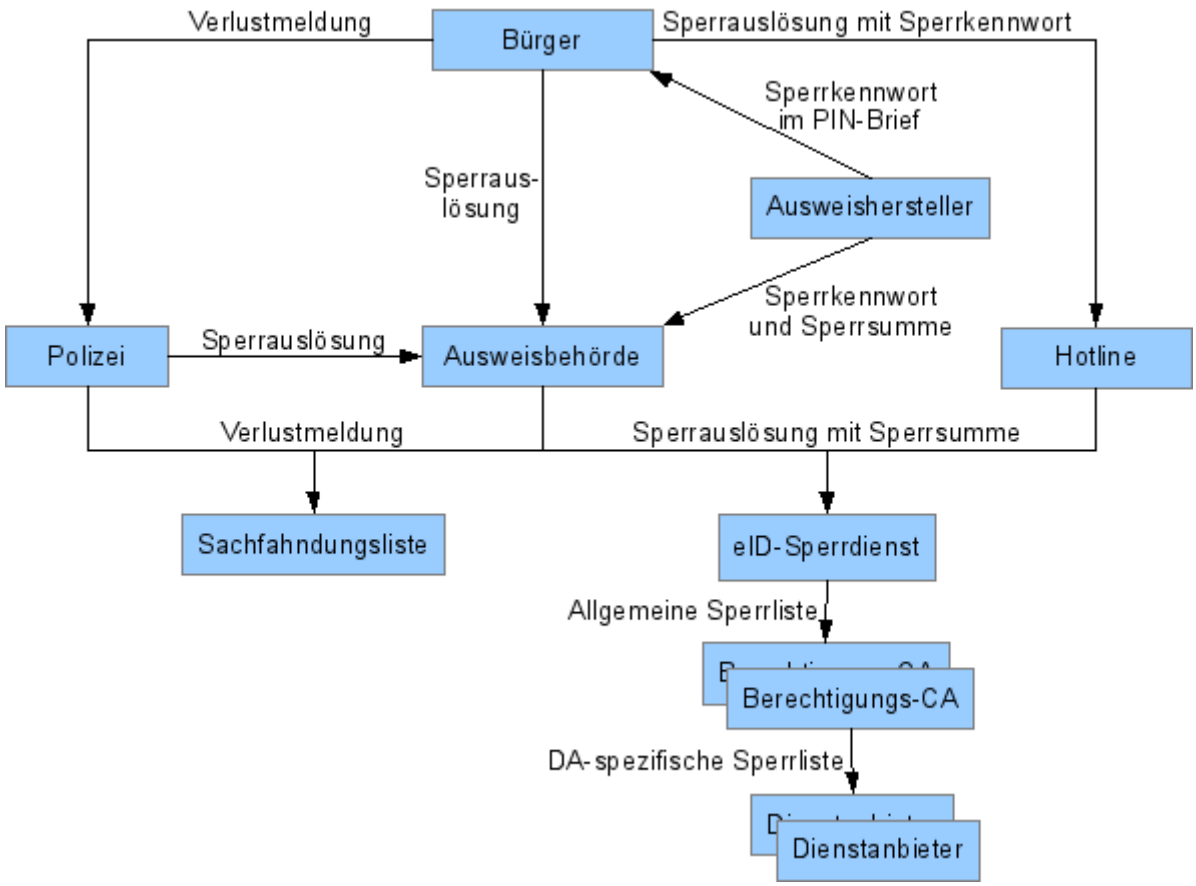

Abbildung 3: Sperrlisten

- Für verlorene / gestohlene Ausweise ist der primäre Weg die Meldung des Ausweises als verloren oder gestohlen über die Ausweisbehörde, die den Ausweis ausgestellt hat, oder die Polizei. Dadurch wird der Ausweis in die polizeiliche Sachfahndungsliste und in die vom Sperrdienst geführte eID-Sperrliste für die eID-Anwendung eingetragen.
- Daneben steht ein Sperrhotline für die Sperrung zur Verfügung. Im Falle verlorener / gestohlener Ausweise ist die Verlustmeldung an die Ausweisbehörde zusätzlich so bald wie möglich durchzuführen.

- Die Zertifikate der Signaturfunktion werden nicht über die Ausweisbehörde oder die Polizei gesperrt, sie müssen beim ausstellenden qualifizierten Zertifizierungsdiensteanbieter gesperrt werden.

Die polizeiliche Sachfahndungsliste dient ausschließlich der Verwendung durch Polizei und andere Kontrollbehörden.

5.3.1 eID-Sperrliste

Die vom Sperrdienst geführte eID-Sperrliste für Diensteanbieter dient nur der Sperre der eID-Anwendung des Ausweises für eBusiness und eGovernment-Diensteanbieter, nicht des Ausweises als hoheitliches Dokument.

5.3.1.1 Sperrauslösung

Die Sperrauslösung erfolgt durch die Angabe eines Sperrkennwortes, das durch den Hersteller während des Herstellungsprozesses erzeugt wird. Dieses Sperrkennwort wird dem Ausweisinhaber über den PIN/PUK-Brief (Abschnitt 6.2) mitgeteilt sowie im jeweiligen Dokumentenregister gespeichert.

Basis für die Sperrung eines Ausweises ist ein während des Herstellungsprozesses erzeugter kryptographischer Sperrschlüssel.

Im Falle einer Sperre wird durch die Hotline bzw. die Ausweisbehörde aus Vorname, Name, Geburtsdatum und Sperrkennwort die *Sperrsumme* erzeugt oder aus dem Ausweisregister abgerufen. Dieser Wert wird an den Sperrdienst übermittelt. Während der Ausweisherstellung wird die Sperrsumme zusammen mit dem Sperrschlüssel erzeugt, an den Sperrdienst übermittelt und dort zur Verwendung für eine spätere Sperre gespeichert. Anhand der gespeicherten Liste wird der Sperrsumme in den Sperrschlüssel übersetzt (siehe auch Anhang B)

Der Ablauf einer Sperrmeldung bei der Ausweisbehörde bzw. Hotline ist dann:

1. Der Ausweisinhaber löst die Sperrung aus;
2. Die Ausweisbehörde bzw. Hotline ruft die Sperrsumme aus dem Ausweisregister ab bzw. berechnet sie aus dem Sperrkennwort und Vorname, Nachname und Geburtsdatum des Ausweisinhabers;
3. Die Sperrsumme wird an den Sperrlistenbetreiber übermittelt;
4. Anhand der empfangenen Sperrsumme ermittelt der Sperrlistenbetreiber den für die Sperrung relevanten Sperrschlüssel und verwendet diesen zum Eintrag in die Sperrliste.

5.3.1.2 Anbieterspezifische Sperrlisten

Um eine Auflösung des Pseudonyms (Abschnitt 4.4.2.2) über die Sperrlistenabfrage zu verhindern, wird zur Abfrage der eID-Sperrliste ein anbieterspezifisches Sperrmerkmal verwendet (Abschnitt 4.4.2.1). Das anbieterspezifische Sperrmerkmal wird vom Diensteanbieter während einer Authentisierung ausgelesen und darf von diesem nur zum Abgleich mit der eID-Sperrliste verwendet werden.

Aus dem Sperrschlüssel werden in einem mehrstufigen Verfahren die anbieterspezifischen Sperrmerkmale erzeugt:

1. Der Sperrdienst rechnet den Sperrschlüssel in ein allgemeines Sperrmerkmal um;
2. Die Berechtigungs-CAs rufen die Liste der allgemeinen Sperrmerkmale beim Sperrdienst ab;
3. Die Berechtigungs-CAs rechnen die Liste der allgemeinen Sperrmerkmale in anbieterspezifische Listen mit Sperrmerkmalen um;
4. Die Diensteanbieter rufen die Listen der anbieterspezifischen Sperrmerkmale bei ihrer Berechtigungs-CA ab.

Die Verfahren zur Umrechnung werden in [TR-03110] spezifiziert, die Protokolle zur Übertragung der Listen in [TR-03129].

Durch dieses Verfahren ist sichergestellt, dass das anbieterspezifische Sperrmerkmal – wie das Pseudonym – weder durch die Diensteanbieter noch durch den Sperrdienst aufgelöst werden kann.

Eine Abfrage nach einzelnen gesperrten Ausweisen beim Sperrdienst (z.B. über OCSP) ist nicht vorgesehen, um zu verhindern, dass der Sperrdienst durch protokollieren der Abfragen Profile der Ausweisinhaber erstellen kann. Die eID-Sperrliste kann nur durch berechtigte Diensteanbieter abgefragt werden.

5.3.1.3 Entsperrung und Sperrauskunft

Über die Ausweisbehörde ist auch die Entsperrung eines Ausweises sowie die Abfrage des Sperrstatus möglich. Der Sperrstatus kann auch telefonisch unter Angabe von Vorname, Name, Geburtsdatum und Sperrkennwort bei der Sperrhotline erfragt werden. Entsperrungen und Sperrabfragen dürfen nur durch den Ausweisinhaber erfolgen.

6. Ausweisausgabe

6.1 Ausweis

Der Ausweis wird durch die Ausweisbehörde ausgegeben. Die einzelnen Anwendungen des Ausweises sind bei Ausgabe an den Inhaber in folgendem Zustand:

- Die Biometrieanwendung ist voll aktiviert.
- Die eID-Anwendung ist ausgerüstet mit einer Transport-eID-PIN und ist durch entsprechend authentisierte *Inspektionssysteme* und *Authentisierungsterminals* mit Recht *CAN allowed* lesbar.
  Die Nutzung durch *Authentisierungsterminals* ohne Recht *CAN allowed*, also insbesondere für den elektronischen Identitätsnachweis, erfordert das Setzen einer operationellen eID-PIN durch den Inhaber.
  Für Jugendliche unter 16 Jahren ist die Nutzung der eID-Anwendung mit eID-PIN abgeschaltet[18].
- Die Signaturanwendung wird ohne Signaturschlüsselpaar ausgeliefert. Die Aktivierung der Signaturanwendung erfolgt durch Setzen einer Signatur-PIN, das Erzeugen eines Schlüsselpaares sowie Nachladen eines Zertifikates durch einen qualifizierten Zertifizierungsdiensteanbieter.

6.2 PIN/PUK-Brief

Vom Ausweishersteller erhält der Inhaber des Ausweises einen PIN/PUK-Brief. Dieser entspricht den üblichen Anforderungen an einen PIN/PUK-Brief und enthält folgende Daten:

- Transport-eID-PIN (Abschnitt 3.3.3)
- PUK (Abschnitt 3.3.5)
- Sperrkennwort (Abschnitt 5.3.1)

6.3 Qualitätssicherung und Visualisierung

Die Ausweisbehörde muss vor Ausgabe des Ausweises an den Bürger zur Sicherstellung der Funktionsfähigkeit des Chips die dort gespeicherten Daten auslesen, vgl. Abschnitt 7. Weiter hat der Inhaber eines Ausweises die Möglichkeit, sich die auf dem Chip gespeicherten Daten anzeigen zu lassen.

6.4 Informationsangebot für den Ausweisinhaber

Dem Ausweisinhaber werden Informationen

- zu den auf dem Chip gespeicherten Daten,
- über die Funktionen des Ausweises,
- über die Sorgfaltspflichten des Inhabers für den Umgang mit dem Ausweis, wie sie sich z.B. aus den gesetzlichen Grundlagen sowie den zugehörigen Verordnungen ergeben,
- sowie über die Möglichkeiten zum Sperren der eID-Funktion, PIN-Änderung usw.

18 Für Ausweise ausgegeben vor dem 15.07.2017 konnte die eID-PIN auch auf Antrag des Inhabers abgeschaltet werden.

bereitgestellt, z.B. über Informationsmaterial bei Ausweisbeantragung oder über eine Hotline/Webseite.

6.5 Verantwortung des Ausweisinhabers

Der Ausweisinhaber muss – soweit dies für ihn möglich/zumutbar ist – einen Missbrauch seines Ausweises einschließlich der eID- und der Signaturanwendung verhindern. Der Ausweisinhaber soll gemäß § 1 (1) Satz 3 und § 27 [PAuswG] sowie den entsprechenden Regelungen zum Aufenthaltstitel/ zur eID-Karte für Unionsbürger:

- den Ausweis möglichst nicht hinterlegen bzw. den Gewahrsam des Ausweises aufgeben, um das Sicherungsmittel „Besitz“ für die eID-Anwendung bzw. die Signaturanwendung zu wahren;
- den Ausweis bei Verlust umgehend über die Ausweisbehörde bzw. die Hotline sperren lassen;
- die eID-PIN geheimhalten und bei Kompromittierung der eID-PIN die PIN unverzüglich ändern oder die eID-Anwendung sperren lassen;
- sowie geeignete Kartenleser und Software verwenden.

Empfohlen wird die Verwendung von durch das BSI zertifizierten Kartenlesern nach [TR-03119] sowie von durch das BSI zertifizierter Client-Software (eID-Client) nach [TR-03124], Teil 1.

Die Regeln zum Umgang mit Ausweis und PIN, die der Ausweisinhaber bei der Benutzung bestimmter Kartenlesertypen und Softwarekomponenten berücksichtigen sollte, sowie geeignete zusätzliche Sicherheitsmaßnahmen, werden dem Inhaber in geeigneter Weise dargelegt.

7. Änderungsdienst/Visualisierung

Einige Daten bzw. Funktionalitäten des Ausweises können auch nach der Personalisierung des Ausweises im Herstellungsprozess geändert werden (Änderungsdienst):

- Ändern der Adresse und des amtlichen Gemeindeschlüssels;
- Nebenbestimmungen I/II beim Aufenthaltstitel;
- Setzen einer neuen eID-PIN;
- Anschalten der Nutzung der eID-Anwendung über die eID-PIN.

Die Ausweisbehörde muss vor Ausgabe des Ausweises an den Inhaber zur Sicherstellung der Funktionsfähigkeit des Chips die dort gespeicherten Daten auslesen. Weiter hat der Inhaber eines Ausweises die Möglichkeit, sich die auf dem Chip gespeicherten Daten anzeigen zu lassen (Visualisierung).

Umgesetzt werden diese Dienste mit Hilfe eines zertifizierten Moduls (vgl. Anhang A) auf Basis einer „EAC-Box“ nach [TR-03131] mit integriertem Kartenleser und PIN-Pad, die die Abwicklung der kryptographischen Protokolle und die Kommunikation mit der Berechtigungs-PKI (Abschnitt 5.2) übernimmt. Zum Auslesen der gespeicherten Daten authentisiert sich das Modul als *hoheitliches nationales Inspektionssystem* mit Recht *Read DG3*. Für Änderungen erfolgt eine Authentisierung als *hoheitliches nationales Authentisierungsterminal* (Abschnitt 4.4) mit Recht *CAN allowed*, d.h. eine Eingabe der geheimen eID-PIN durch den Inhaber ist nicht notwendig.

- Bei einer Änderung der Adresse wird zusätzlich zur elektronischen Änderung ein Adressaufkleber auf dem Ausweis aufgebracht.
- Nur Aufenthaltstitel: Bei einer Änderung der Nebenbestimmungen wird zusätzlich zur elektronischen Änderung ein Zusatzblatt zum Aufenthaltstitel mit den Nebenbestimmungen ausgestellt.
- Da das Anschalten der Nutzung der eID-Anwendung mit eID-PIN auch im Ausweisregister und die geänderte Adresse im Melderegister bzw. in der Ausländerdatei A gespeichert wird, ist der Änderungsdienst in die IT-Verfahren der Ausweisbehörden integriert.
- Da im Zuge der Visualisierung ein Ausweis ausgelesen werden kann, ohne dass der Inhaber durch eine PIN-Eingabe seine Berechtigung nachweist, muss durch die Ausweisbehörde sichergestellt werden, dass nur der rechtmäßige Inhaber eines Ausweises bzw. ein Mitarbeiter der Ausweisbehörde für die Qualitätssicherung diesen auslesen kann.

Anhang A Zertifizierungen

Die Konformität der verschiedenen Komponenten zu den jeweiligen Spezifikationen kann durch Konformitätstests überprüft und durch ein Zertifikat des BSI bestätigt werden. Das Prüfverfahren wird in den jeweiligen Richtlinien dargestellt. Für verschiedene Komponenten kann eine Zertifizierung nach Common Criteria [CC] durchgeführt werden.

Komponente	Zertifizierung	
	Konformität	**Common Criteria**
Hardware zur Erfassung und Echtheitsbewertung von Fingerabdrücken nach [TR-03121]	Verpflichtend: [TR-03122]	Verpflichtend[19]: [PP-0062] / [PP-0063]
Software zur Erfassung, Echtheitsbewertung und Qualitätssicherung des Lichtbilds und der Fingerabdrücke nach [TR-03121]	Verpflichtend: [TR-03122]	
Datenaustauschformat zwischen Ausweisbehörde und Dokumentenhersteller nach [TR-03123]	Verpflichtend: Herstellererklärung	
Modul zur Sicherung der Authentizität/Vertraulichkeit der Antragsdaten nach [TR-03132]	Verpflichtend: [TR-03133]	
Ausweischip (Hard- und Software)	Verpflichtend: [TR-03105], Teile 2 und 3.3	Verpflichtend: [PP-0084], [PP-0061]/[PP-0069]/[PP-0087] bzw. [PP-0087] mit [PP-0090][20]
Modul für den Änderungs- und Visualisierungsdienst in den Ausweisbehörden nach [TR-03131]	Verpflichtend: [TR-03105], Teile 4 und 5.2	Verpflichtend: [PP-0064], [PP-0059][21]
Kartenterminals für Ausweisinhaber (Heimanwender) nach [TR-03119]	Empfohlen: [TR-03105], Teil 4 ggfs. [TR-03105], Teil 5.2	Empfohlen: Für Standard-/Komfortleser: [PP-0083]
eID-Client nach [TR-03124], Teil 1, und [TR-03112]	Empfohlen: [TR-03124], Teil 2	
eID-Server nach [TR-03130], Teil 1, und [TR-03112]	Empfohlen: [TR-03130], Teil 4	Siehe [CP-eID]

19 Verpflichtung ab 2018 gemäß Zeitplan in [TR-03121].

20 Die Anforderungen aus [PP-0061]/[PP-0069]/[PP-0087] bzw. [PP-0087]umfassen auch die Anforderungen an eine qualifizierte Signaturerstellungseinheit gemäß Protection Profile [PP-0059].

21 Oder Schutzprofil mit äquivalentem Schutzniveau, für den Schlüsselspeicher für Terminalauthentisierungs- und Kommunikationsschlüssel.

Anhang B Sperrkennwort, Sperrschlüssel und Sperrsumme

Sperrkennwort

Das Sperrkennwort ist ein während der Ausweisherstellung vom Hersteller zufällig aus einer Wörterliste gewähltes Klartextpasswort.

Das Sperrkennwort wird

- zur Ausweisbehörde übertragen und dort im Ausweisregister gespeichert und
- im PIN-Brief abgedruckt und so dem Ausweisinhaber mitgeteilt.

Ein Wechsel des Sperrkennwortes ist nicht möglich.

Sperrschlüssel

Der Sperrschlüssel ist der öffentliche Schlüssel eines Schlüsselpaares, das während des Herstellungsprozesses erzeugt wird. Er wird zusammen mit der Sperrsumme an den Sperrdienst übertragen und dort für die Verwendung für eine eventuelle Sperre gespeichert. Der private Schlüssel ist auf dem Ausweischip zur Berechnung von Sperrmerkmalen durch den Ausweis gespeichert.

Zur Spezifikation des Sperrschlüssels siehe [TR-03110], die Schlüssellänge ist in [TR-03116], Teil 2, festgelegt.

Sperrsektor

Der Sperrsektor ist das Schlüsselpaar des Sperrdienstes. Der private Schlüssel des Sperrsektors wird zur Umrechnung des Sperrschlüssels in das allgemeine Sperrmerkmal benötigt. Der öffentliche Schlüssel des Sperrsektors ist der Basispunkt für die Erzeugung der anbieterspezifischen Terminal-Sektoren durch die Berechtigungs-CA.

Terminal-Sektor

Für jeden Diensteanbieter wird durch die jeweilige Berechtigungs-CA ein Schlüsselpaar erzeugt. Basispunkt für die Schlüsselerzeugung ist der öffentliche Schlüssel des Sperrsektors.

Der öffentliche Schlüssel des Terminal-Sektors ist über eine Extension Bestandteil des Berechtigungszertifikates und wird vom Ausweischip für die Erzeugung des Sperrmerkmals und des Pseudonyms mittels des kryptographischen Protokolls *Restricted Identification* bzw. *Chipauthentisierung* Version 3 genutzt. Der private Schlüssel des Terminal-Sektors wird von der Berechtigungs-CA für die Umrechnung der allgemeinen Sperrmerkmale in anbieterspezifische Sperrmerkmale genutzt.

Die Schlüssellänge für den Terminal-Sektor wird in [TR-03116], Teil 2, festgelegt. Die Anforderungen aus [CP-eID] an Schlüsselerzeugung, -speicherung und -verwendung gelten entsprechend.

Sperrsumme

Die Sperrsumme besteht aus dem Hash über die Verkettung von Geburtsdatum, Nachname, Vorname und Sperrkennwort. Die Sperrsumme wird

- im Produktionsprozess vom Hersteller erzeugt, zusammen mit dem Sperrschlüssel zum Sperrdienst übertragen und dort gespeichert;
- vom Hersteller zur Speicherung im Ausweisregister an die Ausweisbehörde übertragen;
- im Sperrfalle von der Ausweisbehörde bzw. der Hotline aus dem Ausweisregister abgerufen oder gebildet und zum Sperrdienst übertragen und
- im Falle einer Entsperrung oder einer Abfrage des Sperrstatus von der Ausweisbehörde gebildet und zum Sperrdienst übertragen.

Zur Bildung der Sperrsumme werden die Eingangsdaten Geburtsdatum, Vorname, Nachname und Sperrkennwort wie folgt umgewandelt:

- Alle Buchstaben des Eingangswertes werden in Großbuchstaben konvertiert, Leer- und Sonderzeichen (z.B. Trennstriche) werden entfernt.
- Umlaute und andere diakritische Zeichen werden gemäß der Konvertierungstabelle in [ICAO 9303], Part 3, Section 6, konvertiert. Sofern die Tabelle für ein Zeichen mehrere Konvertierungsmöglichkeiten zulässt, so wird die erste Möglichkeit verwendet. Zeichen, die nicht gemäß dieser Tabelle konvertiert werden können, werden weggelassen.
- Alle Zeichen werden als ASCII kodiert, erlaubte Zeichen sind nur lateinische Großbuchstaben, Ziffern und „+“ als Feldtrenner.

Die Datenfelder werden wir folgt definiert:

- Geburtsdatum: 8 Zeichen im Format YYYYMMDD, unbekannte Teile werden durch „X“ gekennzeichnet (entsprechend dem Aufdruck auf dem Ausweis).
  Bsp.: 13.07.1964 → „19640713“,
  Tag unbekannt.03.1970 → „197003XX“
- Name: Vollständiger Name gemäß Antragsdatensatz, das heißt einschließlich Namensbestandteile wie „Freiherr von und zu“, aber ohne Geburtsname, Ordens- oder Künstlername.
  Bsp.: „Möller“ → „MOELLER“,
  „Freifrau zu Berg geb. Hügel“ → „FREIFRAUZUBERG“
- Vorname: Offizielle Vornamen gemäß Antragsdatensatz bis zum ersten Leerzeichen.
  Bsp.: „Karl Theodor“ → „KARL“,
  „Ann-Kathrin Maria“ → „ANNKATHRIN“
  bei unbekanntem Vornamen bleibt das Feld leer: „---“ → „“
- Sperrkennwort: Wie im PIN-Brief abgedruckt bzw. im Register gespeichert.
  Bsp.: „Rollmops“ → „ROLLMOPS“,
  „Ameisenbär“ → „AMEISENBAER“

Die einzelnen Felder werden mit „+“ in der Reihenfolge Geburtsdatum, Name, Vorname, Sperrkennwort verkettet.

Bsp.: 19640713+MOELLER+KARL+ROLLMOPS

Aus diesen Eingangsdaten wird die Sperrsumme mittels einer Hashfunktion H gebildet. Die zu verwendende Hashfunktion wird in [TR-03116], Teil 2, festgelegt.

Bsp.: Sperrsumme = H(19640713+MOELLER+KARL+ROLLMOPS)

Bei Verwendung von SHA-256 als Hashfunktion H ergibt sich aus diesen Daten

Bsp.: Sperrsumme =
02f96b3578f9cdb473d642037072088d37965a3019b54427beedf994974abebc

Anhang C Bezeichnungen für Datengruppen

Um ein einheitliches Erscheinungsbild zu gewährleisten, sollen die folgenden Bezeichnungen für die Datengruppen und speziellen Funktionen der eID-Anwendung genutzt werden. Sofern erforderlich, können die Bezeichnungen auch abgekürzt werden.

	Bezeichnung	
	Deutsch	**Englisch**
Datengruppen (siehe Tabelle 2)		
DG1	Dokumentenart	Document type
DG2	Ausstellender Staat	Issuing country
DG3	"Gültig bis"	"Valid until"
DG4	Vorname(n)	Given name(s)
DG5	Familienname	Family name
DG6	Ordens-/Künstlername	Religious/artistic name
DG7	Doktorgrad	Doctoral degree
DG8	Geburtsdatum	Date of birth
DG9	Geburtsort	Place of birth
DG10	Staatsangehörigkeit	Nationality
DG13	Geburtsname	Birth name
DG17	Anschrift	Address
DG19	Nebenbestimmungen	Auxiliary conditions
Spezielle Funktionen (siehe Abschnitt 4.4)		
Dienste- und kartenspezifische Kennung (RI oder CA3)	Pseudonym	Pseudonym
Wohnortabfrage	Wohnortbestätigung	Address verification
Altersverifikation	Altersbestätigung	Age verification
Passwörter (siehe Abschnitt 3.3)		
	PIN	PIN
	PUK	PUK
	Zugangsnummer	Access number
	Signatur-PIN	Signature PIN

Tabelle 5: Bezeichnungen für Datengruppen

Anhang D Varianten

In diesem Anhang werden Abweichungen (z.B. durch ältere Versionsstände der Spezifikationen) von ausgegebenen Personalausweisen und Aufenthaltstiteln gegenüber der aktuellen Version der Spezifikation aufgelistet. Dabei werden die Ausweise anhand der Seriennummern der genutzten Document Signer identifiziert. Zu beachten ist, dass mit Document Signern aus der gleichen PKI auch andere Dokumente (Reisepässe) signiert werden. Die Angaben beziehen sich nur auf Document Signer für Personalausweise, Aufenthaltstitel und eID-Karten für Unionsbürger.

Document Signer Serial Number	**Ausgabe bis**	**Variante**	**ObjectIdentifier in `DefectList`**
SN ≤ 106	Q3/2011	Die Ausweise enthalten in EF.CardAccess und EF.ChipSecurity keine Struktur `PrivilegedTerminalInfo`. Der für nicht-privilegierte Terminals verfügbare Schlüssel für die Chipauthentisierung ist der Schlüssel, der in der ersten `ChipAuthenticationInfo` adressiert wird.	`id-EAC2PrivilegedTerminalInfoMissing`
SN ≤ 106	Q3/2011	Die Ausweise enthalten in EF.ChipSecurity kein `eIDSecurityInfo`.	`id-eIDSecurityInfoMissing`
SN ≤ 109	Q4/2011	Die Ausweise erlauben keine mehrfache Authentisierung während einer Kartenaktivierung, d.h. zur Durchführung einer zweiten Authentisierung muss die Karte durch ein Aus- und Anschalten des Lesefeldes zurückgesetzt werden.	`id-PowerDownReq`
PA: SN ≤ 112	Q2/2012	Die Ausweise enthalten keine bzw. eine leere Datengruppe „Geburtsname“ (DG13).	`id-eIDDGMissing` mit Parameter DG13
eAT: SN ≤ 138	Q4/2014		
SN ≤ 122	Q1/2013	Die Ausweise enthalten keine Datengruppe „Staatsangehörigkeit“ (DG10).	`id-eIDDGMissing` mit Parameter DG10
	Q4/2019	Die Ausweise unterstützen keine Chipauthentisierung Version 3	

Die `ObjectIdentifier` und Parameterdefinition für die eID-Anwendung werden im Folgenden definiert. Die entsprechenden `ObjectIdentifier`/Definitionen für die Authentisierungsprotokolle und das Gesamtdokument finden sich in [TR-03129].

```
id-eIDDefect ::= OBJECT IDENTIFIER{id-DefectList 3}
 -- see TR-03129 for id-DefectList

id-eIDDGMalformed         ::= OBJECT IDENTIFIER{id-eIDDefect 1}
 -- The indicated data groups might be incorrectly encoded.
MalformedDGs ::= SET OF INTEGER
 -- DGs as integer

id-eIDIntegrity           ::= OBJECT IDENTIFIER{id-eIDDefect 2}
 -- The integrity of unsigned data groups is not guaranteed.
```

```
id-eIDSecurityInfoMissing ::= OBJECT IDENTIFIER{id-eIDDefect 3}
 -- EF.ChipSecurity does not contain a structure eIDSecurityInfo

id-eIDDGMissing           ::= OBJECT IDENTIFIER{id-eIDDefect 4}
 -- The indicated data groups are not present
MissingDGs ::= SET OF INTEGER
 -- DGs as integer
```

Literaturverzeichnis

[DVDV] BIT: Deutsches Verwaltungsdiensteverzeichnis - Verfahrensbeschreibung

[SiKo] BMI: Sicherheitsrahmenkonzept für das Gesamtsystem des elektronischen Personalausweises (ePA)

[CP-CSCA] BSI: Certificate Policy - Country Signing Certification Authority

[CP-eID] BSI: Certificate Policy für die Country Verifying Certification Authority -- eID-Anwendung

[CP-ePass] BSI: Certificate Policy für die Country Verifying Certification Authority -- ePass-Anwendung

[CP-eSign] BSI: Certificate Policy für die eSign-Anwendung des ePA

[PP-0061] BSI: Common Criteria Protection Profile BSI-CC-PP-0061: Electronic Identity Card

[PP-0062] BSI: Common Criteria Protection Profile BSI-CC-PP-0062: Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP)

[PP-0063] BSI: Common Criteria Protection Profile BSI-CC-PP-0063: Fingerprint Spoof Detection Protection Profile (FSDPP)

[PP-0064] BSI: Common Criteria Protection Profile BSI-CC-PP-0064: Protection Profile for Inspection Systems

[PP-0069] BSI: Common Criteria Protection Profile BSI-CC-PP-0069: Electronic Residence Permit Card

[PP-0083] BSI: Common Criteria Protection Profile BSI-CC-PP-0083: Standard Reader - Smart Card Reader with PIN-Pad supporting eID based on Extended Access Control

[PP-0087] BSI: Common Criteria Protection Profile BSI-CC-PP-0087: Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use

[PP-0090] BSI: Common Criteria Protection Profile Configuration Machine Readable Electronic Documents - Optional Post-Emission Updates

[TR-03104] BSI: Technische Richtlinie TR-03104, Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für hoheitliche Dokumente

[TR-03105] BSI: Technische Richtlinie TR-03105, Conformity Tests for Official Electronic ID Documents

[TR-03107] BSI: Technische Richtlinie TR-03107, Elektronische Identitäten und Vertrauensdienste im E-Government

[TR-03110] BSI: Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token

[TR-03111] BSI: Technische Richtlinie TR-03111, Elliptic Curve Cryptography (ECC)

[TR-03112] BSI: Technische Richtlinie TR-03112, eCard-API-Framework

[TR-03116] BSI: Technische Richtlinie TR-03116, Kryptographische Vorgaben für Projekte der Bundesregierung

[TR-03117] BSI: Technische Richtlinie TR-03117, eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit

[TR-03119] BSI: Technische Richtlinie TR-03119, Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control

[TR-03121] BSI: Technische Richtlinie TR-03121, Biometrics in public sector applications

[TR-03122] BSI: Technische Richtlinie TR-03122, Conformance Test Specification for TR-03121

[TR-03123] BSI: Technische Richtlinie TR-03123, Datenmodell und Geschäftsprozesse zur Beantragung hoheitlicher Dokumente

[TR-03124] BSI: Technische Richtlinie TR-03124, eID-Client

[TR-03128] BSI: Technische Richtlinie TR-03128, Diensteanbieter für die eID-Funktion

[TR-03129] BSI: Technische Richtlinie TR-03129, PKIs for Machine Readable Travel Documents -- Protocols for the Management of Certificates and CRLs

[TR-03130] BSI: Technische Richtlinie TR-03130, eID-Server

[TR-03131] BSI: Technische Richtlinie TR-03131, EAC-Box Architecture and Interfaces

[TR-03132] BSI: Technische Richtlinie TR-03132, Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente (TR SiSKo hD)

[TR-03133]	BSI: Technische Richtlinie TR-03133, Prüfspezifikation zur Technischen Richtlinie BSI-TR 03132 Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente
[VfB]	BVA: Beantragung eines Berechtigungszertifikates
[CC]	CCMB: Common Criteria for Information Technology Security Evaluation
[PP-0059]	CEN: EN 419211-2 -- Protection Profile for Secure signature creation device -- Part 2: Device with key generation, BSI-CC-PP-0059
[EN 419212]	CEN: EN 419212 – Application Interface for smart cards used as Secure Signature Creation Devices
[CEN 15480]	CEN: TS 15480 -- Identification card systems – European Citizen Card
[EU-RP]	EU-Kommission: Verordnung (EG) 380/2008: Residence Permit Specification
[PP-0084]	Eurosmart: Common Criteria Protection Profile BSI-CC-PP-0084: Security IC Platform Protection Profile with Augmentation Packages
[ICAO 9303]	ICAO: Doc 9303, Machine Readable Travel Documents
[ISO 14443]	ISO/IEC: ISO 14443 - Identification cards – Contactless integrated circuit(s) cards – Proximity cards
[ISO 15444]	ISO/IEC: ISO 15444 - Information technology - JPEG 2000 image coding system
[ISO 7816]	ISO/IEC: ISO 7816 - Identification cards – Integrated circuit cards
[OSCI]	OSCI-Leitstelle: OSCI-Transport 1.2, Spezifikation
[AufenthG]	Aufenthaltsgesetz in der Fassung der Bekanntmachung vom 25. Februar 2008 (BGBl. I S. 162), das zuletzt durch Artikel 1 des Gesetzes vom 4. Juli 2019 (BGBl. I S. 914) geändert worden ist
[eIDKG]	Gesetz über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis (eID-Karte-Gesetz – eIDKG)
[PAuswG]	Personalausweisgesetz vom 18. Juni 2009 (BGBl. I S. 1346), das zuletzt durch Artikel 3 des Gesetzes vom 21. Juni 2019 (BGBl. I S. 846) geändert worden ist
[eIDAS]	VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG