Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie TR-03127

eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control

Elektronischer Personalausweis und elektronischer Aufenthaltstitel

Version 1.16

14. Oktober 2015

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

Mit der Einführung des elektronischen Personalausweises und des elektronischen Aufenthaltstitels wird eine Familie hoheitlicher Dokumente mit integriertem Chip geschaffen. Im Rahmen der eCard-Strategie des Bundes werden diese Dokumente – soweit möglich – identisch ausgestaltet, mit dem Ziel, eine gemeinsame Infrastruktur sowohl für die hoheitliche Anwendung als für die Benutzung für eGovernment/eBusiness zu schaffen.

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,
- sowie das „Sicherheitsrahmenkonzept für das Gesamtsystem des elektronischen Personalausweises“ ([SiKo]), welches analog auch auf den Aufenthaltstitel Anwendung findet.

Der im Dokument integrierte Chip ist ein neuartiges 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, den Ausweis um eine Funktion zu erweitern, die dem Ausweisinhaber einerseits und eBusiness- oder eGovernment-Dienstleistern andererseits eine sichere gegenseitige Authentisierung u.a. über eine Internet-Verbindung ermöglicht. Aus dieser Funktion ergibt sich eine Vielzahl von Anwendungsmöglichkeiten.

Eine zusätzliche Anwendung des Ausweises ist eine Signaturanwendung, wie sie bereits heute auf separaten Signaturkarten zu finden ist. Diese Anwendung wird erst vom Karteninhaber nachträglich bei Bedarf aktiviert.

In dieser Technischen Richtlinie werden die für den elektronischen Personalausweis und den elektronischen Aufenthaltstitel verwendeten Verfahren vorgestellt und auf die entsprechenden Spezifikationen verwiesen. Soweit nicht explizit anders angegeben, beziehen sich alle Angaben auf beide Dokumente, im Folgenden generisch als *Ausweis* oder *Dokument* bezeichnet.

2. Datenerfassung und -übertragung

Bei Antragstellung für den Ausweis werden in der Personalausweisbehörde bzw. der Ausländerbehörde (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 bzw. dem Aufenthaltsgesetz sowie den zugehörigen Verordnungen. Die notwendigen Verfahren und Datenformate werden in [TR-03104], [TR-03121] und [TR-03123] festgelegt.

2.1 Persönliche Daten

Neben den biometrischen Daten (Gesichtsbild, Fingerabdrücke (Personalausweis: optional, Aufenthaltstitel: verpflichtend), Unterschrift, Augenfarbe und Größe) werden für den Ausweis folgende personenbezogenen Daten erfasst:

- Vorname(n), Familienname, gegebenenfalls Geburtsname
- Doktorgrad
- Tag und Ort der Geburt
- Anschrift (incl. Postleitzahl) und amtlicher Gemeindeschlüssel des Wohnortes

Für den Personalausweis 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, 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. 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 die Unterschrift des Antragstellers. Die Unterschrift wird nur auf dem Ausweis aufgedruckt und nicht im Chip gespeichert.

2.5 Datenübertragung

Die Datenübertragung zwischen den Ausweisbehörden und dem Ausweishersteller wird in entsprechenden Profilen von [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. Ausweiskarte

Kartenkörper

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

Chip

In den Ausweis wird ein kontaktloser Chip integriert. Dieser Chip bzw. die auf ihm realisierten kryptographischen Protokolle dienen als neuartiges Sicherheitsmerkmal und ermöglicht eine Reihe neuer Anwendungen für den Ausweis.

Der kontaktlose Chip kommuniziert mit einem passenden Kartenterminal, welches als Lese- oder Schreibgerät fungiert. Die Datenübertragung der zwei Komponenten 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 dokumentenbezogenen Daten wie in Kapitel 3.2 beschrieben. Der Chip ist mit einem kryptographisch starken Zufallszahlengenerator ausgestattet und unterstützt Kryptographie mittels elliptischer Kurven gemäß [TR-03111] sowie AES [FIPS 197].

Ferner ist der Ausweis eine nach Signaturgesetz [SigG] bzw. Signaturverordnung [SigV] bestätigte sichere Signaturerstellungseinheit.

Der Chip entspricht dem Profil „Identity Card with Protected MRTD Application“ (Personalausweis) 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);
- Chipauthentisierung Version 2 – CA2 ([TR-03110], Teil 2);
- nur Aufenthaltstitel: Basic Access Control 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] wird aus Datenschutzgründen nicht implementiert (siehe [TR-03110], Teil 1, Anhang B „Challenge Semantics“).

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 (spezifiziert in [TR-03110]) dient dem Aufbau eines verschlüsselten und integritätsgesicherten Kanal 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 eine *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 (spezifiziert in [TR-03110]) dient dem Nachweis der Zugriffsrechte eines Terminals bzw. eines Dienstanbieters.

Der Nachweis der Zugriffsrechte über die Terminalauthentisierung im Rahmen der *General Authentication Procedure* ist beim Personalausweis 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. Dienstanbieter.

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*
- *bestätigtes 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 (spezifiziert in [ICAO 9303], [TR-03110]) dient dem Echtheitsnachweis der auf dem Chip gespeicherten Daten. Dazu werden die in der Biometrieanwendung (Abschnitt 3.2.2) gespeicherten Daten und der öffentliche Schlüssel des Chips mit Hilfe der Dokumenten-PKI (Abschnitt 5.1) signiert. 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) 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.

Die Zertifikate der Dokumenten-PKI sind auf dem Chip gespeichert (DS-Zertifikat) bzw. vom BSI (der Wurzelinstanz der Dokumenten-PKI) bzw. einem nachgelagerten Public Key Directory (PKD) erhältlich. 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. Dienstanbieter und Chip.

Im Rahmen der *General Authentication Procedure* kann das Terminal nach Aufbau des verschlüsselten Kanals gemäß der in der Terminalauthentisierung nachgewiesenen Zugriffsrechte 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 ePass),
- die eID-Anwendung,

- die Signaturanwendung zur Erzeugung qualifizierter elektronischer Signaturen.

Auf alle in den Anwendungen des Personalausweises 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/Advanved ePassport Inspection Procedure* möglich.

3.2.1 Karten-/Anwendungserkennung

Die auf den Ausweisen vorhandenen Anwendungen werden durch korrepsondierende Application Identifier in der Datei EF.DIR im Master File erkannt:

- Biometrieanwendung: Application Identifier `0xA0000002471001` (siehe [ICAO 9303], Part 10)[1];
- eID-Anwendung: Application Identifier `0xE80704007F0007030` (siehe [TR-03110]);
- eSign-Anwendung nach [TR-03117]: Application Identifier `0xA000000167455349474E`.

1 Reisepässe enthalten meist keine Datei EF.DIR.

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.

Zugriff auf die Biometrieanwendung erhalten beim Personalausweis ausschließliche authentisierte *Inspektionsterminals*, beim Aufenthaltstitel zusätzlich *Basic* bzw. *Extended Inspection Systems*. Für den Zugriff auf alle Datengruppen (Personalausweis) bzw. DG3 (Aufenthaltstitel) ist der Nachweis der entsprechenden Rechte über die Terminalauthentisierung notwendig.

Schreiben von Daten nach der Produktion des Ausweises ist nicht 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. Dieses ist auch über eine Internet-Verbindung (d.h. gegenüber eGovernment- und eBusiness-Diensten) möglich.

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	Daten der maschinenlesbaren Zone (MRZ), wie auf dem Ausweiskörper aufgedruckt	IS; nur eAT: BIS/EIS
DG2	Digitales Gesichtsbild, identisch mit dem aufgedruckten Bild	IS; nur eAT: BIS/EIS
DG3	Zwei Fingerabdrücke (im Personalausweis optional, im Aufenthaltstitel verpflichtend). Werden keine Fingerabdrücke gespeichert, enthält diese Datengruppe einen zufälligen Wert	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 enthaltende öffentliche Schlüssel für die Chipauthentisierung ist identisch mit dem Schlüssel aus EF.ChipSecurity.
		nur eAT: BIS/EIS

IS: authentisiertes *Inspektionssystem* (PACE mit CAN o. MRZ, TA2, CA2); BIS: *Basic Inspection System* (BAC/PACE); CA1 sofern vom Terminal unterstützt; EIS: *Extended Inspection System* (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	ePA: 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	ePA: unbenutzt eAT: Staatsangehörigkeit	IS; AT + *Read DG10*	-	-
DG11 - DG12	unbenutzt	-	-	-
DG13	ePA: Geburtsname eAT: unbenutzt	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 ePA: unbenutzt	IS; AT + *Read DG19*	AT + *Write DG19*	-
DG20	eAT: Nebenbestimmungen II ePA: unbenutzt	IS; AT + *Read DG20*	AT + *Write DG20*	-
DG21	unbenutzt	-	-	-
	Vergleichsgeburtsdatum für Altersverifikation	-	-	AT + *Age Verification*
	Schlüssel für dienstspezifisches Sperrmerkmal (Abschnitt 4.4.2)	-	-	AT
	Schlüssel für dienst- und kartenspezifische Kennung (Abschnitt 4.4.3.3)	-	-	AT + *Restricted Identification*
IS: authentisiertes *Inspektionssystem* (PACE mit CAN o. MRZ, TA2, CA2); AT: authentisiertes *Authentisierungsterminal* (PACE mit eID-PIN o. CAN (mit Recht *CAN allowed*), TA2, CA2);				

Tabelle 2: Dateien der eID-Anwendung

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.
- **DG3**: Für diese Datengruppe werden für die Online-Authentisierung keine Berechtigungszertifikate ausgegeben. Ein Auslesen des Ablaufdatums ist für Zertifizierungsdiensteanbieter für das Nachladen qualifizierter Zertifikate zugelassen, um sicherstellen zu können, dass das qualifizierte Zertifikat maximal bis zum Ablaufdatum des Ausweises gültig ist.
- **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 4.4.3.4) 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 gewünschte Alter hat.
- **DG10**: 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 und Postleitzahl) gespeichert. Wohnt der Ausweisinhaber im Ausland, so wird stattdessen der Text „keine Hauptwohnung in Deutschland“ (`noPlaceInfo` gemäß [TR-03110], Teil 4) gespeichert.
- **DG18**: Im Feld *Wohnort-ID* wird der zum Wohnort gehörige Gemeindeschlüssel gespeichert, um eine Abfrage auf den Wohnort mit der speziellen Funktion Wohnortabfrage (Abschnitt 4.4.3.5) zu ermöglichen. Der Inhalt der Datengruppe besteht im Allgemeinen aus einer Folge von 14 dezimalen Ziffern:

  1. Drei Ziffern für den Ländercode gemäß ISO 3166-1 numeric, ergänzt um eine führende „0“ („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. 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.
Wird keine Adresse in der DG17 gespeichert (Wohnsitz im Ausland), so ist diese Datengruppe leer.
Für diese Datengruppen werden für die Online-Authentisierung keine Berechtigungszertifikate ausgegeben.

Zugriff auf die Dateien erhalten nach erfolgreicher Authentisierung

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

- *Inspektionsterminals*.

Die Daten werden nicht signiert. Dadurch wird verhindert, dass ein Dienstanbieter 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 [SigG]. 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 erfolgt durch einen Zertifizierungsdiensteanbieter (Abschnitt 4.4.3.1).

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].

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 4.4.3.3) 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	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+TA2	-	-
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	-
	Privater Schlüssel für die Chipauthentisierung, dessen öffentlicher Schlüssel in EF.CardSecurity angegeben ist.	-	-	Für CA nach PACE + TA2
	Privater Schlüssel für die Chipauthentisierung, dessen öffentlicher Schlüssel in EF.ChipSecurity angegeben ist.	-	-	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);				

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`
  - `PrivilegedTerminalInfo`[2]
  - `TerminalAuthenticationInfo`
  - `CardInfo`
- EF.CardSecurity
  - `PACEInfo`
  - `ChipAuthenticationInfo`
  - `ChipAuthenticationDomainParameterInfo`
  - `ChipAuthenticationPublicKeyInfo`
  - `TerminalAuthenticationInfo`
  - `CardInfo`
  - `RestrictedIdentificationInfo`[3]
  - `RestrictedIdentificationDomainParameterInfo`

  sowie die Signatur über diese Daten einschließlich des zugehörigen DS-Zertifikats.
- EF.ChipSecurity
  - `PACEInfo`
  - `ChipAuthenticationInfo`
  - `ChipAuthenticationDomainParameterInfo`
  - `ChipAuthenticationPublicKeyInfo`
  - `PrivilegedTerminalInfo`[4]
  - `TerminalAuthenticationInfo`
  - `CardInfo`
  - `RestrictedIdentificationInfo`
  - `RestrictedIdentificationDomainParameterInfo`
  - `EIDSecurityInfo` mit Hashwerten der Datengruppen DG4, DG5, DG8 und DG9 der eID-Anwendung[5]

  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:

---

2 Siehe auch Anhang D.

3 Dieses Element ist zweimal enthalten, zum ein für den Schlüssel zur Berechnung des Sperrmerkmals (siehe Abschnitt 4.4.2), zum anderen zur Berechnung des Pseudonyms (siehe Abschnitt 4.4.3.3). Für das Sperrmerkmal ist das Feld `authorizedOnly` in diesem Element auf `FALSE` gesetzt, für das Pseudonym auf `TRUE`; vgl. auch Tabelle 2.

4 Siehe auch Anhang D.

5 Siehe auch Anhang D.

- eine auf dem Kartenkörper aufgedruckte sechsstellige Nummer (CAN – *Card Access Number*);
- 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);
- 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 beim Pass üblichen Durchzugsleser auch für den Personalausweis/Aufenthaltstitel verwendet werden können. Dabei ist zu berücksichtigen, dass sich die MRZ des Ausweises gemäß den ICAO-Vorgaben auf der Rückseite des Ausweises befindet und dreizeilig ist (im Gegensatz zu zwei Zeilen beim Pass).

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 Transport-PIN, d.h. sie kann nur zum Setzen einer operationellen eID-PIN durch den Inhaber (Abschnitt 4.4.3.2), 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/Middleware 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.

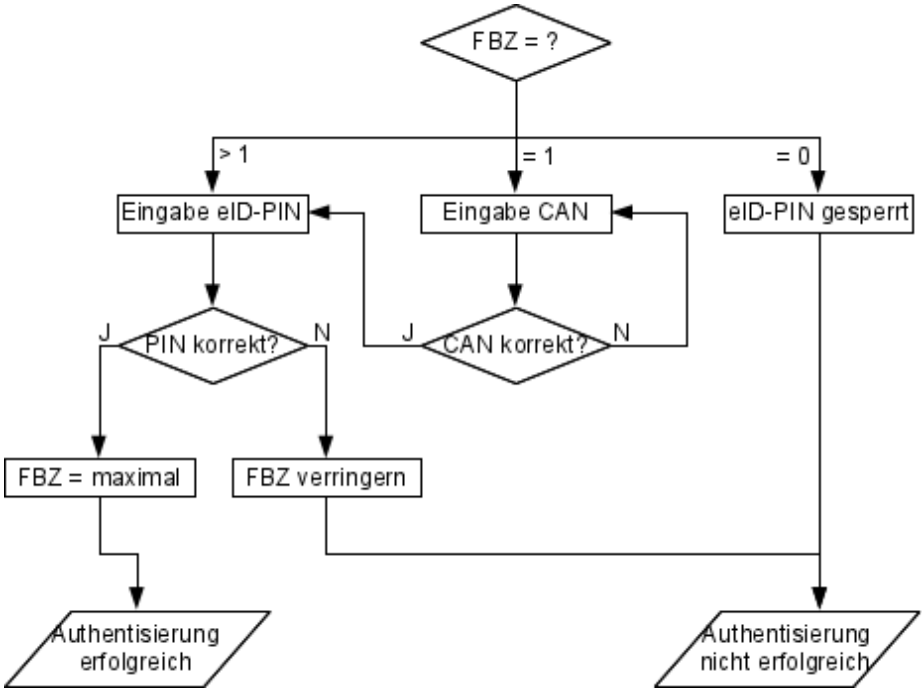

Abbildung 1: Eingabe der eID-PIN

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

Die Signatur-PIN kann

- nach Eingabe der aktuellen Signatur-PIN neu gesetzt werden;
- nach Authentisierung als *bestätigtes 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)	
	Authentisierungsterminal (optional): Sperrlistenabfrage – nur möglich, wenn Ausweis noch gültig (Abschnitt 5.3)
Inspektionssystem: Lesen des EF.SOD	
	Inspektionssystem: Prüfen der Signatur der Datei EF.SOD (Passive Authentisierung)
Optional: Auslesen der freigegebenen Daten (Abschnitt 3.2.3), Ausüben der speziellen Rechte (Abschnitt 4.4.3)	
	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
Bestätigtes 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 werden 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*. *Nicht-hoheitliche/ausländische Authentisierungsterminals* benötigen im Allgemeinen die Eingabe der geheimen eID-PIN, um das Auslesen der Daten an das Einverständnis des Inhabers zu binden und gleichzeitig den Ausweis an den Inhaber zu binden. Verwendet werden *nicht-hoheitliche/ausländische Authentisierungsterminals* z.B. für die Online-Authentisierung, siehe Abschnitt 4.7.

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.

Bevor ein *Authentisierungsterminal* Daten liest, muss das Terminal überprüfen können, dass der Ausweis gültig ist (d.h. der Ausweis nicht abgelaufen ist) und der Ausweis nicht gesperrt ist, z.B. weil er als verloren/gestohlen gemeldet worden ist. Dazu dienen die Funktionen *Abfrage der Dokumentgültigkeit* und *Lesen des Sperrmerkmals*. Die genaue Umsetzung dieser Funktionen wird in [TR-03110] spezifiziert.

4.4.1 Abfrage der Dokumentengültigkeit

Ein Dienstanbieter 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 Dienstanbieter 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 Lesen des Sperrmerkmals

Der Ausweis bietet die Möglichkeit der pseudonymen Authentisierung, d.h. der Ausweisinhaber kann sich gegenüber einem Dienstanbieter authentisieren, ohne persönliche Daten freizugeben. Insbesondere bildet der Ausweis für jeden Dienstanbieter ein anderes Pseudonym, so dass das Verbinden von Pseudonymen über Dienstanbietergrenzen hinweg nicht möglich ist (siehe auch Abschnitt 4.4.3.3). Auf der anderen Seite wird für den Eintrag in eine Sperrliste (z.B. für gestohlene Ausweise) eine Ausweiskennung bzw. ein Sperrmerkmal notwendig, um die Sperrliste abfragen zu können.

Um zu verhindern, dass über das Sperrmerkmal die Pseudonymität aufgehoben wird, ist auch das Sperrmerkmal dienstespezifisch. Für die Abfrage der Sperrliste werden dem Dienstanbieter dienstespezifische Sperrlisten zur Verfügung gestellt (Abschnitt 5.3).

Der Dienstanbieter kann nach erfolgreicher Authentisierung mit der *General Authentication Procedure* sein spezifisches Sperrmerkmal auslesen. Um sicherzustellen, dass jeder Dienstanbieter nur sein

Sperrmerkmal auslesen kann, ist die Kennung des Dienstanbieters (*Terminal Sector*) Bestandteil des Zugriffszertifikats des Dienstanbieters, das vom Chip überprüft wird.

4.4.3 Spezielle Funktionen

Neben dem Lesen personenbezogener Daten bietet die eID-Anwendung einige spezielle Funktionen, für die das *Authentisierungsterminal* spezielle über die Terminalauthentisierung nachgewiesene Zugriffsrechte benötigt. Die genaue Umsetzung dieser Funktionen wird in [TR-03110] spezifiziert.

4.4.3.1 Erzeugung eines Signaturschlüsselpaares

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

Über diese Funktion kann der Ausweisinhaber mit Hilfe eines Zertifizierungsdiensteanbieters 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 Zertifizierungsdiensteanbieter (ZDA) 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 ZDA die Schlüsselerzeugung auf dem Chip gestartet, der so erzeugte öffentliche Schlüssel ausgelesen und ein qualifiziertes Zertifikat auf dem Chip gespeichert.

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

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

4.4.3.2 eID-PIN setzen, eID-Anwendung An-/Ausschalten

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 An- und Ausschalten der eID-Anwendung im Änderungsdienst (Abschnitt 7) realisiert. Abgeschaltet wird hierbei nur die Benutzung der eID-Anwendung mit der eID-PIN als Passwort, 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.

4.4.3.3 Dienste- und kartenspezifische Kennung (Pseudonym)

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

Vom Ausweis wird die Erzeugung einer dienste- und kartenspezifische Kennung (Pseudonym) angeboten. Dazu wird dem Ausweis mit dem Zertifikat des Dienstanbieters eine eindeutige Kennung des Anbieters (*Terminal Sector*) übermittelt. Aus dieser Kennung und einem auf dem Chip gespeicherten Geheimnis erzeugt der Chip ein Pseudonym, das der Dienstanbieter zur zukünftigen Identifizierung der Karte nutzen kann. Das Pseudonym wird so erzeugt, dass aus dem Pseudonym für einen

Dienstanbieter nicht auf das Pseudonym geschlossen werden kann, das für einen anderen Dienstanbieter erzeugt wird.

4.4.3.4 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 Geburtsdatum 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.

4.4.3.5 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 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 Dienstanbieter z.B. möglich, Dienste nur für Einwohner eines bestimmten Bundeslandes anzubieten.

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

4.5 Bestätigtes Signaturterminal

An einem *bestätigten 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 4.4.3.1);
- 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. Beim Verbindungsaufbau mit PACE als nicht authentisiertem Terminal wird kein CHAT übergeben.

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 Online-Authentisierung

Die Online-Authentisierung, d.h. die Authentisierung gegenüber einem Dienstanbieter 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 Dienstanbieter als entferntem Terminal. Voraussetzung für die eigentliche Online-Authentisierung ist eine bestehende Verbindung zwischen lokalem Terminal und entferntem Terminal (Dienstanbieter), beispielsweise in Form einer SSL/TLS-Verbindung.

Eine Online-Authentisierung läuft in folgenden Schritten ab:

<table>
<tr><td>Chip</td><td>Lokales Terminal</td><td>Dienstanbieter</td></tr>
<tr><td></td><td colspan="2">Übertragen des Dienstanbieterzertifikats</td></tr>
<tr><td></td><td>Präsentation des Zertifikats
Einschränken der Zugriffsrechte durch Benutzer
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), 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 (Abschnitt 4.4.3)</td></tr>
</table>

Im zweiten Schritt wird das Zertifikat des Dienstanbieters einschließlich der Informationen über Dienstanbieter und Verwendungszweck (siehe Abschnitt 5.2.1) dem Benutzer durch die lokale Software (eID-Client) präsentiert. Mindestens angezeigt werden müssen:

- Name des Dienstanbieters;
- Erwünschte Zugriffsrechte; Abfragedatum für Altersverifikation, falls eine Altersverifikation durchgeführt werden soll.

Weiterhin müssen angezeigt oder auf Anforderung des Nutzers angezeigt werden:

- Anschrift und Email-Adresse des Dienstanbieters;
- Zweck der Datenübermittlung;
- Hinweis auf die für den Dienstanbieter zuständige Datenschutzbehörde;
- Gültigkeitszeitraum des Zertifikates.

Der Benutzer hat die Möglichkeit, die vom Dienstanbieter durch das Zertifikat erbetenen Zugriffsrechte weiter einzuschränken. Die eingeschränkten Rechte werden als Bestandteil des nachfolgenden PACE-Protokolls an den Chip übertragen.

Da PACE einen sicheren Kanal zwischen Chip und lokalem Terminal aufbaut, wird die Kommunikation zwischen Dienstanbieter 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 Dienstanbieter aufgebaut, so dass das lokale Terminal ab jetzt die Kommandos und die Antworten nur noch unverändert weiterreicht.

Zur Umsetzung der Online-Authentisierung (vgl. Abbildung 2) empfiehlt das BSI die Verwendung von zertifizierten Komponenten:

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

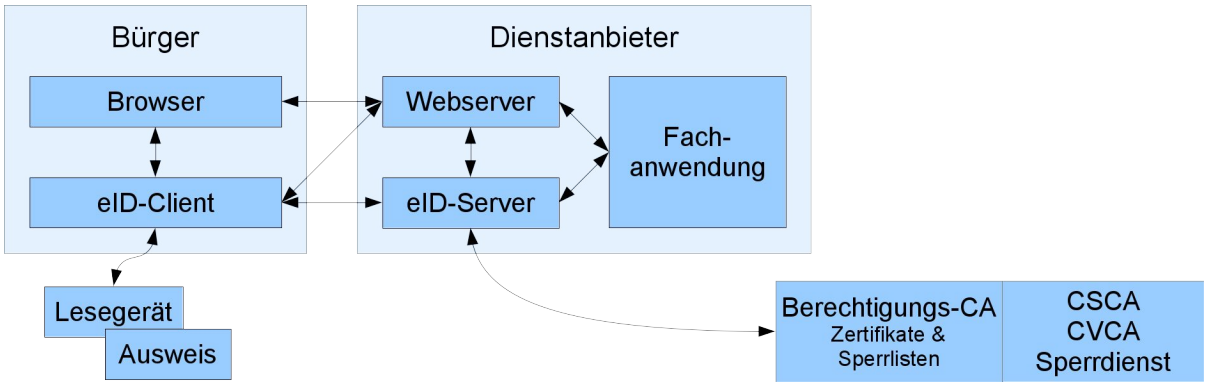

Abbildung 2: Kommunikationsbeziehungen Online-Authentisierung

Das BSI empfiehlt, die Dienstanbieter-Webseite so zu gestalten, dass sie von einem Benutzer, der sich an die Sicherheitsempfehlungen des BSI hält, ohne Einschränkungen nutzbar ist. Die Empfehlungen finden sich auf der Webseite https://www.bsi-fuer-buerger.de und umfassen insbesondere:

- Verwendung eines aktuellen Virenschutzes und Firewall
- Vermeidung aktiver Inhalte
- Einsatz zertifizierter Komponenten (Lesegerät, Client-Software) für die Ausweisnutzung (s.o.).

Weiter wird empfohlen, auf der Login-Seite auf das Download-Portal des Bundes für die AusweisApp zu verweisen.

Zur Zertifizierung der Komponenten siehe auch Anhang A.

5. Hintergrundsysteme

5.1 Dokumenten-PKI

Bestimmte auf dem Chip gespeicherte Daten (Daten der Biometrieanwendung, die Datei EF.CardSecurity, die u.a. den öffentlichen Schlüssel der Chipauthentisierung enthält) 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 Dienstanbieter 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;
- Anwendungen in den Ausweisbehörden – Änderungsdienst/Visualisierung (Abschnitt 7);
- Berechtigungs-CAs für eBusiness/eGovernment-Dienstanbieter (Abschnitt 5.2.1);
- hoheitliches Kontrollwesen – Polizei und Grenzkontrolle;

- Zertifizierung von *Signaturterminals – bestätigte Signaturterminals* erhalten ein Zertifikat als Nachweis der Bestätigung (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 *Bestätigte 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 ist 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 die Verwendung in eBusiness und eGovernment) werden durch Berechtigungs-CAs vergeben. Voraussetzung ist hierfür die Erteilung einer Erlaubnis durch die Vergabestelle für Berechtigungszertifikate (VfB).

Ein Dienstanbieter, der die eID-Anwendung des elektronischen Personalausweises für seine Geschäftsprozesse nutzen möchte, wendet sich an den VfB, um eine Berechtigung zu erhalten. Dazu muss er gemäß [PAuswG] sowie der zugehörigen Verordnung u.a. folgende Unterlagen vorlegen:

- Angaben zur Identität des Dienstanbieters sowie Kontaktdaten (einschließlich Datenschutzbeauftragter);
- Angaben zum Unternehmen und zum Dienstangebot;
- Angaben über die auszulesenden Daten mit Begründung der Notwendigkeit;
- Angaben über die Verwendung der ausgelesenen Daten;
- gegebenenfalls Angaben zur Nutzung eines eID-Services für den Betrieb des eID-Servers.

Weiter muss der Dienstanbieter ein Sicherheitskonzept erstellen, in dem insbesondere folgende Schutzziele betrachtet werden:

- der private Schlüssel des Zugriffszertifikats muss sicher verwahrt werden;
- aus Ausweisen ausgelesene dokumenten- und personenbezogene Daten müssen vor unberechtigtem Zugriff geschützt werden.

Aus dem Schutzbedarf für den privaten Schlüssel des Zugriffszertifikates und der gelesenen Daten ergibt sich auch ein entsprechender Schutzbedarf für die Kommunikationsschlüssel, z.B. für die Kommunikation mit der Berechtigungs-CA/VfB oder gegebenenfalls mit einem eID-Server-Betreiber.

Vorgaben für dieses Sicherheitskonzept finden sich in [TR-03130], Teil 2.

Sind die Unterlagen vollständig und ausreichend, erhält der Dienstanbieter die Erlaubnis, sich für einen begrenzten Zeitraum (maximal drei Jahre) Zugriffszertifikate bei einer Berechtigungs-CA seiner Wahl ausstellen zu lassen.

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:

- der *Terminal Sector* des Dienstanbieters für die dienste- und kartenspezifische Kennung (Abschnitt 4.4.3.3) und das Sperrmerkmal (Abschnitt 4.4.2);
- die *Certificate Description* mit Angaben, die dem Benutzer bei einer Online-Authentisierung (Abschnitt 4.7) angezeigt werden können (siehe auch [CP-eID]):
- Name des Dienstanbieters (*subjectName*);
- Name der ausstellenden Berechtigungs-CA (*issuerName*);
- Anschrift und Email-Adresse des Dienstanbieters, Zweck der Anfrage des Dienstanbieters und die zuständige Datenschutzbehörde (*termsOfUsage*);
- Im Falle von Zertifikaten, die für die Online-Authentisierung ausgestellt werden, sind weiter die Hash-Werte der TLS-Zertifikate des Dienstanbieters (und ggfs. eines eID-Servers) zur Überprüfung durch die Client-Software des Bürgers enthalten (*commCertificates*).

Die *Extensions* werden in [TR-03110] 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 *Bestätigte Signaturterminals*

Bestätigte Signaturterminals sind mit eigenen Berechtigungszertifikaten ausgestattet, die durch den Ausweis im Rahmen der Terminalauthentisierung überprüft werden. Diese Zertifikate weisen die Bestätigung des Lesegerätes im Sinne des Signaturgesetz/Signaturverordnung ([SigG], [SigV]) nach. Dazu wird im Rahmen des Bestätigungsverfahrens 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:

- An-/Ausschalten der eID-Anwendung für *Authentisierungsterminals* ohne Recht *CAN allowed* auf dem Ausweis über den Änderungsdienst (Abschnitte 4.4.3.2 und 7);
- Sperre der eID-PIN durch dreimalige Falscheingabe der eID-PIN (Abschnitt 3.3.3);
- Meldung des Ausweises als verloren bzw. gestohlen (vgl. Abbildung 3):
- Primärer Weg ist hierzu die Verlustmeldung 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.
- Als sekundärer Weg, z.B. außerhalb der Öffnungszeiten der Ausweisbehörde, kann der Eintrag in die eID-Sperrliste über eine Sperrhotline ausgelöst werden. Die Verlustmeldung an die Ausweisbehörde ist zusätzlich so bald wie möglich durchzuführen.
- Die Zertifikate der Signaturfunktion werden nicht über die Ausweisbehörde oder die Polizei gesperrt, sie müssen beim ausstellenden Zertifizierungsdiensteanbieter gesperrt werden.

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

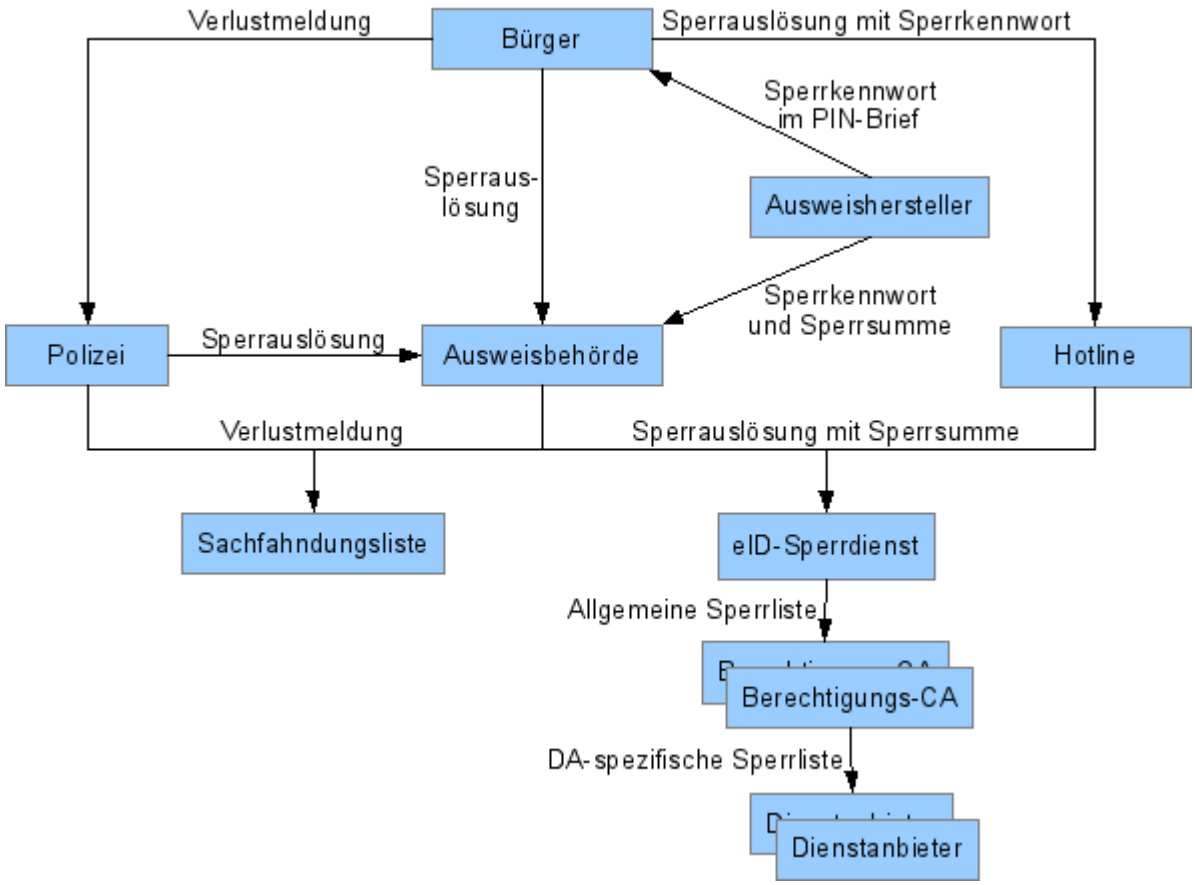

Abbildung 3: Sperrlisten

5.3.1 eID-Sperrliste

Die vom Sperrdienst geführte eID-Sperrliste für Dienstanbieter dient nur der Sperre der eID-Anwendung des Ausweises für eBusiness und eGovernment-Dienstanbieter, 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 der PIN/PUK-Brief (Abschnitt 6.2) mitgeteilt sowie im Personalausweisregister 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 Ausweisbehörde bzw. Hotline ist dann:

1. Der Ausweisinhaber zeigt das Abhandenkommen des Ausweises an;
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 Dienstespezifische Sperrlisten

Um eine Auflösung des Pseudonyms (Abschnitt 4.4.3.3) über die Sperrlistenabfrage zu verhindern, wird zur Abfrage der eID-Sperrliste ein dienstespezifisches Sperrmerkmal verwendet (Abschnitt 4.4.2). Das dienstespezifische Sperrmerkmal wird vom Dienstanbieter während einer Online-Authentisierung ausgelesen und darf von diesem nur zum Abgleich mit der eID-Sperrliste verwendet werden.

Aus dem Sperrschlüssel werden in einem mehrstufigen Verfahren die dienstespezifischen 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 dienstespezifische Listen mit Sperrmerkmalen um;
4. Die Dienstanbieter rufen die Listen der dienstespezifischen 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 dienstespezifische Sperrmerkmal – wie das Pseudonym – weder durch die Dienstanbieter 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 Dienstanbieter abgefragt werden.

5.3.1.3 Entsperrung und Sperrauskunft

Über die Ausweisbehörde ist auch die Entsperrung eines Ausweises sowie die Abfrage des Sperrstatus möglich. 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 die Online-Authentisierung, erfordert das Setzen einer operationellen eID-PIN durch den Inhaber.
  Für Jugendliche unter 16 Jahren oder auf Antrag des Inhabers ist die Nutzung der eID-Anwendung mit eID-PIN abgeschaltet.
- 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 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 dem Personalausweisgesetz/Aufenthaltsgesetz und dem Signaturgesetz sowie den zugehörigen Verordnungen ergeben,
- sowie über die Möglichkeiten zum Abschalten der eID-Funktion, PIN-Änderung usw.

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 der entsprechenden Regelungen zum Aufenthaltstitel:

- 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 bzw. die eID-Anwendung abschalten lassen;
- sowie geeignete Kartenleser und Software verwenden, um einen unberechtigten Zugriff auf die eID-PIN zu verhindern und um die korrekte Darstellung der Zugriffszertifikate sicherzustellen).

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;
- An- und Ausschalten der nicht-hoheitlichen Nutzung der eID-Anwendung.

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 An-/Ausschalten der eID-Anwendung auch im Ausweisregister und die geänderte Adresse im Melderegister bzw. in der Ausländerdatei A gespeichert wird, muss der Änderungsdienst in die vorhandenen IT-Verfahren der Ausweisbehörden integriert werden.
- 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 Evaluierung/Zertifizierung nach Common Criteria [CC] durchgeführt werden. Über die erfolgreiche Evaluierung wird durch das BSI ein Zertifikat ausgestellt.

Komponente	**Konformität**	**Common Criteria**
Fingerabdruckleser nach [TR-03121]	Verpflichtend: [TR-03122]	
Software zur Erfassung und Qualitätssicherung von Gesichtsbild und Fingerabdrücke nach [TR-03121]	Verpflichtend: [TR-03122]	
Datenaustauschformat zwischen Ausweisbehörde und Dokumentenhersteller nach TR-XhD nach [TR-03123]	Verpflichtend: Herstellererklärung	
Modul zur Sicherung der Authentizität und Vertraulichkeit der Antragsdaten nach TR-SiSKo hD 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][6]
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][7]
Kartenterminals für Ausweisinhaber (Heimanwender) nach [TR-03119]	Empfohlen: [TR-03105], Teil 4 ggfs. [TR-03105], Teil 5.2	Empfohlen: Für Standard-/Komfortleser: [PP-0083] Verpflichtend: Bestätigung nach [SigG] für QES-fähige Lesegeräte
eID-Client nach [TR-03124], Teil 1, und [TR-03112]	Empfohlen: [TR-03124], Teil 2	Optional: [PP-0066]
eID-Server nach [TR-03130], Teil 1, und [TR-03112]	Vorgesehen: [TR-03130], Teil 4	Siehe [CP-eID]

6 Die Anforderungen aus [PP-0061]/[PP-0069]/[PP-0087] umfassen auch die Anforderungen an eine sichere Signaturerstellungseinheit gemäß dem Protection Profile [PP-0059]. Zusätzlich zur Zertifizierung ist eine Bestätigung nach SigG/SigV notwendig.

7 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 dienstespezifischen 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* genutzt. Der private Schlüssel des Terminal-Sektors wird von der Berechtigungs-CA für die Umrechnung der allgemeinen Sperrmerkmale in dienstespezifische 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, erlaubt 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 4.4.3)		
Dienste- und kartenspezifische Kennung	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. Diese Informationen stehen zusätzlich elektronisch als `DefectList` gemäß [TR-03129] zur Verfügung. 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 und Aufenthaltstitel.

Document Signer Serial Number	Ausgabe-zeitraum	Abweichung	ObjectIdentifier in `DefectList`
SN ≤ 106	Bis 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	Bis Q3/2011	Die Ausweise enthalten in EF.ChipSecurity kein `eIDSecurityInfo`.	`id-eIDSecurityInfoMissing`
SN ≤ 109	Bis 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`
SN ≤ 112	Bis Q2/2012	Die Ausweise enthalten keine bzw. eine leere Datengruppe „Geburtsname“ (DG13).	`id-eIDDGMissing` mit Parameter DG13
SN ≤ 122	Bis Q1/2013	Die Ausweise enthalten keine Datengruppe „Staatsangehörigkeit“ (DG10).	`id-eIDDGMissing` mit Parameter DG10

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

[CP-eID] BSI: Certificate Policy für die Country Verifying Certification Authority -- eID-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-0064] BSI: Common Criteria Protection Profile BSI-CC-PP-0064: Protection Profile for Inspection Systems

[PP-0066] BSI: Common Criteria Protection Profile BSI-CC-PP-0066: eID-Client based on eCard-API

[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

[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-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-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

[CC] CCMB: Common Criteria for Information Technology Security Evaluation

[PP-0059] CEN: EN 14169-2 -- 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
[FIPS 197]	NIST: FIPS PUB 197, Specification for the Advanced Encryption Standard (AES)
[OSCI]	OSCI-Leitstelle: OSCI-Transport 1.2, Spezifikation
[AufenthG]	Aufenthaltsgesetz in der Fassung der Bekanntmachung vom 25. Februar 2008 (BGBl. I S.162), zuletzt geändert durch Artikel 4 Absatz 5 des Gesetzes vom 30. Juli 2009 (BGBl. I S.2437)
[PAuswG]	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG) vom 18. Juni 2009 (BGBl. I S. 1346)
[SigG]	Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)
[SigV]	Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)