Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie TR-03128 Diensteanbieter für die eID-Funktion

Teil 3: Änderungsdienste mit hoheitlicher Berechtigung

Version 1.1

24.04.2023

Änderungshistorie

Version	*Datum*	*Beschreibung*
0.1 Draft	26.03.2021	Erster Entwurf
0.2 Draft	04.05.2021	Anpassung des Ablaufs, Entfall der Information an die Ausweisbehörde, Festlegung konkreter Werte für Antragswiederholung, Vereinheitlichung der Begrifflichkeiten
0.3 Draft	13.08.2021	Ergänzung des Zentralen Schreibdienstes, kleinere Anpassungen für den PIN-Rücksetz-Dienst
1.0	29.09.2021	Finalisierung
1.1	17.04.2023	Anpassung für Adressanzeige

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung und Geltungsbereich

Teil 1 der vorliegenden Technische Richtlinie [1] beschreibt die Nutzung von Dokumenten mit eID-Funktion basierend auf Extended Access Control (EAC). Dazu zählen der elektronische Personalausweis, der elektronische Aufenthaltstitel und die eID-Karte für Unionsbürger, im Folgenden als „Ausweis“ bezeichnet, zum elektronischen Identitätsnachweis sowie beim Vor-Ort-Auslesen durch Diensteanbieter im eGovernment und eBusiness.

Einige Daten und Funktionalitäten des Ausweises können auch nach Personalisierung im Herstellungsprozess und der Ausgabe an den Inhaber geändert werden:

- Ändern der Adresse und des amtlichen Gemeindeschlüssels;
- Setzen einer neuen eID-PIN;
- Aktivieren der eID-Funktion

Neben der Umsetzung dieser Dienste auf Basis einer „EAC-Box“ nach TR-03131 [2] in den Räumen einer Behörde („klassischer“ Änderungsdienst, vgl. TR-03127 [3] Kapitel 7.1), sieht das PAuswG [4] und das eIDKG [5] derartige Änderungen für Personalausweise und eID-Karten auch auf Basis eines elektronisch gestellten Antrags vor. Der Ausweisinhaber nutzt dabei clientseitig, wie beim elektronischen Identitätsnachweis, eine eID-Client Software in Verbindung mit seinem eigenen Kartenleser oder mobilen Endgerät. Serverseitig betreibt der hierfür gesondert legitimierte Betreiber einen spezialisierten eID-Server mit hoheitlicher Berechtigung.

Der vorliegende Teil dieser Technischen Richtlinie regelt gemäß §2 Nummer 2 PAuswV [6] die technischen Grundlagen, Anforderungen und Prozesse für die folgenden derartigen Änderungsdienste mit hoheitlichen Berechtigungen:

- Der „PIN-Rücksetz-Dienst“ ermöglicht das Neusetzen der eID-PIN und das nachträgliche Aktivieren der eID-Funktion nach elektronischem Antrag durch den Ausweisinhaber (vgl. TR-03127 [3] Kapitel 7.2)..
- Der „Zentrale Schreibdienst“ ermöglicht das Ändern der Adresse und des amtlichen Gemeindeschlüssels nach elektronischer Anmeldung gemäß § 23a BMG [7] durch den Ausweisinhaber (vgl. TR-03127 [3] Kapitel 7.3)..

1.1 Hoheitliche Berechtigungen

Zur Erfüllung ihrer Aufgaben erhalten die Betreiber der Änderungsdienste hoheitliche Berechtigungszertifikate aus der CVCA-eID. Sie agieren damit als *hoheitliches nationales Authentisierungsterminal* (vgl. TR-03127 [3]) und beziehen die benötigten Terminalzertifikate von einem hoheitlichen Document Verifier (DV). Diese Berechtigungszertifikate sind dabei im Umfang der Berechtigungen auf die für die Aufgabenerfüllung notwendigen Rechte beschränkt und enthalten im Gegensatz zu anderen hoheitlichen Zertifikaten zusätzlich die notwendigen *Certificate Extensions* für die Funktionalitäten Sperrlistenabruf und dienste- und kartenspezifische Kennung (DKK), sowie den elektronischen Identitätsnachweis (siehe dazu CP-eID [8], TR-03127 [3] und TR-03110-4 [9]).

Die genauen technischen und organisatorischen Abläufe werden in der Certificate Policy (CP) des hoheitlichen DVs festgelegt, der diese basierend auf der Certificate Policy CP-eID [8] der Wurzel-Instanz der Berechtigungs-PKI erstellt. Die Kommunikationsprotokolle werden in TR-03129 [10] festgelegt.

2 PIN-Rücksetz-Dienst

§7 PAuswG [4] führt aus:

> *(3a) Für das elektronisch beantragte Neusetzen der Geheimnummer sowie für die elektronische Beantragung des nachträglichen Einschaltens der Funktion zum elektronischen Identitätsnachweis ist der Ausweishersteller zuständig.*

Die PAuswV [6] regelt die näheren Bedingungen für das Neusetzen der PIN in §20:

> *(2) Ein Ausweisinhaber, der eine Meldeadresse im Inland hat, kann das Neusetzen der Geheimnummer auch durch Verwendung der Zugangsnummer und eines hierfür vom Ausweishersteller zur Verfügung gestellten elektronischen Formulars beantragen. Der Ausweishersteller schaltet die Funktion zum elektronischen Identitätsnachweis ab und versendet eine neue, zufällig generierte Geheimnummer in einem Brief an die im Speicher- und Verarbeitungsmedium gespeicherte Anschrift des Ausweisinhabers. Bei der Übergabe ist die Identität des Ausweisinhabers durch den Zusteller durch Vorlage des Personalausweises zu überprüfen. Nach Erhalt der neuen Geheimnummer meldet sich der Ausweisinhaber erneut beim Ausweishersteller unter Verwendung der Zugangsnummer an. Der Ausweishersteller schaltet die Funktion zum elektronischen Identitätsausweis wieder ein und schreibt die neue, zufällig generierte Geheimnummer in das Speicher- und Verarbeitungsmedium. Der Ausweisinhaber ändert die neue, zufällig generierte Geheimnummer in eine selbst gewählte Geheimnummer.*

Das nachträgliche Einschalten der eID-Funktion wird in PAuswV [6] §22 geregelt:

> *(2) Der Antrag [Anm: auf nachträgliches Aktivieren der eID-Funktion] nach § 10 Absatz 3 Satz 1 des Personalausweisgesetzes kann durch den Ausweisinhaber, der eine Meldeadresse im Inland hat, auch durch Verwendung der Zugangsnummer und eines hierfür vom Ausweishersteller zur Verfügung gestellten elektronischen Formulars gestellt werden. Der Ausweishersteller versendet eine neue, zufällig generierte Gerheimnummer in einem Brief an die im Speicher- und Verarbeitungsmedium gespeicherte Anschrift des Ausweisinhabers. Bei der Übergabe ist die Identität des Ausweisinhabers durch den Zusteller durch Vorlage des Personalausweises zu überprüfen. Nach Erhalt der neuen Geheimnummer meldet sich der Ausweisinhaber erneut beim Ausweishersteller unter Verwendung der Zugangsnummer an. Der Ausweishersteller schaltet die Funktion zum elektronischen Identitätsausweis ein und schreibt die neue, zufällig generierte Geheimnummer in das Speicher- und Verarbeitungsmedium. Der Ausweisinhaber ändert die neue, zufällig generierte Geheimnummer in eine selbst gewählte Geheimnummer.*

Der Ausweishersteller betreibt für die Umsetzung beider Funktionalitäten einen *PIN-Rücksetz-Dienst (PIN Reset Service - PRS)* gemäß diesem Teil der vorliegenden Technischen Richtlinie. Da auch bei einem nachträglichen Einschalten der eID-Funktion ein Neusetzen der Geheimnummer (eID-PIN, bzw. PIN) erforderlich ist und auch beim Neusetzen der PIN temporär die eID-Funktion abgeschaltet wird, sind beide Vorgänge in technischer Umsetzung und Ablauf eng verwandt. Die folgenden Ausführungen behandeln somit beides, soweit nicht explizit anders erwähnt.

2.1 Rahmenbedingungen der Nutzung

Ausweisinhaber, die zum Zeitpunkt des Antrags mindestens das 16. Lebensjahr vollendet haben und eine Meldeadresse im Inland haben, können den PIN-Rücksetz-Dienst nutzen, um eine vergessene PIN

neusetzen zu lassen (§20 Absatz 2 PAuswV [6]), oder die eID-Funktion nachträglich einzuschalten, falls diese zuvor abgeschaltet war (§22 Absatz 2 PAuswV [6]).

Sie benötigen dafür neben ihrem Ausweisdokument (Personalausweis, eID-Karte) ein internetfähiges Gerät mit einem installierten eID-Client, z.B. die vom Bund bereitgestellte AusweisApp2[1] und einen geeigneten Kartenleser oder ein Smartphone mit NFC[2]-Schnittstelle.

Das Ausweisdokument muss gültig und darf nicht gesperrt sein. Um Missbrauch zu verhindern, wird die Antragstellung auf 10 Anträge innerhalb von 90 Tagen eingeschränkt. Um Fehlbedienungen zu verhindern, soll zudem ein erneuter Antrag auf Neusetzen der PIN erst nach 7 Tagen gestellt werden können. Die Kontrolle geschieht über begrenzte Speicherung und Abgleich des Pseudonyms (DKK).

Die neu gesetzte Ausweis-PIN wird dem Ausweisinhaber postalisch an die aus dem Ausweisdokument ausgelesene Meldeadresse zugestellt. Um sicherzustellen, dass nur der Ausweisinhaber Kenntnis der neu gesetzten PIN erhält, erfolgt eine persönliche Zustellung mit Identitätsfeststellung. Damit sichergestellt werden kann, dass die eID-Funktion erst nach Zustellung der neuen PIN genutzt werden kann, wird die eID-Funktion bei Antragstellung deaktiviert und kann erst nach Zustellung des PIN-Rücksetz-Briefes durch den Ausweisinhaber wieder aktiviert werden.

Die aus dem Dokument ausgelesene Meldeadresse wird dem Ausweisinhaber am Schluss des Antragsvorgangs zur Kontrolle angezeigt und dieser hat die Möglichkeit den Briefversand zu stornieren, sollte er unter dieser Anschrift im Versandzeitraum nicht erreichbar sein, beispielsweise aufgrund eines aktuellen Auslandaufenthalts oder einer unterlassenen Änderung der Meldeanschrift.

2.2 Ablauf

Der Ablauf des Neusetzens der PIN bzw. der Aktivierung der eID-Funktion gliedert sich in die folgenden Schritte:

1. Elektronische Antragstellung durch den Ausweisinhaber.
2. Erzeugen einer neuen PIN und Deaktivieren der eID-Funktion durch den PRS.
3. Persönliche Zustellung der neuen PIN an den Ausweisinhaber.
4. Fortsetzen des Vorgangs durch Verwendung des Aktivierungscodes.
5. Setzen der neuen PIN und Aktivieren der eID-Funktion durch den PRS.

Diese Schritte sind in den nachfolgenden Abschnitten 2.2.1 bis 2.2.5 näher beschrieben sowie in Abschnitt 2.3 als Ablaufdiagramme aufbereitet.

2.2.1 Elektronischer Antrag

Die Antragstellung für das Neusetzen der PIN oder die nachträgliche Aktivierung der eID-Funktion erfolgt über eine durch den Ausweishersteller betriebene Webseite.

Auf dieser Webseite muss der Ausweishersteller über die Bedingungen und Auswirkungen des Antrags sowie die Datenschutzbestimmungen informieren.

Zur Vermeidung späterer Fehler empfiehlt es sich dabei zunächst die folgenden Vorbedingungen explizit durch den Ausweisinhaber bestätigen zu lassen:

- Art des Antrags (Nachträgliches aktivieren oder PIN neusetzen)?
- Vorliegendes Dokument (PA oder eID-Karte)?
- Wurde das 16. Lebensjahr vollendet?
- Inlandsmeldeadresse?

[1] https://www.ausweisapp.bund.de
[2] Near Field Communication (NFC); Funkschnittstelle

Nach Bestätigung erfolgt der Aufruf des eID-Clients durch den Aufruflink (siehe TR-03124-1 [11])(vgl. Abbildung 1, Schritte 1 & 2).

2.2.2 Erzeugen der PIN

Der eID-Client ruft gemäß TR-03124-1 [11] das TCToken ab und verbindet sich mit dem eID-Server des PRS.

eID-Server und eID-Client kommunizieren gemäß TR-03112 [12] und führen gemeinsam die *General Authentication Procedure* (GAP) als Authentisierungsterminal (siehe TR-03110-3 [13]) durch. Als Passwort kommt hierbei die durch den Ausweisinhaber einzugebende Zugangsnummer (Card Access Number, CAN) zum Einsatz (vgl. Abbildung 1, Schritte 3 bis 6).

Über den im Ergebnis zur GAP etablierten Secure-Messaging-Kanal führt der eID-Server dann die folgenden Funktionen gemäß TR-03110-3 [13] durch (vgl. Abbildung 1, Schritte 7 & 8):

- Gültigkeitsprüfung
- Abfrage des Sperrmerkmals
- Altersverifikation (16. Lebensjahr vollendet?)
- Restricted Identification (Pseudonym)
- Auslesen von Dokumententyp, Vorname, Nachname, Geburtsdatum und Anschrift

Für das Auslesen (Datenerhebung) sind insbesondere die „Grundsätze für die Verarbeitung personenbezogener Daten“ laut Artikel 5 der Datenschutz-Grundverordnung (DSGVO) [14] zu beachten. Es dürfen nur die Daten erhoben werden, welche im Prozess auch tatsächlich benötigt werden.

OHNE den Secure-Messaging-Kanal abzubauen prüft nun die Anwendungslogik des PRS folgende Bedingungen (vgl. Abbildung 1, Schritte 9 & 10) für das Neusetzen der PIN bzw. das nachträgliche Aktivieren der eID-Funktion. eID-Server und Webserver des PRS müssen deshalb eine interne Schnittstelle verwenden (siehe Abschnitt 4.1):

- Ausweis ist gültig und nicht gesperrt.
- Der Ausweisinhaber hat das 16. Lebensjahr vollendet.
- Der Dokumententyp ist ID oder UB.
- Für das Pseudonym darf ein Antrag gestellt werden[3].
- Die Meldeadresse liegt in Deutschland.

Sind eine oder mehrere der Bedingungen nicht erfüllt, bricht der eID-Server den Vorgang durch schließen des Secure-Messaging-Kanals ab.

Sind die Bedingungen erfüllt, erzeugt der PRS eine neue, zufällige PIN und speichert diese verschlüsselt ab (vgl. Abbildung 1, Schritte 11 bis 13). Anschließend veranlasst der PRS die Deaktivierung der eID-Funktion (vgl. Abbildung 1, Schritte 14 & 15) und der Secure-Messaging-Kanal wird geschlossen.

Der eID-Server signalisiert dem PRS den erfolgreichen Abschluss des Vorgangs. Dieser veranlasst die Erstellung des PIN-Rücksetz-Briefs mit den zuvor ermittelten Angaben aus dem Dokument und der verschlüsselten PIN (vgl. Abbildung 1, Schritte 16 & 17). Um dem Ausweisinhaber die Möglichkeit einer Stornierung zu bieten, werden Erstellung und Druck des PIN-Briefs nicht unmittelbar ausgeführt, sondern um mindestens zwei Minuten verzögert.

Der eID-Client leitet den Ausweisinhaber anschließend über die Rücksprungadresse zurück zum Webserver des PRS. Hier muss dem Ausweisinhaber das Ergebnis des Vorgangs und die weiteren Schritte angezeigt werden (vgl. Abbildung 1, Schritte 18 & 19).

[3] Um Missbrauch und Fehlbedienung zu verhindern kann, wie in Abschnitt 2.1 beschrieben, die Antragsstellung pro Ausweis temporär eingeschränkt werden.

Im Erfolgsfall erfolgt eine Anzeige der ausgelesenen Meldeadresse, an die der Briefversand erfolgen wird. Es besteht die Möglichkeit für den Ausweisinhaber den Antrag über einen angebotenen Button innerhalb von zwei Minuten zu stornieren. In diesem Fall erfolgt kein Briefversand und die Antragsdaten werden gelöscht.

Im Fehlerfall ist der Ausweisinhaber über den Grund des Fehlschlags zu informieren. Bei mutmaßlich temporärer Ursache für den Fehlschlag, soll dem Ausweisinhaber die Möglichkeit gegeben werden, den Authentisierungsvorgang direkt erneut zu versuchen, ohne den gesamten Antrag erneut zu starten.

2.2.3 Druck und Zustellung des PIN-Rücksetz-Briefs

Hat der Ausweishersteller erfolgreich eine neue PIN erzeugt und verschlüsselt gespeichert und der Ausweisinhaber den Vorgang nicht innerhalb von zwei Minuten storniert, erstellt er einen PIN-Rücksetz-Brief (vgl. Abbildung 1, Schritt 17). Der PIN-Rücksetz-Brief wird an die ausgelesene Meldeadresse des Ausweisinhabers adressiert und informiert den Ausweisinhaber im Anschreiben über den gestarteten Versuch einer PIN-Rücksetzung und die weiteren Schritte. Der Ausweisinhaber soll auch darauf hingewiesen werden, die neu gesetzte PIN anschließend in eine selbstgewählte PIN zu ändern.

Der PIN-Rücksetz-Brief enthält die neu gesetzte PIN unter einer Sicherheitsabdeckung (analog zum initialen Transport-PIN-Brief) verborgen. Zusätzlich enthält der PIN-Rücksetz-Brief einen Aktivierungscode, mit dem nach Empfang des Briefes die gesetzte PIN aktiviert werden muss. Aus drucktechnischen Gründen ist auch der Aktivierungscode unter einer Sicherheitsabdeckung verborgen, obwohl diese aus sicherheitstechnischer Sicht nicht erforderlich ist.

Als Komfortfunktion enthält der PIN-Rücksetz-Brief die URL des PRS zur Eingabe des Aktivierungscodes zusätzlich zur Angabe in Klartext auch als QR-Code, wobei dort der Aktivierungscode auch direkt mit übergeben werden kann.

Der PIN-Rücksetz-Brief wird dem Ausweisinhaber mittels eines sicheren Zustellverfahrens zugestellt (vgl. Abbildung 2, Schritte 1 & 2). Der Zusteller gleicht den Empfänger durch Lichtbildabgleich gegen ein hoheitliches Dokument ab. Nach erfolgreichem Abgleich übergibt der Zusteller den PIN-Rücksetz-Brief. Der Versanddienstleister bestätigt die Zustellung des PIN-Rücksetz-Briefs an den Ausweishersteller (vgl. Abbildung 2, Schritt 2a).

Kann der PIN-Rücksetz-Brief nicht zugestellt werden, erfolgt die Rücksendung an den Ausweishersteller, dieser vernichtet den PIN-Rücksetz-Brief.

2.2.4 Verwendung des Aktivierungscodes

Der Ausweisinhaber kehrt zur Webseite des PRS zurück (durch manuelle URL-Eingabe oder Scannen des QR-Codes) und gibt den Aktivierungscode ein (vgl. Abbildung 2, Schritt 3). Der PRS prüft die Gültigkeit des Aktivierungscodes. Der Aktivierungscode muss gültig sein, damit der Prozess mit den weiteren Schritten fortgesetzt wird (vgl. Abbildung 2, Schritt 4 & 4a). Es sollten Vorkehrungen für einen Missbrauchsschutz umgesetzt werden, so dass sich gültige Aktivierungscodes bspw. nicht durch einen Brute-Force Angriff ermitteln lassen. Eine Limitierung der Anzahl an Anfragen auf Basis der anfragenden IP Adresse kann vorgesehen werden.

Der Aktivierungscode selbst kann innerhalb der Gültigkeit beliebig oft erneut genutzt werden, um den Vorgang fortzusetzen, solange dieser nicht erfolgreich abgeschlossen werden konnte.

Um Fehlbedienungen zu verhindern, soll ein erneuter Antrag auf PIN-Änderung für denselben Ausweis erst nach Ablauf einer Frist von 7 Tagen wieder möglich sein. Diese Frist orientiert sich an der typischen maximalen postalischen Laufzeit des PIN-Rücksetz-Briefs.

2.2.5 Setzen der PIN

Der Aufruflink für das Setzen der PIN startet den eID-Client des Ausweisinhabers, um erneut eine GAP mit Passwort (CAN) durchzuführen und einen Secure-Messaging-Kanal zwischen Dokument und eID-Server zu

etablieren (vgl. Abbildung 2, Schritte 5 bis 9). Um die PIN zu setzen führt der eID-Server dann die folgenden Funktionen gemäß TR-03110-3 [13] durch (vgl. Abbildung 2, Schritte 10 bis 12):

- Gültigkeitsprüfung
- Abfrage des Sperrmerkmals
- Restricted Identification (Pseudonym)

OHNE den Secure-Messaging-Kanal abzubauen prüft nun die Anwendungslogik des PRS die Bedingungen für das Setzen der PIN (vgl. Abbildung 2, Schritt 13):

- Der Ausweis ist gültig und nicht gesperrt.
- Das Pseudonym des Ausweises passt zum Aktivierungscode.

Sind eine oder mehrere der Bedingungen nicht erfüllt, bricht der eID-Server den Vorgang durch schließen des Secure-Messaging-Kanals ab.

Sind die Bedingungen erfüllt, aktiviert der PRS die eID-Funktion und setzt die PIN indem folgende Funktionen gemäß TR-03110-3 [13] durchgeführt werden (vgl. Abbildung 2, Schritte 13a bis 18a):

1. Aktivieren der eID-Funktion.
2. PIN entschlüsseln und setzen.
3. Sicheres löschen der PIN im PRS.
4. Schließen des Secure-Messaging-Kanals

Der eID-Client leitet den Ausweisinhaber anschließend über die Rücksprungadresse zurück zum Webserver des PRS. Hier muss dem Ausweisinhaber das Ergebnis des Vorgangs und die weiteren Schritte angezeigt werden (vgl. Abbildung 2, Schritte 19 & 20).

Im Fehlerfall ist der Ausweisinhaber über den Grund des Fehlschlags zu informieren. Bei mutmaßlich temporärer Ursache für den Fehlschlag, soll dem Ausweisinhaber die Möglichkeit gegeben werden, den Authentisierungsvorgang direkt erneut zu versuchen.

2.3 Ablaufdiagramme

In Abbildung 1 sind die Schritte aus den Abschnitten 2.2.1 bis 2.2.3 als Ablaufdiagramm dargestellt.

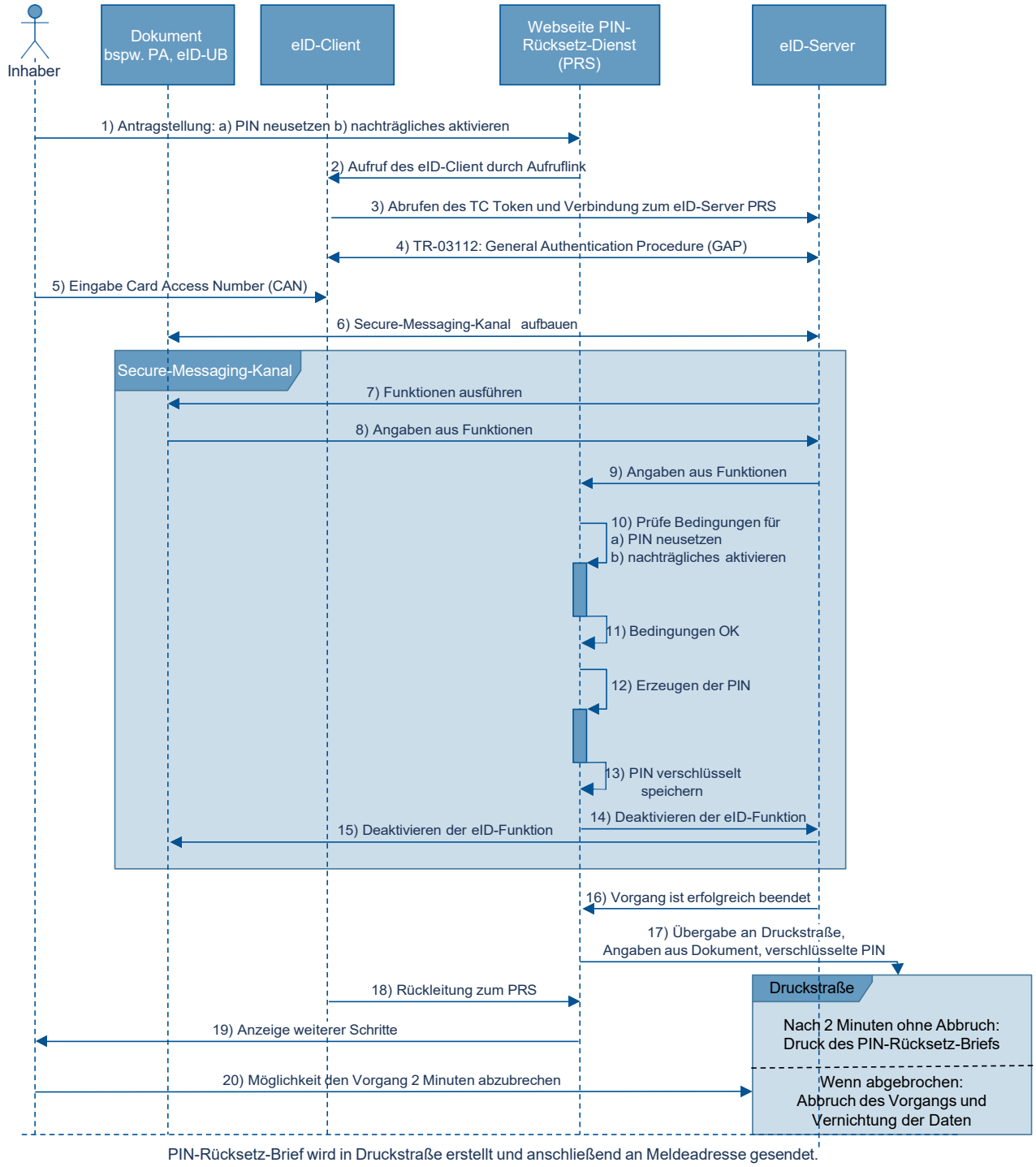

Abbildung 1: Ablaufdiagramm zur Beantragung von Neusetzen der PIN für eID-Funktion via PIN-Rücksetz-Dienst bis Versand des PIN-Rücksetz-Briefs.

In Abbildung 2 sind die Schritte aus den Abschnitten 2.2.3 bis 2.2.5 als Ablaufdiagramm dargestellt.

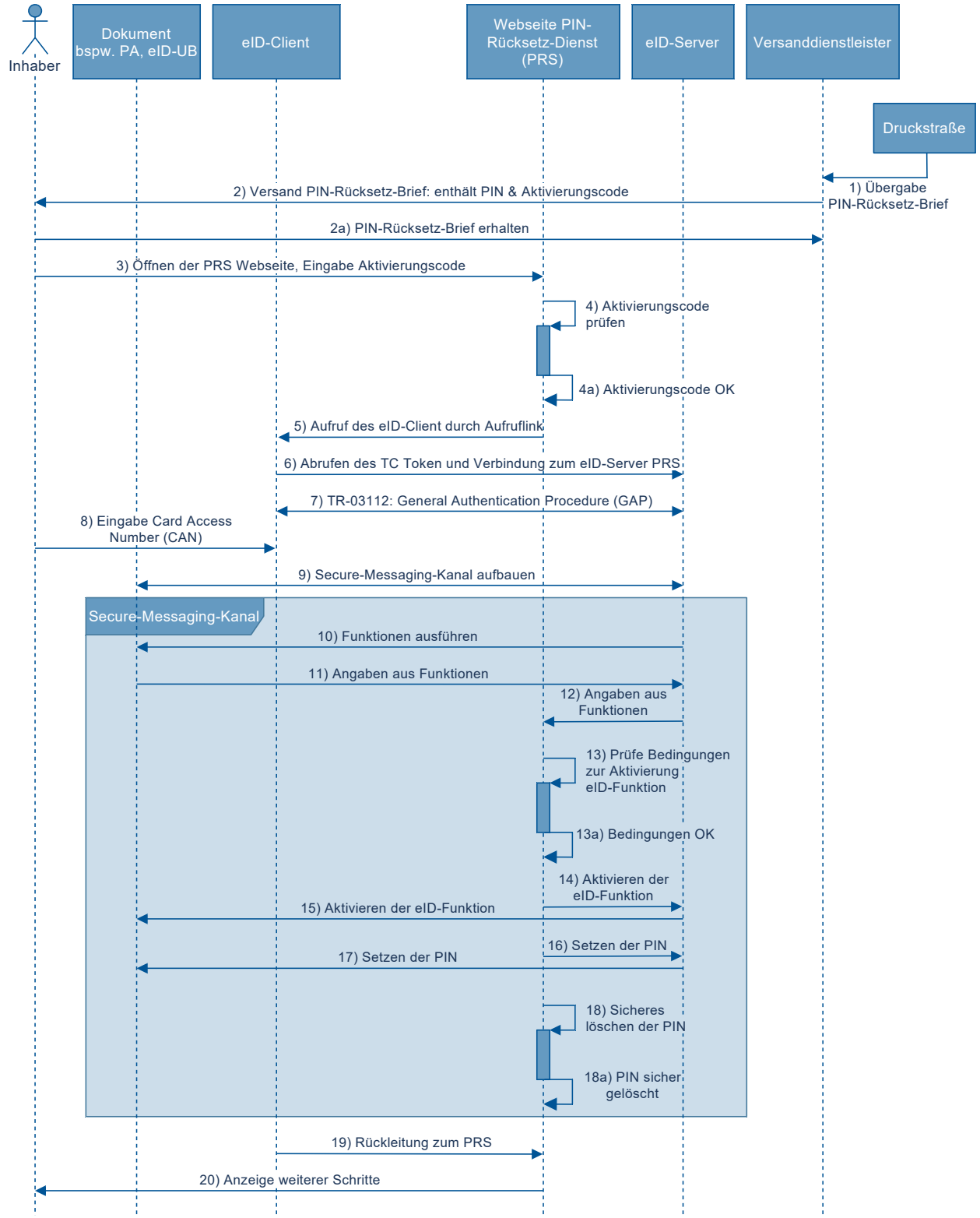

Abbildung 2: Ablaufdiagramm Empfang des PIN-Rücksetz-Briefs und Aktivierung der eID-Funktion via PIN-Rücksetz-Dienst.

3 Zentraler Schreibdienst

Nach einem Wohnsitzwechsel kann die erforderliche Anmeldung bei der zuständigen Meldebehörde gemäß §23a BMG [7] auch elektronisch erfolgen. In diesem Fall kann die notwendige Änderung der Anschrift auf dem Ausweisdokument ebenfalls auf elektronischem Wege erfolgen.

§18 PAuswG [4] führt aus:

> *(6) Personalausweisbehörden dürfen im Rahmen der Änderung der Anschrift auf dem elektronischen Speicher- und Verarbeitungsmedium nach einer elektronischen Anmeldung gemäß § 23a des Bundesmeldegesetzes einen elektronischen Identitätsnachweis durchführen und hierzu ein hoheitliches Berechtigungszertifikat verwenden.*

Die PAuswV [6] regelt die näheren Bedingungen für die elektronische Änderung der Anschrift in §19:

> *(2) Hat der Ausweisinhaber eine elektronische Anmeldung nach §23a des Bundesmeldegesetzes durchgeführt, hat er die Änderung der Anschrift auf dem elektronischen Speicher-und Verarbeitungsmedium einzuleiten. Hierzu wird durch die Personalausweisbehörde ein elektronisches Formular bereitgestellt. Der Ausweisinhaber weist seine Identität gegenüber der Personalausweisbehörde mit einem elektronischen Identitätsnachweis nach §18 Absatz2 Satz1 Nummer1 des Personalausweisgesetzes nach. Die zuständige Personalausweisbehörde ändert die Anschrift auf dem elektronischen Speicher-und Verarbeitungsmedium des Personalausweises und trägt diese in das Personalausweisregister ein. [...]*

Die Personalausweisbehörden können sich hierbei des *Zentralen Schreibdienstes* gemäß diesem Teil der vorliegenden Technischen Richtlinie bedienen. Die Komponente *Zentraler Schreibdienst (ZSD)* arbeitet hierbei mit dem *Onlinedienst elektronische Wohnsitzanmeldung (eWA)* zusammen, der den Gesamt-Workflow der elektronischen Anmeldung nach §23a BMG [7] orchestriert. Sowohl der *Onlinedienst eWA* als auch der *Zentrale Schreibdienst* sollen als EfA-Dienst (Einer für Alle) umgesetzt werden. Eine von einem Bundesland implementierte Leistung soll zentral betrieben und somit allen Ländern zur Verfügung stehen.

3.1 Rahmenbedingungen der Nutzung

Ausweisinhaber, die eine elektronische Anmeldung Ihres Wohnsitzes nach einem Umzug gemäß §23a BMG [7] durchgeführt haben, können im Anschluss mittels des Zentralen Schreibdienstes die auf Ihrem physikalischen Ausweisdokument gespeicherte Anschrift ändern lassen.

Sie benötigen dafür neben ihrem Ausweisdokument (Personalausweis, elektronischer Aufenthaltstitel, eID-Karte) und Ihrer PIN ein internetfähiges Gerät mit einem installierten eID-Client, z.B. die vom Bund bereitgestellte AusweisApp2[4] und einen geeigneten Kartenleser oder ein Smartphone mit NFC[5]-Schnittstelle.

Das Ausweisdokument muss gültig und darf nicht gesperrt sein. Eine elektronische Adressänderung auf Ausweisen von ebenfalls umgemeldeten Familienangehörigen kann nur durch die Ausweisinhaber selbst mit dem jeweiligen Ausweisdokument und der zugehörigen PIN erfolgen.

[4] https://www.ausweisapp.bund.de
[5] Near Field Communication (NFC); Funkschnittstelle

3.2 Ablauf

Die elektronische Änderung der Anschrift erfolgt im Anschluss an den elektronischen Ummeldevorgang, dessen Ablauf hier nicht weiter betrachtet wird. Der *Onlinedienst eWA* leitet die Änderung der Anschrift durch Übermitteln der Auftragsdaten an den Zentralen Schreibdienst ein.

1. Übermittlung der Auftragsdaten und Weiterleitung des Ausweisinhabers zum Zentralen Schreibdienst
2. Elektronischer Identitätsnachweis und anschließendes Schreiben der neuen Anschrift
3. Übermittlung der erfolgten Adressänderung und Weiterleitung des Ausweisinhabers zum Onlinedienst

Diese Schritte sind in den Abschnitten 3.2.1 bis 3.2.3 näher beschrieben sowie in Abschnitt 0 als Ablaufdiagramm aufbereitet.

3.2.1 Übermittlung der Auftragsdaten und Weiterleitung

Der *Onlinedienst eWA* übermittelt über eine durch den ZSD bereitgestellte Schnittstelle die Auftragsdaten für den Schreibvorgang. Um das Ausweisdokument dem Schreibauftrag zuordnen zu können, werden die personenbezogenen Daten des Ausweisinhabers benötigt, damit diese mit dem Ausweisdokument abgeglichen werden können (vgl. Abbildung 3, Schritte 1 & 2). Die Nutzung des DKK (Pseudonyms) für diese Zwecke ist aufgrund der verschiedenen Berechtigungszertifikate von *Onlinedienst eWA* und ZSD nicht möglich.

- Dokumententyp
- Name und Vorname, ggf. Geburtsname
- Geburtsdatum
- Geburtsort
- Alte Anschrift
- Neue Anschrift
- Neuer Gemeindeschlüssel

Beim Anlegen des Schreibauftrags erhält der *Onlinedienst eWA* vom ZSD einen Session-Identifier mitgeteilt. Anschließend leitet der *Onlinedienst eWA* den Browser des Nutzers über einen Redirect unter Angabe des Session-Identifiers an den ZSD weiter (vgl. Abbildung 3, Schritte 3 bis 5).

3.2.2 Identitätsnachweis und Schreiben der Anschrift

Der eService des ZSD prüft die Gültigkeit des Session-Identifiers und durch Nutzerinteraktion erfolgt der Aufruf des eID-Clients durch den Aufruflink (siehe TR-03124-1 [11]).

Der eID-Client ruft gemäß TR-03124-1 [11] das TCToken ab und verbindet sich mit dem eID-Server des ZSD.

eID-Server und eID-Client kommunizieren gemäß TR-03112 [12] und führen gemeinsam die *General Authentication Procedure* (GAP) als Authentisierungsterminal (siehe TR-03110-3 [13]) durch. Als Passwort kommt hierbei die eID-PIN zum Einsatz (vgl. Abbildung 3, Schritte 6 bis 10).

Über den im Ergebnis zur GAP etablierten Secure-Messaging-Kanal führt der eID-Server dann die folgenden Funktionen gemäß TR-03110-3 [13] durch (vgl. Abbildung 3, Schritte 11 & 12):

- Gültigkeitsprüfung
- Abfrage des Sperrmerkmals
- Auslesen von Dokumententyp, Vorname, Nachname, Geburtsname, Geburtsdatum, Geburtsort und Anschrift.

Für das Auslesen (Datenerhebung) sind insbesondere die „Grundsätze für die Verarbeitung personenbezogener Daten“ laut Artikel 5 der Datenschutz-Grundverordnung (DSGVO) [14] zu beachten. Es dürfen nur die Daten erhoben werden, welche im Prozess auch tatsächlich benötigt werden.

OHNE den Secure-Messaging-Kanal abzubauen prüft nun die Anwendungslogik des ZSD folgende Bedingungen (vgl. Abbildung 3, Schritt 13). eID-Server und Webserver des ZSD müssen deshalb eine interne Schnittstelle verwenden (siehe Abschnitt 4.1):

- Ausweis ist gültig und nicht gesperrt.
- Der Dokumententyp ist ID, AR, AS oder UB.
- Die Personendaten und Dokumententyp entsprechen dem zugehörigen Schreibauftrag.
- Die Anschrift entspricht der alten Anschrift.

Sind eine oder mehrere der Bedingungen nicht erfüllt, bricht der eID-Server den Vorgang durch schließen des Secure-Messaging-Kanals ab und behandelt dies intern als Fehler.

Sind die Bedingungen erfüllt, schreibt der eID-Server über den Secure-Messaging-Kanal die neue Anschrift und den neuen Gemeindeschlüssel in das Dokument und liest beides im Anschluss zur Kontrolle erneut aus (vgl. Abbildung 3, Schritte 14 bis 17).

Anschließend wird der Secure-Messaging-Kanal geschlossen und bei erfolgreich geschriebener Anschrift ist der Schreibvorgang erfolgreich abgeschlossen, ansonsten erfolgt auch hier intern eine Fehlerbehandlung.

3.2.3 Übermittlung der Ergebnismeldung und Weiterleitung

Der eID-Server signalisiert dem ZSD den erfolgreichen Abschluss des Vorgangs bzw. einen der beschriebenen Fehlerfälle, sodass der zum Vorgang gehörige Status entsprechend gesetzt und ab dann durch den *Onlinedienst eWA* über die Statusschnittstelle (vgl. Abschnitt 4.1.5) abgerufen werden kann (vgl. Abbildung 3, Schritt 18 & 19).

Der eID-Client leitet den Ausweisinhaber anschließend über die Rücksprungadresse zurück zum Webserver des ZSD (vgl. Abbildung 3, Schritt 20).

Im Fehlerfall ist der Ausweisinhaber dort über den Grund des Fehlschlags zu informieren. Bei mutmaßlich temporärer Ursache für den Fehlschlag, soll dem Ausweisinhaber die Möglichkeit gegeben werden, den Schreibvorgang direkt erneut zu versuchen, ohne den gesamten Antrag erneut zu starten.

Im Positivfall wird der Browser des Ausweisinhabers automatisch über die dem ZSD bekannte oder bei Anlegen des Schreibauftrages übermittelte Rücksprungadresse zurück zum *Onlinedienst eWA* geleitet (vgl. Abbildung 3, Schritt 22). Dort wird dem Ausweisinhaber das Ergebnis des Vorgangs und die weiteren Schritte angezeigt. Auch wenn hierbei der Status des Schreibvorgangs übermittelt werden kann, sollte der Status explizit durch Aufrufen der Statusschnittstelle ermittelt werden. Insbesondere kann der Schreibvorgang erfolgreich abgeschlossen sein, auch wenn der finale Redirect des Nutzers zum *Onlinedienst eWA* fehlschlägt oder abgebrochen wurde.

3.3 Ablaufdiagramm

In Abbildung 3 sind die Schritte aus den Abschnitten 3.2.1 bis 3.2.3 als Ablaufdiagramm dargestellt.

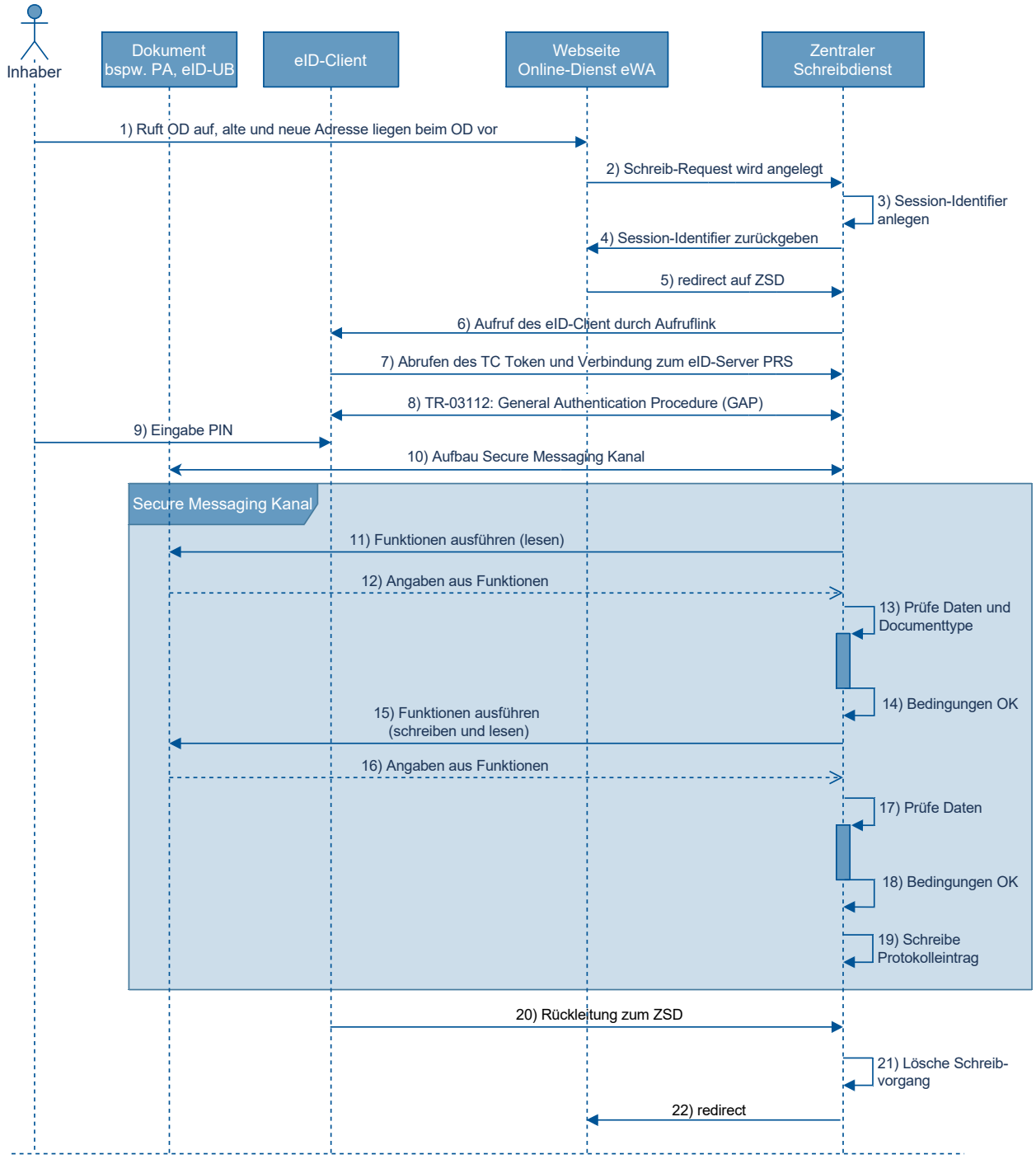

Abbildung 3: Ablaufdiagramm zum Ändern der Anschrift auf dem Ausweisdokument.

4 Funktionale Anforderungen

Dieser Abschnitt formuliert funktionale Anforderungen für Änderungsdienste mit hoheitlicher Berechtigung. Im Folgenden bezeichnet „Dienst“ den PIN-Rücksetz-Dienst (PRS) bzw. den Zentralen Schreibdienst (ZSD) und „Diensteanbieter“ den Ausweishersteller (für den PIN-Rücksetz-Dienst) respektive den Betreiber des Zentralen Schreibdienstes. Unterscheiden sich Anforderungen für die verschiedenen Änderungsdienste sind diese jeweils gekennzeichnet.

4.1 Technische Umsetzung

Die technische Integration des Dienstes erfolgt auf Seiten des Ausweisinhabers durch einen Webbrowser und einen eID-Client (siehe TR-03124-1 [11]), auf Seiten des Diensteanbieters durch einen eID-Server (siehe TR-03130-1 [15]) und einen Webdienst / eService.

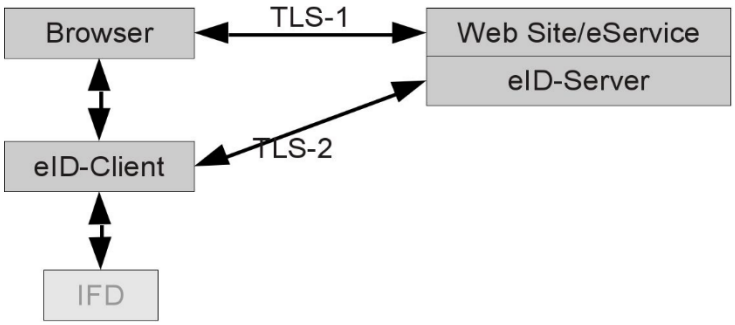

Abbildung 4: Attached eID-Server

4.1.1 Serverseitige Integration

Die serverseitige Integration kann als „Attached eID-Server“ umgesetzt werden (vgl. Abbildung 4). Bei einer abweichenden Umsetzung sind bereits formulierte Anforderungen einzuhalten.

4.1.1.1 eID-Server

Der eID-Server kapselt die Kommunikation mit dem eID-Client / dem Ausweis und der Hintergrundinfrastruktur (Berechtigungs-PKI). Die Realisierung der Website des Dienstes (eService) kann in direkter Verbindung mit dem eID-Server („Attached eID-Server“ gemäß TR-03130-1 [15]) erfolgen.

Die Kommunikation zwischen eID-Client und eID-Server ist in TR-03124 [11] standardisiert. Um die Interoperabilität sicherzustellen, wird der Einsatz von konformitätszertifizierten eID-Clients / eID-Servern (vgl. TR-03124, Teil 2 [16] und TR-03130, Teil 4 [9]) empfohlen.

Für den hoheitlichen Dienst darf auf einem mandantenfähigen eID-Server nur der PRS- bzw. SD-Mandant konfiguriert sein. Weitere Mandanten mit nicht-hoheitlichem Berechtigungszertifikat sind nicht zulässig. Ebenso ist es nicht erlaubt, diesen hoheitlichen Dienst als eID-Service Dritten zur Verfügung zu stellen.

Der eID-Server muss für diesen hoheitlichen Dienst qualitativ hochwertige TLS Zertifikate (Extended-Validation-SSL-Zertifikate, Qualifizierte Zertifikate für die Website-Authentifizierung - QWAC) verwenden.

4.1.1.2 Schlüssel und PKI-Anbindung

Voraussetzung für die Nutzung des Dienstes ist ein hoheitliches Berechtigungszertifikat, das von einer hoheitlichen Document Verifier (hDV) CA bezogen werden kann. Die Zertifikate müssen täglich (automatisiert) erneuert werden, ebenso müssen die von den hDV-CAs bezogenen Sperrlisten regelmäßig aktualisiert werden.

Die zu den Berechtigungszertifikaten gehörenden Schlüssel werden im eID-Server gespeichert. Für die Nutzung von hoheitlichen Zertifikaten ist die Nutzung sicherer Hardware für die Schlüsselspeicherung vorgegeben (Sicherheitslevel 2 nach Key Lifecycle [17]).

Die Kommunikation mit der Hintergrundinfrastruktur zum regelmäßigen Erneuern der Berechtigungszertifikate und der Ausweissperrlisten erfolgt automatisiert durch den eID-Server. Der Betreiber muss sicherstellen, dass die Kommunikation mit dem hDV möglich ist.

Für Details zu diesem Abschnitt siehe [8].

4.1.1.3 Webseite / Applicationserver (eService)

Die Benutzerführung des Dienstes wird über eine Webseite, die der eService bereitstellt, gestartet (vgl. Abbildung 4, TLS-1). Diese Webseite enthält die entsprechenden Links zum eID-Client (siehe TR-03124-1 Kap 2.2 [11]). Über TLS-2 (vgl. Abbildung 4) nimmt der eID-Client zuerst Verbindung zum eService und dann zum eID-Server auf.

[PRS]

Nach erfolgreicher Antragstellung übermittelt der eID-Server die Daten für den PIN-Rücksetz-Brief an den eService. Der eService initiiert den Druck des PIN-Rücksetz-Briefs.

Dem Ausweisinhaber werden die erfolgreiche Änderung und die weiteren Schritte im Browser angezeigt. Sollte es zu Fehlern kommen, erhält der Ausweisinhaber entsprechende Informationen.

Der eService persistiert für die Weiterbearbeitung benötigte Daten, mindestens:

- Datum der Antragstellung
- Pseudonym (DKK)
- Aktivierungscode

Es sind die gesetzlichen Löschfristen (siehe Abschnitt 5.6) einzuhalten. Der Aktivierungscode soll zur Vermeidung von Kollisionen (siehe Abschnitt 4.1.4) für die doppelte Zeit seiner Gültigkeitsdauer gespeichert bleiben.

[ZSD]

Nach Durchführung des Schreibvorgangs und Rückleitung des Ausweisinhabers in den Browser zeigt der eService das Ergebnis des Vorgangs an bzw. leitet den Ausweisinhaber zurück auf die Webseite des *Onlinedienstes eWA.*

[Alle]

Der eService nutzt im Falle der „Attached eID-Server“ Architektur das TLS Zertifikat des eID-Servers („same domain“, siehe TR-03124-1 Kap 2.1 [11]).

4.1.2 Clientseitige Integration

Der Dienst muss als webbasierter Dienst (d.h. der Dienst wird über eine Webseite zur Verfügung gestellt) realisiert werden. Der Dienst muss dabei die Anforderungen aus der TR-03128-1 [1] an die Webseiten-basierte Integration erfüllen. Ein App-basierter Dienst (d.h. für den Dienst wird eine dedizierte App genutzt) ist optional. Details siehe TR-03128-1 Kap. 2.4.2.1 [1].

4.1.3 [PRS] Sichere Erzeugung und Speicherung der PIN

Die Erzeugung der neuen PIN erfolgt durch geeignete Hardware (Zufallswert, wie bei Transport-PIN oder CAN), sie wird Ende-zu-Ende verschlüsselt abgespeichert und transportiert und nur unmittelbar vor dem Beschreiben bzw. Drucken entschlüsselt.

4.1.4 [PRS] Aktivierungscode

Der Aktivierungscode ist ein zufälliger Wert (nicht erratbar, kein direkter Bezug zu Personen- oder Vorgangsdaten), der dem Ausweisinhaber im PIN-Rücksetz-Brief zugesendet wird. Da er vom Ausweisinhaber manuell in ein Online-Formular übertragen werden soll, ist hier ein Kompromiss zwischen Qualität und Handhabbarkeit zu finden. Es muss dabei eine Entropie von mindestens 40 Bit gewährleistet sein. Leicht verwechselbare Zeichen ("1 wie eins" und "I wie Ida") sind zu vermeiden. Auch bei einer hohen Entropie, muss der eService sicherstellen, dass kein bereits im System gespeicherter Aktivierungscode vergeben wird.

Der Aktivierungscode kann vom Ausweisinhaber sofort nach der Zustellung genutzt werden.

4.1.5 [ZSD] Schnittstelle für den Schreibauftrag

Der ZSD stellt eine bzw. zwei Schnittstellen bereit, über die die Auftragsdaten übermittelt werden können und der Status eines Auftrags abgefragt werden kann.

Diese Schnittstellen dürfen nur durch authentisierte Aufrufer (*Onlinedienstes eWA*) genutzt werden können. Bei einer Anbindung mehrerer Onlinedienste ist sicherzustellen, dass nur jeweils zugehörige Aufträge eingesehen werden können.

Darüber hinaus müssen die im Schreibauftrag enthaltenden Inhaltsdaten verschlüsselt und signiert übertragen werden und die Signatur durch den ZSD geprüft werden.

4.2 Nutzerführung

Die Nutzerführung auf der Webseite bzw. in der Anwendungsapp obliegt dem Diensteanbieter. Es sind die im Folgenden dargestellten Punkte zu beachten.

4.2.1 eID-Client

Der webbasierte Dienst erfordert eine vorhandene, funktionsfähige Installation eines geeigneten eID-Clients. Es wird empfohlen auch auf der Webseite, des Dienstes den Ausweisinhaber auf Downloadmöglichkeiten für eID-Clients hinzuweisen (siehe TR-03128-1 Kap 2.6.1 [1]).

4.2.2 Webseitenempfehlungen

Das BSI empfiehlt, die Diensteanbieter-Webseite so zu gestalten, dass sie von einem Ausweisinhaber, der sich an die Sicherheitsempfehlungen des BSI hält, ohne Einschränkungen nutzbar ist. Die Empfehlungen finden sich auf der Webseite https://www.bsi.bund.de/BSIFB bzw. https://www.ausweisapp.bund.de und umfassen insbesondere:

- Verwendung eines aktuellen Virenschutzes und Firewall.
- Vermeidung aktiver Inhalte.
- Einsatz geeigneter Komponenten (Smartcard-Lesegerät / Smartphone mit NFC-Schnittstelle als Kartenleser, eID-Client) für die Ausweisnutzung.

Die Nutzung von aktiven Inhalten oder Cookies auf der Webseite sollte auf die fachlich Notwendigen beschränkt werden. Sofern aktive Inhalte zum Einsatz kommen, sollen ausschließlich verbreitete aktive Webtechniken verwendet werden, deren Unterstützung bereits in modernen Browsern in Verbindung mit geeigneten Sicherheitsmaßnahmen integriert ist.

Es soll dabei beachtet werden, dass die Ausführung von aktiven Inhalten u.a. durch den Ausweisinhaber blockiert werden kann. Die Nutzung des Dienstes sollte daher auch ohne die Verwendung aktiver Inhalte auf Seiten des Ausweisinhabers ermöglicht werden.

Da bei einem hoheitlichen ÄnderungsdienstSchreibvorgänge auf dem Ausweis stattfinden, ist es besonders wichtig, den Ausweisinhaber über das Risiko aufzuklären, wenn die Verbindung (insbesondere stabile Netzwerkverbindungen und sicherer Kontakt Ausweis Kartenleser bzw. Smartphone mit NFC-Schnittstelle), während des Schreibvorgangs unterbrochen wird.

4.2.3 Fehlerbehandlung

[PRS]

Wurde der Antrag zuvor erfolgreich mit Produktion eines PIN-Rücksetz-Briefs abgeschlossen und der Ausweisinhaber versucht es innerhalb von 7 Tagen erneut, erhält er die Information, dass sein Antrag in Arbeit ist und er den Aktivierungscode, den er via PIN-Rücksetz-Brief erhält, eingeben kann. Er erhält auch die Information, ab welchem Datum eine Antragswiederholung möglich ist. Der eService erkennt den erneuten Versuch für den gleichen Ausweis anhand des Pseudonyms (DKK). Ist dieser identisch mit dem Wert, der beim ersten Antrag gespeichert wurde, handelt es sich um einen Wiederholungsversuch. Wurde ein vorheriger Antrag unterbrochen, kann der Ausweisinhaber den Vorgang wiederholen ohne dass ein neuer Antrag gestellt wird. Der PRS soll vorherige Fehler erkennen und den Ausweisinhaber ohne weitere Interaktion eine Wiederholung/Fortsetzung des Vorgangs ermöglichen.

Der Ausweisinhaber kann nach Ablauf von 7 Tagen einen weiteren Antrag stellen. Dadurch storniert er automatisch den vorhergehenden Antrag und der zugehörige Aktivierungscode wird invalidiert. Er muss darüber informiert werden, dass der PIN-Rücksetz-Brief der vorherigen Antragstellung ungültig wird. Der PIN-Rücksetz-Brief soll deshalb auch das Datum der Antragstellung enthalten, damit der Ausweisinhaber diesen eindeutig zuordnen kann.

Mit geeigneten Maßnahmen (Fristen, Anzahl möglicher Wiederholungen, siehe Abschnitt 2.1) ist sicherzustellen, dass kein Missbrauch erfolgt und damit keine größere Anzahl PIN-Rücksetz-Briefe an denselben Ausweisinhaber gesendet wird.

In folgenden Fehlerfällen ist dem Ausweisinhaber anzuzeigen, dass er mit seinem Ausweis den PRS nicht nutzen kann, sondern sich möglicherweise an seine zuständige Ausweisbehörde wenden muss oder die eID-Funktion nicht aktiviert werden kann:

- Ausweis ist gesperrt.
- Ausweis ist abgelaufen.
- Beim verwendeten Ausweis handelt sich um einen Aufenthaltstitel (eAT).
- Der Besitzer des Ausweises hat das 16. Lebensjahr noch nicht vollendet.
- Es gibt keine Meldeadresse im Inland.

In diesen Fällen wird weder auf dem Ausweis noch im eService etwas gespeichert.

[ZSD]

Bei Übergabe des Nutzers an den eService des ZSD prüft dieser zunächst die Existenz und Gültigkeit des referenzierten Schreibauftrags.

Schlägt das Schreiben der Adresse auf den Ausweis fehl, ist der Nutzer entsprechend der Ursache zu informieren. Nach einem Abbruch durch den Benutzer, Serverfehler oder Verbindungsabbruch soll der Schreibvorgang direkt erneut gestartet werden können. Mögliche Fehlersituationen, die eine Wiederholung des Vorgangs hingegen ausschließen umfassen:

- Ausweis ist gesperrt.
- Ausweis ist abgelaufen.
- Personendaten/Dokumententyp passen nicht zum Schreibauftrag (falscher Ausweis).
- Anschrift wurde bereits geändert.

Wird für den Vorgang keine Wiederholung angeboten, erfolgt die Rückleitung des Benutzers zum *Onlinedienst eWA* an die bekannte oder übermittelte Rücksprungadresse. Über die Statusschnittstelle (vgl. Abschnitt 4.1.5) kann zudem der Fehlerstatus abgerufen werden.

[Alle]

Die Webseite erhält über die Rücksprungadresse (Refresh URL) die Möglichkeit dem Ausweisinhaber Informationen anzuzeigen, die der eID-Client generiert (siehe TR-03124-1 [11]):

- `ResultMajor=ok`: es ist kein Fehler aufgetreten, der Ausweisinhaber wird über weitere Schritte informiert. Wird die Erfolgsseite nicht mehr angezeigt (z.B. Netzwerkproblem) ist der Antrag trotzdem erfolgreich.
  [PRS] Der Antrag wird abgespeichert und der PIN-Rücksetz-Brief wird gedruckt.
  [ZSD] Die Anschrift wurde geändert und der *Onlinedienst eWA* kann die Erfolgsmeldung über die Statusschnittstelle abrufen.
- `ResultMajor=error&ResultMinor=res_min`: es ist ein Fehler aufgetreten; die folgenden Fehlercodes für `res_min` sind definiert:
  - `trustedChannelEstablishmentFailed`: Der eID-Client konnte keinen sichern Kanal zum eID-Server aufbauen (der Ausweisinhaber kann es später noch einmal versuchen oder den Support kontaktieren).
  - `cancellationByUser`: Der Ausweisinhaber hat die Bearbeitung abgebrochen (z. B. weil er den Ausweis nicht griffbereit hatte oder weil er nach einer falschen PIN Eingabe nicht fortfahren wollte). Der Ausweisinhaber kann es später noch einmal versuchen.
  - `serverError`: Der eID-Server meldet ein Problem. Der Ausweisinhaber kann es später noch einmal versuchen oder den Support kontaktieren.
  - `clientError`: Jeder andere Fehler. Der Ausweisinhaber kann es später noch einmal versuchen oder den Support kontaktieren.

Wird keine Refresh URL bereitgestellt, wird eine Fehlerseite angezeigt, es sind folgende Optionen möglich:

- Im TCToken gibt es eine „`CommunicationErrorAddress`“: Diese Seite wird aufgerufen mit den URL-Parametern `ResultMajor=error&ResultMinor=communicationError`;
- Es gibt keine „`CommunicationErrorAddress`“: Der eID-Client übermittelt den Fehler „`Bad Request`“.

4.2.4 Barrierefreiheit

Der webbasierte Dienst ist im Einklang mit den Bestimmungen des Behindertengleichstellungsgesetzes des Bundes (BGG) [18] sowie der Barrierefreien-Informationstechnik-Verordnung (BITV 2.0) [19] zur Umsetzung der Richtlinie (EU) 2016/2102 [20] barrierefrei zugänglich zu machen.

Ausnahmen, z.B. durch Verlinkung auf externe Seiten, sind kenntlich zu machen und zu dokumentieren.

5 Anforderungen an den sicheren Betrieb

Dieser Abschnitt formuliert Anforderungen an den sicheren Betreib für Änderungsdienste mit hoheitlicher Berechtigung. Im Folgenden bezeichnet „Diensteanbieter“ den Ausweishersteller (für den PIN-Rücksetz-Dienst) respektive den Betreiber des Zentralen Schreibdienstes. Unterscheiden sich Anforderungen für die verschiedenen hoheitlichen Änderungsdienste sind diese jeweils gekennzeichnet.

5.1 Sicherheitskonzept

Für die Prozesse und Komponenten des hoheitlichen Änderungsdienstes muss ein Sicherheitskonzept erstellt werden.

Das Sicherheitskonzept soll regelmäßige Penetrations-Tests des Application-Servers sowie des eID-Servers vorsehen. Dafür sollen die Auditzyklen der Zertifizierung (siehe Abschnitt 5.2) als wiederkehrende Ausführungszeitpunkte vorgesehen werden.

5.2 Informationssicherheitsmanagementsystem

Das Sicherheitskonzept muss Bestandteil eines zertifizierten Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001 [21] oder ISO 27001 auf Basis IT-Grundschutz [22] sein. Das ISMS muss alle am Betrieb der eID-Infrastruktur beteiligten Organisationseinheiten umfassen.

Im Sicherheitskonzept muss ein Rollenkonzept definiert werden. Es soll eine Rolle spezifiziert werden, welche Zugriff auf Schlüsselmaterial erhält. Bei Bedarf können weitere Rollen entsprechend ISO 27001 [21] definiert werden. Bei der Besetzung von Rollen mit Personen muss beachtet werden, dass Rollen mit Interessenskonflikten nicht von derselben Person eingenommen werden dürfen. Das Rollenkonzept soll für kritische Prozesse zusätzlich ein Vier-Augen-Prinzip definieren.

5.3 eID-Server Betrieb

Das Sicherheitskonzept muss insbesondere die Maßnahmen zum sicheren Betrieb des eID-Servers beschreiben. Die Mindestanforderungen, die durch dieses Sicherheitskonzept im Einzelnen abgedeckt werden müssen, sind in TR-03130-2 [23] beschrieben. Ferner sind die nach der Certificate Policy der Country Verifying Certification Authority (CP CVCA-eID) [8] geforderten Sicherheitsmaßnahmen im Sicherheitskonzept zu berücksichtigen.

5.4 Ausgelagerter Betrieb

[PRS]

Der ausgelagerte Betrieb hoheitlicher Funktionalitäten außerhalb des Sicherheitsbereichs des Ausweisherstellers ist nicht zulässig. Zu den hoheitlichen Funktionalitäten zählen insbesondere die Erzeugung der neuen PIN (siehe Abschnitt 2.2.2), die Erstellung des PIN-Rücksetz-Briefs (siehe Abschnitt 2.2.3) und der operative Betrieb des eID-Servers mit hoheitlichem Berechtigungszertifikat.

Ein ausgelagerter Betrieb beschränkt sich auf nicht-hoheitliche Funktionalitäten, wie bspw. der Versand des PIN-Rücksetz-Brief durch ein sicheres Zustellverfahren (siehe Abschnitt 2.2.3).

[ZSD]

Die Auslagerung des operativen Betriebs des ZSD mit daran angeschlossenem eID-Servers mit hoheitlichem Berechtigungszertifikat ist nur in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik zulässig.

[Alle]

Werden nicht-hoheitliche Komponenten des hoheitlichen Änderungsdienstes für den operativen Betrieb an Dritte ausgelagert, so bleibt der Anbieter des hoheitlichen Änderungsdienstes für die Einhaltung aller IT-Sicherheitsvorschriften und datenschutzrechtlicher Vorgaben verantwortlich. Der Dritte, an den der Betrieb ausgelagert wurde, muss über ein zertifiziertes ISMS nach ISO 27001 [21] oder nach ISO 27001 auf Basis von IT-Grundschutz [22] verfügen.

5.5 Vertraulichkeit und Integrität der Kommunikationsschnittstellen

Werden personenbezogene Daten über öffentliche Netzwerke übermittelt, so müssen die Anforderungen gemäß TR-03116-4 [24] umgesetzt werden.

5.6 Einhaltung gesetzlicher Anforderungen

Der Diensteanbieter muss die einschlägigen rechtlichen Anforderungen, insbesondere PAuswG [4] / PAuswV [6] und BDSG [25] / DSGVO [14], einhalten.

Für die Datenerhebung sind insbesondere die „Grundsätze für die Verarbeitung personenbezogener Daten“ laut Artikel 5 der Datenschutz-Grundverordnung (DSGVO) zu beachten.

[PRS]

Zur Löschung von personenbezogenen Daten ist insbesondere die PAuswV §5, Absatz (5) zu beachten:

> *Der Ausweishersteller löscht die zur Bearbeitung von elektronischen Anträgen nach § 20 Absatz 2 und § 22 Absatz 2 zu erhebenden personenbezogenen Daten, sobald er die Benachrichtigung bekommen hat, dass der Antragsteller die zufällig neu generierte Geheimnummer erhalten hat, spätestens aber nach 30 Tagen. Satz 1 gilt nicht für das dienste- und kartenspezifische Kennzeichen[6], welches spätestens nach 90 Tagen zu löschen ist.*

Des Weiteren verwendet der Ausweishersteller laut PAuswV §20 und §22 für das Ändern der Daten nach Absatz 2 Satz 2 sowie für das Einschalten nach Absatz 2 Satz 5 ein hoheitliches Berechtigungszertifikat.

[ZSD]

Der Betreiber des ZSD muss die Auftragsdaten unmittelbar nach der erfolgreichen Änderung der Anschrift jedoch spätestens nach 30 Tagen (z.B. bei Abbruch des Vorgangs) löschen.

Die Personalausweisbehörde bzw. der von dieser beauftragte Betreiber des ZSD verwendet laut PAuswV §19 Absatz 3 für den elektronischen Identitätsnachweis und die Änderung der Anschrift ein hoheitliches Berechtigungszertifikat.

[6] dienste- und kartenspezifische Kennzeichen (DKK) gleichbedeutend zu Pseudonym.

Literaturverzeichnis

[1] BSI, „Technische Richtlinie TR-03128-1, Diensteanbieter für die eID-Funktion Teil 1: Elektronischer Identitätsnachweis und Vor-Ort-Auslesen“.

[2] BSI, „Technische Richtlinie TR-03131, EAC-Box Architektur und Schnittstellen“.

[3] BSI, „Technische Richtlinie TR-03127, eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control“.

[4] „Personalausweisgesetz vom 18. Juni 2009 (BGBl. I S. 1346), das zuletzt durch Artikel 2 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2281) geändert worden ist,“ 2021.

[5] „eID-Karte-Gesetz vom 21. Juni 2019 (BGBl. I S. 846), das zuletzt durch Artikel 3 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2281) geändert worden ist,“ 2021.

[6] „Personalausweisverordnung vom 1. November 2010 (BGBl. I S. 1460), die zuletzt durch Artikel 3 der Verordnung vom 20. August 2021 (BGBl. I S. 3682) geändert worden ist,“ 2021.

[7] „Bundesmeldegesetz vom 3. Mai 2013 (BGBl. I S. 1084), das zuletzt durch Artikel 4 des Gesetzes vom 28. März 2021 (BGBl. I S. 591) geändert worden ist,“ 2021.

[8] BSI, „Certificate Policy für die Country Verifying Certification Authority eID-Anwendung, Elektronischer Identitätsnachweis und Vor-Ort-Auslesen mit hoheitlichen Ausweisdokumenten“.

[9] BSI, „Technical Guideline TR-03110-4, Advanced Security Mechanisms for Machine Readable Travel Documents; Part 4“.

[10] BSI, „Technical Guideline TR-03129, PKIs for Machine Readable Travel Documents-Protocols for the Management of Certificates and CRLs“.

[11] BSI, „Technical Guideline TR-03124-1 eID-Client, Part 1: Specifications“.

[12] BSI, „Technical Guidelinie TR-03112, eCard-API-Framework“.

[13] BSI, „Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token, Part 3: Common Specifications“.

[14] Europäische Kommission, „DSG-VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung),“ 27 April 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679.

[15] BSI, „Technical Guideline TR-03130-1 eID-Server, Part 1: Functional Specification“.

[16] BSI, „Technical Guideline TR-03124-2 eID-Client, Part2: Conformance Test Specifications“.

[17] BSI, „Key Lifecycle Security Requirements“.

[18] „Behindertengleichstellungsgesetz vom 27. April 2002 (BGBl. I S. 1467, 1468), das zuletzt durch Artikel 9 des Gesetzes vom 2. Juni 2021 (BGBl. I S. 1387) geändert worden ist“.

[19] „Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0)“.

[20] E. Kommission, „RICHTLINIE (EU) 2016/2102 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen," 26 Oktober 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L2102.

[21] ISO / IEC, „ISO / IEC 27001: Information technology - Security techniques - Information security management systems - Requirements".

[22] BSI, „BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise".

[23] BSI, „Technical Guideline TR-03130-2 eID-Server, Part 2: Security Framework for eID-Server operations".

[24] BSI, „Technische Richtlinie TR-03116-4, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen".

[25] „Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist".