Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie TR-03170

Sichere digitale Übermittlung biometrischer Lichtbilder von Dienstleistern (z. B. Fotografinnen und Fotografen) an Pass-, Personalausweis- und Ausländerbehörden

Version 0.95

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
0.1	20.04.2021	BSI	Erster Grobentwurf
0.2	26.08.2021	BSI	Weiterentwicklung
0.3	03.12.2021	BSI	Weiterentwicklung
0.4	24.01.2022	BSI	Umstellung Kapitel und Weiterentwicklung
0.5	21.02.2022	BSI	Fassung Interne Kommentierung
0.6	14.03.2022	BSI	Fertigstellung Entwurfsfassung V 0.6 für externe Kommentierung
0.7	30.06.2022	BSI	Einarbeitung der Kommentierungen aus der 1. Kommentierungsrunde
0.85	18.04.2023	BSI	Anpassung gemäß Entwurfsfassung der RVO
0.9	25.07.2023	BSI	Ergänzung der Themen zu Registrierung und Nachvollziehbarkeit, sowie kleinere Anpassungen
0.95	09.08.2023	BSI	Überarbeitung einiger Anforderungen mit Hinblick auf die Zertifizierung

Tabelle 1: Änderungshistorie

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

Inhalt

1 Einleitung

1.1 Zielsetzung der Technischen Richtlinie

Am 11. Dezember 2020 wurde das vom Deutschen Bundestag und Bundesrat verabschiedete **Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen**[1] im Bundesgesetzblatt veröffentlicht. Ziel des Gesetzes ist es, angemessene Sicherheitsmaßnahmen festzulegen, um eine sichere Übertragung elektronischer Lichtbilder an Pass-, Personalausweis- und Ausländerbehörden sicherzustellen.

Gefährdungslage durch Morphing

Morphing bezeichnet eine Technik, mit der Lichtbilder (i. Allg. für Pass-, Personalausweis- und ausländerrechtliche Ausweisdokumente) elektronisch manipuliert werden können, indem mehrere Gesichtsbilder zu einem einzigen Bild digital verschmolzen werden und somit die Gesichtszüge von verschiedenen Personen in einem Lichtbild erscheinen.

Durch Morphing-Manipulation ist der Pass bzw. Personalausweis als Instrument zur Identitätskontrolle im Kern bedroht, sodass die bisherige Praxis, nach der antragstellende Personen ausgedruckte Lichtbilder bei der Pass-, Personalausweis- oder Ausländerbehörde einreichen, nicht mehr den aktuellen Sicherheitsanforderungen entspricht.

Stärkung der Sicherheit durch Verfahren zur digitalen Übermittlung der Lichtbilder

Das Gesetz sieht vor, dass künftig Manipulationen von hoheitlichen Dokumenten durch Morphing gezielt begegnet werden soll, indem ab dem 1. Mai 2025 das Lichtbild ausschließlich digital erstellt und auf einem gesicherten elektronischen Weg zur Behörde übermittelt wird. Eine Möglichkeit zur Umsetzung besteht darin, nach der **Technischen Richtlinie [BSI TR-03121] – Biometrie in hoheitlichen Anwendungen**[2] die Lichtbilder durch einen Live-Enrolment Prozess zu erstellen und zu übertragen.

Ein Verfahren zur elektronischen Bildübermittlung wurde bereits in der **Technischen Richtlinie [BSI TR-03146] – Elektronische Bildübermittlung zur Beantragung hoheitlicher Dokumente**[3] beschrieben. Diese Technische Richtlinie erlaubt es Dienstleistern (z. B. Fotostudios), digital aufgenommene Lichtbilder zum Zwecke der Beantragung eines Passes oder Personalausweises via De-Mail an die Pass-, Personalausweis- oder Ausländerbehörde zu senden, bei welcher das Dokument beantragt wird. Nach vorliegender Rechtsverordnung wird dieses Verfahren ab dem 01. Mai 2025 nicht mehr genutzt werden können.

Gegenstand der Technischen Richtlinie

Die vorliegende **Technische Richtlinie [BSI TR-03170]** regelt die digitale Übermittlung biometrischer Lichtbilder von Dienstleistern (z. B. Fotografinnen und Fotografen) an Pass-, Personalausweis- oder Ausländerbehörden über einen sicheren Cloud-Dienst und definiert Anforderungen für die Zertifizierung von Diensten für dieses spezielle Verfahren. Allen zuständigen Behörden wird hierbei der Abruf der Lichtbilder von so zertifizierten Dienstanbietern ermöglicht.

1.2 Voraussetzungen der Technischen Richtlinie

Die Technische Richtlinie repräsentiert den Stand der Technik und wird fortlaufend aktualisiert.

---

1 https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl120s2744.pdf%27]

2 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03121/TR-03121_node.html

3 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03146/TR-03146_node.html

1.2.1 Schlüsselwörter

In der Technischen Richtlinie werden Anforderungen als Ausdruck normativer Festlegungen durch die in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS/MÜSSEN, DARF NICHT/DÜRFEN NICHT, SOLLTE/SOLLTEN entsprechend gekennzeichnet.

In den Anforderungen werden die in Versalien geschriebenen Modalverben „SOLLTE“ und „MUSS“ in ihren jeweiligen Formen sowie den zugehörigen Verneinungen genutzt, um deutlich zu machen, wie die jeweiligen Anforderungen zu interpretieren sind. Die hier genutzte Definition basiert auf (BSI IT-Grundschutz, 2022) und verstehen sich, wie folgt:.

MUSS/DARF NUR:	Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss (uneingeschränkte Anforderung).
DARF NICHT/DARF KEIN:	Dieser Ausdruck bedeutet, dass etwas in keinem Fall getan werden darf (uneingeschränktes Verbot).
SOLLTE:	Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.
SOLLTE NICHT/SOLLTE KEIN:	Dieser Ausdruck bedeutet, dass etwas normalerweise nicht getan werden sollte, es aber Gründe gibt, dies doch zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.
KANN	Dieser Ausdruck bedeutet, dass eine bestimmte Umsetzung gewählt werden kann. Diese muss allerdings angezeigt werden.

2 Rahmenbedingungen

2.1 Rechtliche Rahmenbedingungen

2.1.1 Pass- und Personalausweisgesetz

Rechtliche Grundlagen für die vorliegende Technische Richtlinie sind das **Passgesetz (PassG), Personalausweisgesetz (PAuswG), das Aufenthaltsgesetz (AufenthG)** sowie die **Aufenthaltsverordnung (AufenthV)** in der jeweiligen Fassung, die ab dem 1. Mai 2025 gültig sein wird. Die entsprechenden Änderungen wurden durch das Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen eingeführt. Ferner sehen die Gesetze Verordnungsermächtigungen für das Bundesministerium des Innern und für Heimat (BMI) vor, welche durch das Gesetz zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens im PassG ergänzt wird. Das Gesetz zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentwesens, sowie die u. a. auf den genannten Verordnungsermächtigungen basierende Verordnung zur Änderung der Personalausweisverordnung, der Passverordnung, der Aufenthaltsverordnung sowie weiterer Vorschriften, werden voraussichtlich im Oktober 2023 im Bundesgesetzblatt veröffentlicht.

§ 9 Absatz 3 Satz 3 PAuswG-2025 (bzw. entsprechend § 6 Absatz 2 Satz 3 PassG-2025 sowie der Verweis in § 60 Absatz 2 **AufenthG-2025)** lautet:

> *„Das Lichtbild ist nach Wahl der antragstellenden Person*
>
> 1. *durch einen Dienstleister elektronisch zu fertigen und im Anschluss von diesem durch ein sicheres Verfahren an die Personalausweisbehörde zu übermitteln oder*
> 2. *durch die Personalausweisbehörde elektronisch zu fertigen, sofern die Behörde über Geräte zur Lichtbildaufnahme verfügt.*
>
> *Eine Veränderung des Lichtbilds ist nur nach Maßgabe dieses Gesetzes oder nach Maßgabe von Vorschriften, die auf Grund dieses Gesetzes erlassen wurden, zulässig.“*

§ 34 Nummer 3 Buchstabe b **PAuswG-2025** (bzw. entsprechend § 6a Absatz 3 Nummer 2 PassG-2025 sowie § 99 Absatz 1 Nummer 13 Buchstabe c **AufenthG-2025**) lautet:

„Das Bundesministerium des Innern für Bau und Heimat wird ermächtigt, mit Zustimmung des Bundesrates durch Rechtsverordnung

[…]

3. die Einzelheiten zu regeln,

   b. zur sicheren Übermittlung des Lichtbilds an die Personalausweisbehörde sowie zu einer Registrierung und Zertifizierung von Dienstleistern, welche Lichtbilder für die Personalausweisproduktion an die Personalausweisbehörde übermitteln,

[…]“.

§ 6a Absatz 3 Satz 1 Nummer 2a PassG (in der Fassung ab dem 1. November 2023) lautet:

„Das Bundesministerium des Innern und für Heimat wird ermächtigt, durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf, Regelungen zu treffen

[…]

2a. über von § 6 Absatz 2 Satz 3 in der ab 1. Mai 2025 geltenden Fassung abweichende Verfahren zur Fertigung des Lichtbildes sowie zur sicheren Übermittlung des Lichtbildes für Fälle, in denen der Pass im Ausland bei der Passbehörde nach § 19 Absatz 2 beantragt wird,

[…].“

2.1.2 Personalausweisverordnung (PAuswV) und Passdatenerfassungs- und Übermittlungsverordnung (PassDEÜV)

Die Personalausweisverordnung (PAuswV) und die Passdatenerfassungs- und Übermittlungsverordnung (PassDEÜV) erlauben es grundsätzlich, Lichtbilder elektronisch durch einen Dienstleister fertigen und durch ein sicheres Verfahren an die Pass- oder Personalausweisbehörde zu übermitteln.

In § 1a PassDEÜV-2025 „Fertigung und Übermittlung des Lichtbilds durch ein sicheres Verfahren“ heißt es dazu:

„(1) [...] In Fällen, in denen ein Pass bei einer Passbehörde nach § 19 Absatz 1 des Passgesetzes beantragt wird, kann die antragstellende Person einen Dienstleister mit der Fertigung des Lichtbilds beauftragen. Der Dienstleister hat das Lichtbild elektronisch zu fertigen und im Anschluss durch ein sicheres Verfahren an die Passbehörde zu übermitteln. [...]

(2) Ein sicheres Verfahren im Sinne des Absatzes 1 Satz 2 ist:

1. die Übermittlung des Lichtbilds an die Passbehörde von einem Dienstleister unter Einbindung eines Cloudanbieters [...].“

Eine entsprechende Regelung findet sich in § 5a PAuswV-2025.

Der Ablauf des Verfahrens, die Registrierung und Identifizierung des Dienstleisters bei einem Cloudanbieter sowie die Pflichten des Cloudanbieters sind in den §§ 1b bis 1d PassDEÜV-2025 bzw. § 5 Absatz 4 und Absatz 7 und §§ 5a bis 5d PAuswV-2025 geregelt.

Es ist vorgesehen, dass mehrere Personen dem Nutzerkonto des Dienstleisters zugeordnet werden können. Um eine eindeutige Identifizierung der jeweils übermittelnden Person zu ermöglichen, sieht § 1c Absatz 4 PassDEÜV-2025 „Registrierung und Identifizierung eines Dienstleisters bei einem Cloudanbieter“ vor:

„(4) Für jede Person, die sich in einem Nutzerkonto nach Absatz 3 registriert hat, wird durch den Cloudanbieter ein Pseudonym erzeugt.“

[...].“

Eine entsprechende Regelung findet sich in § 5c Absatz 4 PAuswV-2025.

Darüber hinaus müssen sichere Verfahren nach § 1a Absatz 2 Nummer 1 PassDEÜV-2025 dem Stand der Technik entsprechen. In § 2 „Qualitätssicherung“ Absatz 2 heißt es:

„(2) Die technischen und organisatorischen Anforderungen an

[...]

4. das sichere Verfahren der Übermittlung von Lichtbildern von einem Dienstleister an die Passbehörde

[...]

sind nach dem Stand der Technik zu erfüllen. Der Stand der Technik ist als niedergelegt zu vermuten in den Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik. Diese sind in der Anlage 1 aufgeführt und gelten in der jeweils im Bundesanzeiger veröffentlichten Fassung.“

Eine entsprechende Regelung findet sich in § 2 Satz 1 Nummer 2 Buchstabe i) PAuswV-2025.

In der Anlage 1 der PassDEÜV-2025 sind abschließend diejenigen Technischen Richtlinien aufgeführt, die für die Beurteilung des Stands der Technik nach der PassDEÜV-2025 relevant sind. Dort heißt es hinsichtlich der Übermittlung von Lichtbildern an Behörden in Nummer 5:

„Anlage 1 Übersicht über die Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik

[...]

5. BSI: Technische Richtlinie TR-03170, Sichere digitale Übermittlung biometrischer Lichtbilder von Dienstleistern an Pass-, Personalausweis- und Ausländerbehörden.“

2.1.3 Weitere rechtliche Anforderungen

Urheberrechtlich MUSS sichergestellt werden, dass die biometrischen Bilder lizenzfrei von den Behörden zur Erstellung der hoheitlichen Dokumente genutzt werden können. Dies kann beispielsweise über die AGB der Dienstleister gelöst werden.

Auch die Einhaltung der datenschutzrechtlichen Vorgaben aus der EU Datenschutz-Grundverordnung [DS-GVO] MUSS gewährleistet sein.

2.2 Betrachtungsgegenstand

Die vorliegende Technische Richtlinie behandelt zwei Zertifizierungen:

1. Zertifizierung der Cloud (siehe Kapitel 2.4.1), in der die biometrischen Daten gespeichert werden (siehe Kapitel 3)
2. Zertifizierung der zugehörigen Software, mit der die Bilder beim Dienstleister (z. B. Fotografin oder Fotograf) in die Cloud hochgeladen werden und der zugehörige Barcode mitsamt der notwendigen Informationen (siehe Kapitel 4.3) erstellt wird. Zertifiziert werden MÜSSEN die für den in 2.4.2 beschriebenen Prozess notwendigen Funktionalitäten der Anwendung.

Die Konformität zu den Vorgaben dieser Technischen Richtlinie MUSS durch ein TR-Zertifikat bestätigt werden (Informationen zur Zertifizierung nach TR gibt es auf der Webseite des BSI). Es besteht die Möglichkeit der Zertifizierung einer Cloud, sowie der Zertifizierung einer Anwendung zur Anbindung der Dienstleister an die Cloud nach dieser Technischen Richtlinie. Die Zertifizierungen können gemeinsam oder unabhängig voneinander erfolgen.

2.3 Außerhalb der Betrachtung

Der Betrachtungsbereich der Technischen Richtlinie erstreckt sich nicht:

- auf die Erzeugung der Lichtbilder. Für die Sicherstellung der Bildqualität gelten die Regelungen der [BSI TR-03121, in ihrer aktuellen Fassung];
- auf die Verarbeitung der Bilder in den IT-Fachverfahren der Pass-, Personalausweis- oder Ausländerbehörden;
- auf die Übertragung von biometrischen Bildern, die von Live-Enrolment-Stations direkt an die Pass-, Personalausweis- oder Ausländerbehörden übertragen werden. Diese sind ebenfalls nicht Bestandteil der Technischen Richtlinie.

2.4 Zielobjekte und Prozessbeschreibung

2.4.1 Definitionen

Tabelle 2: Definitionen

Zielobjekte	***Beschreibung***
Assets	Im Sinne dieser Technischen Richtlinie sind die Assets die für die Informationssicherheit des Cloud-Dienstes während der Erstellung, Verarbeitung, Speicherung, Übermittlung, Löschung oder Zerstörung von Informationen benötigten Objekte im Verantwortungsbereich des Cloud-Anbieters.

Zielobjekte	*Beschreibung*
Behörde	Von den Ländern bestimmte, für Ausweisangelegenheiten in Deutschland zuständige Behörden (Pass-, Personalausweis- oder Ausländerbehörden) und Empfänger der erstellten digitalen Lichtbilder.
Biometrisches Lichtbild	Im Sinne dieser Technischen Richtlinie ein digitales Bild, welches zum Zeitpunkt der Bildnutzung in hoheitlichen Dokumenten die geltenden gesetzlichen Bildanforderungen der jeweils gültigen PassV, PAuswV, PassDEÜV, AufenthV oder entsprechender gesetzlicher Nachfolgedokumente erfüllt.
Bürgerin oder Bürger	Antragstellerin oder Antragsteller, die/der von einem Dienstleister ein digitales biometrisches Lichtbild für ein neues hoheitliches Dokument erstellen und an den Cloud-Dienst übertragen lässt. Von dort kann die Pass-, Personalausweis- oder Ausländerbehörde diese dann abrufen.
Cloud-Anbieter	Anbieter des im Rahmen dieser Technischen Richtlinie beschriebenen Cloud-Dienstes.
Cloud-Dienst	Dienst, der digitale Lichtbilder von Dienstleistenden entgegennimmt und für den Download durch Behörden bereitstellt. Gemäß C5-Testat ist der Cloud-Dienst eine im Rahmen von Cloud-Computing angebotene Dienstleistung der Informationstechnik. Dieser Dienst speichert die biometrischen Lichtbilder zum Abruf durch die Pass-, Personalausweis- und Ausländerbehörden.
Dienstleister (z. B. Fotografinnen und Fotografen)	Dienstleister einer Bürgerin oder eines Bürgers, der das digitale Lichtbild erstellt, aufbereitet und die Lichtbild-Datei an einen sicheren Cloud-Dienst übermittelt. Von dort kann die Pass-, Personalausweis- oder Ausländerbehörde diese dann abrufen.
Download-Schnittstelle	Schnittstelle, über die Behörden auf den Cloud-Dienst zugreifen, um Bilder aus der Cloud herunterzuladen und in ihre eigenen Fachverfahren einzuspeisen (siehe Kapitel 3.8.4).
Lichtbildidentifier	Die eindeutige Kennung eines Lichtbilds in einer Cloud. In der Schnittstellenspezifikation wird der Lichtbildidentifier auch photoId genannt.
Live-Enrolment-Stations	Selbstbedienungsterminals zur Produktionsdatenerfassung, -qualitätsprüfung und –übermittlung für hoheitliche Dokumente
Nutzerkennung	Die eindeutige Identität einer für einen Dienstleister handelnden natürlichen Person mitsamt Zuordnung zum Nutzerkonto des Dienstleisters und der genutzten Lichtbildcloud, für die Rückverfolgbarkeit der Herkunft eines Lichtbildes.
Nutzerkonto	Ein mittels Registrierung einer Organisation/eines Unternehmens erzeugtes Zugangsprofil bei einem Cloudanbieter. Die genannte Organisation/Das genannte Unternehmen ist im Sinne dieser Technischen Richtlinie Dienstleister für die Fertigung von Lichtbildern für hoheitliche Dokumente.
Nutzerregistrierung	Die Registrierung einer natürlichen Person unter einer Organisation/einem Unternehmen, im Rahmen Ihrer Tätigkeit bei der Erzeugung von Lichtbildern für hoheitliche Dokumente. Beinhaltet die Erzeugung der Nutzerkennung.

Zielobjekte	*Beschreibung*
Sensible Daten	Personenbezogene Daten nach Art.4 Abs.1 DSGVO, sowie insbesondere biometrische Daten nach Art.4 Abs.14 DSGVO.
Upload-Schnittstelle	Schnittstelle, über die Bilder sicher vom Dienstleister (z. B. Fotografinnen und Fotografen) an den Cloud-Dienst übertragen werden.

2.4.2 Prozess

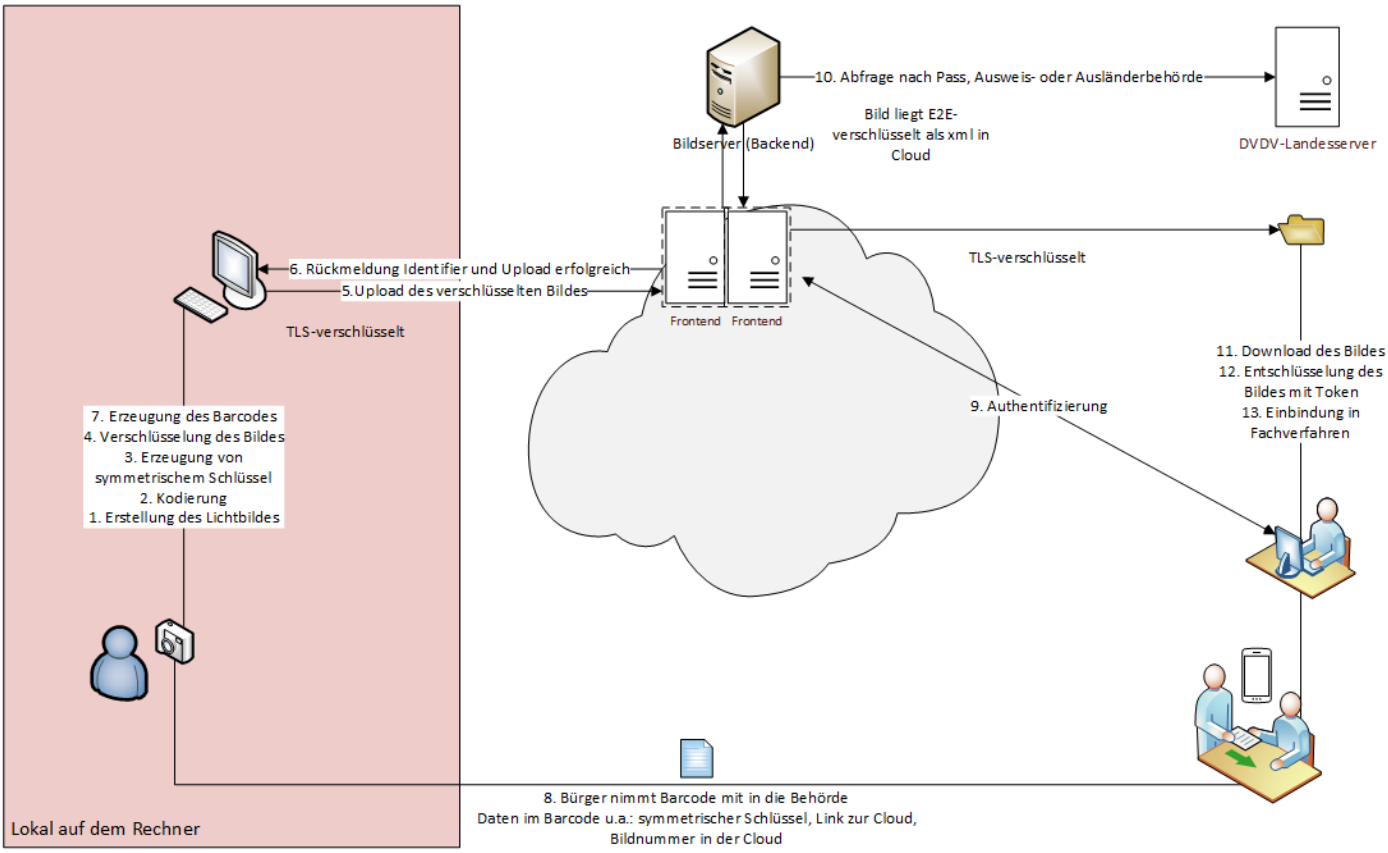

Abbildung 1: Prozessbeschreibung: „Upload und Download eines Lichtbilds Ende-zu-Ende“

Der Prozess gliedert sich in folgende Schritte:

Dienstleister (z. B. Fotografinnen und Fotografen) müssen sich bei dem Cloud-Dienst registrieren, da nur registrierte Dienstleister Bilder zu diesem übertragen dürfen. Der Anbieter des Cloud-Dienstes muss diesen in das Deutsche Verwaltungsdiensteverzeichnis [DVDV] eintragen lassen.

Im Rahmen der sicheren digitalen Lichtbildübermittlung finden die folgenden Prozessschritte statt:

1. Die Bürgerin/der Bürger lässt vom registrierten Dienstleister ein biometrisches Lichtbild (inkl. Meta-Informationen zur Aufnahme, z. B. Marke/Modell der Aufnahmeeinheit, verwendete Software) erstellen.
2. Das ausgewählte Lichtbild wird kodiert (siehe Kapitel 4.1).
3. Der symmetrische Schlüssel wird erzeugt.
4. Das Lichtbild wird mit dem symmetrischen Schlüssel verschlüsselt.
5. Der Dienstleister überträgt das clientseitig verschlüsselte Lichtbild über die Upload-Schnittstelle an den Cloud-Dienst. Die durch den Verordnungstext geforderte Anmeldung des Dienstleisters mit der eID oder einem anderen elektronischen Identifizierungsmittel auf dem Vertrauensniveau „hoch“ gemäß Kapitel 3.7 beim Cloudanbieter MUSS vor Schritt 5 (der Übertragung des Lichtbilds zur Cloud) erfolgen.

6. Der Cloud-Dienst erzeugt einen eindeutigen Identifier für die Integration in den Barcode und sendet diesen zusammen mit einer Bestätigung der erfolgreichen Speicherung des Lichtbilds an den Dienstleister
7. Es wird ein Barcode mit den notwendigen Daten zum Abruf des Lichtbilds aus der Cloud und zur Integration ins Fachverfahren erzeugt.
8. Der Bürger bekommt den Barcode vom Dienstleister und beantragt bei der Behörde das Ausweisdokument.
9. Die Pass-, Personalausweis- oder Ausländerbehörde fragt den Abruf des elektronischen Lichtbildes beim Cloud-Dienst unter Verwendung der vom Bürger zur Verfügung gestellten Zugangsdaten in Form des Barcodes an und übermittelt in diesem Kontext auch seinen Organisationsschlüssel aus dem DVDV.
10. Dazu prüft der Cloud-Dienst über das DVDV die Berechtigung im Rahmen der dort eingetragenen Rolle, und die Behörde authentisiert sich.
11. Die Behörde lädt das Lichtbild herunter.
12. Anschließend wird das Lichtbild entschlüsselt. Die Entschlüsselung ist nur möglich, wenn der Behörde der korrekte Schlüssel als Teil des Barcodes ausgehändigt wurde.
13. Das Lichtbild wird in das behördliche IT-Fachverfahren zur Ausstellung des Dokuments eingebunden.

3 Anforderungen an den Cloud-Dienst

3.1 Vorliegen eines C5-Testats

Der Anbieter des Cloud-Dienst MUSS sich verpflichten,

für die gesamte Beauftragungszeit, und

im Falle einer Vertragsbeendigung, für eine Nachlaufzeit von 6 Monaten, oder

im Falle eines Wechsels des Cloud-Dienstes, für eine zu vereinbarende Übergangszeit,

ein **Testat "Cloud Computing Compliance Criteria Catalogue – C5"** vom **Typ 2** über die Basiskriterien in der aktuellen Fassung vorweisen zu können.

3.2 C5-Kriterien

In diesem Abschnitt werden die Inhalte der im Bericht aufgeführten Rahmenbedingungen (BC-01 bis -04 und BC-06) spezifiziert. Danach werden spezifische Zusatzkriterien aus dem C5-Testat für die Technische Richtlinie herangezogen. Zusätzlich zu den Basiskriterien, welche den Mindestumfang einer Prüfung nach dem Kriterienkatalog C5 bilden, MUSS der Cloud-Dienst nachfolgende Zusatzkriterien erfüllen.

Abweichungen von der Umsetzung der C5 Kriterien werden gemäß Kapitel 3.4.7 des C5-Kriterienkatalogs behandelt.

3.3 Zusatzkriterien

Die im Folgenden genutzten Begrifflichkeiten und Anforderungen beziehen sich auf Begriffe und Basiskriterien aus dem C5-Kriterienkatalog (BSI, 2020).

3.3.1 Rahmenbedingungen

3.3.1.1 BC-01 Angaben zu Gerichtsbarkeit und Lokation

Der Cloud Dienstleister MUSS der Gerichtsbarkeit eines Landes der europäischen Union unterliegen. Der Anbieter des Cloud-Dienstes MUSS erklären, dass die Verarbeitung, Sicherung und Speicherung von Daten zur Bereitstellung des Cloud-Dienstes auf Systemkomponenten in einem Land der europäischen Union erfolgt und ein Konzept vorlegen, wie er dies technisch sicherstellt.

3.3.1.2 BC-02 Angaben zu Verfügbarkeit und Störungsbeseitigung im Normalbetrieb

Der Anbieter des Cloud-Dienstes MUSS anhand eines Betriebskonzeptes nachweisen, dass er einen Normalbetrieb während der Nutzungszeit, definiert als

Nutzungszeit = Randzeit-A + Geschäftszeit + Randzeit-B,

der Pass- und Personalausweis- oder Ausländerbehörden und der Dienstleister (z. B. Fotografinnen und Fotografen), gemäß Tabelle 3 gewährleisten kann:

Tabelle 3: Verfügbarkeit und Störungsbeseitigung im Normalbetrieb

KPI	***Messeinheit***	***Geschäftszeit (Mo – Fr: 6–20 Uhr, Sa: 8–16 Uhr)***	***Randzeit-A (Mo – Fr: 5–6 Uhr, Sa: 7–8 Uhr***	***Randzeit-B (Mo – Fr: 20–21 Uhr, Sa: 16–17 Uhr)***	***Außerhalb der Nutzungszeit***
Verfügbarkeit	Prozent	99,9%	99,9%	99,9%	95,0%

KPI	*Messeinheit*	*Geschäftszeit (Mo – Fr: 6–20 Uhr, Sa: 8–16 Uhr)*	*Randzeit-A (Mo – Fr: 5–6 Uhr, Sa: 7–8 Uhr*	*Randzeit-B (Mo – Fr: 20–21 Uhr, Sa: 16–17 Uhr)*	*Außerhalb der Nutzungszeit*
Störung in der Kommunikationsanbindung des Cloud-Rechen-zentrums (RZ)	Kritikalität	Sehr hoch	Hoch	Hoch	Gering
Störung an Dienstleister-Front-End	Kritikalität	Sehr hoch	Mittel	Hoch	Gering
Störung an Behörden-Front-End	Kritikalität	Sehr hoch	Hoch	Gering	Gering
Störung an Datenbank (DB)	Kritikalität	Sehr hoch	Hoch	Hoch	Gering
Störung an Back-End	Kritikalität	Sehr hoch	Hoch	Hoch	Gering
Wartungszeit	Uhrzeit	Keine	Keine	Keine	0 – 5 Uhr
Reaktionszeit bei Störung	Minuten	<= 10	<= 20	60	60
Wiederher-stellungszeit	Minuten	<= 30	Bis Beginn Geschäftszeit + 15 aber mindestens 30	Bis Beginn nächste Randzeit-A	Bis Beginn Randzeit-A + 15 aber mindestens 30

Geplante Wartungsarbeiten MÜSSEN innerhalb der Wartungszeit durchgeführt und abgeschlossen werden.

Störungen beinhalten alle ungeplanten Ausfälle oder Teilausfälle innerhalb der Geschäfts- und Nutzungszeit.

Reaktionszeit bei Störung beinhaltet sowohl die Störungserkennung als auch die Störungsmeldung.

Wiederherstellungszeit beinhaltet die Reaktionszeit bei Störung bis hin zum Abschluss der Störungsbeseitigung.

Anforderungen an eine Störungsmeldung:

Jede Störungsmeldung MUSS mit Datum, Uhrzeit, den Kontaktdaten der meldenden Person oder technischen Komponente, der Art des Meldeweges und den Kontaktdaten der die Störung aufnehmenden Person dokumentiert werden.

Die erfassten Kontaktdaten MÜSSEN so gestaltet sein, dass eine Rückverfolgung oder Rückmeldung an die jeweilige Kontaktadresse (meldend oder aufnehmend) zu jedem Zeitpunkt möglich ist.

Im Falle einer automatisierten Meldung durch eine technische Komponente MUSS als Kontaktdatum eine eindeutige Geräteidentifikation erfasst werden.

Falls nicht anders möglich, KANN die Eindeutigkeit der Geräteidentifikation auch durch Kombination mehrerer nichteindeutiger Geräteattribute zu einem eindeutigen Attribut hergestellt werden.

Eine Störungsmeldung MUSS über einen vom Kommunikationsverlauf der Störungsmeldung getrennten Rückmeldepfad mit eigenem Kommunikationsverlauf quittiert werden. Bei Meldungen, die durch Menschen erfolgen, z. B. mittels Rückruf oder Antwort-E-Mail.

3.3.1.3 BC-03 Angaben zu Wiederanlaufparametern im Notbetrieb

Unter Berücksichtigung der Definitionen für Geschäftszeit, Randzeit und Nutzungszeit aus Kapitel 3.2 ist von einem Notbetrieb auszugehen, wenn ein Ereignis der Kategorie Notfall, Krise oder Katastrophe nach Definition des [BSI-Standard 100-4 (Notfallmanagement)] eintritt und den Normalbetrieb unterbricht.

Das BSI empfiehlt folgende Wiederanlaufparameter durch den Cloud-Dienst anzustreben:

Tabelle 4: Wiederanlaufparameter

KPI	***Messeinheit***	***Geschäftszeit (Mo – Fr: 6–20 Uhr, Sa: 8–16 Uhr)***	***Randzeit-A (Mo – Fr: 5–6 Uhr, Sa: 7–8 Uhr***	***Randzeit-B (Mo – Fr: 20–21 Uhr, Sa: 16–17 Uhr)***	***Außerhalb der Nutzungszeit***
Recovery Point Objective (RPO)	Minuten	0	0	0	60
Recovery Time Objective (RTO)	Minuten	<= 30	Bis Beginn Geschäftszeit + 15, aber mindestens 30	Bis Beginn nächste Randzeit-A	Bis Beginn nächste Randzeit-A + 15 aber mindestens 30

Um die geforderte Aufgabe zu erfüllen, MUSS das System die volle Funktionalität aufweisen. Es gibt kein Funktionalitätsniveau unter der Vollfunktionalität, welches z. B. im Rahmen eines Notbetriebs den Anforderungen genügt. Entsprechend müssen hierzu keine expliziten Parameter für den Wiederanlauf zum Notbetrieb festgelegt werden.

3.3.1.4 BC-06 Angaben zu Zertifizierungen oder Bescheinigungen

Zusätzlich zum C5-Testat MÜSSEN mindestens folgende Zertifizierungen und Bescheinigungen vorliegen:

IT-Grundschutz Zertifikat bzw. ISO 27001 Zertifikat

Nachweis der Einhaltung der DSGVO (mindestens durch ein geprüftes Datenschutzkonzept)

Nachweis eines wirksamen Business Continuity Management Systems (BCMS) (mindestens durch eine BCM-Leitlinie und Audit-Berichte))

Der Cloud-Anbieter MUSS bestätigen, dass die Organisationseinheiten, Standorte und Verfahren des Cloud-Anbieters zur Bereitstellung des Cloud-Dienstes, wie in dieser Technischen Richtlinie spezifiziert, in den genannten Zertifizierungen enthalten sind.

3.3.2 C5-Zusatzkriterien

3.3.2.1 OIS-05 Kontakt zu relevanten Behörden und Interessenverbänden

Da der Cloud-Dienst durch Pass-, Personalausweis- oder Ausländerbehörden genutzt wird, MUSS der Cloud-Anbieter sich verpflichten, regelmäßigen (mindestens wöchentlich), sowie anlassbezogenen Kontakt zum

Nationalen IT-Lagezentrum und

CERT-Bund des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

zu pflegen, um sich über aktuelle Schwachstellen und Gefährdungen zu informieren.

3.3.2.2 AM-05 Verpflichtung auf zulässigen Gebrauch und sicheren Umgang mit ausgehändigten Assets sowie Rückgabe

Es MUSS durch den Cloud-Anbieter ein Konzept für die zentrale Verwaltung physischer Assets der Mitarbeiter des Anbieters des Cloud-Dienstes gepflegt werden. Dies sind physische Gegenstände, mit denen ein Mitarbeiter Zutritt, Zugang oder Zugriff auf Infrastruktur oder Systeme für die Bereitstellung des Cloud-Dienstes erhält. Der Cloud-Anbieter MUSS sich zur Einhaltung dieses Konzeptes verpflichten. Die zentrale Verwaltung physischer Assets MUSS eine Software-, Daten- und Richtlinienverteilung sowie eine Remote-Deaktivierung, -Löschung, oder –Sperrung ermöglichen.

3.3.2.3 AM-06 Klassifizierung und Kennzeichnung von Assets

Anwendungen zur Protokollierung und Überwachung MÜSSEN den Schutzbedarf der Assets berücksichtigen, um bei Informationssicherheitsvorfällen das dafür zuständige Personal so zu informieren, dass erforderliche Maßnahmen mit einer geeigneten Priorität eingeleitet werden.

Der Cloud-Anbieter MUSS ein Konzept zur Priorisierung von Maßnahmen für Ereignisse bei Assets pflegen. Maßnahmen für Ereignisse bei Assets mit einem erhöhten Schutzbedarf MÜSSEN prioritär, vor Ereignissen bei Assets mit einem geringeren Schutzbedarf behandelt werden.

3.3.2.4 OPS-04 Schutz vor Schadprogrammen – Konzept

Der Cloud-Anbieter MUSS regelmäßige Reports über die durchgeführten Überprüfungen erstellen, welche durch autorisiertes Personal oder Gremien überprüft und analysiert werden. Richtlinien und Anweisungen MÜSSEN die technischen Maßnahmen zur sicheren Konfiguration und Überwachung der Managementkonsole beschreiben, um diese vor Schadprogrammen zu schützen. Die Aktualisierung MUSS mit der höchsten Frequenz, die die Hersteller der Software vertraglich anbieten, erfolgen. Die Erstellung und Überprüfung der Reports MUSS in einem entsprechenden Konzept beschrieben werden.

3.3.2.5 OPS-05 Schutz vor Schadprogrammen – Umsetzung

Die Konfiguration der Schutzmechanismen MUSS automatisch überwacht werden. Abweichungen von den Vorgaben MÜSSEN automatisch an das dafür sachverständige Personal berichtet werden, um diese umgehend einer Beurteilung zu unterziehen und erforderliche Maßnahmen einzuleiten.

3.3.2.6 OPS-17 Protokollierung und Überwachung – Verfügbarkeit der Überwachungs-Software

Die Systemkomponenten zur Protokollierung- und Überwachung MÜSSEN so aufgebaut sein, dass bei Ausfällen einzelner Komponenten die Funktionalität des Cloud-Dienstes insgesamt nicht eingeschränkt ist. Dies MUSS der Cloud-Anbieter durch sein Betriebskonzept nachweisen.

3.3.2.7 OPS-19 Umgang mit Schwachstellen, Störungen und Fehlern – Penetrationstests

Pen-Tests MÜSSEN zwingend durch unabhängige Externe durchgeführt werden. Internes Personal für Penetrationstests darf die externen Dienstleister dabei unterstützen. Pen-Tests MÜSSEN mindestens jährlich stattfinden. Der Cloud-Anbieter MUSS ein Penetrationstestkonzept erstellen, das diese Anforderungen berücksichtigt.

3.3.2.8 OPS-22 Prüfung und Dokumentation offener Schwachstellen

Der Cloud-Anbieter MUSS sich dazu verpflichten, Sicherheitspatches ab dem Zeitpunkt ihrer Verfügbarkeit in Abhängigkeit des nach der jüngsten Version des Common Vulnerability Scoring Systems (CVSS) eingeordneten Schweregrades der dadurch adressierten Schwachstellen einzuspielen:

Kritisch (CVSS = 9.0 - 10.0): 3 Stunden

Hoch (CVSS = 7.0 - 8.9): 3 Tage

Mittel (CVSS = 4.0 - 6.9): 1 Monat

Niedrig (CVSS = 0.1 - 3.9): 3 Monate

3.3.2.9 OPS-24 Separierung der Datenbestände in der Cloud-Infrastruktur

Die strikte und sichere Separierung der biometrischen Lichtbilder von gemeinsam genutzten virtuellen und physischen Ressourcen MUSS durch Zonierung (LUN Bindung und LUN Masking) sichergestellt werden.

3.3.2.10 IDM-05 Regelmäßige Überprüfung der Zugriffsberechtigungen

Es MUSS in einem Zugriffsberechtigungskonzept ein geregelter Prozess definiert und umgesetzt werden, nach dem bei der Vergabe privilegierter Berechtigungen diese zusammen mit einem festgelegten sinnvollen Zeitraum dokumentiert werden. Die Notwendigkeit SOLLTE auf Wiedervorlage zum Ablauf des Zeitraums und spätestens nach einem halben Jahr erneut geprüft werden.

3.3.2.11 IDM-08 Vertraulichkeit von Authentisierungsinformationen

Die Benutzer MÜSSEN in einer Erklärung (z. B. Vertraulichkeitserklärung) bestätigen, dass sie persönliche (bzw. geteilte) Authentisierungsinformationen vertraulich behandeln und ausschließlich für sich (bzw. innerhalb der Gruppe) behalten.

3.3.2.12 CRY-02 Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)

Der Cloud-Anbieter MUSS für das Übertragen aller Daten Verfahren und technische Maßnahmen zur starken Verschlüsselung und Authentifizierung gemäß [BSI TR 03116-4, in ihrer aktuellen Fassung] etabliert haben.

3.3.2.13 CRY-03 Verschlüsselung von sensiblen Daten bei der Speicherung

Die für die Ende-zu-Ende Verschlüsselung genutzten symmetrischen Schlüssel DÜRFEN NICHT in die Cloud hochgeladen, dort verarbeitet und/oder gespeichert werden.

3.3.2.14 COS-01 Technische Schutzmaßnahmen

Der Cloud-Anbieter MUSS mit technischen Maßnahmen sicherstellen, dass seinem (physischen oder virtuellen) Netz keine unbekannten (physischen oder virtuellen) Geräte beitreten.

3.3.2.15 COS-04 Netzübergreifende Zugriffe

Jeder Netzperimeter MUSS von redundanten und hochverfügbaren Sicherheitsgateways kontrolliert werden.

3.3.2.16 COS-06 Segregation des Datenverkehrs in gemeinsam genutzten Netzumgebungen

Bei IaaS/PaaS MUSS die sichere Trennung durch physisch getrennte Netze oder durch stark verschlüsselte VLANs sichergestellt werden. Zur Definition einer starken Verschlüsselung ist die Technische Richtlinie [BSI TR-02102, in ihrer aktuellsten Fassung] zu berücksichtigen.

3.3.2.17 DEV-01 Richtlinien zur Entwicklung/Beschaffung von Informationssystemen

Bei der Beschaffung SOLLTEN Produkte vorgezogen werden, die nach den „Common Criteria for Information Technology Security Evaluation“ (kurz: [Common Criteria] – CC) gemäß Prüftiefe EAL 4 (oder höher) zertifiziert wurden. Soweit bei verfügbaren zertifizierten Produkten abweichend unzertifizierte Produkte beschafft werden sollen, erfolgt eine Risikobeurteilung gemäß OIS-07 (C5-Kriterium). Der Cloud-Anbieter MUSS ein Konzept zur Produktauswahl erstellen und verpflichtet sich zur Berücksichtigung von CC-zertifizierten Produkten. Die Entscheidung bei der Produktauswahl MUSS dokumentiert und begründet und die verschriftlichte Risikobeurteilung erstellt werden.

3.3.2.18 DEV-08 Versionskontrolle

Die Verfahren zur Versionskontrolle MÜSSEN durch geeignete Schutzmaßnahmen sicherstellen, dass Integrität und Verfügbarkeit der Daten nicht beeinträchtigt werden, wenn Systemkomponenten in ihren vorherigen Zustand zurückversetzt werden.

3.3.2.19 SSO-01 Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter

Die Erbringung des Service gemäß dem in Kapitel 2.4.2 beschriebenen Prozess DARF NICHT durch Subdienstleistungsunternehmen des Cloud-Anbieters erbracht werden.

Der Cloud-Anbieter MUSS eine schriftliche Erklärung über im Rahmen der Cloud-Services genutzten Subdienstleistungen abgeben. Es SOLLTE KEINE Subdienstleistungen im Rahmen des Cloud-Services geben.

3.3.2.20 SSO-04 Überwachung der Einhaltung der Anforderungen

Die Verfahren zur Überwachung der Einhaltung der Anforderungen MÜSSEN durch automatische Verfahren hinsichtlich der folgenden Aspekte ergänzt werden:

Konfiguration von Systemkomponenten

Leistung und Verfügbarkeit von Systemkomponenten

Reaktionszeit bei Störungen und Sicherheitsvorfällen

Wiederherstellungszeit (Zeitraum bis zum Abschluss der Störungsbeseitigung).

Identifizierte Verstöße und Abweichungen MÜSSEN automatisch an das dafür zuständige Personal des Cloud-Anbieters berichtet werden, um diese umgehend einer Beurteilung zu unterziehen und erforderliche Maßnahmen einzuleiten.

3.3.2.21 SIM-01 Richtlinie für den Umgang mit Sicherheitsvorfällen

Bei einem Sicherheitsvorfall MÜSSEN Daten beweisfest gesammelt werden. Es MÜSSEN für typische Sicherheitsvorfälle Analysepläne existieren, um die Beweiskraft für die spätere juristische Würdigung zu erhalten. Das Vorgehen MUSS in einem Betriebskonzept beschrieben und festgelegt werden.

3.3.2.22 PSS-02 Identifikation von Schwachstellen des Cloud-Dienstes

Die Verfahren zur Identifikation solcher (siehe dazugehörige Basisanforderung von PSS-02) Schwachstellen MÜSSEN darüber hinaus jährliche Code-Reviews oder Security-Penetration-Tests durch qualifizierte externe Dritte umfassen. Dieses Vorgehen MUSS durch den Cloud-Anbieter in einem entsprechenden Konzept festgelegt werden.

3.3.3 Mitwirkungspflichten

Die im C5-Testat genannten Mitwirkungspflichten des Kunden („complementary user entity controls“ oder „korrespondierende Kundenkontrollen“) MÜSSEN vom Dienstleister erfüllt werden. Die vom Dienstleister für die Nutzung des Cloud-Dienstes eingesetzte Software MUSS nach dieser Technischen Richtlinie [BSI-TR 03170] zertifiziert werden.

3.4 Frontend und Backend

Für das Speichern der biometrischen Lichtbilder MUSS ein eigener Prozess mit eigenem Prozess-User vorgesehen werden. Jeglicher Datenverkehr zwischen einem Dienstleister und dem Cloud-Dienst MUSS über die Frontend-Komponenten laufen. Ein Zugriff direkt auf das eigentliche Backend aus dem Internet DARF NICHT möglich sein.

Die Kommunikation zwischen Serverkomponenten MUSS unter Einhaltung der Vorgaben und Empfehlungen der [BSI TR-03116-4, in ihrer aktuellsten Fassung] gesichert sein.

Im Backend der Cloud werden die folgenden Daten gespeichert:

- Das verschlüsselte Lichtbild
- Zeitpunkt des Uploads bzw. der Speicherung des Lichtbilds in der Cloud
- Die im Rahmen der Protokollierung anfallenden Daten (C5-Kriterien OPS-10 – OPS-17 (Diese sind als Basiskriterien in C5 enthalten))
- Ein eindeutiger Identifier für das verschlüsselte Lichtbild
- Die zur Registrierung der Dienstleister notwendigen Daten entsprechend der Vorgaben aus den jeweiligen Gesetzen ((PassV) (PAuswV) (PassDEÜV) (AufenthV)), sowie die im Rahmen der Registrierung erzeugten UUIDs
- Ein Pseudonym (siehe Kapitel 3.7)

Es MUSS eine eindeutige UUID v4 gemäß [ISO/IEC 9834-8] erzeugt und eindeutig und dauerhaft mit dem Clouddienst verknüpft werden. Diese dient bei der Erzeugung der Nutzerkennung zu einem jeden Lichtbild, der eindeutigen Identifizierung des Clouddienstes.

3.5 Protokollierung

Der Cloud-Anbieter MUSS zusätzlich zu den Protokollierungsanforderungen im C5-Testat eine Erklärung über die Erfüllung der Vorgaben aus den jeweiligen Gesetzen und Verordnungen abgeben (PassV) (PAuswV) (PassDEÜV) (AufenthV).

Protokollierungsdaten MÜSSEN gegen Veränderungen und Austausch von Protokollinhalten geschützt sein, dazu MÜSSEN sie mit mindestens einer fortgeschrittenen elektronischen Signatur oder einem fortgeschrittenen elektronischen Siegel und einem Zeitstempel versehen werden.

Hierbei MÜSSEN die Vorgaben aus der [Leitlinie für digitale Signatur-/Siegel-, Zeitstempelformate, in ihrer aktuellsten Fassung] werden.

3.6 Registrierungsprozess

Es MUSS ein Registrierungsprozess implementiert werden, der es dem Dienstleister ermöglicht, bei einem Cloudanbieter ein Nutzerkonto zu erstellen. Im Rahmen des Erstregistrierungsverfahrens MUSS die Identität des Dienstleisters (bzw. im Falle einer Organisation die der für sie handelnden natürlichen Person) mittels eines elektronischen Identifizierungsmittels nachgewiesen werden, das entweder den Anforderungen des § 18 des Personalausweisgesetzes, des § 12 des eID-Karte-Gesetzes, des § 78 Absatz 5 des Aufenthaltsgesetzes entspricht oder einem anderen elektronischen Identifizierungsmittel entspricht, das gemäß Artikel 6 der Verordnung (EU) Nr. 910/2014 auf dem Sicherheitsniveau „hoch“ notifiziert wurde.

Darüber hinaus MUSS ein Verfahren etabliert werden, das die Entgegennahme und Prüfung des Nachweises der Dienstleistereigenschaft (gemäß der Vorgaben aus (PAuswV), (PassV) oder (AufenthV)) während des Erstregistrierungsverfahrens ermöglicht. Die Person, die das Erstregistrierungsverfahren durchführt, wird zum Hauptkontoinhaber, trägt die primäre Verantwortung für das Nutzerkonto und sollte daher in der Regel nicht aus dem Nutzerkonto entfernt werden können. Sollte eine Änderung der primären Verantwortung für ein Nutzerkonto notwendig sein, MUSS die Zugehörigkeit zu dem entsprechenden Unternehmen nachgewiesen werden. Es MUSS eine Überprüfung durchgeführt werden, um zu bestätigen, dass die Identität, die mittels des Identifizierungsmittels festgestellt wurde, mit den Angaben auf dem Nachweis übereinstimmt. Zudem MUSS eine Prüfung auf offensichtliche Unregelmäßigkeiten erfolgen. Die spezifischen Anforderungen an die Nachweise für die Dienstleistereigenschaft werden in den entsprechenden gesetzlichen Vorschriften festgelegt.

Beim Anlegen des Nutzerkontos MUSS eine eindeutige UUID v4 gemäß [ISO/IEC 9834-8] erzeugt und eindeutig und dauerhaft mit dem Nutzerkonto verknüpft werden.

Zusätzlich MÜSSEN die Mitarbeiter des Dienstleisters die Möglichkeit haben, eine Nutzerregistrierung innerhalb des Nutzerkontos des Dienstleisters durchzuführen. Die Zugehörigkeit zu dem Nutzerkonto MUSS hierbei durch den Hauptkontoinhaber freigegeben werden. Die Bedingungen für die Verwendung von elektronischen Identifizierungsmitteln entsprechen dabei den Anforderungen, die auch für die

Erstregistrierung des Dienstleisters gelten. Eine separate Bestätigung ihrer Zugehörigkeit zum Dienstleister oder ein Nachweis über die Dienstleistereigenschaft ist in diesem Kontext jedoch nicht erforderlich.

Im Rahmen des Erstregistrierungsprozesses MÜSSEN die notwendigen Daten für eine eindeutige Identifizierung des Nutzers (z.B. Pseudonym, Vor-, Nach- und Geburtsname, Geburtsdatum und Geburtsort) erhoben und beim Cloudanbieter gespeichert werden. Dies gilt sowohl für den Dienstleister als auch für dessen Mitarbeiter. Jeder Nutzer MUSS dabei ein individuelles Pseudonym (Im Falle der eID das DKK (Dienste- und kartenspezifisches Kennzeichen)) erhalten, das fest mit diesen Daten verknüpft ist. Diese Verknüpfung MUSS eine dauerhafte und eindeutige Zuordnung zwischen dem Pseudonym und dem eigentlichen Nutzer gewährleisten, unabhängig von späteren Interaktionen mit dem System.

Das individuelle Pseudonym MUSS von dem eingesetzten elektronischen Identifizierungsmittel stammen. Im Falle von deutschen Dokumenten ist dies die Pseudonymfunktion (rID) der eID. Bei anderen elektronischen Identifizierungsmitteln, die gemäß Artikel 6 der Verordnung (EU) Nr. 910/2014 auf dem Sicherheitsniveau „hoch“ notifiziert worden sind, MUSS die eindeutige Kennung, die als Pseudonym verwendet wird, gemäß dem entsprechenden Identifizierungssystem über das eIDAS-Framework bezogen werden.

Zusätzlich MUSS zu jeder Nutzerregistrierung eine persönliche UUID v4 gemäß [ISO/IEC 9834-8] erzeugt und eindeutig und dauerhaft mit dem Nutzeraccount verknüpft werden.

Zur Gewährleistung einer konsequenten und rückverfolgbaren Nutzeridentifikation MUSS eine dauerhafte und unveränderbare Verknüpfung zwischen den während des Registrierungsprozesses erfassten Daten und dem zugewiesenen Pseudonym hergestellt werden. Diese Verknüpfung MUSS unabhängig von nachfolgenden Interaktionen mit dem System oder Änderungen in den Identifizierungsmitteln des Nutzers bestehen bleiben, solange eine Zuordnung des Pseudonyms für die Nachvollziehbarkeit der Herkunft eines Lichtbilds, das durch den entsprechenden Nutzer hochgeladen wurde, im System existiert. Im Falle der Verwendung eines anderen (neuen) Identifizierungsmittels und damit einer Erstellung eines neuen Pseudonyms für einen Nutzer MUSS eine zusätzliche Verknüpfung zwischen der ursprünglichen Identität, dem vorherigen Pseudonym und dem neuen Pseudonym erstellt werden. Dabei MUSS außerdem ein Abgleich des Mindestdatensatzes zur Identifizierung erfolgen, um eine korrekte Zuordnung des neuen Pseudonyms sicherzustellen. Daraus folgt, dass einem Nutzer im Laufe der Zeit mehrere Pseudonyme zugeordnet werden können. Das System MUSS diese Verknüpfungen dauerhaft speichern, um eine Rückverfolgbarkeit zu ermöglichen.

3.7 Nachvollziehbarkeit/Verantwortlichkeit beim Upload

Für die Nachvollziehbarkeit der Herkunft eines Lichtbilds MUSS eine Nutzerkennung aus den vorliegenden UUIDs der Cloud, des Nutzerkontos und der Nutzerregistrierung, durch die ein Lichtbild hochgeladen wurde, erzeugt und im Rahmen der Übertragung zur Speicherung mit an die Behörde gesendet werden. Für die Nutzerkennung werden die drei vorgenannten UUIDs in der eben genannten Reihenfolge konkateniert. Als Trennzeichen werden hierbei jeweils drei Doppelpunkte verwendet.

Zur Integritätssicherung MUSS vor der Übertragung des Lichtbilds ein SHA-256 Hashwert über das verschlüsselte Lichtbild und die Nutzerkennung (ohne weitere Trennzeichen) erzeugt werden. Dieser MUSS dann mit dem privaten Schlüssel des Cloud-Dienstes, dessen zugehöriges Zertifikat im DVDV hinterlegt ist, mindestens fortgeschritten elektronisch gesiegelt oder signiert werden.

Die Nutzerkennung und die Signatur bzw. das Siegel des Hashes MÜSSEN zusammen mit dem verschlüsselten Lichtbild an die Behörde übertragen werden.

Vor jeder Übermittlung eines Lichtbildes an die Cloud MUSS die Identität der handelnden Person durch ein elektronisches Identifizierungsmittel nachgewiesen werden (siehe hierzu die gesetzlichen Vorgaben (PassV) (PAuswV) (PassDEÜV) (AufenthV)). Dieses muss entweder den Anforderungen des § 18 des Personalausweisgesetzes, des § 12 des eID-Karte-Gesetzes, des § 78 Absatz 5 des Aufenthaltsgesetzes genügen oder einem anderen elektronischen Identifizierungsmittel entsprechen, dass gemäß Artikel 6 der Verordnung (EU) Nr. 910/2014 auf dem Sicherheitsniveau „hoch“ notifiziert wurde. Dabei MUSS ausschließlich die durch das verwendete elektronische Identifizierungsmittel erzeugte eindeutige Kennung (Pseudonym) herangezogen werden. Voraussetzung dafür ist, dass bereits ein Nutzerkonto erstellt worden ist und eine Nutzerregistrierung stattgefunden hat.

Für eine Anmeldung am Nutzerkonto MUSS eine Authentisierung auf dem Vertrauensniveau „hoch“ gemäß den Anforderungen nach [BSI TR-03107-1, in ihrer aktuellsten Fassung] genutzt werden.

3.8 Kommunikationswege

Der Cloud-Anbieter MUSS Verfahren implementieren, welche die internen und externen Kommunikationswege sichern und deren Integrität und Vertraulichkeit zusichern. Für die Transportabsicherung sind die Vorgaben und Empfehlungen gemäß [BSI TR-03116-4, in ihrer aktuellsten Fassung] einzuhalten.

Die Datenübertragung sowohl zwischen Dienstleister (Fotografinnen und Fotografen) und Cloud-Dienst als auch zwischen Cloud-Dienst und Behörde MUSS synchron erfolgen.

3.8.1 Aufbau einer Verbindung im Rahmen einer Nutzer Session

Das Sessionhandling SOLLTE mittels sicherer Frameworks (siehe dazu auch Kapitel 4.4.1) realisiert werden.

Session-Identifier MÜSSEN als sensitive Daten geschützt werden.

Session-Identifier DÜRFEN NICHT unverschlüsselt auf permanenten Speichermedien abgelegt werden.

Die Anwendung MUSS die Anwendungssitzung nach einem angemessenen Session-Timeout, gemäß aktueller Best-Practice-Empfehlungen, aktiv beenden. Beim Upload eines Lichtbilds MUSS die Session nach dem Upload wieder beendet werden.

Wird eine Anwendungssitzung beendet, MUSS die Anwendung den Session-Identifier sowohl auf dem Endgerät als auch in der Cloud sicher löschen.

3.8.2 Erzeugung von Zufallszahlen

Für die Erzeugung von Zufallszahlen, z. B. bei der Erstellung eines Session-Identifiers gelten die folgenden Anforderungen:

Für Zufallszahlengeneratoren MUSS die [TR-02102-1, in ihrer aktuellsten Fassung] berücksichtigt werden.

Alle Zufallswerte MÜSSEN über einen sicheren kryptografischen Zufallszahlengenerator erzeugt werden. Die Anwendung MUSS Zufallszahlen von einem Zufallszahlengenerator mit hoher Entropie beziehen.

Die Anwendung SOLLTE dem Zufallszahlengenerator einen Startwert (Seed) zuweisen, der sich aus mindestens drei voneinander unabhängigen Systemparametern zusammensetzt. Die Parameter SOLLTEN von außerhalb der Anwendung nicht ermittelbar sein. Stellt die Plattform Hardware-Zufallszahlengeneratoren zur Verfügung, welche keine Vergabe von Startwerten erlauben, KÖNNEN stattdessen diese verwendet werden.

Anwendungshinweis/Beispiel: Dies betrifft die Zufallszahlengeneratoren auf dem Endgerät der Anwendung sowie die des Backends.

Die Anwendung SOLLTE bei Erstellung eines Startwerts (Seed) für den Zufallszahlengenerator einen geeigneten Zufall vom Backend beziehen.

Anwendungshinweis/Beispiel: Die Anwendung bringt vor der erstmaligen TLS-Verbindung Entropie, gemäß der vorangegangenen Anforderung (z. B. aus Benutzerinteraktion und Gerätesensorik), durch einen Seed in den lokalen Zufallszahlengenerator ein. Sie baut eine initiale Verbindung zum Erhalt zusätzlicher Entropie aus der Zufallszahlenquelle des Backends auf. Die Verbindung wird anschließend sofort wieder abgebaut

Die Anwendung berücksichtigt den erhaltenen Zufall, entsprechend der vorliegenden Anforderung, im lokalen Zufallszahlengenerator. Sie verwendet für die operationelle TLS-Verbindung von nun an Zufall aus der lokalen Zufallsquelle, welche mit der Entropie der Zufallszahlenquelle des Backends angereichert wurde.

3.8.3 Kommunikationswege Dienstleister (z. B. Fotografinnen und Fotografen) – Cloud (Upload)

Für die inhaltliche Absicherung der Daten MUSS auf kryptografische Verfahren gemäß der [BSI TR-03116-4, in ihrer aktuellsten Fassung] zurückgegriffen werden. Bei der Nutzung elektronischer Signaturen und Siegel

im Rahmen dieser Technischen Richtlinie MUSS mindestens fortgeschritten signiert werden nach den Vorgaben der [Leitlinie für digitale Signatur-/ Siegel-, Zeitstempelformate sowie technische Beweisdaten (Evidence Record), in ihrer aktuellsten Fassung].

Der Request (siehe 2.4.2) von der Anwendung des Dienstleisters MUSS, sofern ein Authentifizierungsmittel genutzt wird, was dies unterstützt, über einen mittels Kanalbindung nach [BSI TR-03124, siehe Kapitel 2.9] gesicherten TLS Kanal versendet werden.

Der Identifier, der für den Abruf des Lichtbilds aus der Cloud in den Barcode eingebettet wird, MUSS beim Upload und der Speicherung des verschlüsselten Lichtbilds durch den Cloud-Dienst erzeugt und an die Anwendung zur Einbettung in den Barcode übertragen werden. Der Lichtbildidentifier ist eine 128 Bit-Sequenz zur eindeutigen Identifikation des Lichtbilds in der Cloud und wird für den Abruf des Lichtbilds benötigt. Für den Aufbau und die Erzeugung des Lichtbildidentifiers MUSS die [ISO/IEC 9834-8] angewendet werden. Die Speicherung des verschlüsselten Lichtbilds zu dem erzeugten Identifier MUSS der Anwendung bestätigt werden.

3.8.4 Kommunikation Cloud – Behörde DVDV

Die Kommunikation zum Abruf eines verschlüsselten Lichtbilds bei der Cloud durch die Behörde MUSS folgendermaßen ablaufen:

1. Cloud und Behörde bauen eine sichere Verbindung mittels TLS Client Authentication auf. Hierbei MUSS [BSI TR-03116-4, in ihrer aktuellsten Fassung] beachtet werden. Es MÜSSEN die im [DVDV] hinterlegten Zertifikate von Cloud und Behörde genutzt werden.
2. Die Cloud prüft per DVDV-findCategories-Anfrage unter Verwendung des Organisationsschlüssels der anfragenden Behörde die Behördenkategorie auf Pass-, Personalausweis oder Ausländerbehörde.
3. Prüfung der Behördenkategorie:
   a Bei erfolgreicher Prüfung der Behördenkategorie liefert die Cloud eine Statusmeldung zur erfolgreich abgeschlossenen Prüfung der Behörde zurück.

Bei nicht erfolgreicher Prüfung liefert die Cloud eine Fehlermeldung und einen entsprechenden Fehler-Status "falsche" Organisationskategorie zurück und die Verbindung wird abgebaut.

4. Die Behörde sendet einen Request zum Abruf des Lichtbildes mit der aus dem Barcode ausgelesenen eindeutigen ID des Lichtbildes in der Cloud.
5. Die Cloud sendet das zu der ID gehörende verschlüsselte Lichtbild sowie weitere Daten nach dieser Technischen Richtlinie (siehe Kapitel3.9.2) an die Behörde.
6. Die Verbindung wird abgebaut.

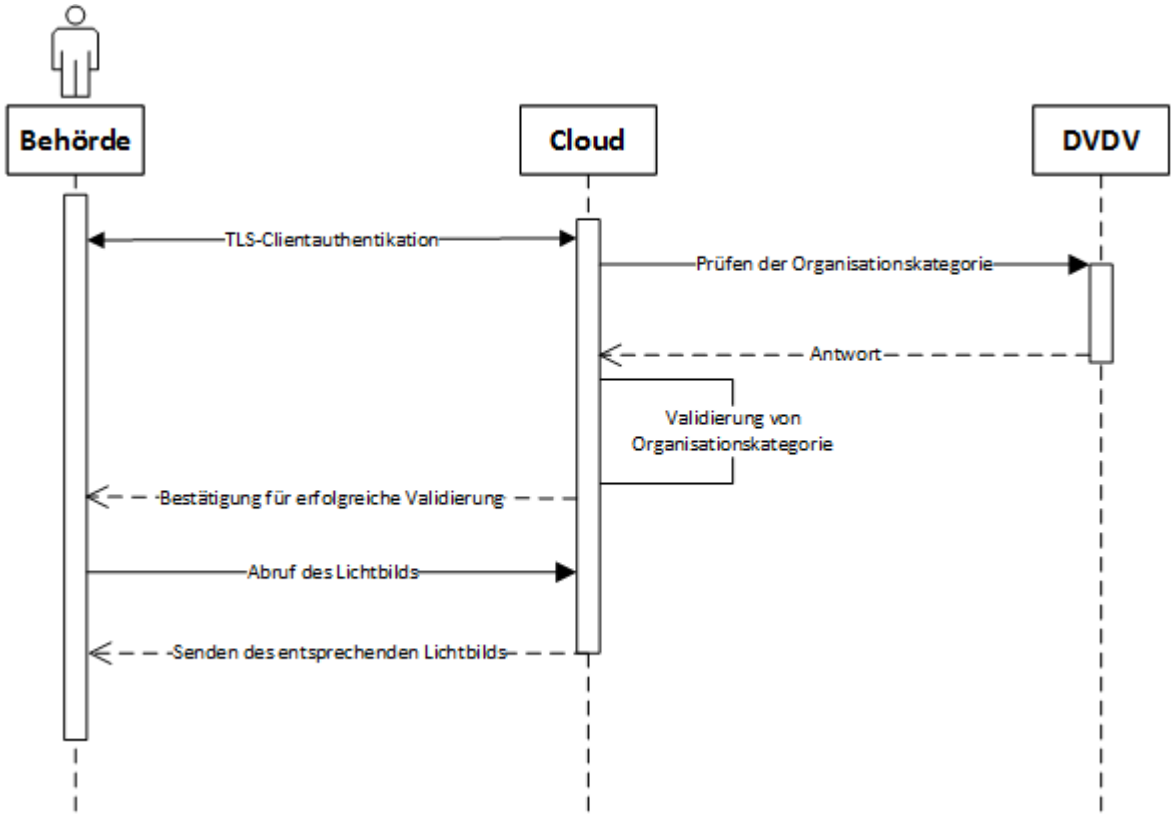

Abbildung 2: Kommunikation Cloud zu Behörde

3.9 Abruf der Lichtbilder durch die Pass-, Personalausweis- oder Ausländerbehörde

Aufbau einer Verbindung zur Cloud im Rahmen einer Session.

3.9.1 Kommunikation mit dem DVDV

Für Abfragen gegen das DVDV-System gelten grundsätzlich die Vorgaben der DVDV-Verfahrensbeschreibung [DVDV].

Für die im Kontext dieser TR stattfindenden Abfragen gegen das DVDV-System gelten die folgenden Regelungen:

1. Die benötigten Daten MÜSSEN grundsätzlich immer aktuell aus dem DVDV-System bezogen werden.
2. Abweichend hiervon ist das Caching (temporäres Speichern von DVDV-Einträgen und Nutzung ohne Neuabfrage) mit folgenden Zeiten erlaubt:
   - Für Cloud-Dienste bis zu 4 Stunden,
   - Für Behörden maximal 2 Tage.

Die diese Technische Richtlinie betreffenden DVDV-spezifischen Abläufe können der Dokumentation des DVDV und der beiliegenden Schnittstellendefinition entnommen werden.

Das Cloudzertifikat, dass im Kontext des DVDV und im Rahmen der Signatur oder des Siegels und des Verbindungsaufbaus genutzt wird, MUSS ein von CAs der PKI-1-Verwaltung (BSI_PKI-1-Verwaltung) ausgestelltes Zertifikat sein. Die jeweils gültigen Anforderungen der PKI-1-Verwaltung sind hierbei einzuhalten.

3.9.2 Abruf von Daten

Für den Abruf des Lichtbilds werden die folgenden Daten über die Schnittstelle von der Behörde an die Cloud übertragen:

- Lichtbildidentifier zur Identifizierung des abzurufenden Lichtbilds in der Cloud
- Organisationsschlüssel der abrufenden Behörde im DVDV

Zusätzlich prüft die Cloud das Zertifikat der abrufenden Behörde mittels DVDV

Für den Abruf des Lichtbilds werden dann die folgenden Daten über die Schnittstelle von der Cloud an die Behörde übertragen:

- Das verschlüsselte Lichtbild, das zu dem Lichtbildidentifier gehört
- Die zu dem Lichtbild passende Nutzerkennung zur Speicherung in der Behörde
- Die Signatur oder das Siegel eines Hashwerts über das verschlüsselte Lichtbild und die Nutzerkennung (siehe 3.7), zur Prüfung durch die Behörde nach dem Download,

3.9.3 Sichere Datenlöschung

Für die Fristen zur Löschung von Daten sind die Vorschriften aus den jeweiligen Rechtsnormen zu beachten (etwa (PassV) (PAuswV) (PassDEÜV) (AufenthV)). Der Cloud-Anbieter MUSS eine schriftliche Erklärung über die Einhaltung der Vorschriften aus den betroffenen Gesetzen und Verordnungen abgeben.

Der Bürgerin / dem Bürger MUSS die Möglichkeit eingeräumt werden, bei Abruf seines Lichtbilds bei der Behörde eine weitere Aufbewahrung des Lichtbilds in der Cloud für spätere Nutzung zu beauftragen. Sollte dies nicht durch die Bürgerin / den Bürger gewünscht sein, so MUSS das Lichtbild unverzüglich durch den Cloudanbieter aus der Cloud gelöscht werden. Wird eine weitere Aufbewahrung des Lichtbilds in der Cloud gewünscht, so MUSS das Lichtbild spätestens nach Ablauf der maximalen gesetzlichen Aufbewahrungsfrist gelöscht werden.

3.9.4 Entschlüsselung

Die Entschlüsselung erfolgt entsprechend den Vorgaben an die Verschlüsselung gemäß Kapitel 4.2. Die für eine Entschlüsselung benötigten Informationen über eingesetzte Algorithmen können, ebenso wie der symmetrische Schlüssel, dem Barcode entnommen werden (siehe Kapitel 4.3)

4 Anforderungen an die Software

Dieses Kapitel und die darin enthaltenen Unterkapitel definieren die Anforderungen, welche seitens der Software zu erfüllen sind.

Die Software zur Lichtbildübertragung durch den Dienstleister hat die Aufgabe:

- das Lichtbild gemäß Kapitel 4.1 zu kodieren,
- einen symmetrischen Schlüssel zu erzeugen,
- das Lichtbild damit zu verschlüsseln,
- das Lichtbild in die Cloud hochzuladen und
- einen Barcode (enthält symmetrischen Schlüssel, Adresse der Cloud und eindeutigen Identifier für das Lichtbild in der Cloud) als Beleg und Übertragungsmedium für den Kunden zu erzeugen.

4.1 Bildkonformität

Für das final zu übermittelnde Lichtbild gelten die Anforderungen der [BSI TR-03121, Part 3, Volume 2, Application Profile „Facial Image Digital-Delivery via Cloud [BSI TR-03170]].

4.2 Kryptografische Anforderungen

Beim Einsatz von Verschlüsselung in der Anwendung DÜRFEN KEINE fest einprogrammierten Schlüssel eingesetzt werden.

Der für die symmetrische Verschlüsselung genutzte Schlüssel DARF NICHT gespeichert werden. Er MUSS nach der Erzeugung für die Verschlüsselung der Daten verwendet, in den Barcode eingebettet und dann verworfen werden.

Der für die Übertragung der Informationen (z. B. symmetrischer Schlüssel, Bild-ID) genutzte Barcode DARF NICHT gespeichert werden. Er MUSS nach Erzeugung und Übergabe an den Kunden verworfen werden.

Für jeden Vorgang bzw. jedes Lichtbild MUSS ein eigener symmetrischer Schlüssel erzeugt und verwendet werden. Der Schlüssel DARF NICHT mehrfach verwendet werden.

Die Anwendung MUSS auf bewährte Implementierungen zur Umsetzung kryptografischer Primitive zurückgreifen gemäß [BSI TR-02102-1, in ihrer aktuellsten Fassung].

Die Wahl kryptografischer Primitive MUSS passend zum Anwendungsfall sein und den Vorgaben des aktuellen Stands der Technik gemäß [BSI TR-02102-1, in ihrer aktuellsten Fassung] entsprechen.

Die Stärke der kryptografischen Schlüssel MUSS dem aktuellen Stand der Technik entsprechen gemäß [BSI TR-02102-1, in ihrer aktuellsten Fassung].

Die Verschlüsselung des Lichtbilds MUSS clientseitig erfolgen.

4.3 Anforderung an den Barcode

Der Barcode MUSS als DataMatrix ECC 200 nach [ISO/IEC 16022] kodiert sein.

Die Symbolgröße des Barcodes MUSS so gewählt werden, dass der Barcode die in der nachfolgenden Tabelle spezifizierten Daten aufnehmen kann. Dabei kann die kleinste mögliche Größe genutzt werden, die alle Daten unter Beachtung der jeweiligen Anforderungen fassen kann. Mögliche Größen können [ISO/IEC 16022] entnommen werden.

Die folgenden Datentypen werden wie folgt in Bytefolgen umgewandelt:

Zeichenketten aus alphanumerischen Zeichen und/oder Sonderzeichen werden als Bytes kodiert. Die genutzte Kodierung wird in der Inhaltsspalte des jeweiligen Eintrags angegeben. Weitere Informationen zu der jeweiligen Kodierung enthält [ISO/IEC 16022].

Sequenzen von Bytes werden, so wie sie sind, übernommen.

Tabelle 5: Bytefolgen

Start Tag	*Länge (Byte)*	*Inhalt*
0x00	1	Magische Konstante. Die magische Konstante ist ein feststehender Wert zur Identifikation des hier genutzten Barcode Schemas und ist auf den Wert `0xE2` festgelegt.
0x01	1	Version. Ein Byte-Wert, der die genutzte Version des hier definierten Barcodes angibt. Aktuell gibt es hierbei nur die hier definierte Version `0x01`. Aufsteigende Versionsnummer werden fortlaufend vergeben.
0x02	1	Längenbyte für die Cloudadresse. Ein Byte, welches die Länge des nachfolgenden Feldes für die URL des Cloudanbieters angibt.
0x03	v	Cloudadresse. Die URL des Cloudanbieters. Die URL wird mittels ASCII kodiert. Damit der Barcode nicht unnötig groß wird, ist eine Zeichenbegrenzung von 100 Zeichen für die URL vorgesehen.
0x03 + v	16	Lichtbildidentifier. Der Lichtbildidentifier ist eine 128-Bit-Sequenz zur eindeutigen Identifikation des Lichtbilds in der Cloud und wird für den Abruf des Lichtbilds benötigt. Für den Aufbau und die Erzeugung des Lichtbildidentifiers gilt die [ISO/IEC 9834-8].
0x13 + v	1	Längenbyte für den Verschlüsselungsalgorithmus. Ein Byte, welches die Länge des nachfolgenden Feldes für den Verschlüsselungsalgorithmus angibt.

Start Tag	*Länge (Byte)*	*Inhalt*
0x14 + v	x	Verschlüsselungsalgorithmus. Der genutzte Verschlüsselungsalgorithmus MUSS in strukturierter Form als OID angegeben werden. Der Verschlüsselungsalgorithmus wird mittels C40 kodiert.
0x14 + v + x	1	Längenbyte für den Initialisierungsvektor. Ein Byte welches die Länge des nachfolgenden Feldes für den Initialisierungsvektor.
0x15 + v + x	y	Initialisierungsvektor. Hier wird der Initialisierungsvektor des gewählten Betriebsmodus angegeben.
0x16 + v + x + y	1	Längenbyte für das Padding. Ein Byte, welches die Länge des nachfolgenden Feldes für das Padding angibt.
0x17 + v + x + y	p	Padding. Falls ein Padding benötigt wird, wird hier das genutzt Padding angegeben. Dies wird in C40 kodiert.
0x17 + v + x + y + p	1	Längenbyte für den Schlüssel. Ein Byte, welches die Länge des nachfolgenden Feldes für den Schlüssel angibt.
0x18 + v + x + y + p	z	Schlüssel. Der symmetrische Schlüssel für die Entschlüsselung des Lichtbilds. Die Länge des Schlüssels ergibt sich aus dem Verschlüsselungsalgorithmus. Der Schlüssel wird als Bit-Sequenz abgelegt.
Summe	0x18 + v + x + y+p+z	

Für die kryptographischen Vorgaben und die Erzeugung des Schlüssels sowie Vorgaben zu damit einhergehenden Betriebsmodi, Initialisierungsvektoren und Padding gelten die Anforderungen aus Kapitel 4.1.

Der Barcode MUSS unter Berücksichtigung von [ISO/IEC 15415] so gedruckt werden, dass Lesegeräte den Barcode zuverlässig dekodieren können. Wenn der Barcode ausgedruckt wird, SOLLTE weißes Papier für den Druck verwendet werden, um zu verhindern, dass es zu Problemen mit dem Kontrast des Barcodes kommt. Bei der Verwendung von Standard-Tintenstrahldruckern SOLLTE mindestens mit einer Modulgröße (Größe eines Blocks eines 2D-Barcodes) von 0,3386 mm Seitenlänge pro Modul gedruckt werden. Dies entspricht 4 Punkten pro Modul-Seitenlänge (d. h. 16 Punkten pro Modul) auf einem 300-dpi-Drucker oder 8 Punkten pro Modul-Seitenlänge (d. h. 64 Punkten pro Modul) auf einem 600-dpi-Drucker. Kleinere Druckformate KÖNNEN akzeptabel sein, wenn hochauflösende Drucker oder Laserdrucker verwendet werden.

4.4 Allgemeine Anforderungen

4.4.1 Erzeugung von Zufallszahlen

Für die Erzeugung von Zufallszahlen, z. B. für die Erstellung des symmetrischen Schlüssels und die Erzeugung des eindeutigen Identifiers für das Lichtbild, gelten die folgenden Anforderungen:

Für Zufallszahlengeneratoren MÜSSEN die Vorgaben der [TR-02102-1, in ihrer aktuellsten Fassung] umgesetzt werden.

Alle Zufallswerte MÜSSEN über einen sicheren kryptografischen Zufallszahlengenerator erzeugt werden.

Die Anwendung MUSS Zufallszahlen von einem Zufallszahlengenerator mit hoher Entropie beziehen.

Die Anwendung SOLLTE dem Zufallszahlengenerator einen Startwert (Seed) zuweisen, der sich aus mindestens drei voneinander unabhängigen Systemparametern zusammensetzt. Die Parameter SOLLTEN von außerhalb der Anwendung nicht ermittelbar sein.

Anwendungshinweis/Beispiel: Dies betrifft die Zufallszahlengeneratoren auf dem Endgerät der Anwendung sowie die des Backends.

Die Anwendung SOLLTE in die Erstellung eines Startwerts (Seed) für den Zufallszahlengenerator einen geeigneten Zufall vom Backend einbeziehen.

Anwendungshinweis/Beispiel: Die Anwendung bringt vor der erstmaligen TLS-Verbindung Entropie, gemäß der vorangegangenen Anforderung (z. B. aus Benutzerinteraktion und Gerätesensorik), durch einen Seed in den lokalen Zufallszahlengenerator ein. Sie baut eine initiale Verbindung zum Erhalt zusätzlicher Entropie aus der Zufallszahlenquelle des Backends auf. Die Verbindung wird anschließend sofort wieder abgebaut. Die Anwendung berücksichtigt den erhaltenen Zufall, entsprechend der vorliegenden Anforderung, im lokalen Zufallszahlengenerator. Sie verwendet für die operationelle TLS-Verbindung von nun an Zufall aus der lokalen Zufallsquelle, welche mit der Entropie der Zufallszahlenquelle des Backends angereichert wurde.

4.4.2 Verwendung von Frameworks und Bibliotheken

Setzt die Anwendung Frameworks und Bibliotheken von Dritten ein, SOLLTEN alle verwendeten Funktionen für den primären Zweck der Anwendung erforderlich sein. Die Anwendung SOLLTE anderweitige Funktionen sicher deaktivieren.

Anwendungshinweis/Beispiel: Eine API für soziale Netzwerke dürfte nur verwendet werden, wenn dies für den primären Zweck der Anwendung notwendig ist.

Nutzt die Anwendung Frameworks oder Bibliotheken von Dritten (etwa für Objektserialisierung), MUSS sie sicherstellen, dass diese Funktionen in sicherer Weise genutzt werden. Die Anwendung MUSS darüber hinaus sicherstellen, dass ungenutzte Funktionen durch Dritte nicht aktiviert werden können. Die genutzten Frameworks und Bibliotheken SOLLTEN auf die für den primären Zweck der Anwendung erforderlichen begrenzt werden. Der Hersteller MUSS die genutzten Frameworks und Bibliotheken und deren Zweck im Rahmen der Anwendung in einer Softwaredokumentation erfassen.

Anwendungshinweis/Beispiel: Diese Anforderung bezieht sich in erster Linie auf die Dokumentation der Sicherheitsmechanismen der Bibliotheken und deren Nutzung.

Externe Bibliotheken und Frameworks SOLLTEN in ihrer aktuellsten verfügbaren Version, bezogen auf das genutzte Betriebssystem, verwendet werden.

Der Hersteller der Software MUSS regelmäßig prüfen, ob für genutzte externe Bibliotheken und Frameworks Schwachstellen bekannt sind. Funktionen aus Bibliotheken und Frameworks DÜRFEN bei bekannten Schwachstellen NICHT eingesetzt werden.

Sicherheitsupdates für externe Bibliotheken und Frameworks MÜSSEN zeitnah eingespielt werden. Der Hersteller MUSS ein Sicherheitskonzept vorlegen, das anhand der Kritikalität ausnutzbarer Schwachstellen die geduldete Weiternutzung für die Anwendung, festlegt. Nachdem die Übergangsfrist (Grace Period) abgelaufen ist, MUSS die Anwendung den Betrieb verweigern. Zur Festlegung dieses Vorgehens MUSS der Hersteller ein Konzept für Schwachstellen- und Patchmanagement pflegen.

Der Hersteller MUSS sich über eine schriftliche Erklärung verpflichten, vor der Verwendung von externen Bibliotheken und Frameworks deren Quelle auf Vertrauenswürdigkeit zu prüfen.

Der Hersteller MUSS sich außerdem über eine entsprechende schriftliche Erklärung dazu verpflichten, die Nutzenden über Mitigationsmaßnahmen zu informieren, sofern diese durch die Nutzenden umsetzbar sind.

Die Anwendung DARF sensible Daten NICHT an Drittanbieter-Software weitergeben.

Über Drittanbieter-Software eingehende Daten SOLLTEN validiert werden.

Drittanbieter-Software, die nicht länger vom Hersteller oder Entwickler gewartet wird, DARF NICHT verwendet werden.

4.4.3 Anforderungen an die Implementierung

Der Hersteller MUSS ein Konzept für Vorgehen und Design der Implementierung pflegen.

IT-Sicherheit MUSS ein fester Bestandteil des Softwareentwicklungs- und Lebenszyklus‘ für die gesamte Anwendung sein und sich in dem Implementierungskonzept wiederfinden.

Bereits in der Design-Phase der Anwendung MUSS berücksichtigt werden, dass die Anwendung in der Produktiv-Phase sensible Daten verarbeiten wird. Die Architektur der Anwendung MUSS dafür die sichere Erhebung, Verarbeitung, Speicherung und Löschung der sensiblen Daten in einem Datenlebenszyklus abbilden. Dies MUSS Bestandteil des Implementierungskonzepts sein.

Sicherheitsfunktionen SOLLTEN immer sowohl in der Anwendung, als auch auf allen Außenschnittstellen und API-Endpunkten implementiert werden.

Der Hersteller MUSS dem Nutzer eine barrierearme Möglichkeit bereitstellen, um Sicherheitsprobleme zu melden.

Die Cloud SOLLTE sicherheitsrelevante Updates der Anwendung erzwingen können.

Anwendungshinweis/Beispiel: Eine Anwendung kann z.B. bei veraltetem Versionsstand nicht genutzt werden (Ggf. nur bei sicherheitskritischen Updates).

Die Anwendung und Updates SOLLTEN durch Einsatz kryptografischer Maßnahmen verschlüsselt und signiert werden.

Nutzereingaben MÜSSEN vor deren Verwendung geprüft werden, um potenziell bösartige Werte vor der Verarbeitung herauszufiltern.

Der Hersteller MUSS alle Eingabedaten vollständig mit einer Escape-Syntax versehen.

Fehlermeldungen und Benachrichtigungen DÜRFEN KEINE sensiblen Daten (z. B. user identifier) enthalten.

Potenzielle Ausnahmen im Programmablauf (Exceptions) MÜSSEN abgefangen, kontrolliert behandelt und protokolliert werden.

Bei Ausnahmen im Programmablauf (Exceptions), mit sicherheitskritischen Auswirkungen, SOLLTE die Anwendung Zugriffe auf sensible Daten abbrechen.

Alle Optionen zur Unterstützung der Entwicklung (z. B. Log-Aufrufe, Entwickler-URLs, Testmethoden, etc.) MÜSSEN in der Produktiv-Version deaktiviert sein.

Der Hersteller MUSS sicherstellen, dass keine Debug-Mechanismen in der Produktiv-Version verbleiben. Die Untersuchung auf Debug-Mechanismen MUSS ein fester Bestandteil eines Konzepts zum Test- und Qualitätsmanagement sein.

Die Anwendung SOLLTE beim Beenden alle nutzerspezifischen Daten im Arbeitsspeicher sicher überschreiben.

Die Anwendung MUSS dem Nutzer barrierearme Best-Practice-Empfehlungen zum sicheren Umgang mit der Anwendung und ihrer Konfiguration bereitstellen.

Die Anwendung MUSS den Start in einer Entwicklungs-/Debugumgebung sicher erkennen und unterbinden.

Die Anwendung SOLLTE Härtungsmaßnahmen, wie etwa eine Integritätsprüfung bei jedem Start der Anwendung, realisieren.

Die Anwendung DARF NUR die Berechtigungen einfordern, die für die Erfüllung ihres primären Zwecks notwendig sind. Die notwendigen Berechtigungen der Anwendung MÜSSEN in einem Berechtigungskonzept dokumentiert und begründet werden.

Die Anwendung MUSS den Nutzer auf den Zweck der anzufragenden Berechtigungen und auf die Auswirkungen hinweisen, die eintreten, falls der Nutzer diese nicht gewährt.

4.4.4 Authentifizierung und Autorisierung

Für die Registrierung und vor jedem Hochladen eines Lichtbilds MUSS die eID oder ein anderes Identifizierungsmittel auf dem Vertrauensniveau „hoch“ nach den Vorgaben aus den Kapiteln 3.6, 3.7 und 3.8.3 genutzt werden.

Der Hersteller MUSS ein Konzept zur Authentifizierung, Autorisierung (Rollenkonzept) und zum Beenden einer Anwendungssitzung dokumentieren. Für die Anbindung an die Cloud MUSS an der Cloud-Schnittstelle eine geeignete Authentifizierung und Autorisierung stattfinden.

Wurde die Anwendung unterbrochen (in den Hintergrundmodus versetzt), MUSS eine erneute Authentifizierung gefordert werden.

4.4.5 Anforderungen an die Sicherheit der Daten

Die Anwendung DARF Daten NICHT erheben und verarbeiten, die nicht dem primären Zweck der Anwendung dienen. Die zu verarbeitenden Daten MÜSSEN in einem Datenverarbeitungskonzept beschrieben werden.

Sofern es nicht für den vorgesehenen primären Zweck einer Anwendung erforderlich ist, DÜRFEN sensible Daten NICHT mit Dritten geteilt werden. Die Anwendung MUSS den Nutzer über die Konsequenzen einer eventuellen Weitergabe der Daten vollumfänglich informieren und sein Einverständnis einholen (OPT-IN).

Anwendungshinweis/Beispiel: Nutzt die Anwendung eine Kartenvisualisierung eines Drittherstellers, muss der Nutzer darauf hingewiesen werden, dass möglicherweise bestimmte Daten an Dritte abfließen.

Die Anwendung DARF sensible Daten NICHT auf dem Bildschirm darstellen, außer dies ist für den Zweck der Anwendung erforderlich.

Die Anwendung DARF KEINE Ressourcen gegenüber Dritten verfügbar machen, die einen Zugriff auf sensible Daten ermöglichen.

Alle erhobenen sensiblen Daten DÜRFEN NICHT über die Dauer ihrer jeweiligen Verwendung hinaus in der Anwendung gehalten werden. Hierbei MUSS die Anwendung die Grundsätze der Datensparsamkeit und Zweckbindung berücksichtigen. Eine Erklärung zur Berücksichtigung der Grundsätze der Datensparsamkeit und der der Zweckbindung seitens des Herstellers ist dem Datenverarbeitungskonzept beizulegen.

Die Anwendung DARF KEINE sensiblen Daten in Logfiles oder andere Meldungen oder Benachrichtigungen, die nicht vom Benutzer explizit eingeschaltet wurden, schreiben.

Die Anwendung MUSS sicherstellen, dass bei ihrer Deinstallation alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen auf dem Endgerät vollständig gelöscht werden.

4.4.6 Softwareseitige Anforderungen an die Kommunikation

Jegliche Netzwerkkommunikation der Anwendung MUSS durchgängig mit TLS verschlüsselt werden.

Die Konfiguration der TLS-Verbindungen MUSS dem aktuellen Stand der Technik entsprechen und den Vorgaben und Empfehlungen der [BSI TR-03116-4, in ihrer aktuellsten Fassung] folgen.

Die Anwendung MUSS entweder die Sicherheitsfunktionalität der jeweilig verwendeten Betriebssystem-Plattform oder sicherheitsüberprüfte Frameworks oder Bibliotheken verwenden, um sichere Kommunikationskanäle aufzubauen.

Die Anwendung MUSS Zertifikatspinning unterstützen, d. h. sie DARF KEINE Zertifikate akzeptieren, deren Zertifikatskette dem Hersteller nicht vertrauenswürdig erscheint, siehe [RFC7469].

Die Anwendung MUSS das Server-Zertifikat der Cloud überprüfen.

Die Anwendung MUSS die Integrität der Antworten der Cloud validieren.

Literaturverzeichnis

AufenthG: Bundesamt für Justiz, Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet, verfügbar unter: https://www.gesetze-im-internet.de/aufenthg_2004/index.html

AufenthV: Bundesamt für Justiz, Aufenthaltsverordnung, verfügbar unter: https://www.gesetze-im-internet.de/aufenthv/index.html

C5-Kriterien: Bundesamt für Sicherheit in der Informationstechnik, BSI Kriterien C5:2020 (Editierbares Format), verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html;jsessionid=9BF5DF3311F814C025AC916867D51811.internet462

C5-Kriterienkatalog: Bundesamt für Sicherheit in der Informationstechnik, BSI Kriterienkatalog Cloud Computing C5, 2020, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

Common Criteria: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/IT-Sicherheiskriterien/CommonCriteria/commoncriteria_node.html

Deutsches Verwaltungsdiensteverzeichnis (DVDV): ITZ-Bund, verfügbar unter: https://www.itzbund.de/DE/itloesungen/standardloesungen/dvdv/dvdv.html

EU Datenschutz-Grundverordnung (DSGVO): Europäische Union, verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504

ISO 27001: International Organization for Standardization, „ISO/IEC 27001“, verfügbar unter: https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 9834-8:2005: International Organization for Standardization, „Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components — Part 8“, verfügbar unter: https://www.iso.org/standard/36775.html

ISO/IEC 15415:2011: International Organization for Standardization, „Information technology – Automatic identification and data capture techniques -- Barcode symbol print quality test specification – Two-dimensional symbols“, verfügbar unter:

ISO/IEC 16022:2006: International Organization for Standardization, „Information technology -- Automatic identification and data capture techniques -- Data Matrix bar code symbology specification“

IT-Grundschutz-Kataloge: Bundesamt für Sicherheit in der Informationstechnik, BSI IT-Grundschutz-Kataloge, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html;jsessionid=1C65C905C036B13AFFCA21FC0A8EB4CD.internet081

IT-Grundschutz-Kompendium: Bundesamt für Sicherheit in der Informationstechnik, BSI IT-Grundschutzkompendium, Edition 2022, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

Leitlinie für digitale Signatur-/Siegel-, Zeitstempelformate: Bundesamt für Sicherheit in der Informationstechnik, TR-03125, verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Leitlinie_fuer_digitale_Signatur-Siegel-Zeitstempelformate.pdf?__blob=publicationFile&v=1

PassG: Bundesamt für Justiz, Gesetz über Personalausweise und den elektronischen Identitätsnachweis, verfügbar unter**:** https://www.gesetze-im-internet.de/pauswg/index.html

PAuswG: Bundesamt für Justiz, Pass-Gesetz, verfügbar unter: https://www.gesetze-im-internet.de/pa_g_1986/index.html

RFC7469: C. Evans, C. Palmer, R. Sleevi, Google Inc, „Public Key Pinning Extension for HTTP“, Version April 2015, verfügbar unter https://tools.ietf.org/html/rfc7469

TR-02102-1: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, in der jeweils aktuellsten Fassung, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

TR-02102-2: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-02102-2: Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS), in der jeweils aktuellsten Fassung, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

TR-03107-1: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government - Teil 1, in der jeweils aktuellsten Fassung, verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.html

TR-03116-4: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03116-4: Kryptographische Vorgaben für Projekte der Bundesregierung - Teil 4, in der jeweils aktuellsten Fassung, verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html

TR-03121: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03121: Biometrie in hoheitlichen Anwendungen, in der jeweils aktuellsten Fassung, verfügbar unter:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03121/TR-03121_node.html

TR-03124: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03124: siehe eID-Client, in der jeweils aktuellsten Fassung, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03124/TR-03124_node.html

TR-03125: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03125: siehe „Leitlinie für digitale Signatur-/ Siegel-, Zeitstempelformate sowie technische Beweisdaten (Evidence Record)“, in der jeweils aktuellsten Fassung, verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Leitlinie_fuer_digitale_Signatur-Siegel-Zeitstempelformate.pdf?__blob=publicationFile&v=1

TR-03146: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03146: Elektronische Bildübermittlung zur Beantragung hoheitlicher Dokumente (E-Bild hD), in der jeweils aktuellsten Fassung, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03146/TR-03146_node.html

TR-03170: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03170: Sichere digitale Übermittlung biometrischer Lichtbilder von Dienstleistern (z. B. Fotografinnen und Fotografen) an Pass-, Personalausweis- und Ausländerbehörden, in der jeweils aktuellsten Fassung, verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03170/TR-03170_node.html;jsessionid=292C86E97DB5BBECE3E96B8042C855A5.internet461

Verwaltungs-PKI: Bundesamt für Sicherheit in der Informationstechnik, Public Key Infrastruktur der Verwaltung: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Verwaltungs-PKI/verwaltungs-pki_node.html

XMLDSIG: World Wide Web Consortium, verfügbar unter: http://www.w3.org/TR/xmldsig-core/

XMLENC: World Wide Web Consortium, verfügbar unter: http://www.w3.org/TR/xmlenc-core/