Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Prüfspezifikation zur Technischen Richtlinie TR-03170

Sichere elektronische Übermittlung von Lichtbildern an die Pass-, Personalausweis- oder Ausländerbehörden

Prüfmodule Cloud-Dienst (Management-Zertifizierung) und Software (Produkt-Zertifizierung)

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

Änderungshistorie

Version	Datum	Name	Beschreibung
0.1	07.07.2023	BSI	Erstentwurf auf Basis der TR-03170 in der Version 0.6
0.5	27.10.2023	BSI	Übertrag und Zusammenfassung der Software- und Cloud-Prüffälle aus dem Excel-Format.
0.7	19.03.2024	BSI	Einarbeitung der Änderungen aus der Version 1.0 der TR-03170
1.0	31.05.2024	BSI	Überarbeitung einzelner Prüfschritte, Einarbeitung von Kommentaren seitens Prüfstellen und Finalisierung

Tabelle 1: Änderungshistorie

Inhalt

1 Einleitung

Am 11. Dezember 2020 wurde das vom Deutschen Bundestag und Bundesrat verabschiedete Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen im Bundesgesetzblatt[1] und am 31. Oktober 2023 die „Verordnung zur Änderung der Personalausweisverordnung, der Passverordnung, der Aufenthaltsverordnung sowie weiterer Vorschriften“[2] 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 Sicherheits-anforderungen entspricht.

Stärkung der Sicherheit durch Verfahren zur digitalen Übermittlung der Lichtbilder

Das verabschiedete Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen sieht vor, dass künftig Manipulation 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.

Ein Verfahren zur sicheren 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.

1.1 Referenzierte Spezifikation

Diese Prüfspezifikation ist eine Umsetzung der Anforderungen der Technischen Richtlinie TR-03170 – „Sichere digitale Übermittlung biometrischer Lichtbilder von Dienstleistern (z.B. Fotografinnen und Fotografen) an Pass-, Personalausweis- und Ausländerbehörden“ und beschreibt die Prüfung der Anforderungen für die Zertifizierung nach der genannten TR.

1 https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__//*[@attr_id='bgbl120s2744.pdf'
2 https://www.recht.bund.de/bgbl/1/2023/290/VO.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

Die Technische Richtlinie bietet dabei zwei verschiedene Zertifizierungen an, deren Anforderungen in zwei Dokumente unterteilt sind. Das Rahmendokument TR-03170 beschreibt dabei den grundsätzlich abgebildeten Prozess für die digitale Übertragung der biometrischen Lichtbilder und dazugehörige Rahmenbedingungen. Das Teildokument TR-03170-1 beschreibt Anforderungen an die Cloud zur Speicherung der biometrischen Lichtbilder. Das Teildokument TR-03170-2 beschreibt Anforderungen an die Anwendung zur Übertragung der biometrischen Lichtbilder, unabhängig davon ob es sich um lokale Clientbestandteile einer Software oder um Teile einer Webanwendung oder eines Webservice handelt, der z.B. in der Cloud betrieben wird.

1.2 Aufbau des Dokuments

Kapitel 2 gibt ein paar grundlegende Informationen zur Aufteilung der TR-03170 nach den zwei möglichen Zertifizierungen. Kapitel 3 ist im Wesentlichen aufgeteilt nach den Prüffällen für die einzelnen Zertifizierungen. Im Kapitel 3.1 befinden sich die Prüffälle für die Zertifizierung nach TR-03170-1 für den Cloud-Dienst (Management-Zertifizierung) und in Kapitel 3.2 befinden sich die Prüffälle für die Zertifizierung nach TR-03170-2 für die Anwendung (Produkt-Zertifizierung). Die den Kapitel zugeorndeten Prüffälle und die dort verwiesenen Anforderungen weisen jeweils eine eigene Nommenklatur je Zertifizierung auf. In Kapitel 0 gibt es ein Anforderungsregister, in dem die einzelnen Anforderungs-IDs den konkreten Anforderungen aus der TR-03170 zugewiesen werden.

Die Anforderungen werden gemäß den Schlüsselworten aus TR-03170 Kapitel 1.2.1 geschrieben. Im Rahmen der Prüfung sind dabei insbesondere die SOLLTE-Anforderungen zu betrachten, da diese normalerweise erfüllt werden müssen, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss sorgfältig abgewogen und stichhaltig begründet werden. Entsprechend ist bei Prüffällen für SOLLTE-Anforderungen entweder die Umsetzung zu prüfen oder zu bewerten, inwiefern eine Begründung für eine alternative Umsetzung oder Nichtumsetzung stichhaltig ist.

2 Zertifizierung nach TR-03170

Die Technische Richtlinie TR03170 behandelt zwei Zertifizierungen:

1. Zertifizierung der Cloud, in der die biometrischen Lichtbilder gespeichert werden (siehe [BSI TR-03170-1] Kapitel 2). Der Nachweis über ein C5-Testat ist Bestandteil der Zertifizierung nach dieser Technischen Richtlinie.
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 den notwendigen Informationen (siehe [BSI TR-03170-2] Kapitel 2) erstellt wird. Zertifiziert werden MÜSSEN die für den in Kapitel 2.4.2 beschriebenen Prozess notwendigen Funktionalitäten der Anwendung.

Die Konformität zu den Vorgaben dieser Technischen Richtlinie MUSS durch ein TR-Zertifikat bestätigt werden. Diese Technische Richtlinie ermöglicht sowohl die Zertifizierung einer Cloud, sowie die Zertifizierung einer Anwendung zur Anbindung der Dienstleister an die Cloud. Die Zertifizierungen können gemeinsam oder unabhängig voneinander erfolgen.

Die Zertifizierung nach TR-03170-1 kann durch „Auditteamleiter“ bzw. „Auditoren“ durchgeführt werden, die für die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert wurden.

Die Zertifizierung nach TR-03170-2 kann durch Prüfstellen und Prüfer durchgeführt werden, die nach den TR-Prüfstellen und TR-Prüfer für die Prüfung der TR-03170-2 anerkannt sind.

2.1 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.
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**[4], **PAuswV**[5], **PassDEÜV**[6], **AufenthV**[7] oder entsprechender gesetzlicher Nachfolgedokumente erfüllt.

[4] Verordnung zur Durchführung des Passgesetzes (PassV), https://www.gesetze-im-internet.de/passv_2007/index.html

[5] Verordnung über Personalausweise, eID-Karten für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums und den elektronischen Identitätsnachweis (PAuswV), https://www.gesetze-im-internet.de/pauswv/index.html

[6] Verordnung zur Erfassung und Qualitätssicherung des Lichtbildes und der Fingerabdrücke in den Passbehörden und der Übermittlung der Passantragsdaten an den Passhersteller (PassDEÜV), https://www.gesetze-im-internet.de/passde_v/

[7] Aufenthaltsverordnung (AufenthV), https://www.gesetze-im-internet.de/aufenthv/

Zielobjekte	*Beschreibung*
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. Dies kann den Anbieter eines Cloud-Dienstes und den Anbieter/Betreiber einer Cloud-Infrastruktur umfassen (Wobei Anbieter des Cloud-Dienstes und Betreiber ein Unternehmen oder mehrere unterschiedliche sein können).
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 biometrische Lichtbild erstellt, aufbereitet und das biometrische Lichtbild an einen sicheren Cloud-Dienst übermittelt. Von dort kann die Pass-, Personalausweis- oder Ausländerbehörde diese dann abrufen.
Download-Schnittstelle	Die Schnittstelle, über die Behörden auf den Cloud-Dienst zugreifen, um biometrische Lichtbilder aus der Cloud herunterzuladen und in ihre eigenen Fachverfahren einzuspeisen (siehe [**BSI TR-03170-1**] Kapitel 2.8.2).
Lichtbildidentifier	Die eindeutige Kennung eines biometrischen Lichtbilds in einer Cloud. In der Schnittstellenspezifikation wird der Lichtbildidentifier auch als photoId bezeichnet.
Live-Enrolment-Stations	Selbstbedienungsterminals zur Produktionsdatenerfassung, -qualitätsprüfung und –übermittlung für hoheitliche Dokumente
Nutzerkennung	Die eindeutige Identität einer im Auftrag eines Dienstleisters handelnden natürlichen Person mitsamt Zuordnung zum Dienstleisterkonto und der genutzten Lichtbildcloud, für die Rückverfolgbarkeit der Herkunft eines biometrischen Lichtbildes.
Dienstleisterkonto	Ein mittels Registrierung einer Organisation, eines Unternehmens oder einer/s selbstständigen Fotografin/en erzeugtes Zugangsprofil bei einem Cloud-Anbieter. 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**[8], sowie insbesondere biometrische Daten nach **Art.4 Abs.14 DSGVO**.
Upload-Schnittstelle	Die Schnittstelle, über die biometrische Lichtbilder sicher vom Dienstleister (z.B. Fotografinnen und Fotografen) an den Cloud-Dienst übertragen werden.

[8] Amtsblatt der Europäischen Union, „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO). https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679

3 Prüfmodule

3.1 Cloud-Dienst

3.1.1 PFF-C-001 Funktionale Anforderungen an Up- und Download des Bildes

Prüffall-ID	PFF-C-001
Anforderungen	ANC-002 (Prozess [BSI TR-03170 Kapitel 2.4.2])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: Im Rahmen der sicheren digitalen Lichtbildübermittlung MUSS der Cloud-Dienst folgende Prozessschritte unterstützen: 1. Die Bürgerin/der Bürger lässt vom registrierten Dienstleister ein biometrisches Lichtbild erstellen. (Bei der Erstellung des Lichtbilds KÖNNEN Meta-Informationen zur Aufnahme, z. B. Marke/Modell der Aufnahmeeinheit, verwendete Software, etc. eingebracht werden). **(nicht Cloud relevant)** 2. Das ausgewählte Lichtbild wird kodiert (siehe [BSI TR-03170-2], Kapitel 2.1). **(nicht Cloud relevant)** 3. Der symmetrische Schlüssel wird erzeugt. **(nicht Cloud relevant)** 4. Das Lichtbild wird mit dem symmetrischen Schlüssel verschlüsselt. **(nicht Cloud relevant)** 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 [BSI TR-03170-1], Kapitel 2.6) beim Cloud-Anbieter 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. **(nicht Cloud relevant)** 8. Der Bürger bekommt den Barcode vom Dienstleister und beantragt bei der Behörde das Ausweisdokument. **(nicht Cloud relevant)**

Prüffall-ID	PFF-C-001		
	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. Das Lichtbild wird von der Behörde aus der Cloud abgerufen. 12. Anschließend wird das Lichtbild entschlüsselt. Die Entschlüsselung ist nur möglich, wenn der Behörde der korrekte Schlüssel als Teil des Barcodes ausgehändigt wurde. **(nicht Cloud relevant)** 13. Das Lichtbild kann aus der Cloud gelöscht werden oder für eine weitere Verwendung, bis zur maximal zulässigen Dauer, in der Cloud aufbewahrt werden (siehe [BSI TR-03170-1],] Kapitel 2.8.3). 14. Das Lichtbild wird in das behördliche IT- Fachverfahren zur Ausstellung des Dokuments eingebunden. **(nicht Cloud relevant)**		
Vorbedingungen	- Ein biometrisches Lichtbild liegt vor. - Es gibt im Cloud-Dienst registrierte (Test-) Dienstleister. - Die (Test-)Version einer Dienstleister-Software ist betriebsbereit. - Der Cloud-Dienst ist betriebsbereit. - Systemdokumentation liegt vor.		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Zugriffsversuch durch nicht registrierten Dienstleister	Der Zugriff wird verwehrt und der Zugriffsversuch nachvollziehbar protokolliert.	
2	Upload eines biometrischen Lichtbilds einschließlich der definierten Metadaten durch (Test-)Dienstleister-Software nach erfolgreicher Anmeldung am Cloud-Dienst	Upload ist nur durch registrierten Dienstleister möglich; biometrisches Lichtbild kann upgeloadet werden incl. aller definierten Metadaten zur Aufnahme; eindeutiger Identifier wird mit der Bestätigung der erfolgreichen Speicherung des Lichtbilds an die Dienstleister-Software gesendet;	

Prüffall-ID	PFF-C-001		
		verschlüsseltes Lichtbild liegt im Backend des Cloud-Dienstes vor	
3	Bewertung der Systemdokumentation bezüglich der Datenübertragung von der Behörde	In der Systemdokumentation ist nachvollziehbar beschrieben, wie der Cloud-Dienst den Lichtbilditentifier sowie den Organisationsschlüssel der Behörde und deren Zertifikat empfängt und im DVDV überprüft.	
4	Bewertung der Systemdokumentation der Datenübertragung zur Behörde	In der Systemdokumentation ist nachvollziehbar beschrieben, welche Daten an die Behörde übertragen werden.	
5	Bewertung auf Systemdokumentation bezüglich der Datenübertragung von der Behörde	In der Systemdokumentation ist nachvollziehbar beschrieben, welche Zustände für die Kommunikation zwischen Cloud und Behörde existieren. Dabei wird genau auf Erfolgs- und Fehlermeldungen eingegangen. Die Fehlermeldungen sind dabei selbsterklärend.	
6	Bewertung der Systemdokumentation zur Umsetzung der Schnittstellenspezifikation bezüglich des Herunterladens des verschlüsselten Lichtbilds gemäß ID aus dem Barcode	Die in der Systemdokumentation beschriebene Schnittstelle zum Abruf des Lichtbilds ist gemäß der zu TR-03170 gehörigen Schnittstellenspezifikation (https://www.bsi.bund.de/dok/TR-03170) designed.	
7	Bewertung der Systemdokumentation bezüglich der Umsetzung der Schnittstellenspezifikation zur Löschung des Lichtbilds gemäß ID aus dem Barcode.	Die in der Systemdokumentation beschriebene Schnittstelle zum Löschen des Lichtbilds ist gemäß der zu TR-03170 gehörigen Schnittstellenspezifikation	

Prüffall-ID	PFF-C-001		
		(https://www.bsi.bund.de/dok/TR-03170) designed.	
Verdict			

3.1.2 PFF-C-002 Vorliegen eines C5-Testats

Prüffall-ID	PFF-C-002		
Anforderungen	ANC-003 (Vorliegen eines C5-Testats [BSI TR-03170-1 Kapitel 2.1])		
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: Der Cloud-Anbieter MUSS: - für die gesamte Beauftragungszeit, und - im Falle einer Vertragsbeendigung, für eine Nachlaufzeit von 6 Monaten, oder - im Falle einer Beendigung des Betriebs des Cloud-Dienstes, für eine zu vereinbarende Übergangszeit, eine Attestierung des “Cloud Computing Compliance Criteria Catalogue” (C5-Kriterienkatalog) vom Typ 2 über die Basiskriterien in der aktuellen Fassung vorweisen können.		
Vorbedingungen	- Verpflichtungserklärung liegt vor - C5 Testat liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**

Prüffall-ID	PFF-C-002		
1	Bewertung der Verpflichtungserklärung	Der Anbieter des Cloud-Diensts hat sich verpflichtet, - 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 vorzuweisen. Nachweise hierzu können durch den Anbieter der Cloudinfrastruktur/ Betreiber erbracht werden.	
2	Bewertung des C5-Testats	Der Anbieter des Cloud-Dienstes kann ein gültiges Testat "Cloud Computing Compliance Criteria Catalogue – C5" vom Typ 2 über die Basiskriterien in der zum Prüfzeitpunkt aktuellen Fassung vorlegen.	
Verdict			

3.1.3 PFF-C-003 Gerichtsbarkeit und Lokation

Prüffall-ID	PFF-C-003
Anforderungen	ANC-004, ANC-005 (Angaben zu Gerichtsbarkeit und Lokationen [BSI TR-03170-1 Kapitel 2.2.1.1])

Prüffall-ID	PFF-C-003		
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Der Cloud Anbieter 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.		
Vorbedingungen	- Beglaubigter Handelsregistereintrag oder Äquivalent eines EU-Staates liegt vor - Erklärung und Datenhaltungskonzept liegen vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung des Handelsregistereintrags bzw. des Äquivalents eines EU-Staates	Der vorgelegte Eintrag ist beglaubigt und aus einem EU-Staat.	
2	Bewertung der Erklärung zur Datenhaltung	Der Anbieter des Cloud-Diensts hat erklärt, dass die Daten nur auf System-Komponenten in der EU verarbeitet werden.	
3	Bewertung des Datenhaltungskonzepts	Im Datenhaltungskonzept ist nachvollziehbar beschrieben, wie sichergestellt wird, dass die Daten die EU nicht verlassen.	
Verdict			

3.1.4 PFF-C-004 Verfügbarkeit und Störungsbeseitigung

Prüffall-ID	PFF-C-004
Anforderungen	ANC-006, ANC-007, ANC-008, ANC-009, ANC-010, ANC-011

<table>
<tr><th>Prüffall-ID</th><th>PFF-C-004</th></tr>
<tr><td></td><td>(Angaben zu Verfügbarkeit und Störungsbeseitigung im Normalbetrieb [BSI TR-03170-1 Kapitel 2.2.1.2])</td></tr>
<tr><td>Ziel</td><td>Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind:

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

Nutzungszeit = Geschäftszeit,

der Pass- und Personalausweis- oder Ausländerbehörden und der Dienstleister (z. B. Fotografinnen und Fotografen), gemäß Tabelle 2 gewährleisten kann:

<table>
<tr><th>Key Performance Indicators (KPI)</th><th>Messeinheit</th><th>Geschäftszeit (Mo – Fr: 7–20 Uhr, Sa: 7–17 Uhr)</th><th>Außerhalb der Nutzungszeit</th></tr>
<tr><td>Verfügbarkeit</td><td>Prozent</td><td>99,9%</td><td>95,0%</td></tr>
<tr><td>Störung in der Netzwerkkommunikation zwischen den Behörden und der Cloud-Infrastruktur</td><td>Kritikalität</td><td>Sehr hoch</td><td>Gering</td></tr>
<tr><td>Störung in der Netzwerkkommunikation zwischen den Fotodienstleistern und der Cloud-Infrastruktur</td><td>Kritikalität</td><td>Sehr hoch</td><td>Gering</td></tr>
<tr><td>Störung in der Cloud-Infrastruktur</td><td>Kritikalität</td><td>Sehr hoch</td><td>Gering</td></tr>
<tr><td>Wartungszeit</td><td>Uhrzeit</td><td>Keine</td><td>beliebig</td></tr>
<tr><td>Reaktionszeit bei Störung</td><td>Minuten</td><td><= 10</td><td>60</td></tr>
<tr><td>Wiederherstellungszeit</td><td>Minuten</td><td><= 60</td><td>180</td></tr>
</table>
</td></tr>
</table>

Prüffall-ID	PFF-C-004		
	- Kritikalität entspricht der Einordnung in Risikokategorien nach BSI Standard 200-3. - Wartungsarbeiten MÜSSEN innerhalb der Wartungszeit durchgeführt und abgeschlossen werden. - 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.		
Vorbedingungen	- Betriebskonzept liegt vor - Betriebsaufzeichnungen liegen vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung des Betriebskonzepts hinsichtlich des Normalbetriebs in der Nutzungszeit	Im Betriebskonzept ist nachvollziehbar beschrieben, wie der Normalbetrieb gemäß Tabelle 2 gewährleistet wird.	
2	Bewertung des Betriebskonzepts hinsichtlich der Wartungszeiten	Im Betriebskonzept ist nachvollziehbar beschrieben, dass Wartungsarbeiten nur außerhalb der Nutzungszeiten gemäß Tabelle 2 erfolgen.	
3	Bewertung Betriebskonzept und Betriebsaufzeichnungen bezüglich Störungsmeldungen	Im Betriebskonzept ist nachvollziehbar beschrieben, dass Datum, Uhrzeit, die Kontaktdaten der meldenden Person oder technischen Komponente, die Art des Meldeweges und die Kontaktdaten der die Störung	

Prüffall-ID	PFF-C-004		
		aufnehmenden Person zu jeder Störungsmeldung dokumentiert werden. Die Informationen finden sich in Betriebsaufzeichnungen wieder.	
4	Bewertung Betriebskonzept und Betriebsaufzeichnungen bezüglich Kontaktdaten	Im Betriebskonzept ist nachvollziehbar beschrieben, dass mit dokumentierten Kontaktdaten die Rückmeldung an die jeweilige Kontaktadresse jederzeit möglich ist. Die Informationen finden sich in Betriebsaufzeichnungen wieder.	
5	Bewertung Betriebskonzept und Betriebsaufzeichnungen bezüglich automatisierter Störungsmeldungen	Im Betriebskonzept ist nachvollziehbar beschrieben, dass meldende Komponenten eindeutig identifizierbar sind. Die Informationen finden sich in Betriebsaufzeichnungen wieder.	
6	Bewertung Betriebskonzept und Betriebsaufzeichnungen bezüglich Rückmeldung zu Störungsmeldungen	Im Betriebskonzept ist nachvollziehbar beschrieben, dass Störungsmeldungen auf einem, von der Meldung unabhängigen Kommunikationspfad quittiert werden. Die Informationen finden sich in Betriebsaufzeichnungen wieder.	
Verdict			

3.1.5 PFF-C-005 Zertifizierungen oder Bescheinigungen

Prüffall-ID	PFF-C-005		
Anforderungen	ANC-012, ANC-013 (Angaben zu Zertifizierungen oder Bescheinigungen [BSI TR-03170-1 Kapitel 2.2.1.4])		
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: -- Zusätzlich zum C5-Testat MÜSSEN mindestens folgende Zertifizierungen und Bescheinigungen vorliegen: -- IT-Grundschutz[9] Zertifikat bzw. ISO 27001[10] Zertifikat (Wenn ein Zertifikat nur für die Cloud-Infrastruktur vorgelegt wird, MUSS der Cloud-Anbieter für über die Cloud-Infrastruktur hinausgehende Leistungen (z.B. Entwicklung und Betrieb des Cloud-Dienstes) die Einhaltung von ISO 27001 bzw. IT-Grundschutz gewährleisten.) -- Nachweis der Einhaltung der DSGVO für den gesamten Prozess (mindestens durch ein von einer/ einem Datenschutzbeauftragten 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.		
Vorbedingungen	- Geforderte Zertifikate und Bescheinigungen liegen vor - Erklärung über Anwendungsbereiche liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung geforderter Zertifikate bezüglich ihrer Vollständigkeit	Der Cloud-Anbieter kann folgende gültige Nachweise vorlegen: - IT-Grundschutz Zertifikat bzw. ISO 27001 Zertifikat - Nachweis der Einhaltung der DSGVO	

9 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
10 https://www.bsi.bund.de/dok/6604686

Prüffall-ID	PFF-C-005		
		(mindestens durch ein von einer/ einem Datenschutzbeauftragten geprüftes Datenschutzkonzept) - Nachweis eines wirksamen Business Continuity Management Systems (BCMS) (mindestens durch eine BCM-Leitlinie und Audit-Berichte)	
2	Bewertung Erklärung zu Anwendungsbereichen	Der Cloud-Anbieter erklärt, dass die Anwendungsbereiche der vorgelegten Nachweise den Cloud-Dienst abdecken.	
3	Bewertung Erklärung zu Umsetzung von IT-Grundschutz oder ISO 27001 in der Cloud betriebenen Anwendung	Der Cloud-Anbieter erklärt, dass die im Rahmen des Cloud-Dienstes über den Betrieb der Cloud-Infrastruktur hinausgehenden Leistungen (z.B. die Entwicklung der im Cloud-Dienst betriebenen Anwendung) nach ISO 27001 oder IT-Grundschutz durchgeführt und abgesichert werden.	
Verdict			

3.1.6 PFF-C-006 Kontakt zu relevanten Behörden und Interessenverbänden

Prüffall-ID	PFF-C-006
Anforderungen	ANC-014 (Kontakt zu relevanten Behörden und Interessenverbänden [BSI TR-03170-1 Kapitel 2.2.1.5])

Prüffall-ID	PFF-C-006		
Ziel	Nachweis, dass folgende Anforderung an den Cloud-Dienst erfüllt ist: 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 zum CERT-Bund des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu pflegen, um sich über aktuelle Schwachstellen und Gefährdungen zu informieren.		
Vorbedingungen	Verpflichtungserklärung liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung Verpflichtungserklärung zum Behördenkontakt	Der Cloud-Anbieter hat sich verpflichtet, regelmäßigen (mindestens wöchentlich), sowie anlassbezogenen Kontakt zum Nationalen IT-Lagezentrum und CERT-Bund zu pflegen, um sich über aktuelle Schwachstellen und Gefährdungen zu informieren.	
Verdict			

3.1.7 PFF-C-007 Management physischer Assets

Prüffall-ID	PFF-C-007
Anforderungen	ANC-015, ANC-016 (Verpflichtung auf zulässigen Gebrauch und sicheren Umgang mit ausgehändigten Assets sowie Rückgabe [BSI TR-03170-1 Kapitel 2.2.1.6])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind:

Prüffall-ID	PFF-C-007		
	- 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 (z.B. ein Schlüssel, ein Token oder eine SmartCard), 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.		
Vorbedingungen	- Assetmanagementkonzept liegt vor - Verpflichtungserklärung liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung Assetmanagementkonzept	Das Assetmanagementkonzept beschreibt den Assetmanagementprozess, der eine Software-, Daten- und Richtlinienverteilung sowie eine Remote-Deaktivierung, -Löschung, oder -Sperrung ermöglicht, nachvollziehbar.	
2	Bewertung Verpflichtungserklärung zum Assetmanagement	Der Cloud-Anbieter hat sich verpflichtet, das Assetmanagementkonzept umzusetzen.	
Verdict			

3.1.8 PFF-C-008 Klassifizierung von Assets

Prüffall-ID	PFF-C-008		
Anforderungen	ANC-017, ANC-018 (Klassifizierung und Kennzeichnung von Assets [BSI TR-03170-1 Kapitel 2.2.1.7])		
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - 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.		
Vorbedingungen	- Assetmanagementkonzept liegt vor - Protokollierungs- und Überwachungskonzept liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung Assetmanagementkonzept bezüglich des Schutzbedarfs	Das Assetmanagementkonzept beschreibt nachvollziehbar, wie der Schutzbedarf der Assets erfasst wird.	
2	Bewertung Protokollierungs- und Überwachungskonzept bezüglich Schutzbedarf	Das Protokollierungs- und Überwachungskonzept beschreibt nachvollziehbar, dass Maßnahmen bei Sicherheitsvorfällen auf Basis des Schutzbedarfs der Assets priorisiert werden.	
3	Bewertung Protokollierungs- und Überwachungskonzept bezüglich Priorisierung von Maßnahmen	Das Protokollierungs- und Überwachungskonzept beschreibt nachvollziehbar, dass Maßnahmen bei Vorfällen mit Assets höheren Schutzbedarfs behandelt werden, bevor Maßnahmen bei	

Prüffall-ID	PFF-C-008		
		Vorfällen mit Assets niedrigeren Schutzbedarfs ergriffen werden.	
Verdict			

3.1.9 PFF-C-009 Schutz vor Schadprogrammen

Prüffall-ID	PFF-C-009
Anforderungen	ANC-019, ANC-020, ANC-021, ANC-022, ANC-023 (Schutz vor Schadprogrammen [BSI TR-03170-1 Kapitel 2.2.1.8 & 2.2.1.9]
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Der Cloud-Anbieter MUSS regelmäßige Reports über die durchgeführten Überprüfungen zum Schutz vor Schadprogrammen erstellen, welche durch autorisiertes Personal oder Gremien überprüft und analysiert werden. - Die Erstellung und Überprüfung der Reports MUSS in einem entsprechenden Konzept beschrieben 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 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.
Vorbedingungen	- Konzept zum Schutz vor Schadsoftware liegt vor - Reports zum Schutz vor Schadsoftware liegen vor

Prüffall-ID	PFF-C-009		
	- Richtlinien und Anweisungen zum Schutz der Managementkonsole vor Schadsoftware liegen vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung Konzept und Reports zum Schutz vor Schadsoftware	Das Konzept zum Schutz vor Schadsoftware beschreibt nachvollziehbar, wie Reports über die durchgeführten Überprüfungen regelmäßig erstellt, geprüft und analysiert werden. Entsprechende Reports belegen die Umsetzung.	
2	Bewertung Richtlinien und Anweisungen zum Schutz der Managementkonsole vor Schadsoftware	Richtlinien und Anweisungen beschreiben nachvollziehbar, welche Maßnahmen zum Schutz der Managementkonsole vor Schadprogrammen ergriffen wurden.	
3	Bewertung Konzept zum Schutz vor Schadsoftware bezüglich der Updatefrequenz	Das Konzept zum Schutz vor Schadsoftware beschreibt nachvollziehbar, mit welcher Frequenz Aktualisierungen erfolgen und dass sie in der höchstmöglichen Frequenz erfolgen.	
4	Bewertung Konzept zum Schutz vor Schadsoftware bezüglich der Überwachung	Das Konzept zum Schutz vor Schadsoftware beschreibt nachvollziehbar, dass die Schutzmechanismen automatisch überwacht werden.	
5	Bewertung Konzept zum Schutz vor Schadsoftware bezüglich des Umgangs mit Abweichungen	Das Konzept zum Schutz vor Schadsoftware beschreibt nachvollziehbar, wie Abweichungen automatisch gemeldet werden und wie mit den Meldungen umgegangen wird.	

Prüffall-ID	PFF-C-009
Verdict	

3.1.10 PFF-C-010 Verfügbarkeit der Überwachungssoftware

Prüffall-ID	PFF-C-010		
Anforderungen	ANC-024 (Protokollierung und Überwachung – Verfügbarkeit der Überwachungs-Software [BSI TR-03170-1 Kapitel 2.2.1.10])		
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - 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.		
Vorbedingungen	- Betriebskonzept liegt vor - Protokollierungs- und Überwachungskonzept liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung des Protokollierungs- und Überwachungskonzepts sowie des Betriebskonzepts	Protokollierungs- und Überwachungskonzept sowie Betriebskonzept beschreiben nachvollziehbar, wie die Überwachungskomponenten aufgebaut sind und die Funktionalität des Cloud-Diensts von ihrer Verfügbarkeit unabhängig ist.	

Prüffall-ID	PFF-C-010
Verdict	

3.1.11 PFF-C-011 Umgang mit Schwachstellen, Störungen und Fehlern

Prüffall-ID	PFF-C-011
Anforderungen	ANC-025, ANC-026, ANC-027, ANC-028, ANC-044 (Umgang mit Schwachstellen, Störungen und Fehlern [BSI TR-03170-1 Kapitel 2.2.1.11 & 2.2.1.12], Identifikation von Schwachstellen des Cloud-Dienstes [BSI TR-03170-1 Kapitel 2.2.1.25])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Pen-Tests MÜSSEN zwingend durch unabhängige externe Dritte durchgeführt werden. Internes Personal für Penetrationstests darf die externen Drittendabei unterstützen. - Pen-Tests MÜSSEN mindestens jährlich stattfinden. - Der Cloud-Anbieter MUSS ein Penetrationstestkonzept erstellen, das diese Anforderungen berücksichtigt. - 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 - Die Verfahren zur Identifikation solcher (siehe dazugehörige Basisanforderung von PSS-02) Schwachstellen MÜSSEN darüber hinaus jährliche Code Reviews oder Penetration-Tests durch qualifizierte externe Dritte umfassen.

Prüffall-ID	PFF-C-011		
	- Dieses Vorgehen MUSS durch den Cloud-Anbieter in einem entsprechenden Konzept festgelegt werden.		
Vorbedingungen	- Penetrationstestkonzept liegt vor - Berichte über durchgeführte Pen-Tests liegen vor - Konzept für Schwachstellen- und Patchmanagement liegt vor - Verpflichtungserklärung liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung des Penetrationstestkonzepts	Das Penetrationstestkonzepts beschreibt nachvollziehbar, in welcher Frequenz (mindestens jährlich) welche Pen-Tests und/oder Code Reviews durchgeführt werden und dass sie durch unabhängige Dritte durchgeführt werden.	
2	Bewertung vorliegender Testprotokolle	Aus den Protokollen geht hervor, das bisherige Pen-Tests durch unabhängige Dritte erfolgten.	
3	Bewertung des Konzepts für Schwachstellen- und Patchmanagement	Das Konzept für Schwachstellen- und Patchmanagement beschreibt nachvollziehbar, wie und wann Sicherheitspatches eingespielt werden und enthält eine Selbstverpflichtung zur Umsetzung des Konzepts.	
Verdict			

3.1.12 PFF-C-012 Separierung der Datenbestände in der Cloud-Infrastruktur

Prüffall-ID	PFF-C-012		
Anforderungen	ANC-029 (Separierung der Datenbestände in der Cloud-Infrastruktur [BSI TR-03170-1 Kapitel 2.2.1.13])		
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Die strikte und sichere Separierung der biometrischen Lichtbilder von gemeinsam genutzten virtuellen und physischen Ressourcen SOLLTE durch Zonierung (LUN Bindung und LUN Masking) sichergestellt werden.		
Vorbedingungen	Systemdokumentation des Cloud-Dienstes mit Übersicht über die Architektur des Cloud-Dienstes liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Überprüfung der Dokumentation der Architektur des Cloud-Dienstes hinsichtlich der Trennung der Lichtbilder von gemeinsam genutzten Ressourcen.	Die Dokumentation der Architektur des Cloud-Dienstes stellt die SAN-Architektur unter der Nutzung von Zonierung für die Trennung der gemeinsam genutzten Ressourcen dar.	
Verdict			

3.1.13 PFF-C-013 Überprüfung von Zugriffsberechtigungen

Prüffall-ID	PFF-C-013
Anforderungen	ANC-030, ANC-031 (Regelmäßige Überprüfung der Zugriffsberechtigungen [BSI TR-03170-1 Kapitel 2.2.1.14])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind:

Prüffall-ID	PFF-C-013		
	- 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.		
Vorbedingungen	- Zugriffsberechtigungskonzept liegt vor - Protokolle der Vergabe, Änderung und Überprüfung priviligierter Berechtigungen liegen vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung des Zugriffsberechtigungskonzepts	Das Zugriffsberechtigungskonzept beschreibt den Prozess zur Vergabe und Dokumentation sowie zur halbjährlichen Überprüfung priviligierter Rechte nachvollziehbar.	
2	Bewertung der Protokolle	Die Vergabe, Änderung und Prüfung priviligierter Rechte ist gemäß beschriebenem Prozess dokumentiert.	
Verdict			

3.1.14 PFF-C-014 Vertraulichkeit von Authentisierungsinformationen

Prüffall-ID	PFF-C-014
Anforderungen	ANC-032 (Vertraulichkeit von Authentisierungsinformationen [BSI TR-03170-1 Kapitel 2.2.1.15])
Ziel	Nachweis, dass folgende Anforderung an den Cloud-Dienst erfüllt ist:

Prüffall-ID	PFF-C-014		
	- Die Fotografinnen und Fotografen, die den Cloud-Dienst nutzen, 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.		
Vorbedingungen	- Zugriffsberechtigungskonzept liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung des Zugriffsbereichtigungskonzepts bezüglich der Mitteilung von Authentisierungsinformationen	Das Zugriffsberechtigungskonzept beschreibt nachvollziehbar, dass Authentisierungs-informationen nur bei Vorliegen einer Vertraulichkeitserklärung der Nutzenden mitgeteilt werden.	
Verdict			

3.1.15 PFF-C-015 Transportverschlüsselung

Prüffall-ID	PFF-C-015
Anforderungen	ANC-033 (Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung) [BSI TR-03170-1 Kapitel 2.2.1.16])
Ziel	Nachweis, dass folgende Anforderung an den Cloud-Dienst erfüllt ist: - 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.
Vorbedingungen	Systemdokumentation liegt vor

Prüffall-ID	PFF-C-015		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung Systemdokumentation bezüglich Transportverschlüsselung	Die Systemdokumentation beschreibt nachvollziehbar, dass Daten bei der Übertragung gemäß BSI TR 03116-4 in ihrer aktuellen Fassung stark verschlüsselt werden. Die verwendeten Cipher Suites und die verwendete TLS Version entsprechen den Vorgaben.	
Verdict			

3.1.16 PFF-C-016 Network Access Control

Prüffall-ID	PFF-C-016		
Anforderungen	ANC-034 (Technische Schutzmaßnahmen [BSI TR-03170-1 Kapitel 2.2.1.18])		
Ziel	Nachweis, dass folgende Anforderung an den Cloud-Dienst erfüllt ist: - Der Cloud-Anbieter MUSS mit technischen Maßnahmen sicherstellen, dass seinem (physischen oder virtuellen) Netz keine unbekannten (physischen oder virtuellen) Geräte beitreten.		
Vorbedingungen	- Systemdokumentation liegt vor - Protokollierungs- und Überwachungskonzept liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**

Prüffall-ID	PFF-C-016		
1	Bewertung Systemdokumentation und Protokollierungs- und Überwachungskonzept bezüglich Netzwerkzugriffskontrolle	Systemdokumentation und Protokollierungs- und Überwachungskonzept beschreiben nachvollziehbar, wie die Nutzung des Netzwerks durch unbekannte Geräte verhindert und unberechtigte Zugriffsversuche entdeckt und behandelt werden.	
Verdict			

3.1.17 PFF-C-017 Netzübergreifende Zugriffe

Prüffall-ID	PFF-C-017		
Anforderungen	ANC-035 (Netzübergreifende Zugriffe [BSI TR-03170-1 Kapitel 2.2.1.19])		
Ziel	Nachweis, dass folgende Anforderung an den Cloud-Dienst erfüllt ist: - Jeder Netzperimeter SOLLTE von redundanten und hochverfügbaren Sicherheitsgateways kontrolliert werden.		
Vorbedingungen	Systemdokumentation liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung Systemdokumentation bezüglich Perimeterschutz	Die Systemdokumentation beschreibt nachvollziehbar, dass der Perimeterschutz existiert sowie redundant und hochverfügbar ausgelegt ist.	

Prüffall-ID	PFF-C-017
Verdict	

3.1.18 PFF-C-018 Segregation des Datenverkehrs in gemeinsam genutzten Netzumgebungen

Prüffall-ID	PFF-C-018		
Anforderungen	ANC-036 (Segregation des Datenverkehrs in gemeinsam genutzten Netzumgebungen [BSI TR-03170-1 Kapitel 2.2.1.20])		
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Bei IaaS/PaaS MUSS die sichere Trennung durch physisch getrennte Netze oder durch stark verschlüsselte VLANs sichergestellt werden. Bezüglich der Umsetzung einer starken Verschlüsselung ist die Technische Richtlinie BSI TR-02102-3, in ihrer aktuellsten Fassung zu berücksichtigen.		
Vorbedingungen	Systemdokumentation liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung Systemdokumentation bezüglich Netztrennung	Der Cloud-Service verwendet kein IaaS/PaaS - oder - Die Systemdokumentation beschreibt nachvollziehbar, dass Netztrennung physikalisch oder durch gemäß BSI TR-02102-3, in ihrer aktuellsten Fassung stark verschlüsselte VLANs realisiert ist.	

Prüffall-ID	PFF-C-018
Verdict	

3.1.19 PFF-C-019 Richtlinien zur Entwicklung/Beschaffung von Informationssystemen

Prüffall-ID	PFF-C-019		
Anforderungen	ANC-037, ANC-038 (Richtlinien zur Entwicklung/Beschaffung von Informationssystemen [BSI TR-03170-1 Kapitel 2.2.1.21])		
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Bei der Beschaffung SOLLTEN Produkte vorgezogen werden, die nach den „Common Criteria for Information Technology Security Evaluation“ (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 werden. Eine verschriftlichte Risikobeurteilung MUSS hierzu erstellt werden.		
Vorbedingungen	- Richtlinien zur Entwicklung/Beschaffung von Informationssystemen liegen vor - Systemdokumentation liegt vor - Produktauswahldokumentation liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**

Prüffall-ID	PFF-C-019		
1	Bewertung der Richtlinien zur Entwicklung/Beschaffung von Informationssystemen	Die Richtlinien zur Entwicklung/Beschaffung von Informationssystemen geben vor, verfügbare, nach Common Criteria EAL 4 zertifizierte Produkte anderen vorzuziehen und die Entscheidung, sie nicht zu verwenden, schriftlich mit einer Risikobeurteilung zu begründen.	
2	Bewertung Systemdokumentation bezüglich des Einsatzes von unzertifizierten Produkten mit CC EAL 4 zertifizierten Alternativprodukten und vorliegender Produktauswahldokumentation	Es werden überall da, wo verfügbar, CC EAL 4 zertifizierte Produkte eingesetzt. Die vorgelegte Produktauswahldokumentation ist richtlinienkonform.	
Verdict			

3.1.20 PFF-C-020 Versionskontrolle

Prüffall-ID	PFF-C-020		
Anforderungen	ANC-039 (Versionskontrolle [BSI TR-03170-1 Kapitel 2.2.1.22])		
Ziel	Nachweis, dass folgende Anforderung an den Cloud-Dienst erfüllt ist: - Die Verfahren zur Versionskontrolle MÜSSEN durch geeignete Schutzmaßnahmen sicherstellen, dass die Integrität und Verfügbarkeit der Daten nicht beeinträchtigt werden, wenn Systemkomponenten in ihren vorherigen Zustand zurückversetzt werden.		
Vorbedingungen	Betriebskonzept liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**

Prüffall-ID	PFF-C-020		
1	Bewertung des Betriebskonzepts bezüglich der Versionskontrolle	Das Betriebskonzept beschreibt nachvollziehbar, wie die Integrität und Verfügbarkeit der Daten sichergestellt werden, wenn Komponenten in ihren vorherigen Zustand versetzt werden.	
Verdict			

3.1.21 PFF-C-021 Überwachung der Einhaltung der Anforderungen

Prüffall-ID	PFF-C-021
Anforderungen	ANC-040, ANC-041 (Überwachung der Einhaltung der Anforderungen [BSI TR-03170-1 Kapitel 2.2.1.23])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - 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.
Vorbedingungen	- Betriebskonzept liegt vor

Prüffall-ID	PFF-C-021		
	- Protokollierungs- und Überwachungskonzept liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung des Betriebskonzepts bezüglich Anforderungsüberwachung	Das Betriebskonzept beschreibt nachvollziehbar, mit welchen automatischen Verfahren die Konfigurationen von Systemkomponenten, deren Leistung und Verfügbarkeit, die Reaktionszeit bei Störungen und Vorfällen sowie der Wiederherstellungszeit überwacht werden.	
2	Bewertung Protokollierungs- und Überwachungskonzept bezüglich Anforderungsüberwachung	Das Protokollierungs- und Überwachungskonzept beschreibt nachvollziehbar, wie Abweichungen gemeldet und behandelt werden.	
Verdict			

3.1.22 PFF-C-022 Richtlinie für den Umgang mit Sicherheitsvorfällen

Prüffall-ID	PFF-C-022
Anforderungen	ANC-042, ANC-043 (Richtlinie für den Umgang mit Sicherheitsvorfällen [BSI TR-03170-1 Kapitel 2.2.1.24])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Bei einem Sicherheitsvorfall MÜSSEN Daten beweisfest gesammelt werden.

Prüffall-ID	PFF-C-022		
	- Es MÜSSEN für typische (Die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten ist nicht mehr gegeben, wie z.B. bei Verlust von Hardware, Verlust von Passwörtern, Befall mit Schadcode, Denial-of-Service oder Fehlkonfiguration mit möglichem Datenabfluss) Sicherheitsvorfälle Analysepläne existieren, um die Beweiskraft für die spätere juristische Würdigung zu erhalten. - Das Vorgehen MUSS in einem Betriebskonzept beschrieben und festgelegt werden.		
Vorbedingungen	Betriebskonzept liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung Betriebskonzept bezüglich des Umgangs mit Sicherheitsvorfällen	Das Betriebskonzept beschreibt nachvollziehbar, wie Daten von Sicherheitsvorfällen beweissicher gesammelt werden. Es enthält Analysepläne für typische Sicherheitsvorfälle.	
Verdict			

3.1.23 PFF-C-023 Frontend und Backend

Prüffall-ID	PFF-C-023
Anforderungen	ANC-045, ANC-046, ANC-047, ANC-048, ANC-049 (Frontend und Backend [BSI TR-03170-1 Kapitel 2.3])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - 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.

Prüffall-ID	PFF-C-023		
	- 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 und Verordnungen (etwa PassV, PAuswV, PassDEÜV, AufenthV). - Nutzerkennungen - Pseudonyme (z.B. im Sinne des DKK siehe [BSI TR-03170-1] Kapitel 2.6)		
Vorbedingungen	- Die Systemdokumentation des Cloud-Dienstes mit Übersicht der Softwarearchitektur liegt vor.		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung der Systemdokumentation bezüglich der Speicherung der Lichtbilder	Der Prozess zur Speicherung der Bilder wird in der Systemdokumentation nachvollziehbar beschrieben. Dafür ist ein eigener Prozess mit eigenem Prozess-User vorgesehen.	
2	Bewertung der Systemdokumentation bezüglich der Kommunikation mit Dienstleistern	In der Systemdokumentation ist nachvollziehbar beschrieben, dass die Kommunikation mit Dienstleistern ausschließlich über das Front-End abläuft.	
3	Bewertung der Systemdokumentation bezüglich des Zugriffs auf das Backend	In der Systemdokumentation ist nachvollziehbar beschrieben, dass kein direkter Zugriff auf das Backend möglich ist.	

Prüffall-ID	PFF-C-023		
4	Bewertung der Systemdokumentation bezüglich der Kommunikation zwischen Serverkomponenten	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die Kommunikation zwischen Serverkomponenten gesichert ist. Die Absicherungen erfolgt gemäß Empfehlungen der BSI TR-03116-4, in ihrer aktuellsten Fassung. Die verwendeten Cipher Suites und die verwendete TLS Version entsprechen den Vorgaben.	
5	Bewertung der Systemdokumentation bezüglich der gespeicherten Daten	In der Systemdokumentation ist nachvollziehbar beschrieben, welche Daten vom Cloud-Dienst gespeichert werden. Sie umfassen das verschlüsselte Bild sowie die geforderten Metadaten.	
Verdict			

3.1.24 PFF-C-024 Protokollierung

Prüffall-ID	PFF-C-024
Anforderungen	ANC-050, ANC-051 (Protokollierung [BSI TR-03170-1 Kapitel 2.4])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - 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 (etwa PassV, PAuswV, PassDEÜV, AufenthV). - Protokollierungsdaten MÜSSEN gegen Veränderungen und Austausch von Protokollinhalten geschützt sein.

Prüffall-ID	PFF-C-024		
Vorbedingungen	- Protokollierungs- und Überwachungskonzept liegt vor - Erfüllungserklärung liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung der Erfüllungserklärung	Der Anbieter des Cloud-Dienstes erklärt, PassV, PAuswV, PassDEÜV, AufenthV einzuhalten.	
2	Bewertung des Protokollierungs- und Überwachungskonzepts bezüglich des Inhaltsschutzes	Im Protokollierungs- und Überwachungskonzept ist nachvollziehbar beschrieben, wie die Protokollierungsdaten gegen Veränderung und Austausch von Protokollinhalten geschützt sind.	
Verdict			

3.1.25 PFF-C-025 Registrierungsprozess

Prüffall-ID	PFF-C-025
Anforderungen	ANC-001, ANC-052, ANC-053, ANC-054, ANC-055, ANC-056, ANC-057, ANC-058, ANC-059, ANC-060, ANC-061, ANC-062, ANC-063, ANC-064, ANC-065 (Prozess [BSI TR-03170 Kapitel 2.4.2], Registrierungsprozess [BSI TR-03170-1 Kapitel 2.5])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Dienstleister (z. B. Fotografinnen und Fotografen) MÜSSEN sich bei dem Cloud-Dienst registrieren, da nur registrierte Dienstleister Lichtbilder zu diesem übertragen dürfen.

Prüffall-ID	PFF-C-025
	- Es MUSS ein Registrierungsprozess implementiert werden, der es dem Dienstleister ermöglicht, bei einem Cloud-Anbieter ein Dienstleisterkonto 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 (PAuswG), des § 12 des eID-Karte-Gesetzes (eIDKG), des § 78 Absatz 5 des Aufenthaltsgesetzes (AufenthG) genügt oder einem anderen elektronischen Identifizierungsmittel entspricht, das gemäß Artikel 6 der Verordnung (EU) Nr. 910/2014 (eIDAS) auf dem Sicherheitsniveau „hoch“ notifiziert wurde. - Darüber hinaus MUSS ein Verfahren etabliert werden, das die Entgegennahme und Prüfung des Nachweises der Dienstleistereigenschaft (gemäß den Vorgaben aus (PassV), (PAuswV), (PassDEÜV), (AufenthV) während des Erstregistrierungsverfahrens ermöglicht. Die Person, die das Erstregistrierungsverfahren durchführt, wird zum Hauptkontoinhaber, trägt die primäre Verantwortung für das Dienstleisterkonto und sollte daher in der Regel nicht aus dem Dienstleisterkonto entfernt werden können. - Sollte eine Änderung der primären Verantwortung für ein Dienstleisterkonto 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. - Neben dem Hauptnutzer KÖNNEN weitere Administratoren mit vergleichbaren Berechtigungen für ein Dienstleisterkonto hinterlegt werden. Die Berechtigungen/Rolle zur Administration DARF NUR vom Hauptnutzer oder einem anderen Administrator erteilt werden. - Beim Anlegen des Dienstleisterkontos MUSS eine eindeutige UUID v4 gemäß (ISO/IEC 9834-8) erzeugt und eindeutig und dauerhaft mit dem Dienstleisterkonto verknüpft werden. - Zusätzlich MÜSSEN die Mitarbeiter des Dienstleisters die Möglichkeit haben, eine Nutzerregistrierung innerhalb des Dienstleisterkontos durchzuführen. Die Zugehörigkeit zu dem Dienstleisterkonto 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 (Mindestdatensatz des notifizierten elektronischen Identifizierungsmittels gem. Art. 11 Durchführungsverordnung (EU) 2015/1501) erhoben und beim Cloud-Anbieter gespeichert werden. Dies gilt sowohl für den Dienstleister als auch für dessen Mitarbeiter.

Prüffall-ID	PFF-C-025		
	- 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. - 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. - 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 eIDAS] 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.		
Vorbedingungen	- Die Systemdokumentation des Cloud-Dienstes mit Übersicht der Softwarearchitektur liegt vor. - Der Registrierungsprozess ist implementiert und aktiviert. - Der Kontoverwaltungsprozess ist implementiert und aktiviert. - Identifizierungsmittel auf dem Sicherheitsniveau "hoch" liegen für Test-Personen für die Erstregistrierung als Dienstleister vor. - Nachweise der Dienstleistereigenschaft für die zu Testzwecken zu registrierenden Dienstleister liegen vor.		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**

Prüffall-ID	PFF-C-025		
1	Bewertung der Systemdokumentation bezüglich der Registrierung und Anmeldung von Dienstleistern.	Der Registrierungs- sowie Anmeldeprozess wird in der Systemdokumentation nachvollziehbar dargestellt. Die Anmeldung ist nur registrierten Dienstleistern möglich.	
2	Bewertung der Systemdokumentation bezüglich des Registrierungsprozesses für Dienstleister.	In der Systemdokumentation ist nachvollziehbar beschrieben, wie sich Dienstleister anforderungsgemäß beim Cloud-Dienst registrieren können.	
3	Durchführung des Registrierungsprozesses mit 3 Personen als Dienstleister	Der in der Systemdokumentation beschriebene Registrierungsprozess ist implementiert und funktioniert fehlerfrei.	
4	Bewertung der Systemdokumentation bezüglich des Dienstleisternachweises	In der Systemdokumentation ist nachvollziehbar beschrieben, wie bei der Registrierung die Dienstleistereigenschaft nachgewiesen und überprüft wird.	
5	Durchführung des Registrierungsprozesses mit gültigen und ungültigen Dienstleisternachweisen	Der in der Systemdokumentation beschriebene Registrierungsprozess ist implementiert und der Nachweis und die Überprüfung der Dienstleistereigenschaft funktionieren in der Praxis.	
6	Prüfung des Kontomanagements bezüglich der Löschung des Hauptkontoinhabers	Der Hauptkontoinhaber kann nicht gelöscht werden.	
7	Bewertung der Systemdokumentation bezüglich der Überprüfung der Zugehörigkeit des Hauptkontoinhabers	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die Unternehmenszugehörigkeit eines neuen Hauptkontonutzers nachgewiesen und überprüft wird.	

Prüffall-ID	PFF-C-025		
8	Änderung des Hauptkontonutzers eines Dienstleisters	Die in der Systemdokumentation beschriebene Überprüfung der Unternehmenszugehörigkeit ist in der Praxis umgesetzt.	
9	Bewertung der Systemdokumentation bezüglich der Überprüfung des Identitätsmittels	In der Systemdokumentation ist nachvollziehbar beschrieben, wie überprüft wird, dass die Identität der sich registrierenden Person mit den Angaben des Identifizierungsmittels übereinstimmt.	
10	Durchführung des Registrierungsprozesses mit gültigen und ungültigen Identitätsnachweisen	Die in der Systemdokumentation beschriebene Identitätsüberprüfung funktioniert in der Praxis.	
11	Bewertung der Systemdokumentation bezüglich der Vergabe von Administrationsrechten.	In der Systemdokumentation ist nachvollziehbar beschrieben, wie sichergestellt wird, dass nur der Hauptnutzer oder ein Administrator anderen Nutzern Administrationsrechte erteilen kann.	
12	Bewertung der Systemdokumentation bezüglich der UUID des Dienstleisterkontos	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die UUID des Dienstleisterkontos erzeugt und damit verknüpft wird.	
13	Bewertung der Systemdokumentation bezüglich der Nutzerregistrierung innerhalb eines Dienstleisterkontos.	In der Systemdokumentation ist nachvollziehbar beschrieben, wie zusätzliche Nutzer eines Dienstleisters registriert werden können.	
14	Durchführung der Registrierung eines zusätzlichen Nutzers für einen existierenden Dienstleister	Die in der Systemdokumentation beschriebene Nutzerregistrierung ist implementiert und funktioniert inklusive der Überprüfung der Identifizierungsmittel in der Praxis.	
15	Bewertung der Systemdokumentation bezüglich der Erhebung und Speicherung der notwendigen	In der Systemdokumentation ist nachvollziehbar beschrieben, welche Daten zur	

Prüffall-ID	PFF-C-025		
	Daten für die eindeutige Identifizierung eines (Haupt-) Nutzers	Nutzeridentifizierung erhoben und gespeichert werden. oder ob hierfür vorhandene Datensätze genutzt und die Daten abgeglichen werden.	
16	Durchführung der Erstregistrierung eines Dienstleisters mit einem Haupt-Nutzer und einem zusätzlichen Mitarbeiter.	Die für die Identifizierung notwendigen Daten werden wie beschrieben erhoben und gespeichert oder mit vorhandenen Daten abgeglichen werden.	
17	Bewertung der Systemdokumentation bezüglich des Nutzer-Pseudonyms	In der Systemdokumentation ist nachvollziehbar beschrieben, wie Nutzer ihr Pseudonym erhalten und es mit dessen Daten verknüpft wird.	
18	Durchführung der Erstregistrierung eines Dienstleisters mit einem Haupt-Nutzer und einem zusätzlichen Mitarbeiter.	Die Pseudonyme der Nutzer werden wie beschrieben mit den Nutzerdaten verknüpft.	
19	Bewertung der Systemdokumentation bezüglich des Bezugs der Nutzer-Pseudonyme von den elektronischen Identifizierungsmitteln	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die Pseudonyme von den elektronischen Identifizierungsmitteln bezogen werden. Für deutsche Dokumente wird die Pseudonymfunktion (rID) der eID verwendet, für solche nach Artikel 6 der Verordnung (EU) Nr. 910/2014 wird das Pseudonym über das eIDAS-Framework bezogen.	
20	Durchführung der Erstregistrierung eines Dienstleisters mit einem Haupt-Nutzer und einem zusätzlichen Mitarbeiter.	Die Pseudonyme der Nutzer werden wie beschrieben von den elektronischen Identifizierungsmitteln bezogen.	

Prüffall-ID	PFF-C-025		
21	Bewertung der Systemdokumentation bezüglich der UUID des Nutzeraccounts	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die UUID des Nutzeraccounts erzeugt und damit verknüpft wird.	
22	Bewertung der Systemdokumentation bezüglich der Änderung von elektronischen Identifizierungsmitteln der Nutzer	In der Systemdokumentation ist nachvollziehbar beschrieben, wie zusätzliche Pseudonyme beim Wechsel elektronischer Identifizierungsmittel bezogen und gespeichert werden, während die Verknüpfung zu vorherigen Pseudonymen bestehen bleibt.	
23	Durchführung der Änderung des elektronischen Identifizierungsmittels eines Nutzers eines bestehenden Dienstleisters	Das Pseudonym des neuen Identifizierungsmittels wird wie beschrieben zusätzlich mit den Nutzerdaten verknüpft.	
Verdict			

3.1.26 PFF-C-026 Nachvollziehbarkeit/Verantwortlichkeit beim Upload

Prüffall-ID	PFF-C-026
Anforderungen	ANC-066, ANC-067, ANC-068, ANC-069, ANC-070, ANC-071, ANC-072 (Nachvollziehbarkeit/Verantwortlichkeit beim Upload [BSI TR-03170-1 Kapitel 2.6])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Es MUSS eine eindeutige UUID v4 gemäß (ISO/IEC 9834-8) erzeugt und eindeutig und dauerhaft mit dem Cloud-Dienst verknüpft werden. Diese dient bei der Erzeugung der Nutzerkennung der eindeutigen Identifizierung des Cloud-Dienstes.

Prüffall-ID	PFF-C-026		
	- Für die Nachvollziehbarkeit der Herkunft eines Lichtbilds MUSS eine Nutzerkennung aus den vorliegenden UUIDs der Cloud, des Dienstleisterkontos 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 (PAuswG), des § 12 des eID-Karte-Gesetzes (eIDKG), des § 78 Absatz 5 des Aufenthaltsgesetzes (AufenthG) genügen oder einem anderen elektronischen Identifizierungsmittel entsprechen, dass gemäß Artikel 6 der Verordnung (EU) Nr. 910/2014 (eIDAS) 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 Dienstleisterkonto erstellt worden ist und eine Nutzerregistrierung stattgefunden hat. - Für eine Anmeldung am Dienstleisterkonto MUSS eine Authentisierung auf dem Vertrauensniveau "hoch" gemäß den Anforderungen nach BSI TR-03107-1 in ihrer aktuellsten Fassung genutzt werden.		
Vorbedingungen	- Systemdokumentation liegt vor - Ein biometrisches Lichtbild liegt vor - Es gibt im Cloud-Dienst registrierte (Test-) Dienstleister - (Test-)Version einer Dienstleister-Software ist betriebsbereit - Der Cloud-Dienst ist betriebsbereit		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**

Prüffall-ID	PFF-C-026		
1	Bewertung der Systemdokumentation bezüglich der UUID des Cloud-Dienstes	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die UUID des Cloud-Dienstes erzeugt und damit verknüpft wird.	
2	Bewertung der Systemdokumentation bezüglich der Übertragung des Lichtbilds mit Nutzerkennung an eine Behörde	In der Systemdokumentation ist nachvollziehbar beschrieben, wie das Lichtbild mit der Nutzerkennung (gebildet aus den durch ":::" getrennte UUIDs des Cloud-Dienstes, des Hauptnutzers des Dienstleisters und des hochladenden Nutzers) kombiniert an die Behörde gesendet wird.	
3	Bewertung der Systemdokumentation bezüglich der Erzeugung und Signierung eines Hashwerts des Lichtbildes und der Nutzerkennung	In der Systemdokumentation ist nachvollziehbar beschrieben, wie vom Lichtbild mit der Nutzerkennung ein SHA-256 Hashwert erzeugt und mit dem im DVDV hinterlegten Zertifikat des Cloud -Dienstes signiert bzw. gesiegelt wird.	
4	Bewertung der Systemdokumentation bezüglich Nutzer-Identifizierung vor Übermittlung eines Lichtbilds	In der Systemdokumentation ist nachvollziehbar beschrieben, wie der Identifitätsnachweis vor der Übermittlung des Lichtbilds durch den Dienstleister erfolgt.	
5	Hochladen eines Lichtbilds in die Cloud durch einen (Test-)Dienstleister	Die Identifikation des Nutzers erfolgt anforderungsgemäß.	
6	Bewertung der Systemdokumentation bezüglich der Verwendung des Pseudonyms zur Nutzer-Authentisierung.	In der Systemdokumentation ist nachvollziehbar beschrieben, dass nur das Pseudonym des verwendeten Identitätsnachweises zur Authentisierung herangezogen wird.	

Prüffall-ID	PFF-C-026		
7	Bewertung der Systemdokumentation bezüglich des Vertrauensniveaus der Authentisierung	In der Systemdokumentation ist nachvollziehbar beschrieben, dass eine Authentisierung auf Vertrauensniveau "hoch" gemäß BSI TR-03107-1, in ihrer aktuellsten Fassung verwendet wird. Der Anbieter erklärt die Konformität zur BSI TR-03107-1.	
Verdict			

3.1.27 PFF-C-027 Kommunikationswege

Prüffall-ID	PFF-C-027		
Anforderungen	ANC-073, ANC-074 (Kommunikationswege [BSI TR-03170-1 Kapitel 2.7])		
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Der Cloud-Anbieter MUSS Verfahren implementieren, welche die internen und externen Kommunikationswege sichern und deren Integrität und Vertraulichkeit sichern. 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.		
Vorbedingungen	- Systemdokumentation liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**

Prüffall-ID	PFF-C-027		
1	Bewertung der Systemdokumentation bezüglich der Transportabsicherung	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die Vorgaben und Empfehlungen der BSI TR-03116-4, in ihrer aktuellsten Fassung zur Transportsicherung erfüllt werden. Die verwendeten Cipher Suites und die verwendete TLS Version entsprechen den Vorgaben.	
2	Bewertung der Systemdokumentation bezüglich der Datenübertragung	In der Systemdokumentation ist nachvollziehbar beschrieben, dass die Datenübertragung zwischen Cloud-Dienst einerseits und Dienstleistern bzw. Behörden andererseits synchron erfolgt.	
Verdict			

3.1.28 PFF-C-028 Aufbau einer Verbindung im Rahmen einer Nutzer Session

Prüffall-ID	PFF-C-028
Anforderungen	ANC-075, ANC-076, ANC-077, ANC-078, ANC-079, ANC-080 (Aufbau einer Verbindung im Rahmen einer Nutzer Session [BSI TR-03170-1 Kapitel 2.7.1])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Das Sessionhandling SOLLTE mittels sicherer Frameworks (siehe dazu auch [BSI TR-03170-2] Kapitel 2.4.2) realisiert werden. - Session-Identifier MÜSSEN als sensitive Daten geschützt werden. - Session-Identifier DÜRFEN NICHT unverschlüsselt auf permanenten Speichermedien abgelegt werden.

Prüffall-ID	PFF-C-028		
	- Die Anwendung MUSS die Anwendungssitzung nach einem angemessenen Session-Timeout (maximal 30 Minuten), gemäß aktueller Best-Practice-Empfehlungen, aktiv beenden. - Beim Upload eines Lichtbilds MUSS die Session nach dem Upload sofort wieder beendet werden. - Wird eine Anwendungssitzung beendet, MUSS die Anwendung den Session-Identifier, sowohl auf dem Endgerät als auch in der Cloud, sicher löschen.		
Vorbedingungen	- Systemdokumentation liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung der Systemdokumentation bezüglich des Sessionhandlings	In der Systemdokumentation ist nachvollziehbar beschrieben, wie das Sessionhandling mittels sicherer Frameworks erfolgt.	
2	Bewertung der Systemdokumentation bezüglich der Behandlung von Session-Identifiern	In der Systemdokumentation ist nachvollziehbar beschrieben, wie das Session-Identifier geschützt werden.	
3	Bewertung der Systemdokumentation bezüglich der Speicherung von Session-Identifiern	In der Systemdokumentation ist nachvollziehbar beschrieben, dass Session-Identifier nicht unverschlüsselt auf permanenten Datenträgern abgelegt werden.	
4	Bewertung der Systemdokumentation bezüglich des Session-Timeouts	In der Systemdokumentation ist nachvollziehbar beschrieben, dass Sessions nach maximal 30 Minuten Inaktivität beendet werden.	
5	Bewertung der Systemdokumentation bezüglich des Session-Endes nach Upload	In der Systemdokumentation ist nachvollziehbar beschrieben, dass Sessions nach dem Upload eines Lichtbilds beendet werden.	

Prüffall-ID	PFF-C-028		
6	Bewertung der Systemdokumentation bezüglich der Löschung des Session-Identifiers	In der Systemdokumentation ist nachvollziehbar beschrieben, wie Session-Identifier nach Session-Ende sicher gelöscht werden.	
Verdict			

3.1.29 PFF-C-029 Erzeugung von Zufallszahlen

Prüffall-ID	PFF-C-029
Anforderungen	ANC-081, ANC-082, ANC-083, ANC-084, ANC-085 (Erzeugung von Zufallszahlen [BSI TR-03170-1 Kapitel 2.7.2])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Für Zufallszahlengeneratoren MUSS die BSI TR-02102-1 in ihrer aktuellsten Fassung berücksichtigt werden. - Alle Zufallswerte MÜSSEN über einen sicheren kryptografischen Zufallszahlengenerator erzeugt werden. Das Frontend MUSS Zufallszahlen von einem Zufallszahlengenerator mit hoher Entropie beziehen. - Das Frontend SOLLTE dem Zufallszahlengenerator einen Startwert (Seed) zuweisen, der sich aus mindestens drei voneinander unabhängigen Systemparametern zusammensetzt. - Die Parameter SOLLTEN von außerhalb des Frontends nicht ermittelbar sein. - Das Frontend SOLLTE bei Erstellung eines Startwerts (Seed) für den Zufallszahlengenerator einen geeigneten Zufall vom Backend beziehen.
Vorbedingungen	- Systemdokumentation liegt vor - Cloud-Dienst ist betriebsbereit

Prüffall-ID	PFF-C-029		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung der Systemdokumentation bezüglich des verwendeten Zufallsgenerators	In der Systemdokumentation ist nachvollziehbar beschrieben, welcher Zufallszahlengenerator eingesetzt wird.	
2	Prüfung der Systemdokumentation bezüglich Sicherheit und Entropie des Zufallsgenerators	In der Systemdokumentation ist nachvollziehbar beschrieben, wie der Einsatz eines anderen als des vorgesehenen Zufallszahlengenerators verhindert wird.	
3	Prüfung der Systemdokumentation bezüglich des Startwerts.	In der Systemdokumentation ist nachvollziehbar beschrieben, dass dem Zufallsgenerator ein aus mindestens drei voneinander unabhängigen Systemparametern zusammengesetzter Startwert zugewiesen wird.	
4	Prüfung der Systemdokumentation bezüglich der Absicherung der Zufallsgenerator-Parameter.	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die Parameter vor Ermittlung von außerhalb der Anwendung geschützt werden.	
5	Prüfung der Systemdokumentation bezüglich des Bezugs eines Zufalls vom Backend.	In der Systemdokumentation ist nachvollziehbar beschrieben, dass das Frontend vom Backend einen Zufall für die Erstellung des Startwerts bezieht.	
Verdict			

3.1.30 PFF-C-030 Kommunikationswege Dienstleister – Cloud

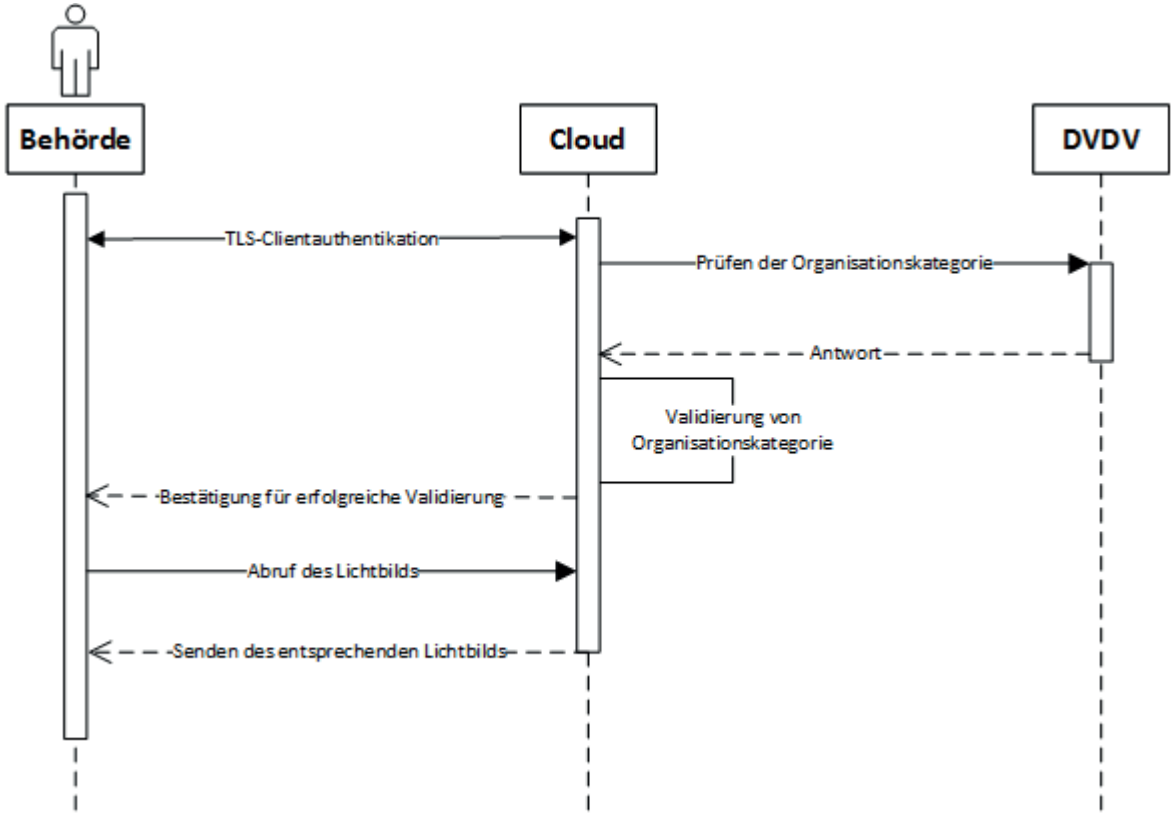
Prüffall-ID	PFF-C-030
Anforderungen	ANC-086, ANC-087, ANC-088, ANC-089, ANC-090, ANC-091 (Kommunikationswege Dienstleister (z. B. Fotografinnen und Fotografen) – Cloud (Upload) [BSI TR-03170-1 Kapitel 2.7.3])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Für die inhaltliche 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. - Die durch den Verordnungstext geforderte Anmeldung des Dienstleisters mit der eID oder einem anderen elektronischen Identifizierungsmittel auf dem Vertrauensniveau „hoch“ (gemäß Kapitel 2.6) beim Cloud-Anbieter MUSS vor der Übertragung des Lichtbilds zur Cloud erfolgen. Der Request (siehe [BSI TR-03170] Kapitel 2.4.2) von der Anwendung des Dienstleisters SOLLTE, sofern ein Authentifizierungsmittel genutzt wird, was dies unterstützt, über einen mittels Kanalbindung nach BSI TR-03124 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.
Vorbedingungen	- Systemdokumentation liegt vor - Ein biometrisches Lichtbild liegt vor - Es gibt im Cloud-Dienst registrierte (Test-) Dienstleister - (Test-Version) einer Dienstleister-Software ist betriebsbereit - Der Cloud-Dienst ist betriebsbereit

Prüffall-ID	PFF-C-030		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung der Systemdokumentation bezüglich Kryptographie	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die Vorgaben und Empfehlungen der BSI TR-03116-4, in ihrer aktuellsten Fassung erfüllt werden. Die verwendeten Cipher Suites und die verwendete TLS Version entsprechen den Vorgaben.	
2	Bewertung der Systemdokumentation und bezüglich Signaturen und Siegeln	In der Systemdokumentation ist nachvollziehbar beschrieben, dass mindestens fortgeschrittene elektronische Signaturen und Siegel gemäß der Leitlinie für digitale Signatur-/ Siegel-, Zeitstempelformate sowie technische Beweisdaten (Evidence Record), in ihrer aktuellsten Fassung verwendet werden.	
3	Bewertung der Systemdokumentation bezüglich Kanalbindung	In der Systemdokumentation ist nachvollziehbar beschrieben, dass Requests über einen mittels Kanalbindung nach BSI TR-03124, siehe Kapitel 2.9 gesicherten TLS Kanal empfangen werden.	
4	Bewertung der Systemdokumentation bezüglich des Lichtbildidentifiers	In der Systemdokumentation ist nachvollziehbar beschrieben, wie der Lichtbildidentifier beim Upload gemäß ISO/IEC 9834-8 erzeugt und an die Dienstleister-Anwendung zurückgegeben wird. Der Anbieter erklärt die Konformität zur ISO/IEC 9834-8.	
5	Bewertung der Systemdokumentation bezüglich der Bestätigung der Speicherung des Lichtbilds	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die Bestätigung der Speicherung	

Prüffall-ID	PFF-C-030		
		unter dem zurückgemeldeten Lichtbildidentifier erfolgt.	
6	Bewertung auf geeignete technische Weise anhand von 3 Beispieldaten.	Die Bestätigung erfolgt in allen Fällen wie dokumentiert mit Angabe des Lichtbildidentifiers.	
Verdict			

3.1.31 PFF-C-031 Kommunikation Cloud – Behörde DVDV

Prüffall-ID	PFF-C-031
Anforderungen	ANC-092 (Kommunikation Cloud – Behörde DVDV [BSI TR-03170-1 Kapitel 2.7.4])
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: 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. Die Prüfung der genutzten Zertifikate gemäß Kapitel 2.8.2 MUSS vor dem Verbindungsaufbau erfolgen. 2. Die Behörde sendet einen Request zum Abruf des Lichtbildes mit der aus dem Barcode ausgelesenen eindeutigen ID des Lichtbildes in der Cloud. 3. Die Cloud prüft per DVDV-findCategories-Anfrage unter Verwendung des Organisationsschlüssels der anfragenden Behörde die Behördenkategorie auf Pass-, Personalausweis oder Ausländerbehörde. 4. Prüfung der Behördenkategorie: a) Bei erfolgreicher Prüfung der Behördenkategorie liefert die Cloud eine Statusmeldung zur erfolgreich abgeschlossenen Prüfung der Behörde zurück.

Prüffall-ID	PFF-C-031
	b) Bei nicht erfolgreicher Prüfung liefert die Cloud eine Fehlermeldung und einen entsprechenden Fehler-Status "falsche" Organisationskategorie zurück und die Verbindung wird abgebaut. 5. Die Cloud sendet das zu der ID gehörende verschlüsselte Lichtbild sowie weitere Daten nach dieser Technischen Richtlinie (siehe [BSI TR-03170-1] Kapitel 2.8.2) an die Behörde. 6. Die Verbindung wird abgebaut.  - Der Vorgang der Löschung eines Lichtbilds MUSS analog zu dem oben beschriebenen Vorgang als neuer Request realisiert werden.
Vorbedingungen	- Systemdokumentation liegt vor.

Prüffall-ID	PFF-C-031		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung der Systemdokumentation bezüglich des Verbindungsaufbaus zwischen Behörde und Cloud	In der Systemdokumentation ist nachvollziehbar beschrieben, wie der Verbindungsaufbau zwischen Cloud und Behörde mittels TLS-Client-Authentication unter den Vorgaben der TR-03116-4 von statten geht. Dabei werden die im DVDV hinterlegten Zertifikate verwendet. Dies wird vor dem Verbindungsaufbau geprüft. Es wird genau auf Erfolgs- und Fehlermeldungen eingegangen. Die Fehlermeldungen sind dabei selbsterklärend. Der beschriebene Verbindungsaufbau entspricht der Beschreibung aus TR-03170-1 (s.o.).	
2	Bewertung der Systemdokumentation bezüglich der Berechtigungsprüfung einer Behörde	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die Berechtigung der Behörde an Hand des Organisationsschlüssels mit dem DVDV findCategories) überprüft wird. Dabei wird auch geprüft, ob der Organisationsschlüssel und das genutzte Behördenzertifikat zusammenpassen (Gehört der Organisationschlüssel zu der Behörde, auf die das Zertifikat ausgestellt ist). Die Behörde muss im DVDV als eine Pass-, Personalausweis- oder Ausländerbehörde eingetragen sein. Die Systemdokumentation beschreibt die Meldungen im Erfolgs und im Fehlerfall.	

3.1.32 PFF-C-032 Kommunikation mit dem DVDV

Prüffall-ID	PFF-C-032		
Anforderungen	ANC-093, ANC-094 (Kommunikation mit dem DVDV [BSI TR-03170-1 Kapitel 2.8.1])		
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - Die benötigten Daten MÜSSEN grundsätzlich immer aktuell aus dem DVDV-System bezogen werden. 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. - Das Cloudzertifikat, das 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.		
Vorbedingungen	- Die Systemdokumentation mit Übersicht der Softwarearchitektur liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung der Systemdokumentation bezüglich des Cachings von DVDV-Einträgen.	In der Systemdokumentation ist nachvollziehbar beschrieben, das die vorgegebenen maximalen Caching-Zeiten nicht überschritten werden.	
2	Bewertung der Systemdokumentation bezüglich des Cloudzertifikats	In der Systemdokumentation ist nachvollziehbar beschrieben, dass ein von CAs der PKI-1-Verwaltung (BSI PKI-1-Verwaltung) ausgestelltes Zertifikat als Signatur, Siegel und zum Verbindungsaufbau mit dem DVDV verwendet wird.	

Prüffall-ID	PFF-C-032
Verdict	

3.1.33 PFF-C-033 Sichere Datenlöschung

Prüffall-ID	PFF-C-033		
Anforderungen	ANC-095 (Sichere Datenlöschung [BSI TR-03170-1 Kapitel 2.8.3])		
Ziel	Nachweis, dass folgende Anforderungen an den Cloud-Dienst erfüllt sind: - 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 Cloud-Anbieter 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.		
Vorbedingungen	- Systemdokumentation liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**

Prüffall-ID	PFF-C-033		
1	Bewertung der Systemdokumentation bezüglich der Löschfristen	In der Systemdokumentation ist nachvollziehbar beschrieben, wie die Daten (Lichtbilder) nach welchen Löschfristen gelöscht werden, falls der Bürger deren Löschung nicht bereits durch die Behörde beauftragt hat.	
Verdict			

3.2 Software

3.2.1 PFF-S-001 Funktionale Anforderungen an Up- und Download des Bildes

Prüffall-ID	PFF-S-001
Anforderungen	ANS-001 (Prozess [BSI TR-03170 Kapitel 2.4.2])
Ziel	Nachweis, dass folgende Anforderung an die Software erfüllt ist: Im Rahmen der sicheren digitalen Lichtbildübermittlung MUSS die Software folgende Prozessschritte unterstützen: 1. Die Bürgerin/der Bürger lässt vom registrierten Dienstleister ein biometrisches Lichtbild erstellen. (Bei der Erstellung des Lichtbilds KÖNNEN Meta-Informationen zur Aufnahme, z. B. Marke/Modell der Aufnahmeeinheit, verwendete Software, etc. eingebracht werden). **(Dieser Schritt ist nicht zertifizierungsrelevant)** 2. Das ausgewählte Lichtbild wird kodiert (siehe [BSI TR-03170-2] Kapitel 2.1). (**Wird geprüft in PFF-S-002**) 3. Der symmetrische Schlüssel wird erzeugt. 4. Das Lichtbild wird mit dem symmetrischen Schlüssel verschlüsselt.

Prüffall-ID	PFF-S-001		
	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 [BSI TR-03170-1] Kapitel 2.6) beim Cloud-Anbieter 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.		
Vorbedingungen	- Ein biometrisches Lichtbild liegt vor - Dienstleister ist im Cloud-Dienst registriert und Cloud-Dienst im DVDV eingetragen - Software ist betriebsbereit - Cloud-Dienst ist betriebsbereit - Verschlüsselung ist eingerichtet - Uploadschnittstelle ist vorhanden und dokumentiert - Testuser Dienstleister sind eingerichtet		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Prüfung Berechtigung des Nutzers: Zugriff durch unberechtigten Nutzer	Es ist nicht möglich ein Lichtbild zu Uploaden ohne sich vorher mit der eID oder einem anderen elektronischen Identifizierungsmittel auf dem Vertrauensniveau „hoch“ (gemäß [BSI TR-03170-1] Kapitel 2.6 anzumelden.	
2	Prüfung des verschlüsselten Uploads	Sowohl der symmetrische Schlüssel als auch der Barcode können erzeugt und das Lichtbild mit dem Schlüssel verschlüsselt werden.	

Prüffall-ID	PFF-S-001		
		Das verschlüsseltes Lichtbild liegt nach dem Upload im Backend des Cloud-Dienstes vor.	
3	Prüfung Ausgabe Barcode	Der Barcode kann durch die Software ausgedruckt werden.	
Verdict			

3.2.2 PFF-S-002 Bildkonformität

Prüffall-ID	PFF-S-002		
Anforderungen	ANS-002 (Bildkonformität [BSI TR-03170-2 Kapitel 2.1])		
Ziel	Nachweis, dass folgende Anforderung an die Software erfüllt ist: - Für das final zu übermittelnde Lichtbild MÜSSEN die Anforderungen der BSI TR-03121, Part 3, Volume 2, Application Profile"Facial Image Digital-Delivery via Cloud" [BSI TR-03170] bereits zum Zeitpunkt des Uploads des Lichtbildes erfüllt werden. Zusätzlich SOLLTEN Metadaten, die zu diesem Zeitpunkt zum Lichtbild vorliegen NICHT gelöscht werden.		
Vorbedingungen	Software ist betriebsbereit		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Bewertung der Systemdokumentation bezüglich der Erzeugung Umwandlung/Kodierung des Lichtbilds nach den Vorgaben der TR-03121.	Die Systemdokumentation beschreibt die Umwandlung/Kodierung des Lichtbilds gemäß den Vorgaben der TR-03121-3.2. Der Anbieter erklärt die Konformität zu TR-03121.	

Prüffall-ID	PFF-S-002
Verdict	

3.2.3 PFF-S-003 Kryptografische Anforderungen

Prüffall-ID	PFF-S-003
Anforderungen	ANS-003, ANS-004, ANS-005, ANS-006, ANS-007, ANS-008, ANS-009, ANS-010, ANS-011, ANS-012, ANS-013 (Kryptografische Anforderungen [BSI TR-03170-2 Kapitel 2.2])
Ziel	Nachweis, dass folgende Anforderungen an die Software erfüllt sind: - 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. - Der Schlüssel 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. - Der Barcode 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 zurückgreifen. - Die Wahl kryptografischer Primitive MUSS passend zum Anwendungsfall sein und dem aktuellen Stand 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.

Prüffall-ID	PFF-S-003		
Vorbedingungen	- Der Quellcode der Software ist in der Entwicklungsumgebung einsehbar - Registrierung als Fotograf beim Cloud-Dienst - Die Systemdokumentation mit einer Übersicht über Softwarearchitektur liegt vor - Ein Testclient ist eingerichtet - Die Software ist betriebsbereit - Die Verschlüsselung ist eingerichtet - Es ist ein geeignetes Monitoring des zur Laufzeit von der Software verwendeten Speichers vorhanden		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Nachvollziehen der Algorithmen zur Schlüsselerstellung und –nutzung im Quellcode.	Es werden keine fest einprogrammierten Schlüssel verwendet.	
2	Nachvollziehen der Verarbeitung des Schlüssels und Barcodes im gesamten Quellcode.	Schlüssel und Barcode werden an keiner Stelle des Quellcodes gespeichert.	
3	Nachvollziehen der Algorithmen zur Bild-Verschlüsselung im Quellcode.	Es wird für jeden Vorgang/ jedes Lichtbild ein neuer Schlüssel erzeugt und nach seiner Verwendung verworfen.	
4	Prozesschritte 1 bis 6 aus Kapitel 2.4.2 der BSI TR-03170 ausführen und Speicher analysieren.	Erzeugte Schlüssel und Barcode sowie dazu verwendete Werte sind zwischengespeichert und deren Speicherorte sind identifiziert.	
5	Prozesschritt 7 aus Kapitel 2.4.2 ausführen und Speicher erneut analysieren.	Zuvor identifizierter Speicherorte sind leer und Schüssel, Barcode und Werte sind nicht mehr auffindbar.	

Prüffall-ID	PFF-S-003		
6	Prüfung der Systemdokumentation, dass kryptografische Primitive der Software BSI TR-02102-1 erfüllen.	Die Einhaltung der TR-02102-1 wird in der Systemdokumentation nachvollziehbar dargestellt.	
7	Prüfung, dass kryptografische Primitive passend zum Anwendungsfall verwendet werden und BSI TR-02102-1 erfüllen.	Die Verwendung der Primitiven in Systemdokumentation ist passend zum Anwendungsfall. Für die Erzeugung des Schlüssels und die Verschlüsselung des Lichtbilds wird im Quellcode der Anwendung geprüft, ob die verwendeten Primitiven anwendungsfallgemäß implementiert sind und BSI TR-02102-1 erfüllen. Es werden die Empfehlungen bezüglich Symmetrischer Schlüssel und Schlüsseleinigung gemäß der entsprechend betrachteten Anwendungsfälle eingehalten.	
8	Prüfung, dass die Verschlüsselung des Lichtbilds clientseitig erfolgt.	Die clientseitige Verschlüsselung wird in der Systemdokumentation nachvollziehbar dargestellt. Nach der Authentisierung durch einen Testuser ist die Verschlüsselung des Lichtbilds am Testclient möglich.	
Verdict			

3.2.4 PFF-S-004 Barcode

<table>
<tr><th>Prüffall-ID</th><th>PFF-S-004</th></tr>
<tr><td>Anforderungen</td><td>ANS-014, ANS-015, ANS-016, ANS-017, ANS-018, ANS-019

(Anforderung an den Barcode [BSI TR-03170-2 Kapitel 2.3])</td></tr>
<tr><td>Ziel</td><td>Nachweis, dass folgende Anforderungen an die Software erfüllt sind:

- 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.

<table>
<tr><th>Start Tag</th><th>Länge (Byte)</th><th>Inhalt</th></tr>
<tr><td>0x00</td><td>1</td><td>Magische Konstante. Die magische Konstante ist ein feststehender Wert zur Identifikation des hier genutzten Barcode Schemas und ist auf den Wert 0xE2 festgelegt.</td></tr>
<tr><td>0x01</td><td>1</td><td>Version. Ein Byte-Wert, der die genutzte Version des hier definierten Barcodes angibt. Aktuell gibt es hierbei nur die hier definierte Version 0x01. Aufsteigende Versionsnummern werden fortlaufend vergeben.</td></tr>
</table>
</td></tr>
</table>

Prüffall-ID	PFF-S-004		
	0x02	1	Längenbyte für die Cloudadresse. Ein Byte, welches die Länge des nachfolgenden Feldes für die URL des Cloud-Anbieters angibt.
	0x03	v	Cloudadresse. Die URL des Cloud-Anbieters. 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.

Prüffall-ID	PFF-S-004		
	0x14 + v	x	Verschlüsselungsalgorithmus. Der genutzte Verschlüsselungsalgorithmus MUSS in strukturierter Form als OID angegeben werden (Algorithmus_Schlüssellänge_Betriebsmodus (z.B. AES_128_CFB)). 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.

Prüffall-ID	PFF-S-004		
	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 [BSI TR-03170-2] Kapitel 2.2. - Der Barcode MUSS unter Berücksichtigung von ISO/IEC 15415 so gedruckt werden, dass Lesegeräte den Barcode zuverlässig dekodieren können. - Auf dem Ausdruck des Barcodes DÜRFEN die im Barcodes enthaltenen Informationen (z.B. symmetrischer Schlüssel, Lichtbildidentifier, etc.) NICHT in menschenlesbarer Form dargestellt werden. - Der Barcode MUSS für die maximale Abrufzeit des Lichtbildes gemäß PassV, PAuswV, PassDEÜV, AufenthV gültig sein.		
Vorbedingungen	- Software ist betriebsbereit - Systemdokumentation liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Prüfung, dass Barcode als DataMatrix ECC 200 nach ISO/IEC 16022 kodiert ist	Die Anforderung wird in der Systemdokumentation nachvollziehbar dargestellt. Erzeugung eines Barcodes und Prüfung, ob der erzeugte Barcode als Datamatrix ECC 200 codiert ist.	
2	Prüfung, dass die Zeichenketten des Barcodes aus alphanumerischen Zeichen und/oder	Die Anforderung wird in der Systemdokumentation nachvollziehbar dargestellt.	

Prüffall-ID	PFF-S-004		
	Sonderzeichen als Bytes kodiert werden. Die Sequenzen von Bytes werden, so wie sie sind, übernommen	Die Zeichenketten von mindestens 3 Beispielbarcodes der Software entsprechen den Vorgaben.	
3	Prüfung des Barcodedrucks in Systemdokumentation	Umsetzung ISO/IEC 15415 und zuverlässige Decodierung sind in der Systemdokumentation nachvollziehbar dargestellt. Der Anbieter erklärt die Konformität zu ISO/IEC 15415.	
4	Bewertung der Decodierung anhand von 3 Beispielausdrucken mit Hilfe eines Lesegerätes	Die ausgedruckten Barcodes können durch Lesegeräte vollständig decodiert werden	
5	Bewertung der Vollständigkeit des Barcodes anhand von 3 Beispielausdrucken mit Hilfe eines Lesegerätes	Die ausgedruckten Barcodes enthalten alle spezifizierten Inhalte. Auf den Ausdrucken sind die im Barcodes enthaltenen Informationen nicht nochmal in menschenlesbarer Form enthalten.	
6	Prüfung der Gültigkeitsdauer des Barcodes in Systemdokumentation	In der Systemdokumentation wird nachvollziehbar dargestellt, dass die Gültigkeitsdauer des Barcodes die maximale Abrufzeit gemäß PassV, PAuswV, PassDEÜV, AufenthV abdeckt.	
Verdict			

3.2.5 PFF-S-005 Erzeugung von Zufallszahlen

Prüffall-ID	PFF-S-005
Anforderungen	ANS-020, ANS-021, ANS-022, ANS-023, ANS-024, ANS-025

Prüffall-ID	PFF-S-005		
	(Erzeugung von Zufallszahlen) [BSI TR-03170-2 Kapitel 2.4.1]		
Ziel	Nachweis, dass folgende Anforderungen an die Software erfüllt sind: - Für Zufallszahlengeneratoren MUSS die BSI 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. - Die Anwendung SOLLTE in die Erstellung eines Startwerts (Seed) für den Zufallszahlengenerator einen geeigneten Zufall vom Backend einbeziehen.		
Vorbedingungen	- Die Software ist betriebsbereit - Die Systemdokumentation liegt vor		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Prüfung der Systemdokumentation	Die Erfüllung der Anforderung ist in der Systemdokumentation nachvollziehbar dargestellt. Es werden wirksame Maßnahmen nachvollziehbar beschrieben, wie der Einsatz eines anderen, als in der Software eingesetzten Zufallszahlengenerators verhindert wird. Es wird BSI TR-02102-1 erfüllt. Die Anwendung weist dem Zufallszahlengenerator einen Startwert (Seed) zu, der sich aus mindestens drei voneinander unabhängigen Systemparametern zusammensetzt, was anhand des Programmcodes oder Systemdokumentation nachvollziebar ist. Die Anwendung bezieht dabei einen geeigneten Zufall	

Prüffall-ID	PFF-S-005		
		vom Backend in die Erstellung eines Startwerts (Seed) für den Zufallszahlengenerator ein. Es ist nachvollziehbar dokumentiert, dass die Parameter des Zufallsgenerators nicht von außerhalb der Anwendung ermittelbar sind.	
Verdict			

3.2.6 PFF-S-006 Verwendung von Frameworks und Bibliotheken

Prüffall-ID	PFF-S-006
Anforderungen	ANS-026, ANS-027, ANS-028, ANS-029, ANS-030, ANS-031, ANS-032, ANS-033, ANS-034, ANS-035, ANS-036, ANS-037, ANS-038, ANS-039, ANS-040, ANS-041, ANS-042, ANS-043 (Verwendung von Frameworks und Bibliotheken [BSI TR-03170-2 Kapitel 2.4.2]
Ziel	Nachweis, dass folgende Anforderungen an die Software erfüllt sind: - 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. - 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.

Prüffall-ID	PFF-S-006
	- Der Hersteller MUSS die genutzten Frameworks und Bibliotheken und deren Zweck im Rahmen der Anwendung in einer Softwaredokumentation erfassen. - 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.
Vorbedingungen	- Die Softwaredokumentation inklusive verwendeter Bibliotheken / Frameworks und Übersicht über Softwarearchitektur liegt vor - Das Konzept für Schwachstellen- und Patchmanagement liegt vor - Das Sicherheitskonzept liegt vor - Die Software nutzt Frameworks / Bibliotheken Dritter - Der Quellcode der Software ist in der Entwicklungsumgebung einsehbar

Prüffall-ID	PFF-S-006		
	- Die Software ist betriebsbereit		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Überprüfung der Beschreibung der genutzten Frameworks / Bibliotheken Dritter in der Softwaredokumentation und Identifizierung der genutzten Funktionen Dritter im Quellcode.	Die genutzten Funktionen Dritter stimmen mit denen in der Softwaredokumentation beschriebenen überein. Ihr Zweck im Rahmen der Anwendung geht nachvollziehbar aus der Softwaredokumentation hervor.	
2	Bewertung der Erforderlichkeit der Funktionen Dritter für den primären Zweck der Software	Es werden nur erforderliche Funktionen Dritter genutzt	
3	Ungenutzte Funktionen Dritter auf Basis der Dokumentation der Frameworks / Bibliotheken identifizieren und deren Deaktivierung im Quellcode nachvollziehen	Alle ungenutzten Funktionen Dritter sind gemäß der Dokumentation der Frameworks / Bibliotheken so sicher deaktiviert, dass sie nicht während der Laufzeit durch Dritte aktiviert werden können.	
4	Nutzung der Funktionen Dritter im Quellcode nachvollziehen und auf Basis der Dokumentation der Frameworks / Bibliotheken beurteilen, ob sie sicher ist	Die Nutzung der Funktionen Dritter durch die Software erfolgt gemäß der Dokumentation der Frameworks / Bibliotheken sicher	
5	Überprüfung, ob die in die geprüfte Softwareversion eingebundenen Frameworks / Bibliotheken Dritter zur Build-Zeit aktuell waren.	Es sind die zur Build-Zeit der Software aktuellen Versionen der verwendeten Frameworks / Bibliotheken Dritter eingebunden.	
6	Prüfung Konzept für Schwachstellen- und Patchmanagement und Softwarepflege-Protokolle	Für die genutzten Bibliotheken und Frameworks Dritter ist nachvollziehbar beschrieben, in welchem Rhythmus Informationen zu ihren	

Prüffall-ID	PFF-S-006		
		Schwachstellen aus welchen Quellen eingeholt / erhalten werden. Die Durchführung der regelmäßigen Überprüfung auf Schwachstellen ist nachvollziebar protokolliert. Für die genutzten Bibliotheken und Frameworks Dritter ist nachvollziehbar beschrieben, in welchem Rhythmus Informationen zu Sicherheitsupdates für sie aus welchen Quellen eingeholt / erhalten werden. Ferner ist der Prozess der Verteilung an die Nutzer der Software nachvollziehbar beschrieben. Die Durchführung der regelmäßigen Überprüfung auf Updates in einem geeigneten Intervall und deren Einspielung bei den Nutzern ist nachvollziebar protokolliert.	
7	Überprüfung, ob zu den in die geprüfte Softwareversion eingebundenen Frameworks / Bibliotheken Dritter zur Build-Zeit Schwachstellen bekannt waren.	Zur Build-Zeit der Software waren keine Schwachstellen der verwendeten Frameworks / Bibliotheken Dritter bekannt.	
8	Prüfung Sicherheitskonzept, Systemdokumentation und Konzept für Schwachstellen- und Patchmanagement hinsichtlich Übergabgefristen für die Nutzung der Software mit bekannten Schwachstellen	Im Sicherheitskonzept ist die geduldete Weiternutzungszeit (Grace Period) der Anwendung nach Bekannt werden ausnutzbarer Schwachstellen in Abhängigkeit von deren Kritikalität festgelegt. Die Technische Umsetzung der Einhaltung der Übergangsfrist ist in der Systemdokumentation nachvollziehbar dargestellt.	

Prüffall-ID	PFF-S-006		
		Der Prozess zur für das Schwachstellen- und Patchmanagement ist im Konzept entsprechenden für Schwachstellen- und Patchmanagement nachvollziebar dokumentiert.	
9	Bewertung der Umsetzung durch Start der Software mit einer eingestellten, abgelaufenen Grace Period.	Die Software informiert den Nutzer über Sicherheitslücke und verweigert eine weitere Nutzung.	
10	Prüfung der schriftlichen Erklärung zur Vertrauenswürdigkeit genutzter Software Dritter und Information über Schwachstellen.	Der Hersteller erklärt, dass vor der Verwendung von externen Bibliotheken und Frameworks deren Quelle auf Vertrauenswürdigkeit geprüft wird. Der Hersteller erklärt, Nutzende über für sie umsetzbare Mitigationsmaßnahmen bei Schwachstellen zu informieren.	
11	Prüfung der Herstellererklärung, dass keine Daten an Funktionen Dritter weitergegeben werden.	Der Anbieter erklärt, dass keine personenbezogene Daten nach Art.4 Abs.1 DSGVO, sowie insbesondere biometrische Daten nach Art.4 Abs.14 DSGVO an Funktionen von Drittanbieter-Software übergeben werden.	
12	Im Quellcode überprüfen, wie Daten von Funktionen Dritter validiert werden.	Von Funktionen Dritter übernommene Daten werden auf Plausibilität geprüft.	
13	Prüfung des Konzepts für Schwachstellen- und Patchmanagement hinsichtlich des Umgangs mit nicht mehr gewarteter Software Dritter.	Es wird nachvollziehbar beschrieben, wie Obsoleszenzen eingebundener Drittanbieter-Software behandelt werden.	
14	Überprüfung, ob die in der geprüften Softwareversion eingebundenen Frameworks /	Die von der geprüften Softwareversion verwendeten Frameworks / Bibliotheken Dritter werden von deren Herstellern noch gewartet.	

Prüffall-ID	PFF-S-006		
	Bibliotheken Dritter noch von ihren Herstellern gewartet werden.		
Verdict			

3.2.7 PFF-S-007 Implementierung

Prüffall-ID	PFF-S-007
Anforderungen	ANS-044, ANS-045, ANS-046, ANS-047, ANS-048, ANS-049, ANS-050, ANS-051, ANS-052, ANS-053, ANS-054, ANS-055, ANS-056, ANS-057, ANS-058, ANS-059, ANS-060, ANS-061, ANS-062, ANS-063 (Anforderungen an die Implementierung [BSI TR-03170-2 Kapitel 2.4.3])
Ziel	Nachweis, dass folgende Anforderungen an die Software erfüllt sind: - 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 (z.B. Schemavalidierung, Authentifizierung und Autorisierung etc.) SOLLTEN sowohl in der Anwendung als auch auf allen Schnittstellen und API-Endpunkten, implementiert werden. - Der Hersteller MUSS dem Nutzer eine barrierearme Möglichkeit bereitstellen, um Sicherheitsprobleme zu melden. - Die Anwendung und Updates SOLLTEN durch Einsatz kryptografischer Verfahren verschlüsselt und signiert werden.

Prüffall-ID	PFF-S-007
	- 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.
Vorbedingungen	- Systemdokumentation liegt vor - Das Design- und Implementierungskonzept liegt vor - Das Sicherheitskonzept liegt vor - Die Nutzerdokumentation liegt vor - Das Konzept für Schwachstellen- und Patchmanagement liegt vor

Prüffall-ID	PFF-S-007		
	- Das Konzept zum Test- und Qualitätsmanagement - Die Testprotokolle liegen vor - Das Berechtigungskonzept liegt vor - Nutzerdokumentation liegt vor - Der Quellcode der Software ist in der Entwicklungsumgebung einsehbar - Installationspakete für Software & Updates sind verfügbar - Die Software ist betriebsbereit - Es ist ein geeignetes Speichermonitoring vorhanden		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Prüfung des Design- und Implementierungskonzepts & Sicherheitskonzepts	Die IT-Sicherheit ist im Design- und Implementierungskonzept durchgängig berücksichtigt und die Sicherheitsaspekte des Software-Lebenszyklus finden sich im Sicherheitskonzept wieder. Beide Konzepte lassen eine risikobasierte Auswahl von Sicherheitsmaßnahmen erkennen, die den Schutzbedarf sensibler Daten berücksichtigt.	
2	Prüfung des Design- und Implementierungskonzepts bezüglich des Datenlebenszyklus	Es ist ein Datenlebenszyklus nachvollziehbar beschrieben, der die sichere Erhebung, Verarbeitung, Speicherung und Löschung sensibler Daten abbildet	
3	Prüfung des Design- und Implementierungskonzept dahingehend, ob die Software-Schnittstellen oder API-Endpunkte	Design und Quellcode enthalten keine Schnittstellen oder API-Endpunkte (Prüfschritt 4 überspringen).	

Prüffall-ID	PFF-S-007		
	enthalten sollte und Prüfung des Quellcodes, ob er diesbezüglich dem Design entspricht.	oder Quellcode enthält Außenschnittstellen oder API-Endpunkte gemäß Design.	
4	Prüfung des Design- und Implementierungskonzept sowie Sicherheitskonzept dahingehend, ob und welche Sicherheitsfunktionen für die Software sowie für Außenschnittstellen oder API-Endpunkte vorgesehen sind.	Sicherheitsfunktionen sind sowohl für die Software als auch für Außenschnittstellen oder API-Endpunkte vorgesehen.	
5	Prüfung des Quellcodes, ob die Sicherheitsfunktionen designgemäß implementiert sind.	Die im Design- und Implementierungskonzept vorgesehenen Sicherheitsfunktionen sind im Quellcode wiederzufinden.	
6	Prüfung der Nutzerdokumentation	Nutzerdokumentation enthält für den Anwender leicht verständlich und nachvollziehbar formulierte Empfehlungen zum sicheren Umgang mit der Software. In der Nutzerdokumentation sind Wege, Sicherheitsprobleme zu melden, angegeben und leicht zu finden.	
7	Prüfung des Sicherheitskonzepts bezüglich des Prozesses zur Behandlung von Meldungen über Sicherheitsproblem	Es ist geregelt, wie mit gemeldeten Sicherheitsproblemen verfahren wird.	
8	Prüfung Design- und Implementierungskonzept sowie Konzept für Schwachstellen- und Patchmanagement	Design sieht bei Anmeldung an der Cloud folgendes vor: - Überprüfung des Update- und Patchstatus der Software	

Prüffall-ID	PFF-S-007		
	bezüglich Behandlung von Patches und Update durch Software.	- Installation Update gemäß Konzept für Schwachstellen- und Patchmanagement, falls die Software nicht aktuell ist.	
9	Prüfung Design- und Implementierungskonzept sowie Konzept für Schwachstellen- und Patchmanagement zur Sicherstellung der Integrität und Vertraulichkeit von Installationsdateien. Prüfung der Installationspakete.	Es sind Maßnahmen zur Sicherstellung der Integrität und Vertraulichkeit der Distributionspakete für die Software und Updates vorgesehen Die konzeptionell vorgesehenen Maßnahmen sind umgesetzt.	
10	Prüfung des Quellcodes hinsichtlich des Umgangs mit Ausnahmen (Exceptions)	Bei allen Nutzereingaben erfolgen Überprüfungen auf kontextbezogener Plausibilität, bevor diese weiterverarbeitet werden. Alle Nutzereingaben sind mit Escape-Syntax versehen Alle von der Software ausgegebenen Meldungen und Benachrichtigungen sind generisch ohne personenbezogene Daten. Exceptions werden abgefangen, kontrolliert behandelt und protokolliert. Der Zugriff auf sensible Daten wird bei Auftreten von Exceptions abgebrochen.	
11	Prüfung des Quellcodes auf Optionen zur Entwicklungsunterstützung	Es gibt keine aktivierten Optionen zur Entwicklungsunterstützung im Quellcode.	

Prüffall-ID	PFF-S-007		
12	Prüfung Konzept zum Test- und Qualitätsmanagement	Es ist nachvollziehbar beschrieben, wie getestet wird, dass keine Debug-Mechanismen in Software-Versionen für die Auslieferung verblieben sind. Testprotokolle belegen, dass die konzeptionell vorgesehenen Tests erfolgreich durchgeführt wurden.	
13	Prozesschritte 1 bis 6 aus Kapitel 2.4.2 der BSI TR-03170 ausführen und nutzerspezifischen Daten im Speicher lokalisieren. Anwendung beenden und Speicher erneut analysieren.	Zwischengespeicherte nutzerspezifischen Daten sind lokalisiert. Zuvor identifizierte Daten sind überschrieben.	
14	Bewertung des Softwareverhaltens bei Aufruf in zwei unterschiedlichen Entwicklungs-/Debugging-Umgebungen mittels eines Testclients.	Die Software erkennt die Umgebung und startet nicht.	
15	Prüfung Design- und Implementierungskonzept sowie Sicherheitskonzept bezüglich Härtungsmaßnahmen Bewertung der Umsetzung im Quellcode.	Härtungsmaßnahmen für die Software sind nachvollziehbar beschrieben. Die im Design- und Implementierungskonzept sowie Sicherheitskonzept vorgesehenen Härtungsmaßnahmen sind im Quellcode wiederzufinden.	
16	Prüfung Berechtigungskonzept Prüfung des Quellcodes	Die eingeforderten Berechtigungen sind nachvollziehbar beschrieben und begründet.	

Prüffall-ID	PFF-S-007		
		Die beschriebenen Berechtigungen werden im Quellcode verwendet. Fordert die Software-Berechtigungen vom Nutzer an, geschieht dies mit Meldungen aus denen hervorgeht, wozu sie erforderlich sind und welche Auswirkung die Nicht-Erteilung hat.	
Verdict			

3.2.8 PFF-S-008 Authentifizierung und Autorisierung

Prüffall-ID	PFF-S-008
Anforderungen	ANS-064, ANS-065, ANS-066 (Authentifizierung und Autorisierung [BSI TR-03170-2 Kapitel 2.4.4])
Ziel	Nachweis, dass folgende Anforderungen an die Software erfüllt sind: - Für die Registrierung und die Anmeldung vor jedem Hochladen eines Lichtbilds gelten die Anforderungen [BSI TR-03170-1] Kapitel 2.5, 2.6 und 2.7.3. - Der Hersteller MUSS ein Konzept zur Authentifizierung, Autorisierung (Rollenkonzept) und zum Beenden einer Anwendungssitzung erstellen. - Wurde die Anwendung unterbrochen (in den Hintergrundmodus versetzt), MUSS eine erneute Authentifizierung gefordert werden.
Vorbedingungen	- Die Systemdokumentation liegt vor - Das Berechtigungskonzept liegt vor

Prüffall-ID	PFF-S-008		
	- Die Software ist betriebsbereit		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Prüfung der Systemdokumentation bezüglich der Registrierung und Anmeldung an der Cloud Bewertung anhand von 3 Beispieldaten mittels eines Testclients	Erfüllung der Anforderung ist in der Systemdokumentation nachvollziehbar dargestellt Vor jedem Upload von Lichtbildern erfolgt die Registrierung und Anmeldung gemäß den Anforderungen unter [BSI TR-03170-1] Kapitel 2.5, 2.6 und 2.7.3.	
2	Bewertung des Berechtigungskonzepts	Es liegt ein schlüssiges, nachvollziehbares Konzept vor	
3	Prüfung der Systemdokumentation bezüglich Neuanmeldung nach Unterbrechung Bewertung anhand von 3 Beispieldaten	Die Authentifizierung nach Unterbrechung der Anwendung ist in der Systemdokumentation nachvollziehbar dargestellt. Die Anwendung wird unterbrochen und eine erneute Authentisierung wird vom System gefordert.	
Verdict			

3.2.9 PFF-S-009 Sicherheit der Daten

Prüffall-ID	PFF-S-009		
Anforderungen	ANS-067, ANS-068, ANS-069, ANS-070, ANS-071, ANS-072, ANS-073, ANS-074, ANS-075 (Anforderungen an die Sicherheit der Daten [BSI TR-03170-2 Kapitel 2.4.5])		
Ziel	Nachweis, dass folgende Anforderungen an die Software erfüllt sind: - 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). - 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 Zweckbindung seitens des Herstellers ist dem Datenverarbeitungskonzept beizulegen. - Die Anwendung DARF KEINE sensiblen Daten in Logfiles oder andere Meldungen oder Benachrichtigungen, die nicht vom Nutzer explizit eingeschaltet wurden, schreiben. - Die Anwendung MUSS sicherstellen, dass bei ihrer Deinstallation alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen auf dem Endgerät vollständig gelöscht werden.		
Vorbedingungen	- Die Systemdokumentation liegt vor - Das Datenverarbeitungskonzept liegt vor - Die Software ist betriebsbereit		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**

Prüffall-ID	PFF-S-009		
1	Prüfung der Systemdokumentation sowie des Datenverarbeitungskonzepts bezüglich der Datenerhebung. Bewertung anhand von 3 Beispieldaten	Es ist nachvollziehbar dargestellt, dass die Anwendung nur Daten erhebt und verarbeitet, die Ihrem primären Zweck dienen Die Anwendung erhebt nur die unmittelbar notwendigen Daten, was anhand der verwendeten Testdaten sowie Protokolldaten nachvollziehbar ist.	
2	Prüfung der Systemdokumentation sowie des Datenverarbeitungskonzepts bezüglich des Teilens sensibler Daten. Bewertung anhand von 3 Beispieldaten	Es ist nachvollziehbar dargestellt, dass sensible Daten nicht mit Dritten geteilt werden. -oder Es ist nachvollziehbar dargestellt, dass das Teilen der sensiblen Daten mit Dritten für den primären Zweck der Anwendung erforderlich ist. Zusätzlich: Wenn keine Weitergabe von sensiblen Daten an Dritte vorgesehen ist: Die als sensibel gekennzeichneten Daten können für eine Datenübermittlung im System nicht ausgewählt werden und werden bei Übermittlung auch nicht übertragen.	
3	Prüfung der Systemdokumentation sowie des Datenverarbeitungskonzepts bezüglich der Nutzer-Einwilligung. Bewertung anhand von 3 Beispieldaten	Es ist nachvollziehbar dargestellt, wie der Nutzer über die Verwendung seiner Daten informiert und sein OPT-IN eingeholt wird. -oder	

Prüffall-ID	PFF-S-009		
		Es ist nachvollziehbar dargestellt, dass Daten der Nutzer nicht mit Dritten geteilt werden. Zusätzlich: Wenn vorgesehen ist, dass Daten an Dritte weitergegeben werden: Dem Testnutzer wird angezeigt, welche Daten erhoben werden sollen und an wen diese aus welchem Grund weitergegeben werden sollen, eine Auswahl ist möglich..	
4	Prüfung der Systemdokumentation sowie des Datenverarbeitungskonzepts bezüglich der Anzeige sensibler Daten. Bewertung anhand von 3 Beispieldaten	Es ist nachvollziehbar dargestellt, dass Sensible Daten nicht angezeigt werden, wenn dies nicht notwendig ist.	
5	Prüfung der Systemdokumentation sowie des Datenverarbeitungskonzepts bezüglich der Löschung sensibler Daten. Bewertung anhand von 3 Beispieldaten	Es ist nachvollziehbar dargestellt, dass Sensible Daten nach der Dauer ihrer Verwendung aus der Anwendung gelöscht werden. Erhobene sensible Daten werden nur temporär gespeichert und beim Beenden der Anwendung gelöscht.	
6	Prüfung des Datenverarbeitungskonzepts bezüglich Datensparsamkeit und Zweckbindung	Die Erklärung des Herstellers, die Grundsätze der Datensparsamkeit und der Zweckbindung zu berücksichtigen ist dem Datenverarbeitungskonzept beigelegt.	
7	Prüfung der Systemdokumentation sowie des Datenverarbeitungskonzepts bezüglich des Schreibens sensibler Daten in Logfiles.	Es ist nachvollziehbar dargestellt, dass Sensible Daten nicht in Logfiles geschrieben werden, wenn	

Prüffall-ID	PFF-S-009		
	Bewertung anhand von 3 Beispieldaten	dies nicht vom Nutzer ausdrücklich eingeschaltet wurde.	
8	Prüfung der Systemdokumentation sowie des Datenverarbeitungskonzepts bezüglich der Löschung von Daten bei der Deinstallation. Deinstallation der Anwendung	Es ist nachvollziehbar dargestellt, wie bei der Deinstallation alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen vollständig vom Endgerät gelöscht werden. Die Rolle Administrator entfernt die Anwendung von einem Testclient (oder einem Äquivalent). Es befinden sich keine Restdaten der Anwendung auf dem Testclient (oder dem Äquivalent)	
Verdict			

3.2.10 PFF-S-010 Kommunikation

Prüffall-ID	PFF-S-010
Anforderungen	ANS-076, ANS-077, ANS-078, ANS-079, ANS-080, ANS-081 (Softwareseitige Anforderungen an die Kommunikation [BSI TR-03170-2 Kapitel 2.4.6])
Ziel	Nachweis, dass folgende Anforderungen an die Software erfüllt sind: - 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.

Prüffall-ID	PFF-S-010		
	- 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 RFC 7469. - Die Anwendung MUSS das Server-Zertifikat der Cloud überprüfen. - Die Anwendung MUSS die Integrität der Antworten der Cloud validieren.		
Vorbedingungen	- Die Systemdokumentation liegt vor - Die Software ist betriebsbereit		
Prüfschritt	**Prüftätigkeit**	**Erwartete Ergebnisse**	**Beobachtung**
1	Prüfung der Systemdokumentation bezüglich der Netzverbindungen. Prüfung aller in der Systemdokumentation dargestellten Netzverbindungen mit einem Testclient anhand von 3 Beispieldaten. Dies kann unter Verwendung eines Tools für die Analyse von Netzwerkverkehr oder Kommunikationsprotokollen erfolgen (z.B. TLS-Testtool TaSK oder Wireshark)	Es ist nachvollziehbar dargestellt, wie die Netzkommunikation TLS-verschlüsselt wird. Alle Netzwerkverbindungen wurden geprüft und erfüllen mit ihrer Konfiguration die Anforderungen an eine TLS-Verschlüsselung nach BSI TR-02102. Die verwendeten Cipher Suites und die verwendete TLS Version entsprechen den Vorgaben.	
2	Prüfung der Systemdokumentation bezüglich der verwendeten Sicherheitsfunktionalität. Prüfung der in der Systemdokumentation beschriebenen Sicherheitsfunktionalität mit einem Testclient anhand von 3 Beispieldaten und ggf. Prüfung der Sicherheitszertifikate /	Es ist nachvollziehbar dargestellt, welche Sicherheitsfunktionalität für die Netzkommunikation genutzt wird. Die Anwendung verwendet die Sicherheitsfunktionalität der jeweilig verwendeten Betriebssystem-Plattform - oder –	

Prüffall-ID	PFF-S-010		
	Fingerprints genutzter Frameworks oder Bibliotheken.	Die Anwendung verwendet sicherheitsüberprüfte Frameworks oder Bibliotheken, um sichere Kommunikationskanäle aufzubauen. Die Sicherheitszertifikate / Fingerprints der im TOT verwendeten Frameworks oder Bibliotheken sind gültig.	
3	Prüfung der Systemdokumentation bezüglich des Zertifikatsspinnings. Prüfung aller in der Systemdokumentation dargestellten Netzverbindungen mit einem Testclient anhand von 3 positiven und 3 negativen Beispieldaten	Es ist nachvollziehbar dargestellt, wie die Anwendung Zertifikatspinning unterstützt. Kommunikationszertifikate werden von der Anwendung überprüft und im positiven Fall akzeptiert oder im negativen Fall abgelehnt. Die Zertifikatsannahme bzw. Ablehnung wird protokolliert.	
4	Prüfung der Systemdokumentation bezüglich der Anmeldung beim Cloud-Dienst. Prüfung der technischen Erfüllung mittels Testclient anhand von 3 Beispieldaten	Es ist nachvollziehbar dargestellt, wie die Anwendung das Server-Zertifikat des Cloud-Diensts überprüft. Die Anwendung prüft das Server-Zertifikat der Cloud und protokolliert das Ergebnis.	
5	Prüfung der Systemdokumentation bezüglich der Validierungen von Antworten des Cloud-Diensts. Prüfung der technischen Erfüllung mittels Testclient anhand von 3 Beispieldaten	Es ist nachvollziehbar dargestellt, wie die Anwendung Antworten des Cloud-Diensts verifiziert. Die Anwendung validiert die Integrität der Antworten der Cloud und protokolliert das Ergebnis.	

Prüffall-ID	PFF-S-010
Verdict	

Anforderungsregister

Anforderungs-ID	Anforderung
	[BSI TR-03170] Kapitel 2.4.2 Prozess
ANC-001	Dienstleister (z. B. Fotografinnen und Fotografen) MÜSSEN sich bei dem Cloud-Dienst registrieren, da nur registrierte Dienstleister Lichtbilder zu diesem übertragen dürfen.
ANC-002	Im Rahmen der sicheren digitalen Lichtbildübermittlung MUSS der Cloud-Dienst folgende Prozessschritte unterstützen: 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 [BSI TR-03170-1] Kapitel 2.6) beim Cloud-Anbieter 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 […] 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. Das Lichtbild wird von der Behörde aus der Cloud abgerufen.
	[BSI TR-03170-1] Kapitel 2.1 Vorliegen eines C5-Testats
ANC-003	Der Cloud-Anbieter MUSS - für die gesamte Beauftragungszeit, und - im Falle einer Vertragsbeendigung, für eine Nachlaufzeit von 6 Monaten, oder - im Falle einer Beendigung des Betriebs des Cloud-Dienstes, für eine zu vereinbarende Übergangszeit, eine Attestierung des “Cloud Computing Compliance Criteria Catalogue” (C5-Kriterienkatalog) vom Typ 2 über die Basiskriterien in der aktuellen Fassung vorweisen können.
	[BSI TR-03170-1] Kapitel 2.2.1.1 Angaben zu Gerichtsbarkeit und Lokationen
ANC-004	Der Cloud-Anbieter MUSS der Gerichtsbarkeit eines Landes der europäischen Union unterliegen.
ANC-005	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.
	[BSI TR-03170-1] Kapitel 2.2.1.2 Angaben zu Verfügbarkeit und Störungsbeseitigung im Normalbetrieb

<table>
<tr><th>Anforderungs-ID</th><th>Anforderung</th></tr>
<tr><td>ANC-006</td><td>Der Cloud-Anbieter des Cloud-Dienstes MUSS anhand eines Betriebskonzeptes nachweisen, dass er einen Normalbetrieb während der Nutzungszeit, definiert als Nutzungszeit = Geschäftszeit,
der Pass- und Personalausweis- oder Ausländerbehörden und der Dienstleister (z. B. Fotografinnen und Fotografen), gemäß Tabelle 2 gewährleisten kann:
<table><tr><th>Key Performance Indicators (KPI)</th><th>Messeinheit</th><th>Geschäftszeit (Mo – Fr: 7–20 Uhr, Sa: 7–17 Uhr)</th><th>Außerhalb der Nutzungszeit</th></tr><tr><td>Verfügbarkeit</td><td>Prozent</td><td>99,9%</td><td>95,0%</td></tr><tr><td>Störung in der Netzwerkkommunikation zwischen den Behörden und der Cloud-Infrastruktur</td><td>Kritikalität</td><td>Sehr hoch</td><td>Gering</td></tr><tr><td>Störung in der Netzwerkkommunikation zwischen den Fotodienstleistern und der Cloud-Infrastruktur</td><td>Kritikalität</td><td>Sehr hoch</td><td>Gering</td></tr><tr><td>Störung in der Cloud-Infrastruktur</td><td>Kritikalität</td><td>Sehr hoch</td><td>Gering</td></tr><tr><td>Wartungszeit</td><td>Uhrzeit</td><td>Keine</td><td>beliebig</td></tr><tr><td>Reaktionszeit bei Störung</td><td>Minuten</td><td><= 10</td><td>60</td></tr><tr><td>Wiederherstellungszeit</td><td>Minuten</td><td><= 60</td><td>180</td></tr></table>Kritikalität entspricht der Einordnung in Risikokategorien nach BSI Standard 200-3.</td></tr>
<tr><td>ANC-007</td><td>Wartungsarbeiten MÜSSEN innerhalb der Wartungszeit durchgeführt und abgeschlossen werden.</td></tr>
<tr><td>ANC-008</td><td>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.</td></tr>
<tr><td>ANC-009</td><td>Die erfassten Kontaktdaten MÜSSEN so gestaltet sein, dass eine Rückverfolgung oder Rückmeldung an die jeweilige Kontaktadresse (meldend oder aufnehmend) zu jedem Zeitpunkt möglich ist.</td></tr>
<tr><td>ANC-010</td><td>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.</td></tr>
<tr><td>ANC-011</td><td>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.</td></tr>
<tr><td></td><td>[BSI TR-03170-1] Kapitel 2.2.1.4 Angaben zu Zertifizierungen oder Bescheinigungen</td></tr>
<tr><td>ANC-012</td><td>Zusätzlich zum C5-Testat MÜSSEN mindestens folgende Zertifizierungen und Bescheinigungen vorliegen:
- IT-Grundschutz Zertifikat bzw. ISO 27001 Zertifikat (Wenn ein Zertifikat nur für die Cloud-Infrastruktur vorgelegt wird, MUSS der Cloud-Anbieter für über die Cloud-</td></tr>
</table>

Anforderungs-ID	Anforderung
	Infrastruktur hinausgehende Leistungen (z.B. Entwicklung und Betrieb des Cloud-Dienstes) die Einhaltung von ISO 27001 bzw. IT-Grundschutz gewährleisten.) - Nachweis der Einhaltung der DSGVO für den gesamten Prozess (mindestens durch ein von einer/ einem Datenschutzbeauftragten geprüftes Datenschutzkonzept) - Nachweis eines wirksamen Business Continuity Management Systems (BCMS) (mindestens durch eine BCM-Leitlinie und Audit-Berichte)
ANC-013	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.
	[BSI TR-03170-1] Kapitel 2.2.1.5 Kontakt zu relevanten Behörden und Interessenverbänden
ANC-014	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 zum CERT-Bund des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu pflegen, um sich über aktuelle Schwachstellen und Gefährdungen zu informieren.
	[BSI TR-03170-1] Kapitel 2.2.1.6 Verpflichtung auf zulässigen Gebrauch und sicheren Umgang mit ausgehändigten Assets sowie Rückgabe
ANC-015	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 (z.B. ein Schlüssel, ein Token oder eine SmartCard), 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.
ANC-016	Die zentrale Verwaltung physischer Assets MUSS eine Software-, Daten- und Richtlinienverteilung sowie eine Remote-Deaktivierung, -Löschung, oder –Sperrung ermöglichen.
	[BSI TR-03170-1] Kapitel 2.2.1.7 Klassifizierung und Kennzeichnung von Assets
ANC-017	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.
ANC-018	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.
	[BSI TR-03170-1] Kapitel 2.2.1.8 Schutz vor Schadprogrammen – Konzept
ANC-019	Der Cloud-Anbieter MUSS regelmäßige Reports über die durchgeführten Überprüfungen zum Schutz vor Schadprogrammen erstellen, welche durch autorisiertes Personal oder

Anforderungs-ID	Anforderung
	Gremien überprüft und analysiert werden. Die Erstellung und Überprüfung der Reports MUSS in einem entsprechenden Konzept beschrieben werden.
ANC-020	Richtlinien und Anweisungen MÜSSEN die technischen Maßnahmen zur sicheren Konfiguration und Überwachung der Managementkonsole beschreiben, um diese vor Schadprogrammen zu schützen.
ANC-021	Die Aktualisierung MUSS mit der höchsten Frequenz, die die Hersteller der Software vertraglich anbieten, erfolgen.
	[BSI TR-03170-1] Kapitel 2.2.1.9 Schutz vor Schadprogrammen – Umsetzung
ANC-022	Die Konfiguration der Schutzmechanismen MUSS automatisch überwacht werden.
ANC-023	Abweichungen von den Vorgaben MÜSSEN automatisch an das dafür sachverständige Personal berichtet werden, um diese umgehend einer Beurteilung zu unterziehen und erforderliche Maßnahmen einzuleiten.
	[BSI TR-03170-1] Kapitel 2.2.1.10 Protokollierung und Überwachung – Verfügbarkeit der Überwachungs-Software
ANC-024	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.
	[BSI TR-03170-1] Kapitel 2.2.1.11 Umgang mit Schwachstellen, Störungen und Fehlern – Penetrationstests
ANC-025	Pen-Tests MÜSSEN zwingend durch unabhängige externe Dritte durchgeführt werden. Internes Personal für Penetrationstests darf die externen Dritten dabei unterstützen.
ANC-026	Pen-Tests MÜSSEN mindestens jährlich stattfinden.
ANC-027	Der Cloud-Anbieter MUSS ein Penetrationstestkonzept erstellen, das diese Anforderungen berücksichtigt.
	[BSI TR-03170-1] Kapitel 2.2.1.12 Prüfung und Dokumentation offener Schwachstellen
ANC-028	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
	[BSI TR-03170-1] Kapitel 2.2.1.13 Separierung der Datenbestände in der Cloud-Infrastruktur

Anforderungs-ID	Anforderung
ANC-029	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.
	[BSI TR-03170-1] Kapitel 2.2.1.14 Regelmäßige Überprüfung der Zugriffsberechtigungen
ANC-030	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.
ANC-031	Die Notwendigkeit SOLLTE auf Wiedervorlage zum Ablauf des Zeitraums und spätestens nach einem halben Jahr erneut geprüft werden.
	[BSI TR-03170-1] Kapitel 2.2.1.15 Vertraulichkeit von Authentisierungsinformationen
ANC-032	Die Fotografinnen und Fotografen, die den Cloud-Dienst nutzen, 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.
	[BSI TR-03170-1] Kapitel 2.2.1.16 Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)
ANC-033	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.
	[BSI TR-03170-1] Kapitel 2.2.1.18 Technische Schutzmaßnahmen
ANC-034	Der Cloud-Anbieter MUSS mit technischen Maßnahmen sicherstellen, dass seinem (physischen oder virtuellen) Netz keine unbekannten (physischen oder virtuellen) Geräte beitreten.
	[BSI TR-03170-1] Kapitel 2.2.1.19 Netzübergreifende Zugriffe
ANC-035	Jeder Netzperimeter MUSS von redundanten und hochverfügbaren Sicherheitsgateways kontrolliert werden.
	[BSI TR-03170-1] Kapitel 2.2.1.20 Segregation des Datenverkehrs in gemeinsam genutzten Netzumgebungen
ANC-036	Bei IaaS/PaaS MUSS die sichere Trennung durch physisch getrennte Netze oder durch stark verschlüsselte VLANs sichergestellt werden. Bezüglich der Umsetzung einer starken Verschlüsselung ist die Technische Richtlinie BSI TR-02102 in ihrer aktuellsten Fassung zu berücksichtigen.
	[BSI TR-03170-1] Kapitel 2.2.1.21 Richtlinien zur Entwicklung/Beschaffung von Informationssystemen

Anforderungs-ID	Anforderung
ANC-037	Bei der Beschaffung SOLLTEN Produkte vorgezogen werden, die nach den „Common Criteria for Information Technology Security Evaluation“ (CC) gemäß Prüftiefe EAL 4 (oder höher) zertifiziert wurden.
ANC-038	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 werden. Eine verschriftlichte Risikobeurteilung MUSS hierzu erstellt werden.
	[BSI TR-03170-1] Kapitel 2.2.1.22 Versionskontrolle
ANC-039	Die Verfahren zur Versionskontrolle MÜSSEN durch geeignete Schutzmaßnahmen sicherstellen, dass die Integrität und Verfügbarkeit der Daten nicht beeinträchtigt werden, wenn Systemkomponenten in ihren vorherigen Zustand zurückversetzt werden.
	[BSI TR-03170-1] Kapitel 2.2.1.23 Überwachung der Einhaltung der Anforderungen
ANC-040	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).
ANC-041	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.
	[BSI TR-03170-1] Kapitel 2.2.1.24 Richtlinie für den Umgang mit Sicherheitsvorfällen
ANC-042	Bei einem Sicherheitsvorfall MÜSSEN Daten beweisfest gesammelt werden.
ANC-043	Es MÜSSEN für typische Sicherheitsvorfälle (Die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten ist nicht mehr gegeben, wie z.B. bei Verlust von Hardware, Verlust von Passwörtern, Befall mit Schadcode, Denial-of-Service oder Fehlkonfiguration mit möglichem Datenabfluss) Analysepläne existieren, um die Beweiskraft für die spätere juristische Würdigung zu erhalten. Das Vorgehen MUSS in einem Betriebskonzept beschrieben und festgelegt werden.
	[BSI TR-03170-1] Kapitel 2.2.1.25 Identifikation von Schwachstellen des Cloud-Dienstes
ANC-044	Die Verfahren zur Identifikation solcher (siehe dazugehörige Basisanforderung von PSS-02) Schwachstellen MÜSSEN darüber hinaus jährliche Code Reviews oder Penetration-Tests durch qualifizierte externe Dritte umfassen. Dieses Vorgehen MUSS durch den Cloud-Anbieter in einem entsprechenden Konzept festgelegt werden.
	[BSI TR-03170-1] Kapitel 2.3 Frontend und Backend

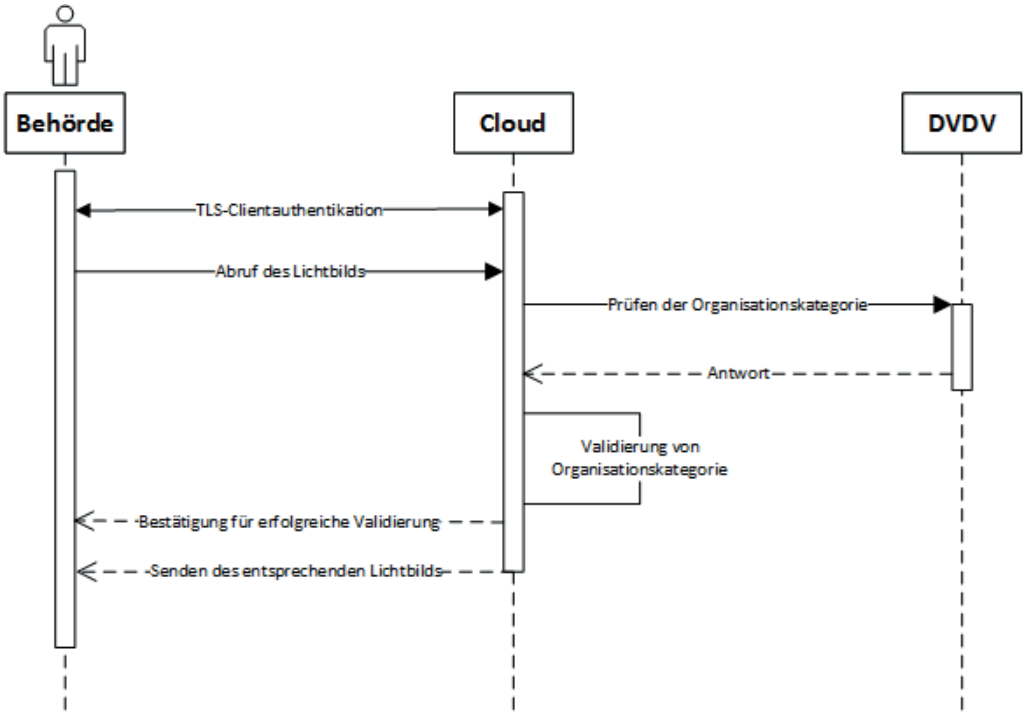
Anforderungs-ID	Anforderung
ANC-045	Für das Speichern der biometrischen Lichtbilder MUSS ein eigener Prozess mit eigenem Prozess-User vorgesehen werden.
ANC-046	Jeglicher Datenverkehr zwischen einem Dienstleister und dem Cloud-Dienst MUSS über die Frontend-Komponenten laufen.
ANC-047	Ein Zugriff direkt auf das eigentliche Backend aus dem Internet DARF NICHT möglich sein.
ANC-048	Die Kommunikation zwischen Serverkomponenten MUSS unter Einhaltung der Vorgaben und Empfehlungen der BSI TR-03116-4 in ihrer aktuellsten Fassung gesichert sein.
ANC-049	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 und Verordnungen (etwa PassV, PAuswV, PassDEÜV, AufenthV). - Nutzerkennungen - Pseudonyme (z.B. im Sinne des DKK siehe [BSI TR-03170-1] Kapitel 2.6)
	[BSI TR-03170-1] Kapitel 2.4 Protokollierung
ANC-050	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 (etwa PassV, PAuswV, PassDEÜV, AufenthV).
ANC-051	Protokollierungsdaten MÜSSEN gegen Veränderungen und Austausch von Protokollinhalten geschützt sein.
	[BSI TR-03170-1] Kapitel 2.5 Registrierungsprozess
ANC-052	Es MUSS ein Registrierungsprozess implementiert werden, der es dem Dienstleister ermöglicht, bei einem Cloud-Anbieter ein Dienstleisterkonto zu erstellen.
ANC-053	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 (PAuswG), des § 12 des eID-Karte-Gesetzes (eIDKG), des § 78 Absatz 5 des Aufenthaltsgesetzes (AufenthG) genügt oder einem anderen elektronischen Identifizierungsmittel entspricht, das gemäß Artikel 6 der Verordnung (EU) Nr. 910/2014 (eIDAS) auf dem Sicherheitsniveau „hoch“ notifiziert wurde.
ANC-054	Darüber hinaus MUSS ein Verfahren etabliert werden, das die Entgegennahme und Prüfung des Nachweises der Dienstleistereigenschaft (gemäß den Vorgaben aus PassV, PAuswV, PassDEÜV, AufenthV) während des Erstregistrierungsverfahrens ermöglicht. Die Person, die das Erstregistrierungsverfahren durchführt, wird zum Hauptkontoinhaber, trägt die

Anforderungs-ID	Anforderung
	primäre Verantwortung für das Dienstleisterkonto und sollte daher in der Regel nicht aus dem Dienstleisterkonto entfernt werden können.
ANC-055	Sollte eine Änderung der primären Verantwortung für ein Dienstleisterkonto notwendig sein, MUSS die Zugehörigkeit zu dem entsprechenden Unternehmen nachgewiesen werden.
ANC-056	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.
ANC-057	Neben dem Hauptnutzer KÖNNEN weitere Administratoren mit vergleichbaren Berechtigungen für ein Dienstleisterkonto hinterlegt werden. Die Berechtigungen/Rolle zur Administration DARF NUR vom Hauptnutzer oder einem anderen Administrator erteilt werden.
ANC-058	Beim Anlegen des Dienstleisterkontos MUSS eine eindeutige UUID v4 gemäß ISO/IEC 9834-8 erzeugt und eindeutig und dauerhaft mit dem Dienstleisterkonto verknüpft werden.
ANC-059	Zusätzlich MÜSSEN die Mitarbeiter des Dienstleisters die Möglichkeit haben, eine Nutzerregistrierung innerhalb des Dienstleisterkontos durchzuführen. Die Zugehörigkeit zu dem Dienstleisterkonto 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.
ANC-060	Im Rahmen des Erstregistrierungsprozesses MÜSSEN die notwendigen Daten für eine eindeutige Identifizierung des Nutzers (Mindestdatensatz des notifizierten elektronischen Identifizierungsmittels gem. Art. 11 Durchführungsverordnung (EU) 2015/1501) erhoben und beim Cloud-Anbieter gespeichert werden. Dies gilt sowohl für den Dienstleister als auch für dessen Mitarbeiter.
ANC-061	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.
ANC-062	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.
ANC-063	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

Anforderungs-ID	Anforderung
	zugeordnet werden können. Das System MUSS diese Verknüpfungen dauerhaft speichern, um eine Rückverfolgbarkeit zu ermöglichen.
ANC-064	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 ((eIDAS] 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.
ANC-065	Zusätzlich MUSS zu jeder Nutzerregistrierung eine persönliche UUID v4 gemäß ISO/IEC 9834-8 erzeugt und eindeutig und dauerhaft mit dem Nutzeraccount verknüpft werden.
	[BSI TR-03170-1] Kapitel 2.6 Nachvollziehbarkeit/Verantwortlichkeit beim Upload
ANC-066	Es MUSS eine eindeutige UUID v4 gemäß ISO/IEC 9834-8 erzeugt und eindeutig und dauerhaft mit dem Cloud-Dienst verknüpft werden. Diese dient bei der Erzeugung der Nutzerkennung der eindeutigen Identifizierung des Cloud-Dienstes.
ANC-067	Für die Nachvollziehbarkeit der Herkunft eines Lichtbilds MUSS eine Nutzerkennung aus den vorliegenden UUIDs der Cloud, des Dienstleisterkontos 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.
ANC-068	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.
ANC-069	Die Nutzerkennung und die Signatur bzw. das Siegel des Hashes MÜSSEN zusammen mit dem verschlüsselten Lichtbild an die Behörde übertragen werden.
ANC-070	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 PAuswG, des § 12 des eID-Karte-Gesetzes eIDKG, des § 78 Absatz 5 des Aufenthaltsgesetzes AufenthG genügen oder einem anderen elektronischen Identifizierungsmittel entsprechen, dass gemäß Artikel 6 der Verordnung (EU) Nr. 910/2014 eIDAS auf dem Sicherheitsniveau „hoch“ notifiziert wurde.
ANC-071	Dabei MUSS ausschließlich die durch das verwendete elektronische Identifizierungsmittel erzeugte eindeutige Kennung (Pseudonym) herangezogen werden. Voraussetzung dafür ist, dass bereits ein Dienstleisterkonto erstellt worden ist und eine Nutzerregistrierung stattgefunden hat.

Anforderungs-ID	Anforderung
ANC-072	Für eine Anmeldung am Dienstleisterkonto MUSS eine Authentisierung auf dem Vertrauensniveau „hoch“ gemäß den Anforderungen nach [BSI TR-03107-1] in ihrer aktuellsten Fassung genutzt werden.
	[BSI TR-03170-1] Kapitel 2.7 Kommunikationswege
ANC-073	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.
ANC-074	Die Datenübertragung sowohl zwischen Dienstleister (Fotografinnen und Fotografen) und Cloud-Dienst als auch zwischen Cloud-Dienst und Behörde MUSS synchron erfolgen.
	[BSI TR-03170-1] Kapitel 2.7.1 Aufbau einer Verbindung im Rahmen einer Nutzer Session
ANC-075	Das Sessionhandling SOLLTE mittels sicherer Frameworks (siehe dazu auch [BSI TR-03170-2] Kapitel 2.4.2) realisiert werden.
ANC-076	Session-Identifier MÜSSEN als sensitive Daten geschützt werden.
ANC-077	Session-Identifier DÜRFEN NICHT unverschlüsselt auf permanenten Speichermedien abgelegt werden.
ANC-078	Die Anwendung MUSS die Anwendungssitzung nach einem angemessenen Session-Timeout (maximal 30 Minuten)aktiv beenden.
ANC-079	Beim Upload eines Lichtbilds MUSS die Session nach dem Upload sofort wieder beendet werden.
ANC-080	Wird eine Anwendungssitzung beendet, MUSS die Anwendung den Session-Identifier sowohl auf dem Endgerät als auch in der Cloud sicher löschen.
	[BSI TR-03170-1] Kapitel 2.7.2 Erzeugung von Zufallszahlen
ANC-081	Für Zufallszahlengeneratoren MUSS die [BSI TR-02102-1] in ihrer aktuellsten Fassung berücksichtigt werden.
ANC-082	Alle Zufallswerte MÜSSEN über einen sicheren kryptografischen Zufallszahlengenerator erzeugt werden. Das Frontend MUSS Zufallszahlen von einem Zufallszahlengenerator mit hoher Entropie beziehen.
ANC-083	Das Frontend SOLLTE dem Zufallszahlengenerator einen Startwert (Seed) zuweisen, der sich aus mindestens drei voneinander unabhängigen Systemparametern zusammensetzt.
ANC-084	Die Parameter SOLLTEN von außerhalb des Frontends nicht ermittelbar sein.
ANC-085	Das Frontend SOLLTE bei Erstellung eines Startwerts (Seed) für den Zufallszahlengenerator einen geeigneten Zufall vom Backend beziehen.

Anforderungs-ID	Anforderung
	[BSI TR-03170-1] Kapitel 2.7.3 Kommunikationswege Dienstleister (z. B. Fotografinnen und Fotografen) – Cloud (Upload)
ANC-086	Für die inhaltliche Absicherung der Daten MUSS auf kryptografische Verfahren gemäß der [BSI TR-03116-4] in ihrer aktuellsten Fassung zurückgegriffen werden.
ANC-087	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.
ANC-088	Die durch den Verordnungstext geforderte Anmeldung des Dienstleisters mit der eID oder einem anderen elektronischen Identifizierungsmittel auf dem Vertrauensniveau „hoch“ (gemäß Kapitel 2.6) beim Cloud-Anbieter MUSS vor der Übertragung des Lichtbilds zur Cloud erfolgen. Der Request (siehe [BSI TR-03170] Kapitel 2.4.2) von der Anwendung des Dienstleisters SOLLTE, sofern ein Authentifizierungsmittel genutzt wird, was dies unterstützt, über einen mittels Kanalbindung nach BSI TR-03124 Kapitel 2.9 gesicherten TLS Kanal versendet werden.
ANC-089	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.
ANC-090	Für den Aufbau und die Erzeugung des Lichtbildidentifiers MUSS die ISO/IEC 9834-8 angewendet werden.
ANC-091	Die Speicherung des verschlüsselten Lichtbilds zu dem erzeugten Identifier MUSS der Anwendung bestätigt werden.
	[BSI TR-03170-1] Kapitel 2.7.4 Kommunikation Cloud – Behörde DVDV
ANC-092	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. Die Prüfung der genutzten Zertifikate gemäß Kapitel 2.8.2 MUSS vor dem Verbindungsaufbau erfolgen. 2. Die Behörde sendet einen Request zum Abruf des Lichtbildes mit der aus dem Barcode ausgelesenen eindeutigen ID des Lichtbildes in der Cloud. 3. Die Cloud prüft per DVDV-findCategories-Anfrage unter Verwendung des Organisationsschlüssels der anfragenden Behörde die Behördenkategorie auf Pass-, Personalausweis oder Ausländerbehörde. 4. Prüfung der Behördenkategorie: a) Bei erfolgreicher Prüfung der Behördenkategorie liefert die Cloud eine Statusmeldung zur erfolgreich abgeschlossenen Prüfung der Behörde zurück. b) Bei nicht erfolgreicher Prüfung liefert die Cloud eine Fehlermeldung und einen entsprechenden Fehler-Status "falsche" Organisationskategorie zurück und die Verbindung wird abgebaut.

Anforderungs-ID	Anforderung
	5. Die Cloud sendet das zu der ID gehörende verschlüsselte Lichtbild sowie weitere Daten nach dieser Technischen Richtlinie (siehe [BSI TR-03170-1] Kapitel 2.8.2) an die Behörde. 6. Die Verbindung wird abgebaut.  Der Vorgang der Löschung eines Lichtbilds MUSS analog zu dem oben beschriebenen Vorgang als neuer Request realisiert werden.
	[BSI TR-03170-1] Kapitel 2.8.1 Kommunikation mit dem DVDV
ANC-093	Die benötigten Daten MÜSSEN grundsätzlich immer aktuell aus dem DVDV-System bezogen werden. 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.
ANC-094	– Das Cloudzertifikat, das 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.
	[BSI TR-03170-1] Kapitel 2.8.3 Sichere Datenlöschung
ANC-095	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 Cloud-Anbieter aus der Cloud gelöscht

Anforderungs-ID	Anforderung
	werden. Wird eine weitere Aufbewahrung des Lichtbilds in der Cloud gewünscht, so MUSS das Lichtbild spätestens nach Ablauf der maximalen gesetzlichen Aufbewahrungsfrist gelöscht werden.
	[BSI TR-03170] Kapitel 2.4.2 Prozess
ANS-001	Im Rahmen der sicheren digitalen Lichtbildübermittlung MUSS die Software folgende Prozessschritte unterstützen: 1. Die Bürgerin/der Bürger lässt vom registrierten Dienstleister ein biometrisches Lichtbild erstellen. (Bei der Erstellung des Lichtbilds KÖNNEN Meta-Informationen zur Aufnahme, z. B. Marke/Modell der Aufnahmeeinheit, verwendete Software, etc. eingebracht werden) 2. Das ausgewählte Lichtbild wird kodiert (siehe [BSI TR-03170-2] Kapitel 2.1). 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 [BSI TR-03170-1] Kapitel 2.6) beim Cloud-Anbieter 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.
	[BSI TR-03170-2] Kapitel 2.1 Bildkonformität
ANS-002	Für das final zu übermittelnde Lichtbild MÜSSEN die Anforderungen der [BSI TR-03121, Part 3, Volume 2, Application Profile"Facial Image Digital-Delivery via Cloud" [BSI TR-03170]] bereits zum Zeitpunkt des Uploads des Lichtbildes erfüllt werden. Zusätzlich SOLLTEN Metadaten, die zu diesem Zeitpunkt zum Lichtbild vorliegen NICHT gelöscht werden.
	[BSI TR-03170-2] Kapitel 2.2 Kryptografische Anforderungen
ANS-003	Beim Einsatz von Verschlüsselung in der Anwendung DÜRFEN KEINE fest einprogrammierten Schlüssel eingesetzt werden.
ANS-004	Der für die symmetrische Verschlüsselung genutzte Schlüssel DARF NICHT gespeichert werden.
ANS-005	Er [Der Schlüssel] MUSS nach der Erzeugung für die Verschlüsselung der Daten verwendet, in den Barcode eingebettet und dann verworfen werden.
ANS-006	Der für die Übertragung der Informationen (z. B. symmetrischer Schlüssel, Bild-ID) genutzte Barcode DARF NICHT gespeichert werden.
ANS-007	Er [Der Barcode] MUSS nach Erzeugung und Übergabe an den Kunden verworfen werden.
ANS-008	Für jeden Vorgang bzw. jedes Lichtbild MUSS ein eigener symmetrischer Schlüssel erzeugt und verwendet werden.

<table>
<tr><th>Anforderungs-ID</th><th>Anforderung</th></tr>
<tr><td>ANS-009</td><td>Der Schlüssel DARF NICHT mehrfach verwendet werden.</td></tr>
<tr><td>ANS-010</td><td>Die Anwendung MUSS auf bewährte Implementierungen zur Umsetzung kryptografischer Primitive zurückgreifen gemäß [BSI TR-02102-1] in ihrer aktuellsten Fassung zurückgreifen.</td></tr>
<tr><td>ANS-011</td><td>Die Wahl kryptografischer Primitive MUSS passend zum Anwendungsfall sein und dem aktuellen Stands der Technik gemäß [BSI TR-02102-1] in ihrer aktuellsten Fassung entsprechen.</td></tr>
<tr><td>ANS-012</td><td>Die Stärke der kryptografischen Schlüssel MUSS dem aktuellen Stand der Technik entsprechen gemäß [BSI TR-02102-1, in ihrer aktuellsten Fassung].</td></tr>
<tr><td>ANS-013</td><td>Die Verschlüsselung des Lichtbilds MUSS clientseitig erfolgen.</td></tr>
<tr><td></td><td>[BSI TR-03170-2] Kapitel 2.3 Anforderung an den Barcode</td></tr>
<tr><td>ANS-014</td><td>Der Barcode MUSS als DataMatrix ECC 200 nach [ISO/IEC 16022] kodiert sein.</td></tr>
<tr><td>ANS-015</td><td>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.
<table>
<tr><th>Start Tag</th><th>Länge (Byte)</th><th>Inhalt</th></tr>
<tr><td>0x00</td><td>1</td><td>Magische Konstante. Die magische Konstante ist ein feststehender Wert zur Identifikation des hier genutzten Barcode Schemas und ist auf den Wert 0xE2 festgelegt.</td></tr>
<tr><td>0x01</td><td>1</td><td>Version. Ein Byte-Wert, der die genutzte Version des hier definierten Barcodes angibt. Aktuell gibt es hierbei nur die hier definierte Version 0x01. Aufsteigende Versionsnummern werden fortlaufend vergeben.</td></tr>
<tr><td>0x02</td><td>1</td><td>Längenbyte für die Cloudadresse. Ein Byte, welches die Länge des nachfolgenden Feldes für die URL des Cloud-Anbieters angibt.</td></tr>
</table>
</td></tr>
</table>

Anforderungs-ID	Anforderung		
	0x03	v	Cloudadresse. Die URL des Cloud-Anbieters. 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.
	0x14 + v	x	Verschlüsselungsalgorithmus. Der genutzte Verschlüsselungsalgorithmus MUSS in strukturierter Form als OID angegeben werden (Algorithmus_Schlüssellänge_Betriebsmodus (z.B. AES_128_CFB)). 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.

Anforderungs-ID	Anforderung
	<table><tr><td>Summe</td><td>0x18 + v + x + y+p+z</td><td></td></tr></table>
ANS-016	Für die kryptographischen Vorgaben und die Erzeugung des Schlüssels sowie Vorgaben zu damit einhergehenden Betriebsmodi, Initialisierungsvektoren und Padding gelten die Anforderungen aus [BSI TR-03170-2] Kapitel 2.2.
ANS-017	Der Barcode MUSS unter Berücksichtigung von [ISO/IEC 15415] so gedruckt werden, dass Lesegeräte den Barcode zuverlässig dekodieren können.
ANS-018	Auf dem Ausdruck des Barcodes DÜRFEN die im Barcodes enthaltenen Informationen (z.B. symmetrischer Schlüssel, Lichtbildidentifier, etc.) NICHT in menschenlesbarer Form dargestellt werden.
ANS-019	Der Barcode MUSS für die maximale Abrufzeit des Lichtbildes gemäß [PassV], [PAuswV], [PassDEÜV], [AufenthV] gültig sein.
	[BSI TR-03170-2] Kapitel 2.4.1 Erzeugung von Zufallszahlen
ANS-020	Für Zufallszahlengeneratoren MUSS [BSI TR-02102-1], in ihrer aktuellsten Fassung umgesetzt werden.
ANS-021	Alle Zufallswerte MÜSSEN über einen sicheren kryptografischen Zufallszahlengenerator erzeugt werden.
ANS-022	Die Anwendung MUSS Zufallszahlen von einem Zufallszahlengenerator mit hoher Entropie beziehen.
ANS-023	Die Anwendung SOLLTE dem Zufallszahlengenerator einen Startwert (Seed) zuweisen, der sich aus mindestens drei voneinander unabhängigen Systemparametern zusammensetzt.
ANS-024	Die Parameter SOLLTEN von außerhalb der Anwendung nicht ermittelbar sein.
ANS-025	Die Anwendung SOLLTE in die Erstellung eines Startwerts (Seed) für den Zufallszahlengenerator einen geeigneten Zufall vom Backend einbeziehen.
	[BSI TR-03170-2] Kapitel 2.4.2 Verwendung von Frameworks und Bibliotheken
ANS-026	Setzt die Anwendung Frameworks und Bibliotheken von Dritten ein, SOLLTEN alle verwendeten Funktionen für den primären Zweck der Anwendung erforderlich sein.
ANS-027	Die Anwendung SOLLTE anderweitige Funktionen sicher deaktivieren.
ANS-028	Nutzt die Anwendung Frameworks oder Bibliotheken von Dritten (etwa für Objektserialisierung), MUSS sie sicherstellen, dass diese Funktionen in sicherer Weise genutzt werden.
ANS-029	Die Anwendung MUSS darüber hinaus sicherstellen, dass ungenutzte Funktionen durch Dritte nicht aktiviert werden können.
ANS-030	Die genutzten Frameworks und Bibliotheken SOLLTEN auf die für den primären Zweck der Anwendung erforderlichen begrenzt werden.

Anforderungs-ID	Anforderung
ANS-031	Der Hersteller MUSS die genutzten Frameworks und Bibliotheken und deren Zweck im Rahmen der Anwendung in einer Softwaredokumentation erfassen.
ANS-032	Externe Bibliotheken und Frameworks SOLLTEN in ihrer aktuellsten verfügbaren Version, bezogen auf das genutzte Betriebssystem, verwendet werden.
ANS-033	Der Hersteller der Software MUSS regelmäßig prüfen, ob für genutzte externe Bibliotheken und Frameworks Schwachstellen bekannt sind.
ANS-034	Funktionen aus Bibliotheken und Frameworks DÜRFEN bei bekannten Schwachstellen NICHT eingesetzt werden.
ANS-035	Sicherheitsupdates für externe Bibliotheken und Frameworks MÜSSEN zeitnah eingespielt werden.
ANS-036	Der Hersteller MUSS ein Sicherheitskonzept vorlegen, das anhand der Kritikalität ausnutzbarer Schwachstellen die geduldete Weiternutzung für die Anwendung festlegt.
ANS-037	Nachdem die Übergangsfrist (Grace Period) abgelaufen ist, MUSS die Anwendung den Betrieb verweigern.
ANS-038	Zur Festlegung dieses Vorgehens MUSS der Hersteller ein Konzept für Schwachstellen- und Patchmanagement pflegen.
ANS-039	Der Hersteller MUSS sich über eine schriftliche Erklärung verpflichten, vor der Verwendung von externen Bibliotheken und Frameworks deren Quelle auf Vertrauenswürdigkeit zu prüfen.
ANS-040	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.
ANS-041	Die Anwendung DARF sensible Daten NICHT an Drittanbieter-Software weitergeben.
ANS-042	Über Drittanbieter-Software eingehende Daten SOLLTEN validiert werden.
ANS-043	Drittanbieter-Software, die nicht länger vom Hersteller oder Entwickler gewartet wird, DARF NICHT verwendet werden.
	[BSI TR-03170-2] Kapitel 2.4.3 Anforderungen an die Implementierung
ANS-044	Der Hersteller MUSS ein Konzept für Vorgehen und Design der Implementierung pflegen.
ANS-045	IT-Sicherheit MUSS ein fester Bestandteil des Softwareentwicklungs- und Lebenszyklus für die gesamte Anwendung sein und sich in dem Implementierungskonzept wiederfinden.
ANS-046	Bereits in der Design-Phase der Anwendung MUSS berücksichtigt werden, dass die Anwendung in der Produktiv-Phase sensible Daten verarbeiten wird.
ANS-047	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.

Anforderungs-ID	Anforderung
ANS-048	Sicherheitsfunktionen (z.B. Schemavalidierung, Authentifizierung und Autorisierung etc.) SOLLTEN sowohl in der Anwendung als auch auf allen Schnittstellen und API-Endpunkten, implementiert werden.
ANS-049	Der Hersteller MUSS dem Nutzer eine barrierearme Möglichkeit bereitstellen, um Sicherheitsprobleme zu melden.
ANS-050	Die Anwendung und Updates SOLLTEN durch Einsatz kryptografischer Verfahren verschlüsselt und signiert werden.
ANS-051	Nutzereingaben MÜSSEN vor deren Verwendung geprüft werden, um potenziell bösartige Werte vor der Verarbeitung herauszufiltern.
ANS-052	Der Hersteller MUSS alle Eingabedaten vollständig mit einer Escape-Syntax versehen.
ANS-053	Fehlermeldungen und Benachrichtigungen DÜRFEN KEINE sensiblen Daten (z. B. user identifier) enthalten.
ANS-054	Potenzielle Ausnahmen im Programmablauf (Exceptions) MÜSSEN abgefangen, kontrolliert behandelt und protokolliert werden.
ANS-055	Bei Ausnahmen im Programmablauf (Exceptions), mit sicherheitskritischen Auswirkungen, SOLLTE die Anwendung Zugriffe auf sensible Daten abbrechen.
ANS-056	Alle Optionen zur Unterstützung der Entwicklung (z. B. Log-Aufrufe, Entwickler-URLs, Testmethoden, etc.) MÜSSEN in der Produktiv-Version deaktiviert sein.
ANS-057	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.
ANS-058	Die Anwendung SOLLTE beim Beenden alle nutzerspezifischen Daten im Arbeitsspeicher sicher überschreiben.
ANS-059	Die Anwendung MUSS dem Nutzer barrierearme Best-Practice-Empfehlungen, zum sicheren Umgang mit der Anwendung und ihrer Konfiguration bereitstellen.
ANS-060	Die Anwendung MUSS den Start in einer Entwicklungs-/Debugumgebung sicher erkennen und unterbinden.
ANS-061	Die Anwendung SOLLTE Härtungsmaßnahmen, wie etwa eine Integritätsprüfung bei jedem Start der Anwendung, realisieren.
ANS-062	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.
ANS-063	Die Anwendung MUSS den Nutzer auf den Zweck der anzufragenden Berechtigungen und auf die Auswirkungen hinweisen, die eintreten, falls der Nutzer diese nicht gewährt.
	[BSI TR-03170-2] Kapitel 2.4.4 Authentifizierung und Autorisierung

Anforderungs-ID	Anforderung
ANS-064	Für die Registrierung und die Anmeldung vor jedem Hochladen eines Lichtbilds gelten die Anforderungen [BSI TR-03170-1] Kapitel 2.5, 2.6 und 2.7.3.
ANS-065	Der Hersteller MUSS ein Konzept zur Authentifizierung, Autorisierung (Rollenkonzept) und zum Beenden einer Anwendungssitzung erstellen.
ANS-066	Wurde die Anwendung unterbrochen (in den Hintergrundmodus versetzt), MUSS eine erneute Authentifizierung gefordert werden.
	[BSI TR-03170-2] Kapitel 2.4.5 Anforderungen an die Sicherheit der Daten
ANS-067	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.
ANS-068	Sofern es nicht für den vorgesehenen primären Zweck einer Anwendung erforderlich ist, DÜRFEN sensible Daten NICHT mit Dritten geteilt werden.
ANS-069	Die Anwendung MUSS den Nutzer über die Konsequenzen einer eventuellen Weitergabe der Daten vollumfänglich informieren und sein Einverständnis einholen (OPT-IN).
ANS-070	Die Anwendung DARF sensible Daten NICHT auf dem Bildschirm darstellen, außer dies ist für den Zweck der Anwendung erforderlich.
ANS-071	Die Anwendung DARF KEINE Ressourcen gegenüber Dritten verfügbar machen, die einen Zugriff auf sensible Daten ermöglichen.
ANS-072	Alle erhobenen sensiblen Daten DÜRFEN NICHT über die Dauer ihrer jeweiligen Verwendung hinaus in der Anwendung gehalten werden.
ANS-073	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.
ANS-074	Die Anwendung DARF KEINE sensiblen Daten in Logfiles oder andere Meldungen oder Benachrichtigungen, die nicht vom Nutzer explizit eingeschaltet wurden, schreiben.
ANS-075	Die Anwendung MUSS sicherstellen, dass bei ihrer Deinstallation alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen auf dem Endgerät vollständig gelöscht werden.
	[BSI TR-03170-2] Kapitel 2.4.6 Softwareseitige Anforderungen an die Kommunikation
ANS-076	Jegliche Netzwerkkommunikation der Anwendung MUSS durchgängig mit TLS verschlüsselt werden.
ANS-077	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.

Anforderungs-ID	Anforderung
ANS-078	Die Anwendung MUSS entweder die Sicherheitsfunktionalität der jeweilig verwendeten Betriebssystem-Plattform oder sicherheitsüberprüfte Frameworks oder Bibliotheken verwenden, um sichere Kommunikationskanäle aufzubauen.
ANS-079	Die Anwendung MUSS Zertifikatspinning unterstützen, d. h. sie DARF KEINE Zertifikate akzeptieren deren Zertifikatskette dem Hersteller nicht vertrauenswürdig erscheint, siehe RFC 7469.
ANS-080	Die Anwendung MUSS das Server-Zertifikat der Cloud überprüfen.
ANS-081	Die Anwendung MUSS die Integrität der Antworten der Cloud validieren.

Begriffserklärung

Grace Period ..... Übergangsfrist, in der die Software mit bekannter Schwachstelle weiter genutzt werden kann.
Sensible Daten ..... Personenbezogene Daten nach Art.4 Abs.1 DSGVO, sowie insbesondere biometrische Daten nach Art.4 Abs.14 DSGVO.
TOT ..... Target of Test

Literaturverzeichnis

Amtsblatt der Europäischen Union. 2016. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO). [Online] 2016. [Zitat vom: 21. 08 2023.] https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679.

Bundesamt für Justiz, BfJ. 2004. Aufenthaltsverordnung (AufenthV). [Online] 2004. [Zitat vom: 09. 01 2024.] https://www.gesetze-im-internet.de/aufenthv/.

Bundesamt für Justiz, BfJ. 2010. Verordnung über Personalausweise, eID-Karten für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums und den elektronischen Identitätsnachweis (PAuswV). Bundesamt für Justiz, BfJ. [Online] 2010. https://www.gesetze-im-internet.de/pauswv/index.html.

Bundesamt für Justiz, BfJ. 2007. Verordnung zur Durchführung des Passgesetzes (PassV). [Online] 2007. [Zitat vom: 09. 01 2024.] https://www.gesetze-im-internet.de/passv_2007/index.html.

Bundesamt für Sicherheit in der Informationstechnik, BSI. 2023. BSI TR-03121 Biometrie in hoheitlichen Anwendungen. [Online] 2023. [Zitat vom: 09. 01 2024.] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03121/TR-03121_node.html.

Bundesgesetzblatt. 2020. Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen. [Online] 11. 12 2020. [Zitat vom: 10. 01 2024.] https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__//*[@attr_id='bgbl120s2744.pdf'].

International Organisation for Standardization, ISO. 2014. *Information technology - Procedures for the operation of object identifier registration - Part 8: Generation of universally unique identifiers (UUIDs) and their use in object identifiers, ISO/IEC 9834-8.* s.l. : ISO, 2014.

2024. Verordnung zur Erfassung und Qualitätssicherung des Lichtbildes und der Fingerabdrücke in den Passbehörden und der Übermittlung der Passantragsdaten an den Passhersteller (PassDEÜV). [Online] 2024. https://www.gesetze-im-internet.de/passde_v/.