Zusammenfassung wichtige Inhalte der BSI TR-03121-3:

Technische Richtlinie TR-03170 Sichere digitale Übermittlung biometrischer Lichtbilder von Dienstleistern (z. B. Fotografinnen und Fotografen) an Pass-, Personalausweis- und Ausländerbehörden

a) **Rahmen-TR, Version 1.0**
b) **Teil 1 – Anforderungen an den Cloud-Dienst, Version 1.0**
c) **Teil 2 – Anforderungen an die Software, Version 1.0**

a) Rahmen-TR, Version 1.0

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

2. 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.

3. Rechtliche Grundlagen für die vorliegende Technische Richtlinie sind das Passgesetz [PassG] [6], Personalausweisgesetz [PAuswG] [7], das Aufenthaltsgesetz [AufenthG] [8] sowie die Aufenthaltsverordnung [AufenthV] [9] in der jeweils ab dem 1. Mai 2025 gültigen Fassung. Die entsprechenden erforderlichen Änderungen wurden durch das Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen vom 3. Dezember 2020 (BGBl. I S. 2744) vorgenommen. Durch diese Änderungen sehen die Gesetze Verordnungsermächtigungen für das Bundesministerium des Innern und für Heimat (BMI) bzgl. der sicheren Übermittlung des Lichtbilds vor, welche durch das Gesetz zur Modernisierung des Pass-, Personalausweis- und ausländerrechtlichen Dokumentenwesens vom 8. Oktober 2023 (BGBl. 2023 I Nr. 271) um eine Regelung ergänzt wird, wonach im Rahmen der Passbeantragung bei der Passbehörde im Ausland auch abweichende Verfahren zur Fertigung und sicheren Übermittlung des Lichtbilds durch das BMI geregelt werden können.

1. Die zulässigen Alternativen zur Lichtbilderstellung werden in § 6 Absatz 2 Satz 3 PassG (bzw. entsprechend § 9 Absatz 3 Satz 3 PAuswG sowie der Verweis in § 60 Absatz 2 AufenthV) abschließend genannt: „Das Lichtbild ist nach Wahl der antragstellenden Person

1. durch einen Dienstleister elektronisch zu fertigen und im Anschluss von diesem durch ein sicheres Verfahren an die Personalausweisbehörde zu übermitteln oder
2. durch die Personalausweisbehörde elektronisch zu fertigen, sofern die Behörde über Geräte zur Lichtbildaufnahme verfügt.

Eine Veränderung des Lichtbilds ist nur nach Maßgabe dieses Gesetzes oder nach Maßgabe von Vorschriften, die auf Grund dieses Gesetzes erlassen wurden, zulässig.

2. Die Personalausweisverordnung [PAuswV] und die Passdatenerfassungs- und Übermittlungsverordnung [PassDEÜV] erlauben es grundsätzlich, Lichtbilder elektronisch durch einen Dienstleister zu fertigen und durch ein sicheres Verfahren an die Pass- oder Personalausweisbehörde zu übermitteln. In § 1a PassDEÜV „Fertigung und Übermittlung des Lichtbilds durch ein sicheres Verfahren“ heißt es dazu: „(1) [...] In Fällen, in denen ein Pass bei einer Passbehörde nach § 19 Absatz 1 des Passgesetzes beantragt wird, kann die antragstellende Person einen Dienstleister mit der Fertigung des Lichtbilds beauftragen. Der Dienstleister hat das Lichtbild elektronisch zu fertigen und im Anschluss durch ein sicheres Verfahren an die Passbehörde zu übermitteln. (2) Ein sicheres Verfahren im Sinne des Absatzes 1 Satz 2 ist:

1. die Übermittlung des Lichtbilds an die Passbehörde von einem Dienstleister unter Einbindung eines Cloudanbieters [...].“ Eine entsprechende Regelung findet sich in § 5a PAuswV. Der Ablauf des Verfahrens der Übermittlung des Lichtbilds, die Registrierung und Identifizierung des Dienstleisters bei einem Cloudanbieter sowie die Pflichten des Cloudanbieters sind in den §§ 1b bis 1d PassDEÜV bzw. § 5 Absatz 4 und Absatz 7 und §§ 5a bis 5d PAuswV geregelt. Es ist vorgesehen, dass mehrere Personen dem Dienstleisterkonto (einem Nutzerkonto) zugeordnet werden können. Um eine eindeutige Identifizierung der jeweils übermittelnden Person zu ermöglichen, sieht § 1c Absatz 4 PassDEÜV „Registrierung und Identifizierung eines Dienstleisters bei einem Cloudanbieter“ vor:

(4) Für jede Person, die sich in einem Nutzerkonto nach Absatz 3 registriert hat, wird durch den Cloudanbieter ein Pseudonym erzeugt.“ [...].“ Eine entsprechende Regelung findet sich in § 5c Absatz 4 PAuswV. Darüber hinaus müssen sichere Verfahren nach § 1a Absatz 2 Nummer 1 PassDEÜV dem Stand der Technik entsprechen. In § 2 „Qualitätssicherung“ Absatz 2 heißt es:

„(2) Die technischen und organisatorischen Anforderungen an […] 4. das sichere Verfahren der Übermittlung von Lichtbildern von einem Dienstleister an die Passbehörde sind nach dem Stand der Technik zu erfüllen. Der Stand der Technik ist als niedergelegt zu vermuten in den Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik. Diese sind in der Anlage 1 aufgeführt und gelten in der jeweils im Bundesanzeiger veröffentlichten Fassung.“

Eine entsprechende Regelung findet sich in § 2 Satz 1 Nummer 2 Buchstabe i), Satz 2 und 3 PAuswV. In der Anlage 1 der PassDEÜV sind abschließend diejenigen Technischen Richtlinien aufgeführt, die für die Beurteilung des Stands der Technik nach der PassDEÜV relevant sind. Dort heißt es hinsichtlich der Übermittlung von Lichtbildern an Behörden in Nummer 5: „Anlage 1 Übersicht über die Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik […] 5. BSI: Technische Richtlinie TR-03170, Sichere digitale Übermittlung biometrischer Lichtbilder von Dienstleistern an Pass-, Personalausweis- und Ausländerbehörden.“ Rahmenbedingungen 8 Bundesamt für Sicherheit in der

Informationstechnik 2.1.3 Weitere rechtliche Anforderungen Urheberrechtlich MUSS sichergestellt werden, dass die biometrischen Bilder lizenzfrei von den Behörden zu

3. Urheberrechtlich MUSS sichergestellt werden, dass die biometrischen Bilder lizenzfrei von den Behörden zur Erstellung der hoheitlichen Dokumente genutzt werden können. Dies kann beispielsweise über die AGB der Dienstleister gelöst werden. Auch die Einhaltung der datenschutzrechtlichen Vorgaben aus der EU Datenschutz-Grundverordnung [DSGVO] [12] MUSS gewährleistet sein.

4. Die vorliegende Technische Richtlinie 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 (Informationen zur Zertifizierung nach TR gibt es auf der Webseite des BSI. 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.

5. Der Betrachtungsbereich der Technischen Richtlinie erstreckt sich nicht:
   • auf die Erzeugung der Lichtbilder. Für die Sicherstellung der Bildqualität gelten die Regelungen der [BSI TR-03121] [2], in ihrer aktuellen Fassung;
   • auf die Verarbeitung der Bilder in den IT-Fachverfahren der Pass-, Personalausweis- oder Ausländerbehörden

6. Im Rahmen der sicheren digitalen Lichtbildübermittlung finden die folgenden Prozessschritte statt:
   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 Cloudanbieter MUSS vor Schritt 5 (der Übertragung des Lichtbilds zur Cloud) erfolgen.

6. Der Cloud-Dienst erzeugt einen eindeutigen Identifier für die Integration in den Barcode und sendet diesen zusammen mit einer Bestätigung der erfolgreichen Speicherung des Lichtbilds an den Dienstleister.
7. Es wird ein Barcode mit den notwendigen Daten zum Abruf des Lichtbilds aus der Cloud und zur Integration ins Fachverfahren erzeugt.
8. Der Bürger bekommt den Barcode vom Dienstleister und beantragt bei der Behörde das Ausweisdokument.
9. Die Pass-, Personalausweis- oder Ausländerbehörde fragt den Abruf des elektronischen Lichtbildes beim Cloud-Dienst unter Verwendung der vom Bürger zur Verfügung gestellten Zugangsdaten in Form des Barcodes an und übermittelt in diesem Kontext auch seinen Organisationsschlüssel aus dem DVDV.
10. Dazu prüft der Cloud-Dienst über das DVDV die Berechtigung im Rahmen der dort eingetragenen Rolle, und die Behörde authentisiert sich.
11. 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.
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.

b) Teil 1 – Anforderungen an den Cloud-Dienst, Version 1.0

7. Vorliegen eines C5-Attestierung:
   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.

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

9. Der Anbieter des Cloud-Dienstes MUSS anhand eines Betriebskonzeptes nachweisen, dass er einen Normalbetrieb während der Nutzungszeit, definiert als Nutzungszeit = Randzeit-A + Geschäftszeit + Randzeit-B, der Pass- und Personalausweis- oder Ausländerbehörden und der Dienstleister (z. B. Fotografinnen und Fotografen), gemäß Tabelle 2 gewährleisten kann:

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

10. Zusätzlich zum C5-Testat MÜSSEN mindestens folgende Zertifizierungen und Bescheinigungen vorliegen:
    - [IT-Grundschutz] [3] Zertifikat bzw. [ISO 27001] Zertifikat
    - Nachweis der Einhaltung der [DSGVO] (mindestens durch ein geprüftes Datenschutzkonzept)
    - Nachweis eines wirksamen Business Continuity Management Systems (BCMS) (mindestens durch eine BCM-Leitlinie und Audit-Berichte)) Der Cloud-Anbieter MUSS bestätigen, dass die Organisationseinheiten, Standorte und Verfahren des Cloud Anbieters zur Bereitstellung des Cloud-Dienstes, wie in dieser Technischen Richtlinie spezifiziert, in den genannten Zertifizierungen enthalten sind.

11. 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 Anforderungen an den Cloud-Dienst Bundesamt für Sicherheit in der Informationstechnik 11
    - Die zur Registrierung der Dienstleister notwendigen Daten entsprechend der Vorgaben aus den jeweiligen Gesetzen und Verordnungen (etwa [PassV] [10], [PAuswV] [11], [PassDEÜV] [12], [AufenthV].
    - Nutzerkennungen
    - Pseudonyme (z.B. im Sinne des DKK siehe Kapitel 2.6)

12. Es MUSS ein Registrierungsprozess implementiert werden, der es dem Dienstleister ermöglicht, bei einem Cloudanbieter 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.

13. Darüber hinaus MUSS ein Verfahren etabliert werden, das die Entgegennahme und Prüfung des Nachweises der Dienstleistereigenschaft (gemäß der 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. Die spezifischen Anforderungen an die Nachweise für die Dienstleistereigenschaft werden in den entsprechenden gesetzlichen Vorschriften festgelegt. 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.

14. Beim Anlegen des Dienstleisterkontos MUSS eine eindeutige UUID v4 gemäß [ISO/IEC 9834-8] [18] erzeugt und eindeutig und dauerhaft mit dem Dienstleisterkonto verknüpft werden.

15. 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.

16. 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) [19] erhoben und beim Cloudanbieter gespeichert werden. Dies gilt sowohl für den Dienstleister als auch für dessen Mitarbeiter. Jeder Nutzer MUSS dabei ein individuelles Pseudonym (im Falle der eID das DKK (Dienste- und kartenspezifisches Kennzeichen)) erhalten, das fest mit diesen Daten verknüpft ist. 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 Anforderungen an den Cloud-Dienst 12 Bundesamt für Sicherheit in der Informationstechnik 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] [17] 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] [18] erzeugt und eindeutig und dauerhaft mit dem Nutzeraccount verknüpft werden.

17. Nachvollziehbarkeit/Verantwortlichkeit beim Upload:
    Es MUSS eine eindeutige UUID v4 gemäß [ISO/IEC 9834-8] erzeugt und eindeutig und dauerhaft mit dem Clouddienst verknüpft werden. Diese dient bei der Erzeugung der Nutzerkennung der eindeutigen Identifizierung des Clouddienstes. 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.

18. Kommunikationswege Dienstleister (z. B. Fotografinnen und Fotografen) – Cloud (Upload):
    Für die inhaltliche Absicherung der Daten MUSS auf kryptografische Verfahren gemäß der [BSI TR-03116-4], in ihrer aktuellsten Fassung zurückgegriffen werden. Bei der Nutzung elektronischer Signaturen und Siegel im Rahmen dieser Technischen Richtlinie MUSS mindestens fortgeschritten signiert werden nach den Vorgaben der [Leitlinie für digitale Signatur-/ Siegel-, Zeitstempelformate sowie technische Beweisdaten (Evidence Record)], in ihrer aktuellsten Fassung. 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 Cloudanbieter MUSS vor der Übertragung des Lichtbilds zur Cloud erfolgen.
Der Request (siehe [BSI TR-03170] Kapitel 2.4.2) von der Anwendung des Dienstleisters MUSS, sofern ein Authentifizierungsmittel genutzt wird, was dies unterstützt, über einen mittels Kanalbindung nach [BSI TR03124], 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 BitSequenz 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.

19. Sichere Datenlöschung:
Für die Fristen zur Löschung von Daten sind die Vorschriften aus den jeweiligen Rechtsnormen zu beachten (etwa [PassV], [PAuswV], [PassDEÜV], [AufenthV]). Der Cloud-Anbieter MUSS eine schriftliche Erklärung über die Einhaltung der Vorschriften aus den betroffenen Gesetzen und Verordnungen abgeben (siehe oben). Der Bürgerin / dem Bürger MUSS die Möglichkeit eingeräumt werden, bei Abruf seines Lichtbilds bei der Behörde eine weitere Aufbewahrung des Lichtbilds in der Cloud für spätere Nutzung zu beauftragen. Sollte dies nicht durch die Bürgerin / den Bürger gewünscht sein, so MUSS das Lichtbild unverzüglich durch den Cloudanbieter aus der Cloud gelöscht werden. Wird eine weitere Aufbewahrung des Lichtbilds in der Cloud gewünscht, so MUSS das Lichtbild spätestens nach Ablauf der maximalen gesetzlichen Aufbewahrungsfrist gelöscht werden.

c) Teil 2, Anforderungen an die Software, Version 1.0

20. Der vorliegende Teil der Technische Richtlinie behandelt Anforderungen, die der Zertifizierung der zugehörigen Software, mit der die Bilder vom Dienstleister (z. B. Fotografin oder Fotograf) in die Cloud hochgeladen werden und der zugehörige Barcode mitsamt den notwendigen Informationen (siehe Kapitel 2.3) erstellt wird, zu Grunde liegen. Zertifiziert werden MÜSSEN die für den in [BSI TR-03170] Kapitel 2.4.2 beschriebenen Prozess notwendigen Funktionalitäten der Anwendung.

21. Anforderungen an die Software:
Dieses Kapitel und die darin enthaltenen Unterkapitel definieren die Anforderungen, welche seitens der Software zu erfüllen sind. Die Software zur Lichtbildübertragung durch den Dienstleister hat die Aufgabe:
- das Lichtbild gemäß Kapitel 2.1 zu kodieren,
- einen symmetrischen Schlüssel zu erzeugen,
- das Lichtbild damit zu verschlüsseln,
- das Lichtbild in die Cloud hochzuladen und
- einen Barcode (enthält symmetrischen Schlüssel, Adresse der Cloud und eindeutigen Identifier für das Lichtbild in der Cloud) als Beleg und Übertragungsmedium für den Kunden zu erzeugen.

Zusätzlich kann die Software Aufgaben im Bereich der Registrierung und Nutzerverwaltung übernehmen.

22. Bildkonformität
    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.

23. Anforderung an den Barcode:
    Der Barcode MUSS als DataMatrix ECC 200 nach [ISO/IEC 16022] kodiert sein. Die Symbolgröße des Barcodes MUSS so gewählt werden, dass der Barcode die in der nachfolgenden Tabelle spezifizierten Daten aufnehmen kann. Dabei kann die kleinste mögliche Größe genutzt werden, die alle Daten unter Beachtung der jeweiligen Anforderungen fassen kann. Mögliche Größen können [ISO/IEC 16022] entnommen werden.
24. Druck des Barcodes:
    Der Barcode MUSS unter Berücksichtigung von [ISO/IEC 15415] so gedruckt werden, dass Lesegeräte den Barcode zuverlässig dekodieren können. Beim Ausdruck SOLLTE weißes Papier für den Druck verwendet werden, um zu verhindern, dass es zu Problemen mit dem Kontrast des Barcodes kommt. Bei der Verwendung von Standard-Tintenstrahldruckern SOLLTE mindestens mit einer Modulgröße (Größe eines Blocks eines 2D-Barcodes) von 0,3386 mm Seitenlänge pro Modul gedruckt werden. Dies entspricht 4 Punkten pro Modul-Seitenlänge (d. h. 16 Punkten pro Modul) auf einem 300-dpi-Drucker oder 8 Punkten pro Modul-Seitenlänge (d. h. 64 Punkten pro Modul) auf einem 600-dpi-Drucker. Kleinere Druckformate KÖNNEN akzeptabel sein, wenn hochauflösende Drucker oder Laserdrucker verwendet werden. Der Barcode MUSS für die maximale Abrufzeit des Lichtbildes gemäß [PassV], [PAuswV], [PassDEÜV], [AufenthV] gültig sein.

25. Authentifizierung und Autorisierung:
    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 dokumentieren. Wurde die Anwendung unterbrochen (in den Hintergrundmodus versetzt), MUSS eine erneute Authentifizierung gefordert werden.

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

27. Teilung sensibler Daten:
    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).

28. Softwareseitige Anforderungen an die Kommunikation:

Jegliche Netzwerkkommunikation der Anwendung MUSS durchgängig mit TLS verschlüsselt werden. Die Konfiguration der TLS-Verbindungen MUSS dem aktuellen Stand der Technik entsprechen und den Vorgaben und Empfehlungen der [BSI TR-03116-4], in ihrer aktuellsten Fassung folgen. Die Anwendung MUSS entweder die Sicherheitsfunktionalität der jeweilig verwendeten Betriebssystem Plattform oder sicherheitsüberprüfte Frameworks oder Bibliotheken verwenden, um sichere Kommunikationskanäle aufzubauen. Die Anwendung MUSS Zertifikatspinning unterstützen, d. h. sie DARF KEINE Zertifikate akzeptieren, deren Zertifikatskette dem Hersteller nicht vertrauenswürdig erscheint, siehe [RFC 7469].