Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

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

Rahmenbedingungen und Call for Proposals

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	05.03.2021	Referat DI 15	Veröffentlichung

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
ausschreibunglichtbild@bsi.bund.de
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2021

Inhalt

1 Einleitung ... 4
2 Grundlegende Rahmenbedingungen ... 5
2.1 Betrachtungsgegenstand ... 5
2.2 Außerhalb der Betrachtung ... 5
2.3 Prozessbeschreibung ... 5
2.4 Rechtliche Rahmenbedingungen ... 6
2.5 Funktionale Anforderungen ... 7
2.5.1 Voraussetzungen und Registrierungsprozess ... 7
2.5.2 Übermittlung der Lichtbilder ... 7
3 Call for Proposals ... 10
3.1 Prozessablauf ... 10
3.1.1 Zielsetzung ... 10
3.1.2 Auswahlverfahren ... 10
3.1.3 Begutachtung und Vollständigkeit der Unterlagen ... 10
3.2 Kontakt ... 10

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**[1] im Bundesgesetzblatt veröffentlicht. Ziel des Gesetzes ist es, technologischen Entwicklungen, insbesondere dem Morphing, durch gezielte Sicherheitsmaßnahmen zu begegnen.

Gefährdungslage durch Morphing

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

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

Stärkung der Sicherheit durch Verfahren zur digitalen Übermittlung der Lichtbilder

Das 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**[2] 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-, Personal-ausweis- oder Ausländerbehörde zu senden, bei welcher das Dokument beantragt wird.

Neues Verfahren zur sicheren digitalen Übermittlung der Lichtbilder

Neben der Übermittlung von digitalen Lichtbildern durch Dienstleister mittels De-Mail soll künftig auch ein weiteres Verfahren für Dienstleister zugelassen werden, welches es der Pass-, Personalausweis- oder Ausländerbehörde ermöglicht, ein elektronisches Lichtbild zum Zeitpunkt des Antrages von einem sicheren Speicher abzurufen.

---

1 http://dipbt.bundestag.de/extrakt/ba/WP19/2656/265665.html

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

2 Grundlegende Rahmenbedingungen

Für die Einführung eines solchen Verfahrens sind nun die Dienstleister aufgerufen, Konzepte einzureichen, wie dies umgesetzt werden könnte. Dazu werden im Folgenden grundlegende sicherheitstechnische Rahmenbedingungen und Anforderungen beschrieben, die als Mindestanforderung für eine technische Umsetzung anzusehen sind.

2.1 Betrachtungsgegenstand

Der Betrachtungsbereich des einzureichenden Konzeptes erstreckt sich

- bei der **Bildübermittlung** auf das Format und die Kennung der Lichtbild-Datei sowie auf den **Übertragungsweg,**
- bei der **Bildbereitstellung auf einem sicheren Speicher** auf das Format und die Kennung der Lichtbild-Datei (im Folgenden kurz Bildformat und Bildkennung) und
- auf den **Bildspeicher** (z.B. Cloud-Plattform), aus dem die Lichtbilder durch die Pass-, Personalausweis- oder Ausländerbehörde manuell oder automatisiert abgerufen und an die entsprechenden IT-Fachverfahren übergeben werden können.

2.2 Außerhalb der Betrachtung

Die Erzeugung der Lichtbilder ist nicht Gegenstand des einzureichenden Konzeptes. Hierfür gelten die Regelungen der [BSI TR-03121, Version 5.1].

Auch die Verarbeitung der Bilder in den IT-Fachverfahren der Pass-, Personalausweis- oder Ausländerbehörden werden im Rahmen des einzureichenden Konzeptes nicht betrachtet.

2.3 Prozessbeschreibung

Darstellung der Prozessbeteiligten und Rollenzuordnung

- Anbieter Cloudlösung (privat, Öffnung für mehrere Anbieter)
- Pass-, Personalausweis- oder Ausländerbehörde

Beschreibung des Prozesses

- Bürgerin/Bürger lässt vom Dienstleister ein biometrisches Lichtbild aufnehmen;
- Dienstleister lädt dieses Bild beim Cloud-Anbieter hoch;
- Bürgerin/Bürger bekommt Zugangsdaten vom Dienstleister;
- Bürgerin/Bürger beantragt bei der Behörde das Ausweisdokument;
- Die Pass-, Personalausweis- oder Ausländerbehörde ruft das elektronische Lichtbild beim Online-Dienstleister unter Verwendung der von der Bürgerin/dem Bürger zur Verfügung gestellten Zugangsdaten ab und integriert dieses in ihr IT-Fachverfahren.

2.4 Rechtliche Rahmenbedingungen

Personalausweisverordnung (PAuswV)

Die Personalausweisverordnung (PAuswV) erlaubt es grundsätzlich, Lichtbilder elektronisch an die Pass- oder Personalausweisbehörde zu übermitteln. In § 7 PAuswV „Qualitätssicherung des Lichtbildes und der Fingerabdrücke“ heißt es dazu:

„(1) [...] Wenn die Personalausweisbehörde die technischen Voraussetzungen geschaffen hat, kann das Lichtbild auch

1. von Dritten elektronisch verschlüsselt und signiert an die Personalausweisbehörde übermittelt werden, soweit diese Form der Übermittlung durch eine Technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik vorgesehen ist, oder
2. durch die Personalausweisbehörde gefertigt werden“ [...].

Dabei ist „signiert“ in dem Sinne zu verstehen, dass Authentizität des Absenders und Integritätsschutz der Nachricht gewährleistet sein müssen. Darüber hinaus muss die Verschlüsselungsanforderung aus der PAuswV erfüllt werden.

Entsprechende Regelungen finden sich in der Aufenthaltsverordnung (vgl. §§ 60, 61b, 76b, 76c AufenthV).

Änderungen an der PAuswV sind im weiteren Verfahren nicht ausgeschlossen.[3]

Weitere gesetzliche Anforderungen

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

Auch die Einhaltung der datenschutzrechtlichen Vorgaben aus der EU Datenschutz-Grundverordnung müssen gewährleistet sein.

[3] Die einzureichenden Konzepte müssen sich demnach nicht zwingend in dem derzeit bestehenden regulativen Rahmen bewegen.

2.5 Funktionale Anforderungen

2.5.1 Voraussetzungen und Registrierungsprozess

Voraussetzungen seitens Behörden

- Das eingereichte Konzept muss mit mindestens einer Pass-, Personalausweis- oder Ausländerbehörde abgestimmt sein, die bereit ist, dieses als Sponsoring-Behörde umzusetzen. Hierbei sollen notwendige technische Voraussetzungen seitens der Kommune berücksichtigt und überprüft werden (z. B. Zugriff auf das offene Internet zum Abruf der Lichtbilder).

Voraussetzungen seitens Dienstleister

- Die Registrierung zur E-Passfoto-Cloud steht jedem offen. Die Schnittstelle zur E-Passfoto-Cloud wird dokumentiert und kann unter Einhaltung von Sicherheitsvorkehrungen gegen Entgelt genutzt werden.

Registrierungsprozess des Dienstleisters

- Die Cloudlösung soll einen Registrierungsprozess[4] der Dienstleister durch den Anbieter vorsehen. Dieser soll es ermöglichen, dass die Identität des Dienstleiters eindeutig und fest verbunden mit dem Lichtbild an die zuständige Behörde übermittelt werden kann. Grundsätzlich sollte die Identität der lichtbildaufnehmenden Stelle (vgl. § 21 Abs. 2 Nr. 17 PassG-2025 bzw. § 23 Abs. 3 Nr. 20 PAuswG-2025) so individuell wie möglich erfasst werden (Daten zur handelnden Person und ggf. zum entsprechenden Gewerbe). Wo dies nicht möglich ist (z.B. bei einem Self Service Terminal), ist das verantwortliche Unternehmen als lichtbildaufnehmenden Stelle zu benennen.
- Registrierung und Anmeldung der Dienstleister zur E-Passfoto-Cloud erfolgt auf dem eIDAS-Sicherheitsniveau „hoch“. Zur Umsetzung muss ein nach eIDAS notifiziertes Verfahren eingesetzt werden. Zudem muss die Anerkennung aller auf dem Sicherheitsniveau „hoch“ notifizierten Verfahren der europäischen Partner berücksichtigt werden (Art. 6 eIDAS-Verordnung).

2.5.2 Übermittlung der Lichtbilder

Minimalanforderungen nach BSI TR-03121 Version 5.1 (seit 01.11.2020 verpflichtende TR-Version nach Passgesetz/Passausweisverordnung)

- Keine mehrfache Komprimierung
- Kein Hochskalieren
- Kein Postprocessing (Überarbeitung des Bildes, Pose-Correction, etc.)
- Es sind mindestens 2 Formate zu erstellen:
  - JPEG (Personalausweisregister) & JPEG2000 (Chipbild), plus ggf. „Hologrammbild“ (größer) (könnte ggf. auch von Behörde/Cloud erstellt werden)
  - Es muss sichergestellt werden, dass es sich bei den verschiedenen Formaten immer um das identische Bild handelt.

[4] Das Bundesministerium des Innern, für Bau und Heimat und das Bundesamt für Sicherheit in der Informationstechnik behalten sich vor, davon abweichend den Prozess der Identifizierung von Dienstleistern so zu regeln, dass dieser in den Zuständigkeitsbereich einer Behörde fällt.

Elektronische medienbruchfreie Übermittlung

- Passbildsoftware E-Passfoto-Cloud ist per Schnittstelle an die Geräte der Dienstleister angeschlossen. Von der Aufnahme bis zur Abspeicherung in der sicheren Cloud findet kein Medienbruch statt.
- Kryptografische Absicherung des Bildes gegen Veränderung
- Signaturen/Siegel und Zeitstempel sollten eingesetzt werden. Diese müssen entweder von der Behörde validiert werden können oder vom Dienstleister, der der Behörde die korrekte Validierung bestätigt.

Technische Prüfung des Bildes auf Geeignetheit / Biometrieprüfung

- Prüfung des Passbildes auf biometrische Qualität durch den Dienstleister
- Definition des Parametersatzes (ist noch festzulegen)
- Es muss vor dem Abruf des Bildes durch die jeweilige Pass-, Personalausweis- oder Ausländerbehörde gemäß [BSI TR-03121, Version 5.1] eine Software-Qualitätsbewertung auf dem Bild durchgeführt werden (siehe TR-Funktionsmodul QA-FI-SB, Qualitätsbewertung nach ISO 19794-5:2005/2011). Hierzu soll umgehend eine Rückmeldung über das System an den Dienstleister erfolgen. Dies hat den Hintergrund, dass die Aufnahme ggf. wiederholt werden kann und dem Bürger so ein unnötiger Gang in die jeweilige Behörde erspart bleibt.
- Übermittlung der zu speichernden Daten des Dienstleisters an die Pass-, Personalausweis- oder Ausländerbehörde in einem für die Pass-, Personalausweisregister oder Ausländerzentralregister (AZR) übernahmefähigen Format
- Für das Bildformat und die Bilderkennung werden die folgenden Parameter vorgesehen:

Parameter	Spezifikation JPEG-2000 (Chipbild)	Spezifikation JPEG (Registerbild)	Hologramm-Bild
Dateiformat	JPEG-2000	JPEG	Noch festzulegen
Dateigröße	ca. 15 kB	ca. 25 KiB	Noch festzulegen
Farbtiefe	24-Bit RGB oder 8-Bit Graustufen	24-Bit RGB oder 8-Bit Graustufen	Noch festzulegen
Auflösung	413 Pixel (Breite) x 531 Pixel (Höhe)	413 Pixel (Breite) x 531 Pixel (Höhe)	Noch festzulegen
Dateisendung	.jp2	.jpeg/.jpg	Noch festzulegen
Bildkennung	14-stellig, Kleinbuchstaben und Ziffern; entsprechend der unten folgenden Beschreibung	14-stellig, Kleinbuchstaben und Ziffern; entsprechend der unten folgenden Beschreibung	14-stellig, Kleinbuchstaben und Ziffern; entsprechend der unten folgenden Beschreibung
Dateiname	Bildkennung + Dateiendung	Bildkennung + Dateiendung	Bildkennung + Dateiendung

Tabelle 2: Technische Parameter Bildformat und Bildkennung

Als Dateigröße für das Chipbild sind 15 kB vorgesehen, mit einer Abweichung von +/- 5% gemäß [BSI TR-03121], Version 5.1, Teil 3.2. Es ist zu beachten, dass für die Komprimierung der Bilddaten eine bestätigte Implementierung von JPEG-2000 verwendet werden muss, z.B. JASPER, LuraWave, Aware. Darüber hinaus ist zu beachten, dass die Bilddaten nur einmal komprimiert werden dürfen, d.h. mehrere verlustbehaftete Komprimierungen nacheinander sind verboten.

Sichere Speicherumgebung

- BSI-zertifizierte Cloud (C5-Testat) inkl. IT-Grundschutz bzw. ISO 27001 Zertifikat müssen eingesetzt werden (siehe BSI IT-Grundschutz).
- Die Lichtbilder müssen in einer durch das BSI zertifizierten Methode in der Cloud abgespeichert werden.
- Eine Bearbeitung auf Basis der erlaubten Anpassung des Lichtbildes erfolgt nur in der Cloud. Eine Anpassung kann sinnvoll sein, damit das Lichtbild druckbar wird. Die Geräte in den Fotostudios dienen der Bilddarstellung. Sollte hier eine manuelle Anpassung möglich sein, dann würde diese nicht auf dem Gerät im Fotostudio erfolgen, sondern nur per Steuerbefehl in der Cloud.
- Die biometrischen Bilder dürfen nicht unverschlüsselt in der Cloud liegen.

Abruf der Lichtbilder durch Pass- oder Personalausweisbehörde

- Die Lichtbilder müssen DSGVO-konform abgelegt und mit einem Beiblatt/Token versehen werden. Über diesen Token kann im Amt das korrekte Lichtbild in das IT-Fachverfahren der Behörde integriert werden.

3 Call for Proposals

3.1 Prozessablauf

Nutzen Sie die Möglichkeit, sich mit einem eigenen Konzept an der Erstellung einer Technischer Richtlinie zum Thema „Neues Übertragungsverfahren zur sicheren elektronischen Übermittlung von Lichtbildern an die Pass-, Personalausweis- oder Ausländerbehörde“ zu beteiligen und Ihre Ideen einzubringen.

3.1.1 Zielsetzung

Erstellung einer Technischen Richtlinie zum Thema „Sichere elektronische Übermittlung von Lichtbildern durch Dienstleister mittels Cloud-Plattform zum Abruf durch Pass-, Personalausweis- oder Ausländer-behörde“.

3.1.2 Auswahlverfahren

Die Einreichungen unterliegen einem Auswahlverfahren, in dem neben den inhaltlichen Aspekten der Konzepte auch deren mögliche Umsetzung Berücksichtigung findet.

3.1.2.1 Umfang

Einreichungen sollen in deutscher Sprache erfolgen. Die Einreichung besteht aus einem Deckblatt mit Titel, Name/n und Kontaktangaben sowie einem anonymisierten Textteil.

3.1.2.2 Zeitplan

09.03.2021: Veröffentlichung Call for Proposals auf der BSI-Webseite

16.04.2021: Deadline für die Einreichung der Konzeptpapiere (Fristverlängerung)

07.05.2021: Beginn Erstellung des Entwurfs einer Technischen Richtlinie

3.1.3 Begutachtung und Vollständigkeit der Unterlagen

Nach der Einreichungsfrist sichtet ein Ausschuss – bestehend aus **Experten aus unterschiedlichen Referaten des BSI und BMI** – alle Einreichungen.

Alle Einreichungen werden anonym (double-blind) begutachtet. Der Ausschuss bewertet die Einreichungen fachlich. Anschließend erstellt er aus den Einreichungen eine Technische Richtlinie.

Bitte beachten Sie, dass unvollständige Vorschläge keine Berücksichtigung finden können.

Ebenfalls erfolgt eine inhaltliche Bewertung in Bezug auf sicherheitstechnische Anforderungen, sodass ggf. nicht jedes Konzept, welches die Rahmenbedingungen erfüllt, in der Erstellung der Technischen Richtlinie Berücksichtigung findet.

3.2 Kontakt

Bitte senden Sie Ihre Einreichungen bis zum 16.04.2021 als PDF-Dokument per E-Mail an: ausschreibunglichtbild@bsi.bund.de.