Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

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

Konzept zur Eintragung von Cloud-Diensten zur sicheren elektronischen Übermittlung von biometrischen Lichtbildern in das Deutsche Vewaltungsdiensteverzeichnis (DVDV)

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
0.1	12.01.2022	Referat DI 15	Erster Grobentwurf
0.2	20.03.2023	Referat DI 15	Besprochene Anpassungen mit DVDV-Koordinierungsstelle des ITZ-Bund

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

Inhalt

1 Einleitung 5
1.1 Rechtsgrundlage 5
1.2 Prozessbeschreibung 6
2 Kommunikationsbeziehungen 8
2.1 Kommunikation der Pass-, Personalausweis- und Ausländerbehörden mit den Anbietern der Lichtbild-Cloud 9
3 DVDV-Organisationskategorien, DVDV-Präfixe und DVDV-Schlüssel 10
3.1.1 Passbehörde (psb) 10
3.1.2 Personalausweisbehörde (pab) 10
3.1.3 ausländerrechtliche Behörde (azr) 10
3.1.4 Auslandsvertretung (?) ..... **Fehler! Textmarke nicht definiert.**
3.1.5 Anbieter Lichtbild-Cloud 10
4 Dienstprovider, pflegende Stellen, etc. 12
4.1 DVDV-Dienstprovider 12
4.2 E-Mailadresse 12
4.3 Pflegende Stellen 12
4.4 DVDV-Server 12
4.5 Intermediäre 12
4.6 Eintragung der Dienste 12

1 Einleitung

Die Technische Richtlinie (BSI TR-03170) zur „Sicheren Übermittlung von biometrischen Lichtbildern an Pass-, Personalausweis-, oder ausländerrechtliche Behörden“ beschreibt die elektronische Übermittlung von biometrischen Lichtbildern von Dienstleistern (z.B. Fotografen) über eine zertifizierte Cloud-Umgebung an Pass-, Personalausweis oder ausländerrechtliche Behörden.

Ihre Anwendung ist ab dem 1. Mai 2025 gemäß der Verordnung *(in Erstellung, vsl. ab Sommer 2022 verfügbar)* zum **Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen (PassAuswRÄndG)** verbindlich vorgegeben.

Das vorliegende Eintragskonzept beschreibt, wie die in der Technischen Richtlinie definierten Dienste und Kommunikationsszenarien im DVDV abzubilden sind.

1.1 Rechtsgrundlage

Am 11. Dezember 2020 wurde das vom Deutschen Bundestag und Bundesrat verabschiedete **Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen (PassAuswRÄndG)**[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 ausländer-rechtliche 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.

Die vorliegende Version der Technischen Richtlinie (TR) regelt die Form der digitalen Übermittlung von biometrischen Lichtbildern von Dienstleistern über eine sichere Cloud-Umgebung an Pass-, Personalausweis- oder Ausländerbehörden und definiert Anforderungen für die Zertifizierung von Cloud-Diensten für dieses spezielle Verfahren.

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

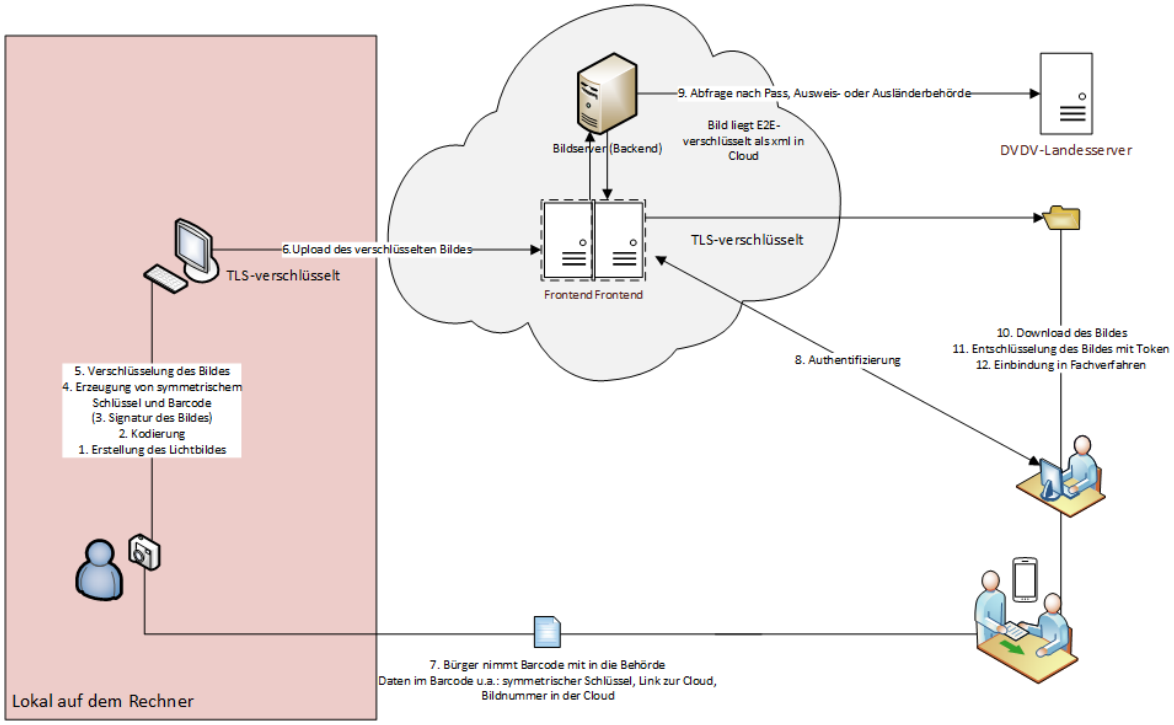
1.2 Prozessbeschreibung

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

1. Die Bürgerin/der Bürger lässt vom registrierten Dienstleister ein biometrisches Lichtbild (inkl. Meta-Informationen zur Aufnahme, z. B. Marke/Modell der Aufnahmeeinheit, verwendete Software) erstellen.
2. Das ausgewählte Lichtbild wird kodiert (s. Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**).
3. *Gegebenenfalls wird das Lichtbild durch den Dienstleister signiert.* [2]
4. Sowohl der symmetrische Schlüssel als auch der Barcode werden erzeugt.
5. Das Lichtbild wird mit dem symmetrischen Schlüssel verschlüsselt.
6. Der Dienstleister überträgt das verschlüsselte Lichtbild über die Upload-Schnittstelle an den Cloud-Dienst.
7. Der Bürger bekommt einen Barcode vom Dienstleister und beantragt bei der Behörde das Ausweisdokument.
8. 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.
9. Dazu prüft der Cloud-Dienst über das DVDV die Berechtigung im Rahmen der dort eingetragenen Rolle, und die Behörde authentisiert sich.
10. Die Behörde lädt das Lichtbild herunter.
11. Anschließend wird *die ggf. vorgenommene Signatur* validiert und das Lichtbild entschlüsselt. Die Entschlüsselung ist nur möglich, wenn der Behörde der korrekte Schlüssel als Teil des Barcodes ausgehändigt wurde.
12. Das Lichtbild wird in das behördliche IT-Fachverfahren zur Ausstellung des Dokuments eingebunden.

[2] Die Signatur des Bildes hängt vom Registrierungsprozess ab, der durch die BMI-Verordnung zu spezifizieren ist.

Upload und Download des Lichtbildes - Lokale Lösung (E2E)



2 Kommunikationsbeziehungen

Details zu den Kommunikationsbeziehungen können der jeweils gültigen Fassung der TR-03170 entnommen werden. Der fertigen TR-03170 wird eine Spezifikation für die Abrufschnittstelle beiliegen.

Die Kommunikation zum Abruf eines verschlüsselten Lichtbilds bei der Cloud durch die Behörde läuft folgendermaßen ab:

1. Cloud und Behörde bauen eine sichere Verbindung mittels TLS Client Authentication auf. Hierbei muss [BSI TR-03116-4, in ihrer aktuellsten Fassung] beachtet werden. Es müssen die im [DVDV] hinterlegten Zertifikate von Cloud und Behörde genutzt werden.
2. Die Cloud prüft per DVDV-VerifyCategory-Anfrage die Behördenkategorie auf Pass-, Personalausweis oder Ausländerbehörde.
3. Prüfung der Behördenkategorie:
   a Bei erfolgreicher Prüfung der Behördenkategorie liefert die Cloud eine Statusmeldung zur erfolgreich abgeschlossenen Prüfung der Behörde zurück.
   b Bei nicht erfolgreicher Prüfung liefert die Cloud eine Fehlermeldung und einen entsprechenden Fehler-Status "falsche" Organisationskategorie zurück und die Verbindung wird abgebaut.
4. Die Behörde sendet einen Request zum Abruf des Lichtbildes mit der aus dem Barcode ausgelesenen eindeutigen ID des Lichtbildes in der Cloud.
5. Die Cloud sendet das zu der ID gehörende verschlüsselte Lichtbild sowie weitere Daten nach dieser Technischen Richtlinie (siehe TR-03170 Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) an die Behörde.
6. Die Verbindung wird abgebaut.

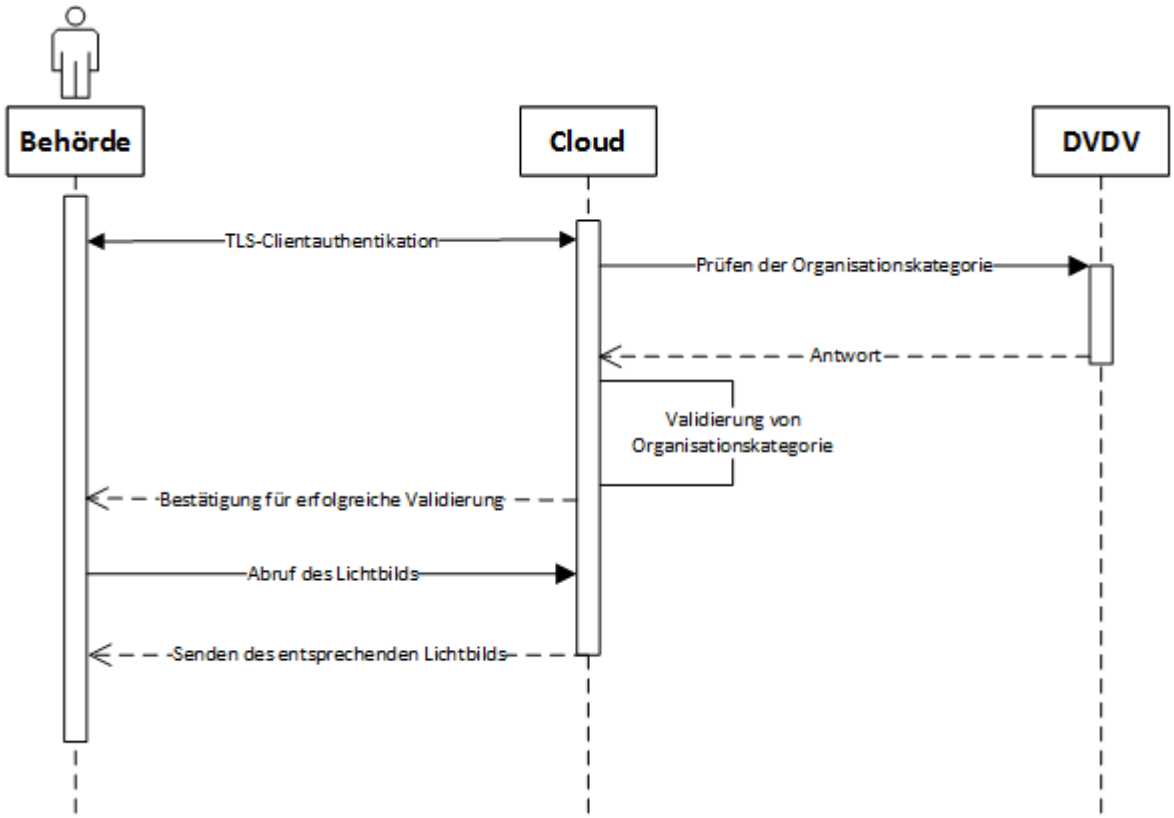


Abbildung 1: Kommunikation Cloud zu Behörde

Die Datenübertragung Cloud-Dienst und Behörde muss synchron erfolgen.

Kommunikation mit dem DVDV

Für Abfragen gegen das DVDV-System gelten grundsätzlich die Vorgaben der DVDV-Verfahrensbeschreibung [DVDV].
Für die im Kontext dieser TR stattfindenden Abfragen gegen das DVDV-System gelten die folgenden Regelungen:

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

2.1 Kommunikation der Pass-, Personalausweis- und Ausländerbehörden mit der Lichtbild-Cloud

Die Kommunikation deckt die Datenübermittlungen zwischen Pass-, Personalausweis- und Ausländerbehörden und den Cloudanbietern der Cloud für die elektronische Übertragung der Lichtbilder ab.

Die Kommunikation geht von den Pass-, Personalausweis- oder Ausländerbehörden aus.

Für die Kommunikation wird eine Abfragemethode genutzt, die im Rahmen der TR-03170 spezifiziert und der Spezifikation gemeinsam mit der TR-03170 veröffentlicht wird.

Dieser Dienst wird außerhalb des DVDV genutzt und das DVDV dient lediglich der Identifizierung der Kommunikationsteilnehmer Cloud und Pass-, Personalausweis- oder Ausländerbehörde und dem Verbindungsaufbau über die dort hinterlegten Zertifikate. Entsprechend wird kein Dienst im DVDV hinterlegt.

2.2 Cloudanbieter Zertifikate

Sämtliche Zertifikate für Anbieter der Lichtbildclouds müssen von CAs der PKI-1-Verwaltung (BSI PKI-1-Verwaltung) ausgestellt werden. Die jeweils gültigen Anforderungen der PKI-1-Verwaltung sind hierbei einzuhalten. Diese Zertifikate werden für den Aufbau der Kommunikation auf Transportebene verwendet.

3 DVDV-Organisationskategorien, DVDV-Präfixe und DVDV-Schlüssel

Im Kontext der Technischen Richtlinie sind folgende Behördenkategorien relevant:

3.1.1 Passbehörde (psb)

Im Kontext der Erstellung von hoheitlichen Dokumenten wird im DVDV bereits der Dienst Dh2BehService OSCI im Rahmen des Fachstandards xhD geführt.
Diesen Dienst nutzen auch Passbehörden aus der gleichnamigen Organisationskategorie (Präfix psb). Alle Behörden aus dieser Organisationskategorie sollen auch den Dienst zum Abruf von Lichtbildern aus der Cloud (2.1) nutzen können.

3.1.2 Personalausweisbehörde (pab)

Im Kontext der Erstellung von hoheitlichen Dokumenten wird im DVDV bereits der Dienst Dh2BehService OSCI im Rahmen des Fachstandards xhD geführt.
Diesen Dienst nutzen auch Personalausweisbehörden aus der gleichnamigen Organisationskategorie (Präfix pab). Alle Behörden aus dieser Organisationskategorie sollen auch den Dienst zum Abruf von Lichtbildern aus der Cloud (2.1) nutzen können.

3.1.3 Ausländerbehörde (azr)

Im Kontext der Erstellung von hoheitlichen Dokumenten wird im DVDV bereits der Dienst Dh2BehService OSCI im Rahmen des Fachstandards xhD geführt.
Diesen Dienst nutzen auch ausländerrechtliche Behörden aus der Organisationskategorie „Ausländerbehörde“ (Präfix azr). Alle Behörden aus dieser Organisationskategorie sollen auch den Dienst zum Abruf von Lichtbildern aus der Cloud (2.1) nutzen können.

3.1.4 Lichtbild-Cloud

Für die elektronische Übertragung von Lichtbildern an Pass-, Personalausweis- und Ausländerbehörden, soll die Organisationskategorie „Lichtbild-Cloud“ eingeführt werden.
Dem Organisationsschlüssel der Organisationskategorie „Lichtbild-Cloud“ wird der Präfix „lic“ zugewiesen

Für die Organisationskategorie „Lichtbild-Cloud“ gibt es keine nutzbaren und vorhandenen Schlüsselsystematiken. Die Codetabelle für die Organisationskategorie „Lichtbild-Cloud“ wird vom Diensteprovider für den Abruf der Lichtbilder aus der Cloud geführt und ist im XRepository unter

https://www.xrepository.de/details/urn:xoev-de:bsi:codeliste:dvdv.lichtbildclouddienste

verfügbar. Die DVDV-pflegende Stelle muss im Rahmen der Eintragung in dem Schlüsselbereich ihres Bundeslandes einen Schlüssel vergeben und diesen dem Diensteprovider für den Abruf der Lichtbilder aus der Cloud melden. Der Vorschlag für den Aufbau der 12-stelligen-Schlüsseltabelle lautet wie folgt:

- Stelle 1-2: Länderschlüssel für den Sitz des Cloudbetreibers
- Stelle 3-10: Vergabebereich für die DVDV-pflegende Stelle. Dabei wäre die Verwendung der Stellen 3-10 wie folgt möglich:
    - Stelle 3-4: Bundeslandkennzeichen und Kennzeichen für bundeslandübergreifende Anwendungen

    - Stelle 5-7: Laufende Nummer
- Stelle 8-10: Reservebereich für noch nicht absehbare Bedürfnisse z.B. Policies
- Stelle 11-12: 00 = Produktion, 01-99= Test

Beispiel:
- DVDV-Organisationskategorie: "Lichtbild-Cloud"
- DVDV-Organisationsschlüssel: "lic:491200100000"

4 Dienstprovider, pflegende Stellen, etc.

4.1 Dienstprovider

Die fachliche Verantwortung für den in diesem Dokument beschriebenen Dienst übernimmt das:
Bundesamt für Sicherheit in der Informationstechnik
Referat DI15 – eID-Lösungen für die digitale Verwaltung
Godesberger Allee 185-189
D-53175 Bonn

4.2 E-Mailadresse

Zur Kommunikation mit dem Dienstprovider dient folgende E-Mail-Adresse:
ausschreibunglichtbild@bsi.bund.de

4.3 Pflegende Stellen

Die DVDV-Pflege wird entsprechend der festgelegten Zuständigkeiten für die Behörden der Länder und der Bundesbehörden vorgenommen.

4.4 DVDV-Server

Die beteiligten Kommunikationspartner bei TR-03170 „Sichere elektronische Übermittlung von Lichtbildern an die Pass-, Personalausweis- oder Ausländerbehörden“ nutzen die bestehenden DVDV-Server entsprechend der festgelegten Zuständigkeiten für die Behörden der Länder und der Bundesbehörden.

4.5 Intermediäre

Die Intermediäre können von den beteiligten Behörden grundsätzlich frei gewählt werden.

4.6 Eintragung der Dienste

Die in diesem Dokument beschriebenen Dienste sollen nicht im DVDV verzeichnet werden. Die Cloudanbieter sollen im DVDV eingetragen werden. Dies soll ab spätestens 1. Mai 2025 produktiv genutzt werden.