Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie TR-03170

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

Teil 2, Anforderungen an die Software, Version 1.2

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
0.1	20.04.2021	BSI	Erster Grobentwurf
0.3	03.12.2021	BSI	Weiterentwicklung
0.4	24.01.2022	BSI	Umstellung und Weiterentwicklung
0.5	21.02.2022	BSI	Fassung Interne Kommentierung
0.6	14.03.2022	BSI	Entwurfsfassung V 0.6 für externe Kommentierung
0.7	30.06.2022	BSI	Einarbeitung der Kommentierungen aus der 1. Kommentierungsrunde
0.85	18.04.2023	BSI	Anpassung gemäß Entwurfsfassung der RVO
0.9	25.07.2023	BSI	Ergänzung der Themen zu Registrierung und Nachvollziehbarkeit, sowie kleinere Anpassungen
0.95	09.08.2023	BSI	Überarbeitung einiger Anforderungen mit Hinblick auf die Zertifizierung
1.0	14.02.2024	BSI	Einarbeitung der Kommentare aus der 2. Kommentierungsrunde und Finalisierung.
1.1	01.08.2024	BSI	Überarbeitung und Aktualisierung einiger Anforderungen bezüglich Ihrer Praxistauglichkeit
1.2	15.01.2025	BSI	Anpassung Barcode und Zertifikatspinning

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 4
1.1 Einordnung 4
2 Anforderungen an die Software 5
2.1 Bildkonformität 5
2.2 Kryptografische Anforderungen 5
2.3 Anforderung an den Barcode 5
2.4 Allgemeine Anforderungen 8
2.4.1 Erzeugung von Zufallszahlen 8
2.4.2 Verwendung von Frameworks und Bibliotheken 8
2.4.3 Anforderungen an die Implementierung 9
2.4.4 Authentifizierung und Autorisierung 10
2.4.5 Anforderungen an die Sicherheit der Daten 10
2.4.6 Softwareseitige Anforderungen an die Kommunikation 10
Literaturverzeichnis 12

1 Einleitung

Die 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 Einordnung

Der vorliegende Teil der Technische Richtlinie behandelt Anforderungen, die der Zertifizierung der 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.

Beschreibung von Kontext und Zielsetzung der Technischen Richtlinie, Voraussetzungen, Definition der Schlüsselwörter (MUSS, SOLLTE, KANN, etc.), rechtliche Rahmenbedingungen, Betrachtungsgegenstand und Abgrenzung, Definition der Zielobjekte und Begrifflichkeiten sowie eine Prozessbeschreibung finden sich im Rahmendokument [**BSI TR-03170**].

Für [**BSI TR-03170-2**] gelten die Anforderungen der **„Anerkennung von Prüfstellen: Programm im Bereich Technischer Richtlinien (TR)“** [1] und der **„Kompetenzfeststellung: Programm im Bereich Technischer Richtlinien (TR)“** [2]. Die Zertifizierung nach TR-03170-1 muss durch, für die Durchführung von Audits zur **Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz zertifizierte „Auditteamleiter“ bzw. „Auditoren“** [3] oder durch nach „**Kompetenzfeststellung: Programm im Bereich der Common Criteria (CC)“** [4] anerkannte **CC-Evaluatoren mit Erfahrung im Bereich ALC (Assurance: Life-Cycle)**, entsprechend anerkannter **CC-Prüfstellen** [5] [6] durchgeführt werden.

2 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.

2.1 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**] [7] bereits zum Zeitpunkt des Uploads des Lichtbildes erfüllt werden. Zusätzlich SOLLTEN Metadaten, die zu diesem Zeitpunkt zum Lichtbild vorliegen, NICHT gelöscht werden.

2.2 Kryptografische Anforderungen

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

Der für die symmetrische Verschlüsselung des Lichtbildes genutzte Schlüssel MUSS nach der Erzeugung, für die Verschlüsselung der Daten verwendet, in den Barcode eingebettet und dann sicher gelöscht werden. Der Schlüssel DARF an KEINER anderen Stelle als in dem spezifischen Barcode gespeichert werden.

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

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

Die Anwendung MUSS für Implementierungen zur Umsetzung kryptografischer Primitive die Empfehlungen der [**BSI TR-02102-1**] [8] in ihrer aktuellsten Fassung umsetzen.

Die Wahl kryptografischer Primitive MUSS passend zum Anwendungsfall sein und dem aktuellen Stand der Technik gemäß [**BSI TR-02102-1**] [8], in ihrer aktuellsten Fassung entsprechen.

Die Stärke der kryptografischen Schlüssel MUSS dem aktuellen Stand der Technik entsprechen gemäß [**BSI TR-02102-1**] [8], in ihrer aktuellsten Fassung.

Die Verschlüsselung des Lichtbilds MUSS clientseitig durch die Software erfolgen.

2.3 Anforderung an den Barcode

Der Barcode MUSS als DataMatrix ECC 200 nach [**ISO/IEC 16022**] [9] 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**] [9] 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**] [9].

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

Tabelle 2: Bytefolgen

Start Tag	***Länge (Byte)***	***Inhalt***
0x00	1	Magische Konstante. Die magische Konstante ist ein feststehender Wert zur Identifikation des hier genutzten Barcode Schemas und ist auf den Wert `0xE2` festgelegt.
0x01	1	Version. Ein Byte-Wert, der die genutzte Version des hier definierten Barcodes angibt. Aktuell gibt es hierbei nur die hier definierte Version `0x01`. Aufsteigende Versionsnummern werden fortlaufend vergeben.
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**] [10].
0x13 + v	1	Längenbyte für den Verschlüsselungsalgorithmus. Ein Byte, welches die Länge des nachfolgenden Feldes für den Verschlüsselungsalgorithmus angibt.

Start Tag	*Länge (Byte)*	*Inhalt*
0x14 + v	x	Verschlüsselungsalgorithmus. Der genutzte Verschlüsselungsalgorithmus MUSS in strukturierter Form als OID angegeben werden (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.
0x15 + v + x + y	1	Längenbyte für das Padding. Ein Byte, welches die Länge des nachfolgenden Feldes für das Padding angibt.
0x16 + v + x + y	p	Padding. Falls ein Padding benötigt wird, wird hier das genutzt Padding angegeben. Dies wird in C40 kodiert.
0x16 + v + x + y + p	1	Längenbyte für den Schlüssel. Ein Byte, welches die Länge des nachfolgenden Feldes für den Schlüssel angibt.
0x17 + 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	0x17 + v + x + y+p+z	

Die Bytefolgen des Barcodes MÜSSEN in Base64 kodiert werden. Dies dient der besseren Interpretation des Barcodes durch die Scanner.

Für die kryptographischen Vorgaben und die Erzeugung des Schlüssels sowie Vorgaben zu damit einhergehenden Betriebsmodi, Initialisierungsvektoren und Padding gelten die Anforderungen aus Kapitel 2.2.

Der Barcode MUSS unter Berücksichtigung von [**ISO/IEC 15415**] [11] 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.

Auf dem Ausdruck des Barcodes DÜRFEN die im Barcode 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**] [12], [**PAuswV**] [13], [**PassDEÜV**] [14], [**AufenthV**] [15] gültig sein.

2.4 Allgemeine Anforderungen

2.4.1 Erzeugung von Zufallszahlen

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

Für Zufallszahlengeneratoren MUSS [**BSI TR-02102-1**] [8], in ihrer aktuellsten Fassung umgesetzt werden.

Alle Zufallswerte MÜSSEN über einen sicheren kryptografischen Zufallszahlengenerator erzeugt werden.

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

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

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

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

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

2.4.2 Verwendung von Frameworks und Bibliotheken

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

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

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

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

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

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

2.4.3 Anforderungen an die Implementierung

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

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.

Der Versionstand der Software MUSS vor der Verbindung mit der Cloud geprüft und auf den aktuellsten Stand aktualisiert werden.

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

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

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

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

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

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

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

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

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

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

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

Die Anwendung 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.

2.4.4 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 erstellen.

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

2.4.5 Anforderungen an die Sicherheit der Daten

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

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

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

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

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

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

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

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

2.4.6 Softwareseitige Anforderungen an die Kommunikation

Jegliche Netzwerkkommunikation der Anwendung MUSS durchgängig mit TLS verschlüsselt werden.

Die Konfiguration der TLS-Verbindungen MUSS dem aktuellen Stand der Technik entsprechen und den Vorgaben und Empfehlungen der [**BSI TR-03116-4**] [16], in ihrer aktuellsten Fassung folgen.

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

Die Anwendung SOLLTE Zertifikatspinning gemäß [**RFC 7469**] [17] unterstützen.

Die Anwendung MUSS das Server-Zertifikat der Cloud überprüfen. Dabei MUSS mindestens die Gültigkeit, der Aussteller und die Domain auf Plausibilität geprüft und der Zertifikatspfad validiert werden.

Die Anwendung MUSS die Integrität der Antworten der Cloud validieren.

Anwendungshinweis/Beispiel: Dies kann z.B. sofern der eingesetzte Betriebsmodus dies ermöglicht im Rahmen von TLS geschehen (z.B. GCM) oder durch eine zusätzliche Methode zur Integritätssicherung sichergestellt werden (z.B. mittels HMAC).

Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik, BSI, „Anerkennung von Prüfstellen: Programm im Bereich Technischer Richtlinien (TR) TR-Prüfstellen," 2024. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/TR-Pruefstellen.pdf. [Zugriff am 17 07 2024].

[2] Bundesamt für Sicherheit in der Informationstechnik, BSI, „Kompetenzfeststellung bei TR-Prüfern," 2024. [Online]. Available: https://www.bsi.bund.de/dok/6616388. [Zugriff am 17 07 2024].

[3] Bundesamt für Sicherheit in der Informationstechnik, BSI, „Zertifizierung als Auditteamleiter," 2024. [Online]. Available: https://www.bsi.bund.de/dok/6617756. [Zugriff am 17 07 2024].

[4] Bundesamt für Sicherheit in der Informationstechnik, BSI, „Kompetenzfeststellung: Programm im Bereich Common Criteria (CC) CC-Evaluatoren," 2021. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/CC-Evaluatoren.html?nn=127548. [Zugriff am 17 07 2024].

[5] Bundesamt für Sicherheit in der Informationstechnik, BSI, „Liste CC / ITSEC Prüfstellen," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-TR/Pruefstellen-Auditoren/Liste_CC-Pruefstellen/Liste_CC-Pruefstellen_node.html. [Zugriff am 31 07 2024].

[6] Bundesamt für Sicherheit in der Informationstechnik, BSI, „Anerkennung: Programm zur Anerkennung als Prüfstelle im Bereich Common Criteria (CC)," 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/CC-Pruefstellen.pdf?__blob=publicationFile&v=10. [Zugriff am 31 07 2024].

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

[8] Bundesamt für Sicherheit in der Informationstechnik, BSI, „BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen," 2023. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html. [Zugriff am 21 08 2023].

[9] International Organisation for Standardization, ISO, Information technology - automatic identification and data capture techniques - Data Matrix bar code symbology specification, ISO/IEC 16022, ISO, 2006.

[10] International Organisation for Standardization, ISO, 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, ISO, 2014.

[11] International Organisation for Standardization, ISO, Information technology - Automatic identification and ata capture techniques - Barcode symbol print quality test specification - Two dimensional symbols, ISO/IEC 15415, ISO, 2011.

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

[13] Bundesamt für Justiz, BfJ, „Verordnung über Personalausweise, eID-Karten für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums und den elektronischen Identitätsnachweis (PAuswV),“ 2010. [Online]. Available: https://www.gesetze-im-internet.de/pauswv/index.html. [Zugriff am 09 01 2024].

[14] Bundesamt für Justiz, BfJ, „Verordnung zur Erfassung und Qualitätssicherung des Lichtbildes und der Fingerabdrücke in den Passbehörden und der Übermittlung der Passantragsdaten an den Passhersteller (PassDEÜV),“ 2007. [Online]. Available: https://www.gesetze-im-internet.de/passde_v/. [Zugriff am 09 01 2024].

[15] Bundesamt für Justiz, BfJ, „Aufenthaltsverordnung (AufenthV),“ 2004. [Online]. Available: https://www.gesetze-im-internet.de/aufenthv/. [Zugriff am 09 01 2024].

[16] Bundesamt für Sicherheit in der Informationstechnik, BSI, „BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung,“ 2023. [Online]. Available: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html. [Zugriff am 21 08 2023].

[17] RFC-Editor, „RFC 7469 - Public Key Pinning Extension for HTTP,“ 2015. [Online]. Available: https://www.rfc-editor.org/rfc/rfc7469. [Zugriff am 09 01 2024].