Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie TR-03147 Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen

Version 1.0.6
28.12.2021

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

Inhaltsverzeichnis

1 Einleitung ... 7
1.1 Zielsetzung und Inhalt der Technischen Richtlinie ... 7
1.2 Struktur und Aufbau der Technischen Richtlinie ... 7
2 Definitionen und Bewertungsmethodik ... 8
2.1 Grundbegriffe ... 8
2.2 Angriffspotential ... 8
2.3 Erfolgreicher Angriff ... 9
2.4 Berücksichtigung und Bewertung des Angriffspotentials ... 10
2.5 Durchführung von Angriffen ... 10
3 ID-Nachweis und ID-Prüfung ... 11
3.1 Schutzziele ... 11
3.2 Bedrohungen ... 11
3.3 Anforderungen ... 11
3.4 Abdeckung der Schutzziele und Bedrohungen ... 12
4 Vertrauenswürdige ID-Dokumente ... 14
4.1 Bedrohungen ... 14
4.2 Anforderungen für Vertrauensniveaubewertung ... 14
4.3 Abdeckung der Bedrohungen ... 19
5 Sicherheit der Übertragungskanäle ... 20
5.1 Bedrohungen ... 21
5.2 Anforderungen für Vertrauensniveaubewertung ... 21
5.3 Abdeckung der Bedrohungen ... 25
6 Prüfung der ID-Nachweise ... 26
6.1 Echtheit und Unverfälschtheit ... 26
6.2 Gültigkeit ... 26
6.3 Bedrohungen ... 26
6.4 Anforderungen für Vertrauensniveaubewertung ... 26
6.5 Abdeckung der Bedrohungen ... 28
7 Abgleich von Personen mit ID-Nachweisen ... 29
7.1 Bedrohungen ... 29
7.2 Anforderungen für Vertrauensniveaubewertung ... 29
7.3 Abdeckung der Bedrohungen ... 32
8 Korrekte Erfassung der benötigten ID-Attribute ... 33
8.1 Bedrohungen ... 33
8.2 Anforderungen für Vertrauensniveaubewertung ... 33
8.3 Abdeckung der Bedrohungen ... 35
9 Sicherung der Integrität der Prozesse ... 36
9.1 Bedrohungen ... 36
9.2 Anforderungen ... 36

9.3 Abdeckung der Bedrohungen 36
Literaturverzeichnis 38

Tabellenverzeichnis

Tabelle 1: Zu berücksichtigendes Angriffspotential je Vertrauensniveau 10
Tabelle 2: Abdeckung der Schutzziele der ID-Prüfung 12
Tabelle 3: Abdeckung der Bedrohungen der ID-Prüfung 13
Tabelle 4: Anforderungen an vertrauenswürdige ID-Dokumente gemäß Vertrauensniveau 15
Tabelle 5: Abdeckung der Bedrohungen der Vertrauenswürdigkeit von ID-Dokumenten 19
Tabelle 6: Anforderungen an die Sicherheit der Übertragungskanäle gemäß Vertrauensniveau 22
Tabelle 7: Abdeckung der Bedrohungen der Sicherheit der Übertragungskanäle 26
Tabelle 8: Anforderungen an die Prüfung der ID-Nachweise gemäß Vertrauensniveau 28
Tabelle 9: Abdeckung der Bedrohungen bei der Prüfung der ID-Nachweise 29
Tabelle 10: Anforderungen an den Abgleich von Personen und ID-Nachweisen gemäß Vertrauensniveau 31
Tabelle 11: Abdeckung der Bedrohungen beim Abgleich von Personen und ID-Nachweis 33
Tabelle 12: Anforderungen an die Erfassung eindeutiger ID-Attribute gemäß Vertrauensniveau 35
Tabelle 13: Abdeckung der Bedrohungen bei der Erfassung eindeutiger ID-Attribute 36
Tabelle 14: Abdeckung der Bedrohungen der Integrität der Prozesse 38

1 Einleitung

1.1 Zielsetzung und Inhalt der Technischen Richtlinie

Die (initiale) Identifizierung natürlicher Personen ist grundlegend für die Sicherheit im E-Government und anderer digitaler Geschäftsprozesse. Wichtig ist dabei die zuverlässige Prävention und Detektion von Betrugsversuchen, z. B. Identitätsdiebstahl oder der Vorgabe einer nicht existierenden Identität. Basierend auf den Bedrohungen müssen die Anforderungen an die Verfahren zum Identitätsnachweis und zur Identitätsprüfung definiert und umgesetzt werden.

Komplementär zu der für eID-Systeme und Verfahren einschlägigen [TR-03107-1] betrachtet die hier vorliegende Technische Richtlinie die Bedrohungen und Anforderungen für Verfahren zum Identitätsnachweis und zur Identitätsprüfung natürlicher Personen basierend auf ID-Dokumenten (z. B. Personalausweis oder Reisepass). Hierbei wird analog zu [TR-03107-1] berücksichtigt, dass das benötigte Mindestvertrauensniveau von Dienst zu Dienst unterschiedlich ist. Für die Bewertung der Vertrauensniveaus verschiedener Verfahren werden dieselben Kategorien „normal“, „substantiell“ und „hoch“ wie in [TR-03107-1] verwendet. Zusätzlich sind in der hier vorliegenden Technischen Richtlinie die Anforderungen an die Vertrauensniveaus „normal“, „substantiell“ und „hoch“ jeweils so definiert, dass jeweils die Mindestanforderungen für die in [eIDAS LoA] definierten Sicherheitsniveaus „niedrig“, „substanziell“ und „hoch“ erfüllt werden, soweit sie den ID-Nachweis und die ID-Prüfung betreffen.

Das für spezifische Anwendungen notwendige Vertrauensniveau muss von dem jeweiligen Betreiber des Dienstes anwendungsbezogen festgelegt werden. Die hierfür notwendige Berücksichtigung anwendungsspezifischer Risiken und rechtlicher Rahmenbedingungen ist nicht Bestandteil dieser Richtlinie. Auch Aspekte um die Serviceverfügbarkeit oder die nicht-Abstreitbarkeit („non-repudiation“) einer Registrierung sicherzustellen, werden nicht betrachtet. Notwendige Maßnahmen zur Sicherstellung der Vertraulichkeit übermittelter oder gespeicherter Daten oder Datenschutzaspekte werden ebenfalls nicht betrachtet.

1.2 Struktur und Aufbau der Technischen Richtlinie

Abschnitt 2 erläutert einige in der TR verwendete Begriffe. Abschnitt 3 gibt einen Überblick über die prinzipiellen Schutzziele (Existenz, Legitimität und ggf. Eindeutigkeit), Bedrohungen und Anforderungen der ID-Nachweis- und Prüfverfahren. Die hier spezifizierten Anforderungen an die Verfahren zielen darauf ab, die von einer Anwendung benötigten Schutzziele auch unter den genannten Bedrohungen zu gewährleisten.

Diese Anforderungen aus Abschnitt 3 werden dann in den Abschnitten 4 bis 8 detaillierter ausgearbeitet: top-down werden hier die spezifischen Bedrohungen betrachtet, sowie die sich wiederum daraus ergebenden detaillierteren Anforderungen, abgestuft nach den betrachteten Vertrauensniveaus. Abschnitt 4 behandelt die Anforderungen an sichere ID-Dokumente. Mit der Sicherheit der Übertragungskanäle erläutert Kapitel 5 die Schnittstelle zwischen dem Erbringen eines ID-Nachweises und dessen Überprüfung für den Fall, dass ein informationstechnischer Übertragungskanal zwischengeschaltet ist. Die Abschnitte 6 und 7 betrachten die Prüfung von ID-Nachweisen im Hinblick auf die verwendeten ID-Dokumente und deren (biometrischen) Abgleich mit Personen. Insbesondere für den Fall dass eine eindeutige Identitätsfeststellung gefordert ist, diskutiert Abschnitt 8 die Bedrohungen und Anforderungen bei der Erfassung eindeutiger ID-Attribute.

Abschnitt 9 betrachtet allgemeine Querschnittrisiken und dazugehörige Sicherheitsanforderungen an Stellen die die ID-Prüfprozesse durchführen.

2 Definitionen und Bewertungsmethodik

2.1 Grundbegriffe

Identitätsnachweis (ID-Nachweis): Die über eine natürliche Person für eine Identitätsprüfung verfügbaren Informationen (z. B. ID-Nachweisdokumente, biometrische Charakteristika oder biometrische Daten) in Kombination mit allen Merkmalen, die zur Bestätigung der Authentizität und Integrität der Daten dienen. In dieser TR wird vorausgesetzt, dass der ID-Nachweis stets von der zu identifizierenden Person selbst erbracht wird, d. h. ID-Nachweise für oder im Namen von Dritten werden nicht betrachtet.

Identitätsprüfung (ID-Prüfung): Die Konsistenz- und Echtheitsprüfung der bei einem ID-Nachweis erbrachten Daten. Eine ID-Prüfung im Sinne dieser TR basiert stets auf einem erbrachten ID-Nachweis.

Verlässliche Quelle: „Eine beliebige Informationsquelle, die auf verlässliche Weise präzise Daten, Informationen und / oder Beweismittel bereitstellt, die zum ID-Nachweis verwendet werden können“ [eIDAS LoA].

ID-Nachweisdokument (ID-Dokument): Von einer verlässlichen Quelle (z. B. Einwohnermeldeamt, Ausländerbehörde) herausgegebenes physisches Objekt, das einen ID-Nachweis ermöglicht und somit selbst als verlässliche Quelle dienen kann. ID-Dokumente im Sinne dieser TR können sowohl von hoheitlichen als auch privatwirtschaftlichen Stellen herausgegeben sein. Mögliche Beispiele sind der deutsche Personalausweis, Reisepässe, elektronische Aufenthaltstitel, Mitarbeiterausweise, Führerscheine[1].

ID-Nachweisregister (ID-Register): Verlässliche Quellen die nicht als ID-Dokument herausgegeben werden bzw. herausgegeben werden können. Beispiele in Deutschland sind Einwohnermelderegister oder das Ausländerzentralregister.

Für die in dieser TR betrachteten ID-Prüfungen wird als verlässliche Quelle stets ein ID-Dokument vorausgesetzt. Optional können zusätzliche Informationen, z. B. aus einem ID-Register, herangezogen werden. Die Einstufung einer Informationsquelle als verlässliche Quelle bezieht sich ausschließlich auf die Korrektheit und Integrität der Daten wie sie von der Informationsquelle herausgegeben bzw. abgeschickt werden. Schutzmechanismen gegenüber nachträglichen Manipulationen werden getrennt betrachtet.

Die Begriffe **Entität**, **ID-Attribut**, **Identität** und **eindeutige Identität** werden im Sinne von [TR-03107-1] verwendet.

2.2 Angriffspotential

Angriffspotential bezeichnet ein Maß für den notwendigen Aufwand eines bestimmten Angriffs auf das Evaluierungsobjekt (TOE), i. A. ausgedrückt in den Kategorien Expertise, Ressourcen und Motivation des Angreifers [CC1]. TOEs im Sinne dieser TR sind Verfahren zur ID-Prüfung. Gegenstand einer TOE Prüfung sind hier sowohl die bei der ID-Prüfung verwendeten Produkte (z. B. ID-Nachweise, zur ID-Prüfung verwendete Software/Hardware) als auch die bei der ID-Prüfung durchgeführten Prozesse (z. B. eine Hologrammprüfung auf einem Reisepass).

Konkret sind für die Bewertung des Angriffspotentials die notwendigen Ressourcen aus folgenden fünf Kategorien zu bewerten:

- **Zeit** („elapsed time“): Zeit zur Vorbereitung und Durchführung des Angriffs.
- **Expertenwissen** („specialist expertise“): Verwendete bzw. benötigte generische Fachkenntnisse über die bei der ID-Prüfung eingesetzten Methoden und Techniken.

1 Die Auflistung beinhaltet keinerlei Bewertung hinsichtlich Eignung oder Vertrauensniveau der genannten ID-Dokumente. Der in diesem Dokument ebenfalls verwendete Begriff „explizites ID-Dokument“ bezeichnet ID-Dokumente die (auch) ausdrücklich für den Zweck des sich ausweisen Könnens ausgegeben wurden. Beispielsweise sind EU-Führerscheine demnach ID-Dokumente jedoch keine expliziten ID-Dokumente.

- **Insiderkenntnisse** („knowledge of the TOE“): Verwendete bzw. benötigte interne Kenntnisse über das konkrete TOE, d. h. über die konkrete ID-Prüfung.
- **Zugangs- / Zugriffsgelegenheiten** („window of opportunity“): Verfügbare bzw. benötigte Zugangs- / Zugriffsgelegenheiten, um einen Angriff vorzubereiten und durchzuführen. Hier sind insbesondere notwendige offline oder online Zugriffe auf das TOE oder Restriktionen bei der Anwendbarkeit von Angriffen zu berücksichtigen. Z. B., wenn ein Manipulationsverfahren für Kalibrierzwecke wiederholten Zugang zu bzw. Zugriff auf das TOE benötigt oder, wenn es nur bei Personen funktioniert, die bereits eine hohe Ähnlichkeit zu einer Referenzperson haben.
- **Ausrüstung** („equipment“): Verfügbarkeit und Kosten der für einen Angriff verwendeten Materialien und Ausrüstung.

Für die Gesamtbewertung des notwendigen Angriffspotentials zur erfolgreichen Durchführung eines Angriffs ist [CEM], Anhang B.4 zugrundezulegen. Basierend auf den für einen erfolgreichen Angriff notwendigen Ressourcen sind nach [CEM] Anhang B.4.2.3, Tabelle 3 („Calculation of attack potential“) die insgesamt erreichten Punkte zu berechnen. Das Angriffspotential, gegenüber dem eine Anforderung noch als sicher eingestuft werden kann, ergibt sich dann aus [CEM], Anhang B.4.2.3, Tabelle 4 („Rating of vulnerabilities and TOE resistance“).

2.3 Erfolgreicher Angriff

Die Durchführung eines Angriffs ist genau dann als erfolgreich zu bewerten, wenn beim ID-Nachweis eine falsche Identität angegeben wird und die ID-Prüfung die angegebene Identität bestätigt. Gibt es einen – im Rahmen der angestrebten Widerstandsfähigkeit des TOE gegen ein bestimmtes Angriffspotential – erfolgreichen Angriff (siehe Abschnitt 2.4) der reproduzierbar funktioniert, so ist das Verfahren zur ID-Prüfung für das angestrebte Vertrauensniveau untauglich. Hat der Angriff eine statistische Erfolgswahrscheinlichkeit, so ist er insgesamt als erfolgreich zu bewerten, wenn die erreichte „False Acceptance Rate“ (FAR[2], „falsch positiv“) den für die Anwendung bzw. für das angestrebte Vertrauensniveau zulässigen Wert überschreitet.

Bei der Bewertung von Angriffen auf kryptographische Verfahren oder Protokolle bzw. deren konkrete Implementierungen in Soft- oder Hardware ist teilweise eine binäre Bewertung möglich. D. h. es ist dann eine abschließende Aussage möglich, ob z. B. ein auf einer Chipkarte gespeicherter Schlüssel mit einem konkreten Angriff reproduzierbar kompromittiert werden kann. Demgegenüber stehen probabilistische Aussagen zur Sicherheit, also quantitative Angaben zur Wahrscheinlichkeit mit der ein TOE bei der Durchführung eines Angriffs kompromittiert werden kann.

Bei der Bewertung von Angriffen auf biometrische Identifizierungen sind i. d. R. nur probabilistische Aussagen möglich. Die Qualität wird üblicherweise in der Gegenüberstellung der FAR und der „False Rejection Rate“ (FRR, „falsch negativ“) gemessen. Beide sind für die praktische Nutzbarkeit von Verfahren wesentlich und i. d. R. besteht ein inhärenter Zielkonflikt in der gleichzeitigen Optimierung beider Parameter. Für die Sicherheit im engeren Sinn ist jedoch nur die FAR relevant, die FRR wird deshalb in dieser TR nicht weiter explizit berücksichtigt. Bei der Bestimmung der mit einem Angriff erzielbaren FAR sind die in der ID-Prüfung verwendeten Matchingverfahren (z. B. geschultes Personal, maschinelle Verfahren) in Kombination mit den jeweiligen Rahmenbedingungen der Datenerfassung (z. B. Remoteübertragung) zu berücksichtigen. Neben Angriffen auf den Abgleich biometrischer Referenzdaten mit biometrischen Charakteristika ist analog die Manipulierbarkeit des verwendeten ID-Dokuments, d. h. der personalisierten ID-Attribute, zu betrachten und die erreichbare FAR für die relevanten Angriffe zu bestimmen.

Die maximal akzeptable FAR ist vor der Durchführung eines Audits vorab zu definieren, in Abhängigkeit von der Anwendung und dem benötigten Vertrauensniveau. Ein Beispiel hierfür ist [TR-03121-3] für

2 Hier wird in der Literatur meistens der spezifischere Begriff „False Match Rate“ (FMR) verwendet. Wir verwenden hier durchgängig den allgemeineren Begriff „False Acceptance Rate“ (FAR) in dem Sinne, dass eine falsch vorgegebene Identität auf irgendeine Art und Weise erfolgreich legitimiert wird.

Biometrie in hoheitlichen Anwendungen in Deutschland. Hier wird für das biometrische Matching (Fingerabdruck oder Gesicht), jeweils eine garantierte maximale „False Match Rate“ (FMR) von 0.1% (1:1.000) gefordert.

Bei der Bestimmung der FAR ohne gezielter Manipulationsversuche ist eine zufällige Auswahl aus der jeweiligen Grundgesamtheit, d. h. bei der zu identifizierenden Person und bei den biometrischen Daten, zwischen denen der Abgleich durchgeführt wird, zugrundezulegen. Die FAR ohne Berücksichtigung gezielter Manipulationsversuche kann zwar ebenfalls von Interesse sein, für Vertrauensniveaubewertungen nach dieser Technischen Richtlinie müssen gezielte Manipulationsversuche berücksichtigt werden.

2.4 Berücksichtigung und Bewertung des Angriffspotentials

Wurde ein erfolgreicher Angriff auf ein Verfahren zur ID-Prüfung praktisch umgesetzt oder theoretisch identifiziert, so ist zu bewerten, ob er für die konkrete Anwendung bzw. das angestrebte Vertrauensniveau relevant ist. Ein Angriff ist genau dann relevant für ein bestimmtes Vertrauensniveau, wenn das zu seiner Identifizierung und Durchführung notwendige Angriffspotential nach Tabelle 1 berücksichtigt werden muss.

	Angestrebtes Vertrauensniveau		
	normal	**substantiell**	**hoch**
Zu berücksichtigendes Angriffspotential gemäß [CEM]	bis einschließlich *enhanced-basic*	bis einschließlich *moderate*	bis einschließlich *high*

Tabelle 1: Zu berücksichtigendes Angriffspotential je Vertrauensniveau

Ergeben sich, z. B. durch technische Fortschritte oder das öffentlich werden vertraulicher Informationen, vereinfachte Angriffsmöglichkeiten, so dass das notwendige Angriffspotential beispielsweise nur noch *moderate* statt *high* beträgt, so bleibt i. d. R. das ursprünglich zum Zeitpunkt der Durchführung einer konkreten ID-Prüfung erreichte Vertrauensniveau gültig. Eine Ausnahme ist beispielsweise wenn nachträglich bekannt wird, dass Angriffsmethoden mit niedrigerem Angriffspotential bereits früher verbreitet oder bekannt waren.

2.5 Durchführung von Angriffen

Bei jeder ID-Prüfung besteht das Risiko von Manipulationen. Zur Bewertung der Manipulierbarkeit und damit des Vertrauensniveaus eines Verfahrens zur ID-Prüfung können Angriffe praktisch durchgeführt werden und anschließend kann das notwendige Angriffspotential ermittelt werden. Sofern hinreichend empirisch oder theoretisch abgesichert, können potentielle Angriffe auch ohne (vollständige) praktische Durchführung bewertet werden. Zur Beurteilung der Durchführbarkeit von Angriffen müssen insbesondere die implementierten Prüfprozesse und Qualitätssicherungsmaßnahmen berücksichtigt werden. Beispiele sind verwendete technische Prüfmittel oder eine mindestens geforderte Ausleuchtung oder Auflösung bei Videoübertragungen.

3 ID-Nachweis und ID-Prüfung

3.1 Schutzziele

Die potentiellen Schutzziele einer ID-Prüfung sind:

S1. **Existenz**: Es existiert eine Entität (natürliche Person) auf die alle angegebenen ID-Attribute zutreffen.

S2. **Legitimität**: Alle angegebenen ID-Attribute gehören zu der sich identifizierenden Person (impliziert die Existenz).

Die Identitätsfeststellung erfordert nicht notwendigerweise die eindeutige Zuordnung zu einer natürlichen Person; regelmäßig ist jedoch explizit eine eindeutige Identität gefordert (z. B. in [eIDAS]).

S3. **Eindeutigkeit**: Keine zwei Personen verfügen über identische Werte für alle erfassten ID-Attribute.

Die tatsächlich relevanten Schutzziele und ihre Prioritäten hängen von der Anwendung ab, für die eine ID-Prüfung benötigt wird. Sind für bestimmte Anwendungen ein Teil der Schutzziele nicht relevant, kann der entsprechende Teil der nachfolgend genannten Bedrohungen und damit auch der Sicherheitsanforderungen unberücksichtigt bleiben. Auf jeden Fall ist sicherzustellen, dass für alle relevanten Schutzziele die damit verbundenen Bedrohungen und Anforderungen berücksichtigt werden.

3.2 Bedrohungen

Um die Schutzziele Existenz, Legitimität und Eindeutigkeit zu gewährleisten, müssen Maßnahmen zur Prävention oder Detektion der folgenden Bedrohungen umgesetzt werden:

B1. Vorgelegte ID-Attribute treffen weder auf die zu identifizierende[3] noch auf eine andere existierende Person zu.

B2. Erfolgreich geprüfte und bereits registrierte ID-Attribute verlieren ihre Gültigkeit (z. B. durch Namens- oder Adressänderungen).[4]

B3. Eine Person verwendet die ID-Attribute einer anderen Person, um sich unberechtigt als diese andere Person auszugeben (Identitätsdiebstahl).

B4. Vorgelegte ID-Attribute treffen auf mehr als eine Person zu.

3.3 Anforderungen

Aus den Schutzzielen Existenz, Legitimität und Eindeutigkeit sowie den in Abschnitt 3.2 genannten Bedrohungen lassen sich die folgenden Anforderungen für die Sicherheit der ID-Prüfung ableiten:

A1. Vertrauenswürdige ID-Dokumente (als verlässliche Quelle nach [eIDAS LoA]).

A2. Vertrauenswürdige Übertragungskanäle. Dies ist relevant wenn bei der ID-Prüfung kein unmittelbarer Präsenzkontakt zwischen Prüfinstanz und zu identifizierender Person besteht, oder die Prüfinstanz keinen unmittelbaren Zugriff auf die verwendeten ID-Dokumente hat.

A3. Zuverlässige Prüfung der ID-Dokumente.

3 Sind die vorgelegten ID-Attribute nicht mehr aktuell (z. B. nach einem Wohnsitzwechsel oder einer Namensänderung) aber waren es zu einem definierten Zeitpunkt in der Vergangenheit, so können sie grundsätzlich immer noch für eine eindeutige Identifizierung geeignet sein. Für konkret in einer Anwendung benötigte ID-Attribute (z. B. Wohnsitz) muss unabhängig davon die Aktualität gewährleistet sein.

4 Diese Bedrohung ist ausschließlich für Anwendungsfälle relevant bei denen eine dauerhafte Verfügbarkeit aktueller ID-Attribute benötigt wird. Für einmalige, zeitpunktbezogene ID-Prüfungen ist diese Bedrohung nicht relevant.

A4. Zuverlässige Prüfung verwendeter Übertragungskanäle

A5. Zuverlässiger Abgleich zwischen der zu identifizierenden Person und dem ID-Dokument (Integrität des ID-Nachweises).

A6. Erfasste ID-Attribute ermöglichen eine eindeutige Identifizierung.

A7. Korrekte Erfassung der benötigten ID-Attribute.

A8. Sicherung der Integrität aller Prozessschritte.

A9. Verbindliche und dokumentierte Vorgaben für alle Prozessschritte und Entscheidungen die den Anforderungen an die ID-Prüfung genügen.

Die Punkte A1. und A2. adressieren die Qualität des ID-Nachweisprozesses, die Punkte A3., A4. und A5. die Qualität des ID-Prüfprozesses. Zusammen definieren die Punkte A1. bis A5. das unmittelbare Sicherheitsniveau der ID-Nachweis- und Prüfprozesse und damit das notwendige Angriffspotential für erfolgreiche Angriffe „von außen“ mittels gefälschter ID-Nachweise. Punkt A7. adressiert die Qualität, damit Fehler „aus Versehen“ vermieden werden. Punkt A8. adressiert die Integrität, damit insbesondere auch Manipulationen „von Innen“ (bzw. unter Mitarbeit von Innentätern) verhindert werden. Punkt A9. beschreibt als Querschnittthema die Dokumentationsanforderungen für sämtliche Prozesse und Vorgaben.

3.4 Abdeckung der Schutzziele und Bedrohungen

Für die Abdeckung der Schutzziele Existenz, Legitimität und Eindeutigkeit durch die in Abschnitt 3.3 genannten Sicherheitsanforderungen gelten die Zusammenhänge aus Tabelle 2.

Schutzziel	**Abgedeckt durch Anforderung Nr.**	**Begründung**	
S1. Existenz	A1., A2., A3., A4.	A1. stellt sicher, dass die Existenz basierend auf vertrauenswürdigen ID-Dokumenten geprüft wird. A2., A3. und A4. stellen die Authentifizierung der verwendeten ID-Dokumente sicher.	A8. und A9. definieren organisationsübergreifende Sicherheitsmaßnahmen und gewährleisten die Umsetzung der notwendigen Anforderungen
S2. Legitimität	A1., A2., A3., A4., A5.	A1., A2. und A3. stellen sicher, dass Personen nur mit einer tatsächlich existierenden Identität (gem. ID-Dokument) abgeglichen werden. A4. und A5. stellen sicher, dass nur berechtigte Personen über die nachgewiesene Identität verfügen können.	
S3. Eindeutigkeit	A6., A7.	A6. stellt die Eindeutigkeit der zu erfassenden ID-Attribute sicher, A7. deren korrekte Erfassung.	

Tabelle 2: Abdeckung der Schutzziele der ID-Prüfung

Für die Prävention und Detektion der Bedrohungen aus Abschnitt 3.2 durch die in Abschnitt 3.3 genannten Sicherheitsanforderungen gelten die Zusammenhänge aus Tabelle 3.

Bedrohung	**Abgedeckt durch Anforderung Nr.**	**Begründung**
B.1	A1., A2., A3., A4.	A1., A2., A3. und A4.stellen zusammen sicher, dass die behauptete Identität tatsächlich existiert, basierend auf einem zuverlässig geprüften, vertrauenswürdigem ID-Dokument.
B.2	A9.	A9. stellt sicher, dass für ggf. benötigte Wiederholungen der Gültigkeitsprüfungen die zur Durchführung notwendigen organisatorischen

Bedrohung	Abgedeckt durch Anforderung Nr.	Begründung
		Prozessschritte definiert sind.
B.3	A1., A2., A3., A4., A5.	Auf Grundlage von A1. und A2. stellen A3., A4. und A5. sicher, dass die zu identifizierende Person diejenige ist für die sie sich mittels des verwendeten ID-Dokuments ausgibt.
B.4	A6., A7.	A6. und A7. gewährleisten, dass die Daten der erfassten ID-Attribute die Eindeutigkeit sicherstellen.

Tabelle 3: Abdeckung der Bedrohungen der ID-Prüfung

Eine ID-Prüfung kann durch die Verletzung einer einzigen der in Abschnitt 3.3 genannten Anforderungen fehlerhaft sein. Das insgesamt erreichte Vertrauensniveau einer ID-Prüfung ist daher nach dem Minimumprinzip aus den jeweils für die einzelnen notwendigen Anforderungen erreichten Vertrauensniveaus zu bestimmen.

4 Vertrauenswürdige ID-Dokumente

Grundlage für eine reguläre ID-Prüfung ist die Verfügbarkeit von mindestens einem vertrauenswürdigen ID-Dokument, das die zuverlässige Prüfung der Authentizität und Integrität der relevanten ID-Attribute ermöglicht[5]. Zusätzlich können ID-Register (z. B. Einwohnermelderegister, Ausländerzentralregister) als verlässliche Quelle herangezogen werden, die Vertrauensniveaubewertungen dieser TR basieren jedoch auf ID-Dokumenten als primären Nachweis. Nach dem Minimumprinzip bestimmt das für eine ID-Prüfung zulässige ID-Dokument mit dem niedrigsten Vertrauensniveau das insgesamt maximal erreichbare Vertrauensniveau des Verfahren zur ID-Prüfung. Dies gilt gleichermaßen, wenn dem ID-Dokument durch die mit der Ausstellung verbundenen (initialen) ID-Feststellung oder Festlegung inhärent kein oder nur ein normales bzw. substantielles Vertrauensniveau zugeordnet werden kann.

4.1 Bedrohungen

Für die Vertrauenswürdigkeit von ID-Dokumenten sind folgende mögliche Bedrohungen relevant:

B1. Quelle des ID-Dokuments (d. h. alle beteiligten Stellen, ggf. einschließlich eingebundener Dienstleister z. B. für Produktion und Logistik) ist nicht vertrauenswürdig bzw. wurde kompromittiert.

B2. ID-Dokument ist nicht manipulations- und fälschungssicher.

B3. ID-Dokument ermöglicht keinen zuverlässigen Abgleich mit dem Verwender.

B4. Verfügbare ID-Attribute ermöglichen keine eindeutige Identifizierung einer Person.

B5. ID-Dokument bzw. relevante ID-Attribute sind nicht mehr aktuell.

4.2 Anforderungen für Vertrauensniveaubewertung

Zur Prävention und Detektion der Bedrohungen aus Abschnitt 4.1 sind die im Folgenden diskutierten Anforderungen für vertrauenswürdige ID-Dokumente zu berücksichtigen. Für die Zuordnung von ID-Dokumenten zu einem Vertrauensniveau ist für die meisten der genannten Anforderungen eine abgestufte Bewertung in Abhängigkeit des jeweiligen Vertrauensniveaus notwendig. Einige Anforderungen müssen erst ab einem bestimmten Vertrauensniveau berücksichtigt werden, andere Anforderungen mit einer in Abhängigkeit des Vertrauensniveaus abgestuften Resistenz gegenüber Angriffspotentialen. In allen Fällen ist ein gültiges, d. h. insbesondere ein nicht abgelaufenes ID-Dokument notwendig. Weitere, je nach Vertrauensniveau notwendige Anforderungen sind in Tabelle 4 zusammengefasst.

Nr.	Anforderung	Notwendig für Vertrauensniveau		
		Normal	**Substantiell**	**Hoch**
A.1	Verlässliche Quelle	Ja[6]	Ja; explizites ID-Dokument	Ja; explizites ID-Dokument das Ausweispflicht im Inland[7] erfüllt oder

5 Initiale Verfahren zur Feststellung bzw. Festlegung einer Identität müssen insbesondere für Personen definiert werden, für die noch kein vertrauenswürdiger ID-Nachweis verfügbar ist (z. B. Geburtsurkunden für Neugeborene). Solche Verfahren werden in dieser Technischen Richtlinie nicht betrachtet.

6 D. h., für eine Vertrauensniveaubewertung nach dieser Technischen Richtlinie könnte dies z. B. auch durch einen Führerschein erfüllt sein, obwohl dieser in Deutschland kein hoheitliches ID-Dokument ist.

7 D. h. nach der Rechtsordnung des jeweiligen Landes aufgrund derer ein ID-Nachweis benötigt wird, bzw. gemäß der Rechtsordnung die bei privatrechtlichen Verträgen explizit vereinbart wurde. Für Deutschland etwa gemäß der jeweils aktuellen „Allgemeinverfügung über die Anerkennung eines ausländischen Passes oder Passersatzes“.

Nr.	Anforderung	Notwendig für Vertrauensniveau		
		Normal	**Substantiell**	**Hoch**
				technisch gleichwertig[8]
A.2	Enthält eine hinreichende Menge an ID-Attributen	Ja	Ja	Ja
A.3	Manipulations- und fälschungssicher	Ja; sicher bei Angriffspotential „enhanced-basic“	Ja; sicher bei Angriffspotential „moderate“	Ja; sicher bei Angriffspotential „high“
A.4	Sicherheitsmerkmale sind bekannt und effektiv überprüfbar	Ja; sicher bei Angriffspotential „enhanced-basic“	Ja; sicher bei Angriffspotential „moderate“	Ja; sicher bei Angriffspotential „high“
A.5	Ermöglicht einen zuverlässigen Abgleich mit dem Verwender	Ja	Ja; biometrisches Fotodokument, nicht älter als 10 Jahre bzw. rechtlich und technisch gleichwertig	Ja, wie substantiell
A.6	ID-Attribute sind aktuell	-	Ja[9]	Ja, wie substantiell
A.7	Sperrmeldungen werden überprüft	-	Ja (soweit verfügbar)	Ja, wie substantiell
A.8	Regelmäßige Prüfung der Menge der zulässigen ID-Dokumente	Ja	Ja	Ja

Tabelle 4: Anforderungen an vertrauenswürdige ID-Dokumente gemäß Vertrauensniveau

4.2.1 Verlässliche Quelle (A.1)

Das ID-Dokument ist von einer verlässlichen Quelle herausgegeben und stellt somit selbst eine verlässliche Quelle dar. Insbesondere wird die Vertrauenswürdigkeit und Integrität aller an der Bereitstellung des ID-Dokuments beteiligten Stellen (im Wesentlichen ausgebende und produzierende Stellen) gefordert. Folgende Punkte müssen erfüllt sein damit ein ID-Dokument als verlässliche Quelle eingestuft werden kann:

1. Die für die Ausstellung des jeweiligen ID-Dokuments gesamtverantwortliche Stelle ist bekannt. Verfügbare Informationen zu weiteren (z. B. lokal) beteiligten Stellen sind plausibel.
2. Über die für die für die Ausstellung der zugelassenen ID-Dokumente verantwortlichen Stellen (einschließlich etwaiger Übertragungsdienste und -medien), werden öffentlich verfügbare Informationen über Kompromittierungen gesammelt und zeitnah berücksichtigt.[10]

8 Unter „technisch gleichwertig“ ist hier ein gleichwertiges Sicherheitsniveau von Merkmalen und deren Prüfbarkeit zum Schutz vor Fälschungen und Manipulationen zu verstehen. Durch eine festgestellte technische Gleichwertigkeit ist keine rechtliche Gleichwertigkeit impliziert.

9 Bei Anwendungen, die ID-Prüfungen auf Vertrauensniveau „substantiell“ oder „hoch“ benötigen und explizit nicht auf die Aktualität einiger ID-Attribute angewiesen sind, kann diese Anforderung entfallen.

10 Beispielsweise müssen Medienberichte zur Kompromittierung von Stellen, die relevante ID-Dokumente herausgeben, berücksichtigt werden. Für hoheitlich herausgegebene Dokumente, die die Ausweispflicht im Inland erfüllen, kann vermutet werden, dass die für die Herausgabe verantwortlichen Stellen nicht kompromittiert sind.

3. Aktuelle Informationen über Manipulationen und Fälschungen bei ID-Dokumenten werden gesammelt und zeitnah berücksichtigt.
4. ID-Dokumente werden nur für die jeweils berechtigte Person ausgestellt. D. h., die Berechtigung und Identität eines Antragstellers wird vor Aushändigung des ID-Dokuments hinreichend sicher geprüft.

Unabhängig von technischen Anforderungen können für bestimmte Zwecke und Anwendungen ausschließlich hoheitliche ID-Dokumente (bzw. eine explizit begrenzte Menge an ID-Dokumenten) zugelassen sein. Solche etwaigen Anforderungen müssen anwendungsbezogen und unabhängig von einer technischen Bewertung berücksichtigt werden.

Als rechtlich und technisch gleichwertig können daneben auch ID-Register betrachtet werden, die als vertrauenswürdige Quelle zur Ausstellung entsprechender ID-Dokumente zugelassen sind. Die unmittelbare Verwendung von ID-Registern zum Zweck des ID-Nachweises wird in dieser TR jedoch nicht betrachtet.

4.2.2 Enthält eine hinreichende Menge an ID-Attributen (A.2)

Die hinreichende Menge an benötigten ID-Attributen ergibt sich aus den Anwendungen, für die der ID-Nachweis durchgeführt wird. Falls dies für die Anwendung erforderlich ist, müssen die verfügbaren ID-Attribute insbesondere eine eindeutige Identifizierung ermöglichen. Hier ist keine technische Sicherheit zu bewerten.

4.2.3 Manipulations- und fälschungssicher (A.3)

Für den deutschen Personalausweis, EU-Aufenthaltstitel[11] und Reisepässe die von Mitgliedstaaten der EU oder der EFTA ausgestellt sind, wird eine für Vertrauensniveau „hoch“ hinreichende Manipulations- und Fälschungssicherheit im Sinne dieser TR widerleglich vermutet.

Für die technische Bewertung der Manipulations- und Fälschungssicherheit ist das notwendige Angriffspotential maßgeblich, um mit manipulierten bzw. gefälschten Dokumenten eine erfolgreiche ID-Prüfung durchzuführen. Für eine Bewertung ist jeweils der aktuelle Stand der Technik maßgeblich. Das notwendige Angriffspotential kann nicht isoliert für ein ID-Dokument bewertet werden, sondern nur in Kombination mit einem angenommenen ID-Prüfverfahren, d. h. der Umfang und die Tiefe der ID-Prüfung (siehe folgende Kapitel) ist unbedingt mit zu berücksichtigen.

Es sind die verschiedensten Arten von Angriffen denkbar. So kann ein Angreifer z. B. Daten auf einem authentischen ID-Dokument manipulieren, basierend auf mehreren authentischen ID-Dokumenten eine Fälschung erstellen oder „von Grund auf“ eine Fälschung herstellen (Nachahmung). Je nach Angriff werden sehr unterschiedliche Ressourcen benötigt. Im Folgenden sind einige Beispiele und deren Einordnung für eine Bewertung des notwendigen Angriffspotentials, angelehnt an [CEM] Anhang B.4, genannt.

Expertenwissen: Unabhängig von dem betrachteten Angriff können von Laien i. d. R. keine hochwertigen Manipulationen oder Fälschungen erwartet werden. Die konkret notwendige Expertise für einen erfolgreichen Angriff lässt sich nicht isoliert basierend auf dem ID-Dokument und dem ID-Prüfverfahren bewerten. Hier besteht insbesondere ein enger Zusammenhang zu der verfügbaren Ausrüstung. Umgekehrt erfordert die Verwendung spezialisierter Ausrüstung häufig einschlägige Fertigkeiten und Kenntnisse (z. B. eine Ausbildung im Druckbereich) oder anderes dezidiertes Expertenwissen.

Insiderkenntnisse: Komplett personalisiert sind ID-Dokumente i. d. R. als öffentlich verfügbar zu betrachten. Möglicherweise werden für einen Angriff auch nicht-öffentliche Informationen (z. B. Zusammensetzung der verwendeten Materialien, verwendete Produktionsparameter) benötigt.

Zugangs- / Zugriffsgelegenheiten: Hier ist beispielsweise der Zugriff auf benötigte original Fertigungs- und Personalisierungsmaschinen zu betrachten oder auch der Zugriff auf benötigte original Roh- oder

11 Soweit vermutet werden kann dass sie explizit als ID-Dokument ausgestellt wurden, d. h. auf überprüften und bestätigten ID-Attributen basieren.

Hilfsmaterialien bzw. vorproduzierte Blanko-Dokumente. Diese Möglichkeit ist insbesondere bei den Herstellern dieser Maschinen oder Materialien gegeben, sowie bei den ID-Dokument Herstellern bzw. Personalisierern. Ein freier oder einfacher Zugang wird hier üblicherweise nicht möglich sein. Bei der konkreten Bewertung von Zugangs- und Zugriffsrestriktionen sollen die Kriterien aus [JILSS] Kapitel 9.3 berücksichtigt werden.

Ausrüstung: Für das Durchführen von Manipulationen und Fälschungen werden üblicherweise Werkzeuge und Materialien benötigt. Deren Art und Umfang ist ganz wesentlich durch die Sicherheitsmerkmale des ID-Dokuments und die Vorgehensweise des Angriffs bestimmt. Sofern es sich um die Verwendung von Originalmaterialien und Maschinen handelt, sind hier die notwendigen **Zugangs- / Zugriffsgelegenheiten** zu betrachten. Einfache Kartenkörper, Folien oder Hologrammstreifen sind ohne erhebliche Kosten frei verfügbar. Je nach Sicherheitsmerkmalen die bei einem Angriff gefälscht werden, können Materialien (z. B. Mikrolinsenfolien für Kippbilder, UV- und IR-Farben) oder Maschinen (z. B. Laser für die optische Personalisierung, Druckmaschinen) benötigt werden, die typischerweise als „bespoke“ oder „multiple bespoke“ einzuordnen sind.

4.2.4 Sicherheitsmerkmale sind bekannt und effektiv überprüfbar (A.4)

Die Bekanntheit von Sicherheitsmerkmalen zusammen mit Informationen zu ihrer Überprüfbarkeit ist die notwendige Ergänzung zu deren Vorhandensein auf ID-Dokumenten. Das in Abschnitt 4.2.3 diskutierte notwendige Angriffspotential zur Manipulation und Fälschung von ID-Dokumenten ist für ein ID-Prüfverfahren nur insoweit notwendig, als deren Sicherheitsmerkmale bekannt sind und tatsächlich überprüft werden. D. h. für ein konkretes ID-Prüfverfahren ist das notwendige Angriffspotential für eine erfolgreiche Manipulation oder Fälschung eines ID-Dokuments basierend auf der tatsächlich implementierten ID-Prüfung (Umfang und Prüftiefe) zu bestimmen, nicht basierend auf der Gesamtheit der prinzipiell vorhandenen Sicherheitsmerkmale.

Potentiell besteht für einen Angreifer ggf. noch die Hürde, dass nicht öffentlich bekannt ist welche Sicherheitsmerkmale tatsächlich mit welchen Verfahren überprüft werden. Analog zur Sicherheitsbewertung kryptographischer Verfahren ist jedoch auch hier grundsätzlich die Annahme zugrundezulegen, dass eine Geheimhaltung der Verfahren und Methoden das für einen erfolgreichen Angriff notwendige Angriffspotential nicht heraufsetzt.

Als Grundlage für eine effektive Überprüfung sollten die relevanten Sicherheitsmerkmale und deren Prüfkriterien klar definiert sein. Idealerweise erfolgt dies in Abstimmung mit der ausgebenden Stelle oder dem Produzenten der ID-Dokumente. Idealerweise sind auch „specimen“ Exemplare als Referenz oder für Schulungen verfügbar. Daneben kommt die Nutzung von geeigneten Datenbanken in Betracht die Informationen zu den auf ID-Dokumenten verfügbaren Sicherheitsmerkmalen und geeigneten Prüfmethoden enthalten.

4.2.5 Ermöglicht einen zuverlässigen Abgleich mit dem Verwender (A.5)

Diese Anforderung adressiert Art, Umfang und Qualität (z. B. Auflösung) der für einen Abgleich auf dem ID-Dokument grundsätzlich zur Verfügung stehenden Daten. Mögliche Fälschungen oder Manipulationen der auf dem ID-Dokument personalisierten Datensätze werden hier nicht betrachtet und durch Abschnitt 4.2.3 i. V. m. Abschnitt 4.2.4 berücksichtigt. Um unabhängig von dem Faktor Besitz eine eindeutige Zuordnung zu dem legitimen Inhaber zu ermöglichen enthalten ID-Dokumente üblicherweise wissensbasierte und/oder biometrische Daten.

- **Wissensbasierte Daten**: Hier ist typischerweise die Sicherheit von PIN/PUK basierten Verfahren zu bewerten. Deren statistische Sicherheit kann basierend auf [RAND] bewertet werden.
- **Biometrische Daten**: Hier ist die Qualität (ggf. auch die Aktualität) maßgeblich, die sich aus der Erfassung biometrischer Charakteristika beim Enrolment und einer möglichen Weiterverarbeitung oder Komprimierung nach dem Speichern auf dem ID-Dokument ergibt. Basierend auf einem ausgestellten ID-Dokument und dem dazugehörigen Enrolment alleine kann nur eine „best case“ Betrachtung

durchgeführt werden. Das zum Überschreiten der maximal zulässigen FMR notwendige Angriffspotential kann dann nur unter der einschränkenden Annahme bewertet werden, dass die für den Abgleich gespeicherten biometrischen Daten auf genuinen biometrischen Charakteristika der sich identifizierenden Person basieren. D. h. „spoofing“ bzw. „presentation attacks“ müssen zusätzlich berücksichtigt werden. Dies ist erst in Kombination mit den eingesetzten Verfahren zur Erfassung und Prüfung der für den Abgleich verwendeten biometrischen Charakteristika und Daten möglich. Diese werden in Abschnitt 7 betrachtet.

Durch eine unterschiedlich gute Erfassbarkeit biometrischer Charakteristika verschiedener Personen kann sich inhärent eine schwankende Qualität der auf den ID-Dokumenten gespeicherten biometrischen Daten ergeben. Dies ist nicht durch Schwächen der verwendeten ID-Dokumente bzw. der Datenerfassung im Ausstellungsprozess bedingt aber dennoch bei der Bewertung der für Angreifer erreichbaren FMR zu berücksichtigen.

4.2.6 ID-Attribute sind aktuell (A.6)

Unmittelbar durch das ID-Dokument selbst kann eine Aktualität der ID-Attributen nur sehr eingeschränkt durch den maximalen Gültigkeitszeitraum gewährleistet werden. Daneben könnten die ID-Attribute, insbesondere biometrische Daten, mit Metadaten gekennzeichnet werden, die das Datum ihrer Erfassung bzw. letzten Aktualisierung kennzeichnen.

Einen wesentlichen Anteil bei der Gewährleistung, dass Änderungen bei ID-Attributen (z. B. Name oder Anschrift) zeitnah berücksichtigt werden haben die mit den ID-Dokumenten verbundenen administrativen Prozesse und Vorschriften. Basierend darauf kann bewertet werden, inwieweit von einer hinreichenden Aktualität sämtlicher ID-Attribute ausgegangen werden kann.[12]

4.2.7 Verfügbare Sperrmeldungen werden überprüft (A.7)

Sofern für das ID-Dokument vorab eine maximale Gültigkeitsdauer festgesetzt ist, ist diese i. d. R. direkt aus dem ID-Dokument ablesbar und muss für alle Vertrauensniveaus geprüft werden.

Grundvoraussetzung für die Überprüfbarkeit von Sperrmeldungen ist zunächst, dass für das ID-Dokument ein System zum Erfassen und Abfragen von Sperrmeldungen (insbesondere „verloren“ bzw. „gestohlen“-Meldungen) umgesetzt ist. Ist diese Grundvoraussetzung gegeben, hängt es von dem ID-Prüfverfahren ab, ob die Abfrage von Sperrmeldungen durchgeführt werden kann. Eine Überprüfung auf Sperrmeldungen ist nach dieser TR auch für Vertrauensniveau „substantiell“ und „hoch“ nur dann verpflichtend, wenn sie im Rahmen des ID-Prüfverfahrens umgesetzt werden kann.

4.2.8 Weitere Anforderungen

Die Festlegung der gemäß dieser Anforderungen zulässigen ID-Dokumente muss hinreichend regelmäßig aktualisiert werden (A.8). Dies ist insbesondere implizit durch A.1 und A.3 gefordert. Dabei kann für Vertrauensniveau „normal“ ein längeres Zeitintervall definiert werden als für Vertrauensniveau „substantiell“ und entsprechend kürzer für Vertrauensniveau „hoch“. Insbesondere müssen neu bekanntgewordene Fälschungen und Manipulationen von ID-Dokumenten berücksichtigt werden.

12 Beispielsweise kann bei einem in Deutschland ausgestellten und gültigem Führerschein nicht von der Aktualität der ID-Attribute ausgegangen werden. Da der Führerschein juristisch nicht als Identitätsnachweis gilt, besteht i. d. R. keine gesetzliche Verpflichtung zur Änderung auf dem Führerschein wenn sich z. B. der Name geändert hat. Werden für einen bestimmten Anwendungsfall keine aktuellen Namens- oder Adressdaten benötigt, so kann u. U. auch ein Führerschein Vertrauensniveau „normal“ im Sinne dieser TR erfüllen. Für hoheitliche ID-Nachweise wie z. B. dem deutschen Personalausweis, für die eine Verpflichtung zur Aktualisierung von ID-Attributen besteht kann die Aktualität der ID-Attribute vermutet werden.

4.3 Abdeckung der Bedrohungen

Für die Prävention und Detektion der Bedrohungen aus Abschnitt 4.1 durch die in Abschnitt 4.2 genannten Sicherheitsanforderungen gelten die Zusammenhänge aus Tabelle 5.

Bedrohung Nr.	**Abgedeckt durch Anforderung Nr.**	**Begründung**
B.1	A.1, A.8	A.1 stellt sicher, dass ID-Dokumente nur akzeptiert werden wenn sie als vertrauenswürdig eingestuft sind und es keine Anhaltspunkte für Kompromittierungen gibt. A.8 stellt sicher, dass die Informationen zur Vertrauenswürdigkeit und Integrität regelmäßig aktualisiert werden.
B.2	A.3, A.4, A.8	A.3 stellt sicher, dass nicht erkennbare Manipulationen und Fälschungen im Rahmen des berücksichtigten Angriffspotentials nicht zu erwarten sind. A.4 stellt sicher, dass effektive Methoden zum Erkennen von Manipulationen und Fälschungen bekannt sind. A.8 stellt sicher, dass neue Fälschungs- und Angriffsmethoden bei der Beurteilung von ID-Dokumenten zeitnah berücksichtigt werden.
B.3	A.5, A.8	A.5 stellt sicher, dass ein zuverlässiger Abgleich zwischen dem Verwender und den ID-Attributen des ID-Dokuments möglich ist. A.8 stellt sicher, dass neue Manipulationsmethoden zeitnah berücksichtigt werden.
B.4	A.2	A.2 stellt sicher, dass die für die Anwendungen benötigte Menge an ID-Attributen erfasst wird.
B.5	A.6, A.8	A.6 stellt sicher, dass die ID-Attribute vom ID-Dokument als aktuell angesehen werden können. A.8 stellt sicher, dass diese Eigenschaft der zulässigen ID-Dokumente regelmäßig überprüft wird.

Tabelle 5: Abdeckung der Bedrohungen der Vertrauenswürdigkeit von ID-Dokumenten

5 Sicherheit der Übertragungskanäle

Referenzniveau für die Sicherheit einer ID-Prüfung, einschließlich des Abgleichs zwischen ID-Dokument und Verwender, ist der unmittelbare Zugriff der Prüfinstanz auf das ID-Dokument und der unmittelbare Präsenzkontakt mit der zu identifizierenden Person. In verschiedenen Bereichen werden auch öffentliche informationstechnische Übertragungskanäle, insbesondere das Internet, im Rahmen von ID-Prüfungen genutzt. Neben der Berücksichtigung der technischen Sicherheit, die in dieser Richtlinie behandelt wird, sind unabhängig davon auch rechtliche Anforderungen bzw. Einschränkungen (z. B. nach [De-Mail-G], GwG, [eIDAS], VDG) hinsichtlich der Nutzungsmöglichkeiten öffentlicher Übertragungskanäle zu beachten.

Die Risiken physikalischer Manipulationen sind bei allen Übertragungskanälen relevant, auch bei unmittelbaren Kontakt zwischen Prüfinstanz und zu identifizierender Person. Bei Nutzung informationstechnischer Übertragungskanäle ergeben sich i. d. R. erhöhte Risiken aufgrund eingeschränkter Prüfmöglichkeiten. Die Risiken informations- und videotechnischer Manipulationen der übertragenen Daten sind nur bei Nutzung informationstechnischer Übertragungskanäle relevant. Bei der Nutzung informationstechnischer Übertragungskanäle muss einerseits die Sicherheit der verwendeten Kommunikationsprotokolle auf bzw. oberhalb der Transportebene sichergestellt werden. Dies gilt gleichermaßen wenn ein ID-Register oder ein ID-Dokument für die ID-Prüfung verwendet wird. Für eine Absicherung des Transportkanals mittels TLS ist [TR-03116-4] zu berücksichtigen. Auch unter der Voraussetzung eines sicheren Transportkanals bzw. -protokolls ergeben sich bei der Nutzung informationstechnischer Übertragungskanäle auf der Anwendungsebene zusätzliche Bedrohungen gegenüber einer unmittelbaren Präsenzprüfung. Bei dezidierten eID-Verfahren kann auch die Anwendungsebene unmittelbar durch kryptographische Maßnahmen abgesichert werden, so dass eine zur Präsenzprüfung gleichwertige Sicherheit erreicht werden kann. Die Absicherung der Transportebene und die Sicherheit dezidierter eID-Anwendungen werden in dieser TR nicht behandelt, hier sind [TR-03107-1] und [TR-03116-4] zu berücksichtigen. Für die Online-Ausweisfunktion des deutschen Personalausweises, elektronischen Aufenthaltstitels und der eID-Karte für Bürgerinnen und Bürger der EU und des EWR können [TR-03127], [TR-03124-1] und [TR-03130] verwendet werden.

Werden informationstechnisch gesicherte Übertragungskanäle, aber kein dezidiertes eID-Verfahren verwendet, so ist die (Sicht)prüfung physikalischer (optischer) Merkmale auch stets mit einem Informations- und Detailverlust verbunden, z. B. durch Samplingfehler, limitierte Tiefenschärfe, eingeschränkter Farbraum, maximale Bandbreite des Übertragungskanals und Auflösung der Aufzeichnungs- und Wiedergabegeräte. Darüber hinaus können die auf der Anwendungsebene dargestellten Daten vom Sender auch unmittelbar informationstechnisch erzeugt oder manipuliert werden. Damit ergeben sich für die hier betrachteten zusätzlichen Risiken der Manipulation auf der Anwendungsebene zwei Aspekte:

1. Reduzierte Qualität / reduzierter Informationsgehalt durch begrenztes Auflösungsvermögen, eingeschränkten Erfassungsbereich der Übertragungsmittel sowie i. d. R. zweidimensionale Darstellung. Dies betrifft als „Querschnittrisiko“ den gesamten Prüfprozess. So können beispielsweise taktile/haptische Sicherheitsmerkmale nicht geprüft werden, i. d. R. auch keine UV- oder IR-Sicherheitsmerkmale. Optische Sicherheitsmerkmale im sichtbaren Spektrum (Tageslicht) können nur mit reduzierter Qualität geprüft werden. Dadurch werden gefälschte oder manipulierte ID-Nachweise schlechter erkannt bzw. das notwendige Angriffspotential für eine erfolgreiche Fälschung der zu berücksichtigende Sicherheitsmerkmale und deren Qualität wird reduziert. Analog lassen sich Manipulationen biometrischer Charakteristika bei der zu identifizierenden Person („presentation attacks“) bei einer Videoübertragung schlechter erkennen.
2. Informationstechnische Manipulation eines übertragenen Signals, d. h. das übertragene Videosignal des ID-Dokuments und/oder der zu identifizierenden Person wurde vorsätzlich gegenüber der physikalischen Realität geändert oder künstlich erzeugt. Dadurch ergibt sich ein zusätzliches, eigenständiges Angriffspotential im Vergleich zu einer unmittelbaren Präsenzprüfung.

In dieser TR werden die spezifischen Risiken informationstechnischer Übertragungskanäle ausschließlich unter diesen beiden Aspekten betrachtet.

5.1 Bedrohungen

Für die Sicherheit der Übertragungskanäle müssen folgende Bedrohungen berücksichtigt werden:

B1. Die übertragenen biometrischen Daten (z. B. Gesichtsbild) der zu identifizierenden Person werden videotechnisch manipuliert (so dass sie zum ID-Nachweis einer anderen Person passen).

B2. Die Übertragung des ID-Dokuments wird videotechnisch manipuliert hinsichtlich

1. biometrischer Daten (z. B. Gesichtsbild), so dass sie zu einem nicht berechtigten Antragsteller passen
2. optisch personalisierter ID-Attribute (z. B. Name) oder Gültigkeitsattribute
3. Sicherheitsmerkmale (z.B. Einblendung nicht vorhandener oder Aufbereitung der Merkmale bei einem gefälschten ID-Dokument).

B3. Eingeschränkte Übertragungsqualität, Unterbrechungen oder Videoschnitte oder andere Manipulationen verhindern oder erschweren die Erkennung physikalischer Manipulationen (z. B. Masken) biometrischer Charakteristika der zu identifizierenden Person.

B4. Eingeschränkte Übertragungsqualität, Unterbrechungen oder Videoschnitte verhindern oder erschweren die Erkennung des Nichtvorhandenseins bzw. der Fälschung von Merkmalen auf dem präsentierten ID-Nachweis.

B5. Es werden frühere, ggf. veraltete Aufzeichnungen wiederverwendet (replay attack), ggf. ohne den Willen oder das Wissen der identifizierten Person.

5.2 Anforderungen für Vertrauensniveaubewertung

Zur Prävention und Detektion der Bedrohungen aus Abschnitt 5.1 sind die im Folgenden diskutierten Anforderungen für die Sicherheit der Übertragungskanäle zu berücksichtigen. Bei der Nutzung informationstechnischer Übertragungskanäle in ID-Prüfverfahren sind für die Zuordnung dieses Teilaspekts zu einem Vertrauensniveau die einzelnen Anforderungen in Abhängigkeit einer abgestuften Resistenz gegenüber Angriffspotentialen zu betrachten. Dabei sind sowohl bekannte als auch nach dem Stand der Technik als umsetzbar erscheinende Angriffe, im Rahmen des jeweils betrachteten Angriffspotentials, zu berücksichtigen. Dies ist in Tabelle 6 zusammengefasst.

Nr.	**Anforderung**	**Notwendig für Vertrauensniveau**		
		Normal	**Substantiell**	**Hoch**
A.1	Video-/Informationstechnische Manipulationen biometrischer Daten der zu identifizierenden Person werden erkannt	Ja; bei Angriffspotential „enhanced-basic“	Ja; bei Angriffspotential „moderate“	Ja; bei Angriffspotential „high“
A.2	Informationstechnische Manipulationen vom ID-Dokument übertragener Informationen werden erkannt			
A.3	Physikalische Manipulationen biometrischer Charakteristika der zu identifizierenden Person werden erkannt			
A.4	Physikalische Manipulationen am präsentierten ID-Dokument werden erkannt			
A.5	Liveübertragung sämtlicher Daten ist			

Nr.	Anforderung	Notwendig für Vertrauensniveau		
		Normal	Substantiell	Hoch
	gewährleistet. Insbesondere wird auch eine teilweise Wiedereinspielung von Aufzeichnungen erkannt.			
A.6	Ein Austausch des präsentierten ID-Dokuments oder der zu identifizierenden Person während der Prüfung wird erkannt			
A.7	Die gleichzeitige Manipulation biometrischer Charakteristika (bzw. Daten) der zu identifizierenden Person und entsprechender biometrischer Referenzdaten auf dem ID-Dokument wird erkannt			

Tabelle 6: Anforderungen an die Sicherheit der Übertragungskanäle gemäß Vertrauensniveau

Bei Nutzung eines auf Anwendungsebene nicht ausreichend abgesicherten informationstechnischen Übertragungskanals werden Authentisierungsfaktoren, die originär aus unterschiedlichen Kategorien stammen (z. B. ID-Dokument und Gesicht der Person) und unterschiedliche Angriffsvektoren für Manipulationen erfordern, durch die gemeinsame Abbildung auf einen informationstechnischen Übertragungskanal (z. B. Videostream) durch Angriffsvektoren aus der selben Kategorie (z. B. videotechnische Manipulationen) angreifbar. Dies ist insbesondere bei der Bestimmung des Angriffspotentials zu berücksichtigen.

Im Folgenden werden zu jeder Anforderung Richtlinien genannt, die bei einer Bewertung des erreichten Vertrauensniveaus zu berücksichtigend sind.

5.2.1 Video-/Informationstechnische Manipulationen biometrischer Daten der zu identifizierenden Person werden erkannt (A.1)

Hier sind die Maßnahmen und Prozesse zur Prävention und Detektion videotechnischer Manipulationen zu bewerten. Dies beinhaltet insbesondere das Erkennen, wenn Software biometrische Daten, z. B. die Repräsentation eines Gesicht, einer zu identifizierenden Person so manipuliert, dass sie zum ID-Nachweis einer anderen Person passen. Basierend auf dem Stand der Technik ist der notwendige Aufwand bzw. das notwendige Angriffspotential zu bewerten um eine FAR oberhalb des zulässigen Maximums zu erreichen. Dabei ist für eine Bewertung des Angriffspotentials der kombinierte Aufwand aus initialer Implementierung bzw. Vorbereitung und der Durchführung zu betrachten[13].

Expertenwissen: Hier ist das notwendige fachspezifische Wissen für die videotechnische Manipulationen zu bewerten. Anforderungen, die nicht wesentlich über Installation von Software und deren Bedienung über grafische Nutzeroberflächen hinausgehen können auch von Laien erfüllt werden. Sind Spezialkenntnisse z. B. für die Nutzung von Videobearbeitungssoftware notwendig die eine einschlägige Ausbildung oder vergleichbare Kenntnisse erfordern so ist dies als „proficient“ einzustufen. Kenntnisse und Methoden auf dem aktuellen Stand der Forschung sind als „expert“ einzustufen, als „multiple expert“ wenn verschiedene Fachbereiche kombiniert werden müssen.

Sofern für einen Angriff spezifische **Insiderkenntnisse** relevant und zu berücksichtigen sind, sind diese nach [CEM], B.4.2.2 zu bewerten.

13 Mutmaßlich ist die initiale Implementierung eines Angriffs die wesentlichere Hürde und die Grenzkosten sowie das notwendige Know-how für die (wiederholte) Durchführung sind vergleichsweise gering. Die daraus resultierende hohe Skalierbarkeit eines Angriffs ist ggf. in einer Risikoanalyse für das ID-Nachweisverfahren zusätzlich zu betrachten.

Ob für die Durchführung eines Angriffs zusätzlich spezielle **Zugangs- / Zugriffsgelegenheiten** erfüllt sein müssen, hängt von der Art der videotechnischen Manipulation ab. Wird z. B. für einen Angriff das ID-Dokument und eine vorab aufgezeichnete („RGB“ / „RGB-D“) Videoaufnahme des Kopfs der Person benötigt unter dessen Identität sich anschließend ein Angreifer ausgibt, so ist dies i. d. R. als „einfach“ einzustufen, wenn eine beliebige Person verwendet werden soll. Sollen ID-Dokument und Videoaufnahme von einer bestimmten Person stammen, so ist dieser Faktor als „moderat“, in begründeten Einzelfällen (bei bestimmten Personen) ggf. auch als „schwierig“ einzustufen.

Ausrüstung: Hier ist insbesondere die benötigte Hard- und Software zu berücksichtigen. Standardprodukte die im Fachhandel direkt verfügbar sind, sind als „Standard“-Ausrüstung zu betrachten. Werden Standardkomponenten verwendet die individuell für diesen Zweck konfiguriert werden müssen (z. B. Arrays von Grafikkarten, Integration verschiedener Softwarekomponenten) so ist sie als „specialised“ einzustufen. Hard- oder Softwarekomponenten die dem neuesten Stand der Forschung und Technik entsprechen und noch nicht oder nur als Einzelfertigung kommerziell verfügbar sind, sind als „bespoke“ einzustufen. Analog „multiple bespoke“ wenn „bespoke“ Komponenten aus mehreren verschiedenen Bereichen kombiniert werden müssen.

5.2.2 Informationstechnische Manipulationen vom ID-Dokument übertragener Informationen werden erkannt (A.2)

Dies beinhaltet videotechnische Manipulationen optisch personalisierter Daten auf einem ID-Dokument und auch allgemein die Manipulation elektronisch auf dem ID-Dokument gespeicherter Daten, z. B. eines elektronisch gespeicherten Gesichtsbilds. Die Methodik zur Ermittlung des notwendigen Angriffspotentials ist in weiten Teilen analog zum vorangehenden Abschnitt 5.2.1 (A.1). Als methodischer Unterschied ist jedoch eine Bewertung basierend auf den individuellen Charakteristika jedes zulässigen ID-Nachweises erforderlich. Bei der abschließenden Bewertung des notwendigen Angriffspotentials um eine FAR oberhalb des zulässigen Maximums zu erreichen, ist dann nach dem Minimumprinzip der ID-Nachweis relevant, der das niedrigste Angriffspotential erfordert.

5.2.3 Physikalische Manipulationen biometrischer Charakteristika der zu identifizierenden Person werden erkannt (A.3)

Dies berücksichtigt das Szenario, dass nicht der berechtigte Inhaber eines ID-Nachweises auftritt. Also insbesondere alle Arten von „presentation attacks“, d. h. dass eine Person mit manipulierten Merkmalen (z. B. durch Schminke, Masken, Perücken, Prosthetiks) auftritt oder, weiter gefasst, auch dass ein Gegenstand (z. B. Foto, 3D Modell) verwendet wird.

Unter welchen Umständen ein Angriff als erfolgreich einzustufen ist und damit die Bewertung des notwendigen Angriffspotentials hängt ganz erheblich davon ab wie die biometrischen Charakteristika der Person erfasst und ausgewertet werden.

Expertenwissen: Wird für eine Manipulation biometrischer Charakteristika Expertenwissen im Sinne einer Ausbildung, z. B. als Maskenbildner oder vergleichbar benötigt ist dies in Anlehnung an [CEM] als „proficient“ einzustufen. Sind Kenntnisse und Fähigkeiten erforderlich die den bestmöglichen Stand der Technik erfordern ist dies als „expert“ einzustufen, als „multiple experts“ wenn entsprechende kombinierte Kenntnisse aus verschiedenen Bereichen benötigt werden.

Sofern für einen Angriff spezifische **Insiderkenntnisse** relevant und zu berücksichtigen sind, sind diese nach [CEM], B.4.2.2 zu bewerten.

Zugangs- / Zugriffsgelegenheiten: Je nach Art des Angriffs können unter Umständen besondere Zugangs- / Zugriffsgelegenheiten für die Entwicklung oder Durchführung notwendig sein. Beispielsweise kann der (testweise) Zugriff auf die eingesetzten Verfahren zum Erkennen von Manipulationen notwendig sein um einen Angriff zu entwickeln. Die Bewertung ist nach [CEM], B.4.2.2 durchzuführen.

Ausrüstung: Die Bewertung notwendiger Ausrüstung ist an [CEM], B.4.2.2 anzulehnen. So sind Materialien (z. B. Masken) und Ausrüstung (z. B. Kameras) die im einschlägigen Fachhandel verfügbar sind sind als „standard“ Ausrüstung zu betrachten. Materialien und Maßanfertigungen, die nicht im Fachhandel angeboten werden, sind i. d. R. als „specialised“ einzuordnen.

5.2.4 Physikalische Manipulationen am ID-Dokument werden erkannt (A.4)

Für die Bewertung des Angriffspotentials durch manipulierte oder gefälschte ID-Nachweise dient Abschnitt 4.2.3 als Grundlage. Für die Bewertung des notwendigen Angriffspotentials bei konkreten ID-Prüfverfahren müssen i. d. R. zusätzlich Einschränkungen durch die tatsächlich vorhandenen Prüfmöglichkeiten und durchgeführten Überprüfungen berücksichtigt werden. Hat die Prüfinstanz keinen unmittelbaren Zugriff auf den präsentierten ID-Nachweis, kann i. d. R. ein Teil der Sicherheitsmerkmale (z. B. UV oder IR-Aufdruck, taktile Merkmale) überhaupt nicht überprüft werden, andere Sicherheitsmerkmale (z. B. Guillochen) sind aufgrund der begrenzten Auflösung des Übertragungskanals leichter fälschbar als bei einer physikalischen Prüfung. Das notwendige Angriffspotential ist somit nach Abschnitt 4.2.3 zu bewerten, unter Berücksichtigung der genannten Einschränkungen bei der ID-Dokument Überprüfung.

5.2.5 Liveübertragung sämtlicher Daten ist gewährleistet (A.5)

Hier muss insbesondere auch der Angriff berücksichtigt werden, dass einmal aufgezeichnete Daten für weitere Authentisierungen wiederverwendet werden können. Durch randomisierte und dynamische Abläufe der ID-Prüfprozesse kann die unerkannte Verwendung vorab produzierten Materials erschwert werden. Daneben kann die Verwendung von Hardware oder Software gefordert werden die technisch das Einspielen vorab produzierter Daten erschwert. Für die Bewertung des notwendigen Angriffspotentials ist also der Aufwand zu berücksichtigen mit dem vorab produzierte Daten technisch an die Prüfinstanz übertragen werden können und zusätzlich der Aufwand die im Prüfprozess geforderten Daten unerkannt aus ganz oder teilweise vorab erstellten Datenquellen bereitzustellen.

Expertenwissen, Insiderkenntnisse, Zugangs- / Zugriffsgelegenheiten und Ausrüstung zur Umgehung technischer Maßnahmen zur Verhinderung des Einspielens vorab produzierter Daten soll in Anlehnung an [CEM] bewertet werden.

Für die Produktion, Kombination und unerkannte Verwendung vorab produzierter Videodaten sollen zusätzlich folgende spezifische Maßstäbe berücksichtigt werden:

Expertenwissen analog zu Abschnitt 5.2.1.

Insiderkenntnisse: Hier ist die Verfügbarkeit der Informationen zu bewerten die in der Planung, Produktion und Verwendung vorab produzierten Materials verwendet werden. Ggf. zusätzlich Insiderkenntnisse zur Umgehung von Schutzmechanismen die das Einspielen vorab produzierter Daten verhindern.

Zugangs- / Zugriffsgelegenheiten: Für die Vorbereitung eines Angriffs wird es regelmäßig notwendig sein, vorab den Ablauf einer (erfolgreichen) ID-Prüfung möglichst genau zu kennen. Beispielsweise kann es dadurch ermöglicht werden, Aufzeichnungen oder andere Informationen über den Ablauf des Verfahrens (einschließlich möglicher Varianten) zu erhalten.

Ausrüstung analog zu Abschnitt 5.2.1.

5.2.6 Ein Austausch des präsentierten ID-Dokuments oder der zu identifizierenden Person während der Prüfung wird erkannt (A.6)

Grundsätzlich kann dieser Punkt als Sonderfall manipulierter ID-Dokumente bzw. manipulierter biometrischer Charakteristika betrachtet werden, da die Integrität der vorgelegten ID-Dokumente bzw. der präsentierten biometrischen Charakteristika manipuliert wird. Hat die Prüfinstanz unmittelbaren Zugriff auf das ID-Dokument während des gesamten ID-Prüfprozesses kann dadurch ein unerkannter Austausch

i. d. R. ausgeschlossen werden. Bei unmittelbarem Sichtkontakt mit der zu überprüfenden Person kann i. d. R. auch ausgeschlossen werden, dass ID-Nachweise von mehr als einer Person erbracht werden.

Bei der Nutzung audiovisueller Übertragungskanäle kann das Angriffspotential in Anlehnung an die Produktion, Bereitstellung und Kombination vorab produzierter Videodaten in Abschnitt 5.2.5 bewertet werden.

5.2.7 Die gleichzeitige Manipulation biometrischer Charakteristika der zu identifizierenden Person und entsprechender Referenzdaten auf dem ID-Dokument wird erkannt (A.7)

Durch A.1, A.2, A.3 und A.4 sind bereits Manipulationen biometrischer Charakteristika oder Daten der zu identifizierenden Person als auch Manipulationen entsprechender Referenzdaten auf ID-Dokumenten adressiert. Durch A.7 wird zusätzlich sicher gestellt, dass eine Detektion von Merkmalsmanipulationen der zu identifizierenden Person nicht notwendigerweise genuine Referenzdaten auf dem ID-Dokument voraussetzen kann und umgekehrt.

5.3 Abdeckung der Bedrohungen

Für die Prävention und Detektion der Bedrohungen aus Abschnitt 5.1 durch die in Abschnitt 5.2 genannten Sicherheitsanforderungen gelten die Zusammenhänge aus Tabelle 7.

Bedrohung Nr.	**Abgedeckt durch Anforderung Nr.**	**Begründung**
B.1	A.1, A.6	A.1 stellt sicher, dass videotechnische Manipulationen bei den übertragenen biometrischen Daten der zu identifizierenden Person erkannt werden. Daneben stellt A.6 sicher, dass übertragene und dargestellte biometrischen Charakteristika nicht von mehr als einer Person stammen können ohne dass dies erkannt wird.
B.2	A.2, A.6	A.2 stellt sicher, dass videotechnische Manipulationen des präsentierten ID-Nachweisdokuments erkannt werden. Daneben stellt A.6 sicher, dass übertragene ID-Attribute nicht von mehr als einem ID-Nachweisdokument stammen können ohne dass dies erkannt wird.
B.3	A.3	A.3 stellt sicher, dass physikalische Manipulationen biometrischer Charakteristika der zu identifizierenden Person auch bei Nutzung informationstechnischer Übertragungskanäle erkannt werden.
B.4	A.4	A.4 stellt sicher, dass physikalische Manipulationen am verwendeten ID-Nachweis auch bei Nutzung informationstechnischer Übertragungskanäle erkannt werden.
B.5	A.5	A.5 stellt sicher, dass die Verwendung vorab aufgezeichneter Daten erkannt wird.

Tabelle 7: Abdeckung der Bedrohungen der Sicherheit der Übertragungskanäle

6 Prüfung der ID-Nachweise

Grundsätzlich können für einen bestimmten Typ von ID-Nachweis verschiedene Prüfmethoden definiert sein. Hinsichtlich des Vertrauensniveaus das der ID-Nachweisprüfung zugeordnet werden kann ist wieder das Minimumprinzip, hier über alle relevanten Kombinationen aus ID-Nachweis und jeweils zugelassener Prüfmethode, anzuwenden.

6.1 Echtheit und Unverfälschtheit

Das Vertrauensniveau der Echtheitsprüfung bzw. das notwendige Angriffspotential für eine unerkannte Fälschung hängen insbesondere davon ab, welche der bei einem ID-Dokument vorhandenen Sicherheitsmerkmale tatsächlich überprüft werden, mit welchen Methoden und Hilfsmitteln geprüft wird und über welche Kenntnisse und Erfahrungen die Prüfer verfügen. Dabei lassen sich die Perspektiven „Echtheit des ID-Dokuments“ bzw. „Unverfälschtheit der Daten bzw. Personalisierung“ betrachten. Dies entspricht den Bedrohungen, dass ein ID-Dokument von Grund auf gefälscht ist bzw. dass bei einem (ursprünglich) genuinen ID-Dokument personalisierte ID-Attribute nachträglich manipuliert wurden. Hinsichtlich „Echtheit des ID-Dokuments“ ist i. d. R. auch zu prüfen, dass es sich nicht um ein geklontes Dokument handelt.

Je nach ID-Dokument und Prüfkriterien können physikalische Sicherheitsmerkmale (Optik, Haptik, akustische Reaktionen) und/oder auf einem ggf. vorhanden Chip mit eID-Funktion elektronisch gespeicherte Sicherheitsmerkmale (z. B. signierte Daten) geprüft werden. Dabei ergibt sich das Vertrauensniveau für Echtheitsprüfung aus dem Maximum der Vertrauensniveaus aus einer physikalischen und/oder digitalen Prüfung. Grundsätzlich ist für eine Prüfung eine der beiden Merkmalsklassen (physikalische oder digitale Sicherheitsmerkmale) ausreichend.

6.2 Gültigkeit

Neben der Echtheit und Unverfälschtheit muss auch die Gültigkeit des ID-Dokuments überprüft werden. Dies umfasst den ursprünglichen und ggf. verlängerten Gültigkeitszeitraum sowie, je nach Verfügbarkeit, Anwendung und erforderlichem Vertrauensniveau, die ein- oder mehrmalige Abfrage verfügbarer Sperrlisten, um ggf. auch die mögliche Zeitspanne zwischen Verlust/Diebstahl und Sperrmeldung zu berücksichtigen.

6.3 Bedrohungen

Für eine sichere Prüfung von ID-Nachweisen müssen folgende Bedrohungen berücksichtigt werden:

B1. Es wird ein als gestohlen, verloren oder ungültig gemeldetes ID-Dokument verwendet.

B2. Es wird ein abgelaufenes ID-Dokument verwendet.

B3. Es wird ein gefälschtes ID-Dokument verwendet.

B4. Es wird ein ID-Dokument mit manipulierten ID-Attributen verwendet.

6.4 Anforderungen für Vertrauensniveaubewertung

Zur Prävention und Detektion der Bedrohungen aus Abschnitt 6.3 sind die im Folgenden diskutierten Anforderungen an die Prüfung der ID-Nachweise zu berücksichtigen. Die je nach Vertrauensniveau abgestuften Anforderungen sind in Tabelle 8 zusammengefasst.

Nr.	Anforderung	Notwendig für Vertrauensniveau		
		Normal	**Substantiell**	**Hoch**
A.1	Typ des verwendeten ID-Dokuments lässt sich ermitteln	Ja	Ja	Ja
A.2	ID-Dokument ist gültig	Ja; nur Prüfung Gültigkeitsdatum	Ja; wie normal	Ja
A.3	Gefälschte Sicherheitsmerkmale werden erkannt	Ja; entsprechend Angriffspotential „enhanced-basic“	Ja; entsprechend Angriffspotential „moderate“	Ja; entsprechend Angriffspotential „high“
A.4	Fälschungen der personalisierten Daten werden erkannt	Ja; entsprechend Angriffspotential „enhanced-basic“	Ja; entsprechend Angriffspotential „moderate“	Ja; entsprechend Angriffspotential „high“

Tabelle 8: Anforderungen an die Prüfung der ID-Nachweise gemäß Vertrauensniveau

6.4.1 Typ des verwendeten ID-Dokuments lässt sich ermitteln (A.1)

Für eine sichere ID-Prüfung ist es notwendig, dass ID-Nachweise nur akzeptiert werden, wenn sie auf einem vorab als zulässig definierten ID-Dokument basieren. Dazu muss für jedes vorgelegte ID-Dokument der genaue Typ festgestellt und überprüft werden, ob er für das angestrebte Vertrauensniveau prinzipiell zugelassen ist. Bei Reisepässen ist der Typ z. B. durch das Tupel (CountryCode, Document Type, ID-Number, Year of first issuance) definiert. Bekanntheit und Akzeptanz des für den ID-Nachweis vorgelegten ID-Dokuments implizieren auch dass hinreichend zuverlässige Kriterien für die Echtheitsprüfung definiert sind (vergleiche Abschnitt 4.2.4).

6.4.2 ID-Dokument ist gültig (A.2)

Hier umfasst die Gültigkeit den formalen Status des ID-Dokuments, hinsichtlich eines definierten maximalen Gültigkeitsdatums sowie, sofern möglich, Sperrstatus, z. B. aufgrund einer Verlust- oder Gestohlenmeldung. Dieser Teil des ID-Prüfprozesses ist komplementär zu der Überprüfbarkeit von Gültigkeit und Sperrmeldungen nach Abschnitt 4.2.7. Weiterhin umfasst dies auch die Gültigkeit und damit Aktualität der ID-Attribute (vergleiche Abschnitt 4.2.6). Für die Prüfung des Sperrstatus ist die Verfügbarkeit und der Zugriff auf entsprechende Hintergrundsysteme / Sperrlisten notwendig.

6.4.3 Gefälschte Sicherheitsmerkmale werden erkannt (A.3)

Auf Grundlage bekannter und effektiv überprüfbarer Sicherheitsmerkmale (vgl. Abschnitt 4.2.4) sind für jedes zulässige ID-Dokument verbindliche Prüfvorgaben festzulegen. Dies umfasst insbesondere

- Klare Kriterien wann ein ID-Nachweis als echt und unverfälscht anerkannt wird
- Ggf. zu verwendende Hilfsmittel (z. B. UV-, IR-Lampe, ID-Dokumenten Lese- und Prüfgeräte) deren Verfügbarkeit und Funktionsfähigkeit sichergestellt sein muss
- Nachgewiesene Kompetenz der ID-Prüfer im Umgang mit allen zulässigen ID-Dokmenten und den jeweils einzusetzenden Hilfsmitteln
- Kenntnis und Berücksichtigung existierender „best practices“ zur Erkennung von Fälschungen und Manipulationen
- Ausreichende Zeit für jeden Prüfschritt

Basierend auf der in Abschnitt 4.2.3 diskutierten Fälschungssicherheit des ID-Dokuments sind die tatsächlich durchgeführten ID-Prüfungen der effektive Maßstab für den relevanten Fälschungsaufwand. D. h. der ID-Prüfprozess definiert letztlich den Aufwand für eine erfolgreiche Fälschung und damit für das notwendige Angriffspotential nach Abschnitt 4.2.3.

Um den ID-Nachweis als gefälscht zu erkennen genügt die Detektion eines einzigen gefälschten Sicherheitsmerkmals. Damit ist für die Ermittlung des tatsächlich notwendigen Angriffspotentials aus der Perspektive der Fälschungssicherheit des ID-Dokuments der kumulative Aufwand zu bewerten um alle geprüften Sicherheitsmerkmale in jeweils hinreichender Qualität für alle Prüfschritte zu fälschen.

6.4.4 Fälschungen der personalisierten Daten werden erkannt (A.4)

Dieser Aspekt der ID-Prüfung umfasst das Erkennen von Fälschungen bzw. Verfälschungen der Personalisierung (d. h. der ID-Attribute) oder Kombinationen aus verschiedenen ID-Nachweisen. Hier handelt es sich um einen Sonderfall der Prüfung nach Abschnitt 6.4.3, jedoch ist das notwendige Angriffspotential nach dem Minimumprinzip zu ermitteln: Für eine sichere Feststellung der ID-Attribute ist es notwendig, dass jedes einzelne der erfassten und benötigten ID-Attribute unverfälscht ist. Ein Angriff ist bereits dann erfolgreich, sobald eine relevante Menge an ID-Attributen erfolgreich manipuliert wurde.

Darüber hinaus soll hier auch eine Konsistenzprüfung der ID-Attribute durchgeführt werden. Z. B. müssen Gesichtsbild, Geburtsdatum und Ausstellungsdatum zusammen passen oder die Daten aus einer Maschinenlesbaren Zone (MRZ) müssen konsistent sein und zu den sonstigen personalisierten Daten passen.

6.5 Abdeckung der Bedrohungen

Für die Prävention und Detektion der Bedrohungen aus Abschnitt 6.3 durch die in Abschnitt 6.4 genannten Sicherheitsanforderungen gelten die in Tabelle 9 zusammengefassten Zusammenhänge:

Bedrohung Nr.	**Abgedeckt durch Anforderung Nr.**	**Begründung**
B.1	A.2	A.2 stellt sicher, dass keine als gestohlen/verloren/ungültig gemeldeten ID-Nachweise verwendet werden können.
B.2	A.2	A.2 stellt sicher, dass kein abgelaufener ID-Nachweis verwendet werden kann.
B.3	A.1, A.3	A.1 stellt sicher, dass nur vordefinierte und bekannte ID-Nachweise mit bekannten und überprüfbaren Sicherheitsmerkmalen zulässig sind. A.3 stellt sicher, dass gefälschte ID-Nachweise anhand definierter Kriterien erkannt werden.
B.4	A.1, A.5	A.1 stellt sicher, dass nur vordefinierte und bekannte ID-Nachweise mit bekannten und überprüfbaren Sicherheitsmerkmalen zulässig sind. A.5 stellt sicher, dass manipulierte ID-Nachweise anhand definierter Kriterien erkannt werden.

Tabelle 9: Abdeckung der Bedrohungen bei der Prüfung der ID-Nachweise

7 Abgleich von Personen mit ID-Nachweisen

Regelmäßig wird die Identität einer Person durch die Vorlage eines ID-Dokuments und dem Abgleich darauf gespeicherter Daten mit biometrischen Charakteristika (z. B. Gesicht) einer Person geprüft. Ein bedeutendes Bedrohungsszenario ist hier die Verwendung eines ID-Dokuments durch einen illegitimen Besitzer (Identitätsdiebstahl). Es muss deshalb insbesondere sichergestellt werden, dass nur der legitime Inhaber einen erfolgreichen ID-Nachweis erbringen kann[14]. Bei einer Multi-Faktor-Authentisierung muss die legitime Inhaberschaft durch zusätzliche Faktoren neben dem Besitz des ID-Dokuments nachgewiesen werden. Nach [ISO/IEC 19790] lassen sich Authentisierungsfaktoren in die folgenden Kategorien einteilen:

1. Wissen (z. B. PIN)
2. Besitz (hier ID-Dokument)
3. Inhärente Faktoren (biometrische Charakteristika, z. B. Gesicht, „Fingerabdruck“) oder Verhaltensmuster (z. B. Unterschrift)

Die konkret erforderliche Art und Anzahl der zu prüfenden Authentisierungsfaktoren bestimmt sich aus dem jeweiligem Anwendungsfall und dem erforderlichen Vertrauensniveau. Für einen sicheren Abgleich von einer Person mit einem ID-Dokument sollten möglichst viele und komplementäre Authentisierungsfaktoren, d. h. Faktoren aus verschiedenen Kategorien, geprüft werden. Bei allen verwendeten Authentisierungsfaktoren sollte sich für den legitimen Inhaber in aller Regel ein jeweils positives Prüfergebnis ergeben. Deshalb wird für ein positives Gesamtergebnis gefordert, dass das Ergebnis jedes einzelnen durchgeführten Tests positiv ist.

Die Richtlinien aus diesem Abschnitt setzen eine Multi-Faktor Authentisierung voraus. Grundlage ist der Besitz eines ID-Dokuments zusammen mit dem Nachweis mindestens eines weiteren Faktors aus den Kategorien „Wissen“ oder „Inhärenter Faktor / Verhaltensmuster“ mit dem die legitime Inhaberschaft bestätigt wird.

7.1 Bedrohungen

Für einen zuverlässigen Abgleich von einer Person mit einem ID-Dokument müssen insbesondere folgende Bedrohungen berücksichtigt werden:

B1. Ein vertraulicher Wissensfaktor, der nur dem legitimen Inhaber bekannt sein darf, wird kompromittiert.

B2. Eine nicht berechtigte Person benutzt den ID-Nachweis einer anderen Person.

B3. Biometrische Charakteristika oder Verhaltensmuster des legitimen Inhabers werden imitiert.

Wird bei einem ID-Prüfverfahren kein Wissensfaktor bzw. kein biometrischer Faktor geprüft, so muss die jeweilige Bedrohung nicht betrachtet werden.

7.2 Anforderungen für Vertrauensniveaubewertung

Der Abgleich von Personen mit ID-Dokument erfordert organisatorisch zwingend eine Interaktion mit der zu identifizierenden Person. Für die Vertrauensniveaubewertung dieses Verfahrens sind die Anforderungen gemäß Tabelle 10 zu berücksichtigen.

14 Wie in den übrigen Abschnitten dieser Technischen Richtlinie werden wiederum nur ID-Nachweise betrachtet, die auf bereits vorhandenen ID-Nachweisdokumenten basieren.

Nr.	Anforderung	Notwendig für Vertrauensniveau		
		Normal	**Substantiell**	**Hoch**
A.1	Vertrauliche Wissensfaktoren werden ausschließlich dem legitimen Inhaber mitgeteilt	Ja	Ja; wie „normal“ plus getrennte Übermittlungswege	Ja; wie „substantiell“ plus explizite Aktivierung
A.2	Sicherheit der verwendeten Authentisierungsmittel	Ein Faktor	Zwei Faktoren, sicher bei Angriffspotential „moderate“	Zwei Faktoren, sicher bei Angriffspotential „high“
A.3	Die tatsächliche Verfügungsgewalt der zu identifizierenden Person über das ID-Dokument ist sichergestellt	-	Ja	Ja
A.4	Abzugleichende ID-Attribute werden in hinreichender Qualität erfasst	Ja; entsprechend maximal zulässiger FMR und Schutz vor gezielten Angriffen bei Angriffspotential „enhanced-basic“	Ja; entsprechend maximal zulässiger FMR und Schutz vor gezielten Angriffen bei Angriffspotential „moderate“	Ja; entsprechend maximal zulässiger FMR und Schutz vor gezielten Angriffen bei Angriffspotential „high“
A.5	Zuverlässiger Abgleich relevanter biometrischer ID-Attribute zwischen ID-Dokument und zu identifizierender Person			

Tabelle 10: Anforderungen an den Abgleich von Personen und ID-Nachweisen gemäß Vertrauensniveau

7.2.1 Vertrauliche Wissensfaktoren werden ausschließlich dem legitimen Inhaber mitgeteilt (A.1)

Bei der Übermittlung vertraulicher Wissensfaktoren, die an das ID-Dokument gekoppelt sind, muss sichergestellt werden, dass sie nur dem legitimen Inhaber zugänglich sind. Neben einer Zustellung die den Zugang nicht berechtigter Personen ausschließt („tamper proof“) kann diese Anforderung auch dadurch erfüllt sein, dass ein unberechtigter Zugriff während der Zustellung rechtzeitig und sicher erkannt wird („tamper evident“). Die Anforderungen orientieren sich an den Anforderungen von [TR-03107-1] für die Ausgabe der Authentisierungsmittel.

Ab Vertrauensniveau „substantiell“ muss die Zustellung getrennt von der Übermittlung anderer ID-Nachweisfaktoren erfolgen. Für Vertrauensniveau „hoch“ müssen vertrauliche Wissensfaktoren zusätzlich durch den Inhaber aktiviert werden.

Auch nach der vertraulichen Übermittlung müssen die Wissensfaktoren geheim gehalten werden. Dazu bestätigt i. d. R. der Empfänger die Kenntnisnahme und Akzeptanz der jeweils gültigen Regeln über den sicheren Umgang mit vertraulichen Wissensfaktoren. Entsprechende Hinweise müssen an einer für den Inhaber klar ersichtlichen Stelle platziert sein. Die Regeln können Bestandteil von AGBs sein, ein bloßer Verweis auf z.B. AGBs ist jedoch keine ausreichende Nutzersensibilisierung.

Der Abgleich von Personen mit ID-Nachweisen kann auch ohne Verwendung vertraulicher Wissensfaktoren erfolgen, z. B. wenn die Sicherheit auf den Faktoren Besitz und dem Abgleich biometrischer ID-Attribute (inhärenter Faktoren) basiert.

7.2.2 Sicherheit der verwendeten Authentisierungsmittel (A.2)

Hier sind insbesondere die Anforderungen aus [TR-03107-1] (Abschnitt 3.3.1) zu berücksichtigen.

Für einen Wissensfaktor setzt dies insbesondere voraus, dass er (neben der Mitteilung an den legitimen Inhaber, siehe A.1), ausschließlich und zugriffsgeschützt auf dem ID-Dokument gespeichert ist[15] und nur zusammen mit dem ID-Nachweis selbst verifiziert werden kann. Für die vertrauliche Speicherung von Wissensfaktoren auf ID-Dokumenten werden i. d. R Chipkarten eingesetzt. In diesem Fall ist für die Bewertung des notwendigen Angriffspotentials zur Kompromittierung des Wissensfaktors [JILAPS] maßgeblich.

7.2.3 Die tatsächliche Verfügungsgewalt der zu identifizierenden Person über das ID-Dokument ist sichergestellt (A.3)

Diese Anforderung kann z. B. durch die effektive Vorlage bzw. das Vorzeigen des ID-Dokuments erfüllt werden. In jedem Fall ist zusätzlich die Authentizität des vorgelegten ID-Dokuments gemäß dem angestrebten Vertrauensniveau zu prüfen.

7.2.4 Abzugleichende ID-Attribute werden in hinreichender Qualität erfasst (A.4)

Abzugleichende (biometrische) ID-Attribute müssen sowohl auf dem ID-Dokument als auch bei der zu identifizierenden Person in einer hinreichenden Qualität erfasst werden, die zuverlässig eine 1-zu-1 Zuordnung ermöglicht.

Die spezifischen Qualitätskriterien bestimmen sich durch das jeweils verwendete Matchingverfahren. Dies kann personell oder maschinell erfolgen. Hier ist maßgeblich, dass die für das angestrebte Vertrauensniveau maximal zulässige FMR nicht überschritten wird.

Für eine ggf. erforderliche Mindestqualität um Fälschungen am Dokument selbst zu erkennen, siehe Abschnitte 4.2.3, 5.2.4 und 6.4.4.

Für Aspekte um „presentation attacks“ zu erkennen, siehe Abschnitt 5.2.3. Insbesondere müssen biometrische Charakteristika zuverlässig, nach dem Stand der Technik, auf „presentation attacks“ (bzw. „liveness detection“) und andere bekannte Täuschungsversuche geprüft werden.

7.2.5 Zuverlässiger Abgleich relevanter biometrischer ID-Attribute zwischen ID-Dokument und zu identifizierender Person (A.5)

Maßstab für die Zuverlässigkeit des Abgleichs ist die zu erwartende FMR, hier unter Berücksichtigung gezielter Manipulationsversuche. Manipulationsversuche sind jedoch nur zu berücksichtigen, wenn für das verwendete Angriffspotential das ID-Nachweisverfahren als sicher eingestuft werden soll. Die FMR soll nach Möglichkeit statistisch bestimmt werden. Mindestens muss die zur erwartende maximale FMR plausibel gemacht werden.

Für einen zuverlässigen Abgleich sollen bevorzugt mehrere komplementäre biometrische ID-Attribute abgeglichen werden, z. B. Fingerabdruck und Gesichtsbild. Insbesondere bei personellen Abgleich ist, neben der Vertrauenswürdigkeit und Fachkenntnis der Prüfer, insbesondere ausreichend Zeit für den Prüfvorgang notwendig.

Der Abgleich von Personen mit ID-Nachweisen kann auch ohne Verwendung biometrischer ID-Attribute (bzw. inhärenter Faktoren) erfolgen, z. B. wenn die Sicherheit auf den Faktoren Wissen und Besitz basiert.

15 Dies schließt die Änderungsmöglichkeit des vertraulichen Wissensfaktors durch den legitimen Inhaber nicht aus. Jedoch darf die Änderungsmöglichkeit, wie der Referenzwert des Wissensfaktors selbst, nur dem legitimen Inhaber des ID-Dokuments zugänglich sein.

7.3 Abdeckung der Bedrohungen

Für die Prävention und Detektion der Bedrohungen aus Abschnitt 7.1 durch die in Abschnitt 7.2 genannten Sicherheitsanforderungen gelten die Zusammenhänge aus Tabelle 11.

Bedrohung Nr.	**Abgedeckt durch Anforderung Nr.**	**Begründung**
B.1	A.1, A.2	A.1 erzwingt Maßnahmen um das Risiko der Kompromittierung von Wissensfaktoren zu minimieren. A.2 erzwingt zusätzlich, dass ein (ggf. kompromittierter) Wissensfaktor nur in Verbindung mit dem ID-Nachweis verwendet werden kann. Anders als bei einem kompromittierten Wissensfaktor wird das Abhandenkommen eines physikalischen ID-Nachweises i. d. R. zeitnah bemerkt und der ID-Nachweis kann gesperrt werden.
B.2	A.3	A.3 stellt sicher, dass erkannt wird wenn eine nicht berechtigte Person den ID-Nachweis einer anderen Person benutzt.
B.3	A.4, A.5	A.4 stellt sicher, dass die abzugleichenden ID-Attribute bei der zu identifizierenden Person und beim ID-Nachweis in hinreichender Qualität erfasst werden. A.5 stellt sicher, dass die jeweils erfassten ID-Attribute zuverlässig auf ein Matching überprüft werden.

Tabelle 11: Abdeckung der Bedrohungen beim Abgleich von Personen und ID-Nachweis

8 Korrekte Erfassung der benötigten ID-Attribute

Dieses Kapitel adressiert insbesondere die Qualität des Erfassungsprozesses um Fehler „aus Versehen“ zu verhindern, d. h. Fehler denen kein Manipulationsversuch durch Innen- oder Außentäter zugrunde liegt. Hier handelt es sich primär um einen (internen) Qualitätsaspekt, weniger um einen Sicherheitsaspekt zum Schutz vor gezielten (externen) Angriffen. Damit korreliert dieses Kapitel mit [eIDAS LoA] 2.1.1 „Application and Registration“, weniger mit 2.1.2 „Identity proofing and verification“.

Innerhalb des Anwendungskontexts können auch weitere interne ID-Attribute definiert und erfasst werden (z. B. E-Mailadresse, Telefonnummer, IBAN, ...) die nicht Teil des ID-Prüfprozesses waren. Anders als verifizierte externe ID-Attribute können zusätzlich im System erzeugte bzw. nachträglich erfasste interne ID-Attribute nur beschränkt auf den jeweiligen Anwendungskontext zur Definition einer eindeutigen Identität verwendet werden.

8.1 Bedrohungen

Für die korrekte Erfassung ggf. eindeutiger ID-Attribute sind folgende mögliche Bedrohungen relevant:

B1. Die Menge der ID-Attribute gewährleistet keine ggf. notwendige Eindeutigkeit.

B2. Die Menge der ID-Attribute erlaubt keine ggf. gesetzlich vorgeschriebene Identifizierung (z. B. Geldwäschegesetz), insbesondere falls Pseudonyme verwendet werden.

B3. Übertragungsfehler beim Erfassen der ID-Attribute, insbesondere

1. Schreibfehler;

2. Transkriptionsfehler, z. B. wenn Zeichen auf Grund mangelnder Funktionalität im Erfassungssystem nicht nativ unterstützt werden; Fehler wenn bei ID-Attributen nicht die volle Länge der Zeichenkette erfasst werden kann;

3. Fehlerhafte Zuordnung von ID-Attributen (z. B. Verwechslung von Vor- und Nachname bei unbekannter fremdsprachiger Beschriftung).

B4. Erfassung unvollständiger oder veralteter ID-Attribute.

Insbesondere hier ist die Relevanz der Bedrohungen stark anwendungsabhängig. So ist z. B. Eindeutigkeit oder explizite Identifizierung einer Person für einen Altersverifikationsdienst nicht relevant.

8.2 Anforderungen für Vertrauensniveaubewertung

Für die Zuordnung von Verfahren zur Erfassung ggf. eindeutiger ID-Attribute zu einem Vertrauensniveau sind die Anforderungen gemäß Tabelle 12 zu berücksichtigen.

Nr.	Anforderung	Notwendig für Vertrauensniveau		
		Normal	Substantiell	Hoch
A.1	Zu erfassende ID-Attribute erlauben eine eindeutige Identifizierung	Ja, sofern Anwendung Eindeutigkeit erfordert	Ja, sofern Anwendung Eindeutigkeit erfordert	Ja, sofern Anwendung Eindeutigkeit erfordert
A.2	Spezifische Sachkenntnis der Prüfer und ggf. zu verwendende Hilfsmittel sind vorhanden	--	Ja	Ja
A.3	ID-Attribute werden vollständig und Fehlerfrei in das Erfassungssystem übertragen	Ja	Ja	Ja

Nr.	Anforderung	Notwendig für Vertrauensniveau		
		Normal	Substantiell	Hoch
A.4	Erfasste Daten werden auf Aktualität, Konsistenz und Plausibilität geprüft	--	Ja	Ja

Tabelle 12: Anforderungen an die Erfassung eindeutiger ID-Attribute gemäß Vertrauensniveau

8.2.1 Zu erfassende ID-Attribute erlauben eine eindeutige Identifizierung (A.1)

Innerhalb des relevanten Kontext ist häufig eine eindeutige Repräsentanz jeder registrierten Person gefordert. Dies kann eine strikte Forderung sein, d. h. jede Entität, definiert durch das Tupel aller erfassten ID-Attribute, muss eindeutig sein oder, in abgeschwächter Form, die Kombination aus ID-Attributen soll höchstwahrscheinlich Eindeutigkeit gewährleisten. Je nach Anwendung sollen die ID-Attribute die referenzierte Person ggf. auch global, also auch außerhalb des jeweiligen Anwendungskontextes, eindeutig identifizieren.

Während sich die biometrischen Charakteristika die i. d. R. unveränderlich sind oder sich nur sehr langsam ändern (wie z. B. Fingerabdrücke, Venenmuster, Irismuster oder Gesichtsbild) gut zur Unterscheidung von verschiedenen Personen sowie zum Abgleich von Personen und ID-Nachweisen eignen, sind sie für eine „sprechende“ Beschreibung einer eindeutigen Identität häufig wenig geeignet. Als Menge von ID-Attributen für eine global eindeutige Identifizierung eignet sich beispielsweise „Commission Implementing Regulation (EU) 2015/1501, Annex 'Requirements concerning the minimum set of person identification data uniquely representing a natural or legal person'“.

Bei geforderter Eindeutigkeit soll durch das Erfassungssystem verhindert werden, dass eine neue Entität angelegt werden kann, wenn bereits ein Eintrag mit identischen ID-Attributen vorhanden ist.

8.2.2 Spezifische Sachkenntnis der Prüfer und ggf. zu verwendende Hilfsmittel sind vorhanden (A.2)

Die ID-Prüfer bzw. das an der Interpretation und Erfassung der ID-Attribute beteiligte Personal muss ab Vertrauensniveau substantiell für alle zugelassenen ID-Nachweise über nachgewiesene Sachkunde verfügen. Vorgesehene Hilfsmittel müssen für Erfassungsvorgänge stets verfügbar sein.

8.2.3 ID-Attribute werden vollständig und fehlerfrei in das Erfassungssystem übertragen (A.3)

Maßnahmen um versehentliche Fehler bei der Erfassung von ID-Attributen zu vermeiden, insbesondere Schreib- bzw. Tippfehler, sind beispielsweise die Mehrfacheingabe der Daten oder die Prüfung und Bestätigung der erfassten Daten durch eine zweite Person (ggf. auch durch die zu identifizierende Person selbst). Das Erfassungssystem ist technisch geeignet alle relevanten ID-Attribute vollständig und exakt aufzunehmen.

8.2.4 Erfasste Daten werden auf Aktualität, Konsistenz und Plausibilität geprüft (A.4)

Konsistenz und Plausibilitätsprüfungen können z. B. das Überprüfen der angegebenen Adresse oder der Plausibilität des Geburtsdatums (ggf. im Zusammenhang mit verfügbaren biometrischen Daten) umfassen. Die ID-Prüfung darf nicht als erfolgreich abgeschlossen werden, wenn nicht alle vordefinierten Pflichtfelder für die ID-Attribute erfasst werden können. Soweit möglich sind die ID-Attribute bei der Erfassung auf Aktualität zu prüfen (siehe hierzu auch Abschnitt 4.2.6).

8.3 Abdeckung der Bedrohungen

Für die Prävention und Detektion der Bedrohungen aus Abschnitt 8.1 durch die in Abschnitt 8.2 genannten Sicherheitsanforderungen gelten die Zusammenhänge aus Tabelle 13.

Bedrohung Nr.	**Abgedeckt durch Anforderung Nr.**	**Begründung**
B.1	A.1	A.1 stellt sicher, dass die zu erfassenden ID-Attribute die Eindeutigkeit gewährleisten.
B.2	A.1	A.1 stellt sicher, dass die Identität der zu identifizierenden Person festgestellt werden kann.
B.3	A.2, A.3, A.4	A.2 gewährleistet die erforderliche Sachkenntnis und ggf. notwendige Hilfsmittel. A.3 und A.4 gewährleisten zusammen die notwendige Sorgfalt.
B.4	A.4	A.4 stellt sicher, dass basierend auf den aktuellsten verfügbaren Daten alle zur Anlage notwendigen ID-Attribute erfasst werden.

Tabelle 13: Abdeckung der Bedrohungen bei der Erfassung eindeutiger ID-Attribute

9 Sicherung der Integrität der Prozesse

Basis für sichere ID-Prüfungen sind die in Kapitel 4 bis 7 definierten Anforderungen. Hinzu kommt als übergreifende Querschnittsaufgabe die organisatorische Gewährleistung, dass die jeweils definierten Maßnahmen auch durchgehend eingehalten werden. Darüber hinaus nennt dieses Kapitel Anforderungen zum Schutz vor vorsätzlichen Manipulationen durch Innen- und Außentäter die nicht auf manipulierten ID-Nachweisen basieren. Die dazu notwendigen technischen und organisatorischen Maßnahmen müssen jeweils dem Niveau, auf dem ID-Prüfungen durchgeführt werden angemessen sein.

Aspekte wie Serviceverfügbarkeit oder notwendige Maßnahmen zum Datenschutz werden in dieser TR nicht betrachtet.

9.1 Bedrohungen

B1. Für den ID-Nachweis geforderte ID-Prüfungen werden nicht vorschriftsgemäß durchgeführt.

B2. Nicht befugtes Anlegen von Identitäten durch Innen- oder Außentäter.

B3. Nicht befugtes Manipulieren (oder Löschen) gespeicherter ID-Attribute durch Innen- oder Außentäter.

Neben diesen unmittelbaren Bedrohungen müssen auch die vorgeschalteten mittelbaren Gefahren berücksichtigt werden, dass z. B. Prüfmittel oder Prüfer kompromittiert werden.

9.2 Anforderungen

9.2.1 Die Einhaltung der vorgeschriebenen Prüfkriterien ist sichergestellt (A.1)

Die Einhaltung der ID-Prüfkriterien kann durch technische und organisatorische Maßnahmen bzw. Kombinationen daraus sichergestellt werden. Die Maßnahmen können auch die Anforderung umfassen sämtliche erfolgreich durchgeführte ID-Prüfungen nachvollziehbar zu dokumentieren.

Basis dieser Anforderung ist die, gemäß den Anforderungen aus Abschnitt 4, Definition der für jedes ID-Dokument zu prüfenden Sicherheitsmerkmale einschließlich der Anforderung, dass diese regelmäßig aktualisiert werden.

Für manuell durchgeführte Prüfschritte ist insbesondere die Fachkunde und die Vertrauenswürdigkeit des eingesetzten Personals sicherzustellen.

9.2.2 ISMS (A.2)

Zur generischen Sicherung der Integrität IT-basierter Prozesse muss ein ISMS nach ISO/IEC 27001:2013 und ISO/IEC 27002:2013 oder gleichwertig implementiert sein. Das ISMS muss alle IT-Komponenten und IT-Prozesse umfassen, die für die Identitätsprüfung bzw. Speicherung oder Übertragung hierbei erfasster Daten verwendet werden.

9.3 Abdeckung der Bedrohungen

Für die Prävention und Detektion der Bedrohungen aus Abschnitt 9.1 durch die in Abschnitt 9.2 genannten Sicherheitsanforderungen gelten die Zusammenhänge aus Tabelle 14.

Bedrohung Nr.	**Abgedeckt durch Anforderung Nr.**	**Begründung**
B.1	A.1	A.1 stellt die Einhaltung der vorgeschriebenen Prüfkriterien sicher.

Bedrohung Nr.	Abgedeckt durch Anforderung Nr.	Begründung
B.2	A.2	A.2 gewährleistet Schutz vor unberechtigten Anlegen von Datensätzen durch Innen- und Außentäter.
B.3	A.2	A.2 gewährleistet Schutz vor unberechtigten Löschen und Manipulieren von Datensätzen durch Innen- und Außentäter.

Tabelle 14: Abdeckung der Bedrohungen der Integrität der Prozesse

Literaturverzeichnis

TR-03107-1	BSI: Technische Richtlinie TR-03107 Elektronische Identitäten und Vertrauensdienste im E-Government; Teil 1: Vertrauensdienste und Mechanismen
eIDAS LoA	: DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
CC1	: Common Criteria for Information Technology Security Evaluation
CEM	: Common Methodology for Information Technology Security Evaluation
TR-03121-3	BSI: Technische Richtlinie TR-03121 Technical Guideline Biometrics for Public Sector Applications
eIDAS	: VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
JILSS	: Joint Interpretation Library Minimum Site Security Requirements
RAND	Wolfgang Killmann, Werner Schindler: A proposal for: Functionality classes for random number generators
De-Mail-G	: De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666), das durch Artikel 2 Absatz 3 des Gesetzes vom 22.Dezember 2011 (BGBl. I S. 3044) geändert worden ist
TR-03116-4	BSI: Technische Richtlinie TR-03116, Kryptographische Vorgaben für Projekte derBundesregierung
TR-03127	BSI: Technische Richtlinie TR-03127 eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control
TR-03124-1	BSI: Technische Richtlinie TR-03124 eID-Client
TR-03130	BSI: Technische Richtlinie TR-03130 eID-Server
ISO/IEC 19790	: Information technology -- Security techniques -- Security requirements for cryptographic modules
JILAPS	: Joint Interpretation Library Application of Attack Potential to Smartcards