Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Bewertung von Authentisierungslösungen gemäß TR-03107 in Version 1.1.1

Anwendungs- und Vorgehensbeschreibung

Version 1.06
05.10.2022

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

Tabellenverzeichnis

1 Einleitung

Die [TR-03107-1] bewertet Verfahren zu elektronischen Identitäten und Vertrauensdiensten für verschiedene Prozesse des E-Governments. Die Bewertung ermöglicht es, Verfahren zu definierten Vertrauensniveaus zuzuordnen. Dafür werden unterschiedliche Kriterien betrachtet, die generisch oder spezifisch für bestimmte Verfahren sind.

In einem Prüfverfahren werden die relevanten Kriterien auf ein zu prüfendes Verfahren (nachfolgend „Prüfobjekt“ genannt) angewendet und die Ergebnisse ausgewertet. Ziel ist es, das Prüfobjekt einem der drei möglichen Vertrauensniveaus nach [TR-03107-1] zuzuordnen: *normal*, *substantiell* oder *hoch*. Falls ein Prüfobjekt die Mindestanforderungen für *normal* nicht erreicht, so kann das Verfahren als ungeeignet für den Einsatz im E-Government gewertet werden.

Dieses Dokument ist, zusammen mit der Prüfberichtsvorlage ([PrüfB/TR-03107]) in der jeweils gleichen Version (derzeit 1.06), die Grundlage für eine einheitliche Bewertung verschiedener Prüfobjekte, die auf unterschiedlichen Technologien basieren können. Ziel ist das Ermitteln des jeweils erreichten Vertrauensniveaus. Dieses Dokument bietet einen Leitfaden für die Durchführung einer Prüfung und Auswertung der Ergebnisse.

2 Prüfungsablauf

In diesem Kapitel wird der grundlegende Ablauf einer Prüfung nach [TR-03107-1] beschrieben. Es wird erklärt, welche Schritte vom Prüfer und vom Verfahrensbetreiber erwartet werden.

2.1 Allgemeine Hinweise

Das Prüfobjekt wird gemäß den Angaben des Verfahrensbetreibers bewertet. Grundlage hierfür ist der im Anhang von [PrüfB/TR-03107] enthaltene Fragenkatalog sowie die allgemeinen Angaben des Verfahrensbetreibers zu seinem Verfahren. Darüber hinaus sind für das Vertrauensniveau *substantiell* Umsetzungsprüfungen (z. B. Codeanalysen) sowie für das Vertrauensniveau *hoch* unabhängige Tests erforderlich, siehe Abs. 2.9. Sollte die Erfüllung bestimmter Anforderungen durch bereits vorab für das Prüfobjekt vorgenommene und durch das BSI anerkannte Zertifizierungen bestätigt worden sein, fließen diese ebenfalls in die Bewertung mit ein und können ggf. ansonsten notwendige Prüfungen und Tests ersetzen.

Dies bedeutet insbesondere, dass die Ergebnisse der Prüfung auf der Auswertung der Angaben des Verfahrensbetreibers basieren. Diese werden auf Plausibilität geprüft und kritisch hinterfragt. Weiterführende Maßnahmen des Prüfers sind gem. Abs. 2.9 notwendig.

2.2 Zeitlicher Ablauf der Prüfung

Eine Prüfung besteht aus folgenden Schritten, die in den folgenden Abschnitten erläutert werden.

1. Ausfüllen der allgemeinen Produktbeschreibung durch den Verfahrensbetreiber (Abs. 2.3). Hierbei kann durch den Verfahrensbetreiber ein anvisiertes Vertrauensniveau entsprechend [TR-03107-1] benannt werden.
2. Auswertung der Angaben und Erstellung eines prüfobjekt-/produktspezifischen Fragenkatalogs durch den Prüfer (Abs. 2.4). Sollte der Verfahrensbetreiber ein anvisiertes Vertrauensniveau benannt haben, so ist dies in der Erstellung des Fragenkatalogs hinsichtlich der Prüftiefe zu berücksichtigen (Abs. 2.9).
3. Beantwortung der Fragen aus dem Fragenkatalog durch den Verfahrensbetreiber (Abs. 2.5).
4. Evaluierung der Antworten durch den Prüfer. Ggf. Vorbereitung und Durchführung von praktischen Tests (Abs. 2.6).
5. Bei Bedarf: optionale Rückfragerunden (Abs. 2.7).
6. Finale Auswertung der Ergebnisse und Verfassung eines Prüfberichts durch den Prüfer (Abs. 2.8).

2.3 Allgemeine Produktbeschreibung

Eine Prüfung bezieht sich immer auf eine konkrete Ausprägung eines Verfahrens. Dies bedeutet, dass das Ergebnis einen eindeutigen Bezug zu einem bestimmten Produkt eines bestimmten Verfahrensbetreibers hat. Insbesondere sind die Ergebnisse nicht notwendigerweise auf andere Ausprägungen des Produkts (z. B. andere Versionsnummer, Konfiguration etc.) übertragbar. In Kapitel 2 von [PrüfB/TR-03107] muss der Prüfgegenstand eindeutig identifiziert werden. Grundlage hierfür sind die Angaben des Verfahrensbetreibers, welche in einem ersten Schritt bei ihm erfragt werden. Hierzu dient der Fragebogen aus Abschnitt 7.1 von [PrüfB/TR-03107].

Die Antworten des Verfahrensbetreibers sind in Abschnitt 7.1 von [PrüfB/TR-03107] einzutragen, sodass die Antworten dokumentiert und bei Bedarf überprüfbar sind.

2.4 Erstellung des Fragenkatalogs für den Verfahrensbetreiber

Anhand der zuvor erhaltenen Informationen entscheidet der Prüfer, welche der Kriterien aus [TR-03107-1] auf das vorliegende Prüfobjekt anwendbar sind. Als Grundlage hierfür dienen die erhaltenen Ablaufdiagramme und Systembeschreibungen. Der Prüfer entfernt die nicht auf das Prüfobjekt anwendbaren Abschnitte (7.2.2 – 7.2.11) aus [PrüfB/TR-03107], sodass nur die relevanten Fragen übrig bleiben. Es dürfen jedoch keine Fragen einzeln entfernt werden, sondern stets ganze nicht zutreffende Module. Der generische Fragenkatalog (Kapitel 3 von [PrüfB/TR-03107]) muss stets vollumfänglich beantwortet werden. Der angepasste Fragebogen wird dem Verfahrensbetreiber bereitgestellt und dessen Antworten anschließend in den Prüfbericht zurück übertragen.

Der Prüfer entfernt zudem sämtliche nicht für das Prüfobjekt relevante Abschnitte aus Kapitel 4 von [PrüfB/TR-03107].

Abhängig von dem angestrebten Vertrauensniveau, falls vom Verfahrensbetreiber angegeben, werden zudem weitere notwendige Vorbereitungen getroffen. Diese beinhalten bspw. die Rücksprachen bezüglich möglicher Codeanalysen oder praktischer Tests.

2.5 Beantwortung der Fragen

In dieser Prüfungsphase bekommt der Verfahrensbetreiber die für sein Verfahren zugeschnittenen Fragen. Es ist notwendig, dass er diese korrekt und so vollständig und präzise wie möglich beantwortet. Seine Antworten haben eine unmittelbare Auswirkung auf die Vertrauensniveaubewertung. Ohne hinreichend vollständige und präzise Angaben kann keine Zuordnung vorgenommen werden. Bei fehlenden oder nicht ausreichenden Antworten stellt der Prüfer Rückfragen. Während der Beantwortung der Fragen muss der Prüfer seinerseits für Rückfragen des Verfahrensbetreibers zur Verfügung stehen, damit Unklarheiten vor Beginn der Evaluierung ausgeräumt werden können.

Weiterhin muss der Verfahrensbetreiber dem Prüfer für die Vertrauensniveaus *substantiell* und *hoch* eine Möglichkeit zur Verfügung stellen, eine Umsetzungsprüfung und unabhängige Tests durchzuführen (siehe Abschnitt 2.9).

2.6 Evaluierung der Antworten

Nachdem der Verfahrensbetreiber die Fragen beantwortet hat, muss er die Antworten an den Prüfer übermitteln. Der Prüfer evaluiert diese anschließend anhand der in den Kapiteln 3 und 4 beschriebenen Inspektionsvorschriften. Diese sind so aufgebaut, dass die ID der Frage aus [PrüfB/TR-03107] grundsätzlich mit der ID der Inspektionsvorschrift in diesem Dokument übereinstimmt.

Eine Anforderung gilt dann als erfüllt, wenn der Prüfer begründet darlegen kann, dass die durch den Verfahrensbetreiber getätigten Angaben die Anforderungen auf geeignete Weise erfüllen[1]. Neben den Antworten spielen für die Bewertung der Erfüllung der Anforderungen insbesondere auch ggf. bereits vorhandene Zertifizierungen des Prüfobjekts bzw. dessen Komponenten eine wichtige Rolle.

Für die Vertrauensniveaus *substantiell* und *hoch* fließen außerdem die Erkenntnisse aus einer Umsetzungsprüfung und praktischen Test in die Bewertung ein.

Sollten die Antworten des Verfahrensbetreibers unklar sein, muss der Prüfer die Einhaltung der Anforderungen anhand von Ablaufdiagrammen und vorhandenen Dokumenten analysieren. Ferner steht es dem Prüfer frei, weitere Nachfragen zu stellen (siehe nächster Abschnitt).

1 Die Inspektionsvorschriften können nicht alle am Markt befindlichen Lösungen in allen Teilaspekten abdecken. Dies gilt insbesondere, wenn es sich um neue, erst nach Erscheinen der Technischen Richtlinie oder dieses Dokuments entwickelte Lösungen handelt. In diesen Fällen sollte die Begründung besonders ausführlich ausfallen.

Die Inspektionsvorschriften sind genau zu befolgen. Jede Anforderung kann hierbei die Einhaltung einer oder mehrerer Vorschriften notwendig machen. Der Prüfer muss sowohl im Positiv- als auch im Negativfall stets vollständig dokumentieren, wie er zu seiner Entscheidung für die jeweilige Anforderung gelangt ist. Die Bewertung selbst darf ausschließlich eine der folgenden Antworten enthalten:

1. Eines der Vertrauensniveaus gemäß [TR-03107-1]
2. „Mindestanforderungen nicht erfüllt“ falls das Niveau *normal* nicht erreicht wird
3. „Nicht anwendbar“ falls das Kriterium für das Prüfobjekt nicht anwendbar ist

2.7 Nachfragen und Klarstellungen

Dieser Schritt der Prüfung ist konditional. Wenn die Antworten des Verfahrensbetreibers eine hinreichend klare und vollständige Grundlage für die Vertrauensniveaubewertung darstellen, so besteht keine Notwendigkeit zusätzliche Fragen zu stellen. Andernfalls sind sämtliche Unklarheiten unverzüglich mit dem Verfahrensbetreiber des Prüfobjekts zu klären. Der Prüfer darf nach eigenem Ermessen weitere Fragen stellen. Bei erkennbaren Ungereimtheiten oder Lücken in den Aussagen des Verfahrensbetreibers ist er dazu verpflichtet, dies auch zu tun.

In sämtlichen Inspektionsvorschriften dieses Dokuments wird davon ausgegangen, dass der erste Schritt des Prüfers bei Unklarheiten die Kontaktaufnahme mit dem Verfahrensbetreiber ist. Erst wenn dadurch die Unklarheiten nicht vollständig beseitigt werden können, sind die in der jeweiligen Vorschrift beschriebenen Schritte durchzuführen (beispielsweise die Analyse des Ablaufdiagramms der Authentisierung).

2.8 Auswertung der Ergebnisse und Erstellung des Prüfberichts

Nachdem alle für die Vertrauensniveaubewertung erforderlichen Schritte gemacht wurden und der Prüfer keine Nachfragen mehr hat, kann der Prüfer die Ergebnisse in [PrüfB/TR-03107] zusammenfassen. Das Gesamtergebnis der Prüfung ergibt sich aus den Bewertungen der Unterkategorien. Hier gilt:

1. Grundsätzlich gilt für das Gesamtverfahren das Minimumprinzip. Dies bedeutet, dass das niedrigste Vertrauensniveau in einer beliebigen, für das Prüfobjekt relevanten Kategorie das Endergebnis der Prüfung darstellt.
2. Kommen in einem Prüfobjekt mehrere Authentisierungsmittel zum Einsatz und sind diese als unabhängig deklariert, so gelten insbesondere die Anforderungen aus den Abschnitten 4.5.2 sowie 4.5.3. Es gilt im Hinblick auf **die Kombination mehrerer Authentisierungsmittel für einen Authentisierungsvorgang** stattdessen das Maximumsprinzip. Dies bedeutet, dass das Nicht-Erreichen eines bestimmten Vertrauensniveaus durch ein Authentisierungsmittel keinen negativen Einfluss auf sonstige Teile des Prüfobjekts hat.

   Beispiel: Ein Prüfobjekt kombiniert (als „UND-Verknüpfung“) die beiden Authentisierungsmittel Benutzername / Passwort (Faktor Wissen) mit einer Smartcard-Authentisierung (Besitz + Wissen). Hierbei werden für den Benutzernamen und das Passwort keine Vorgaben gemacht, für die Smartcard allerdings eine Zertifizierung auf hohem Vertrauensniveau vorausgesetzt. Das Prüfobjekt kann, obwohl das erste Authentisierungsmittel Benutzername / Passwort die Anforderungen von [TR-03107-1] nicht erfüllt, dennoch das Vertrauensniveau hoch *erreichen.*

   Diese Regelung ist **nicht** auf die Kombination mehrerer Faktoren eines einzelnen Authentisierungsmittels anwendbar.

Die Entscheidung sowie, falls notwendig, die dazugehörige Begründung sind in Kapitel 5 von [PrüfB/TR-03107] festzuhalten. Sollten für die Evaluierung der Erfüllung der Anforderungen bestimmte Annahmen zum Prüfobjekt, dessen Einsatzumgebung oder sonstigen Parametern notwendig gewesen sein, muss der Prüfer diese eindeutig in Abschnitt 2.5 von [PrüfB/TR-03107] dokumentieren und auch in der Begründung nochmals darauf verweisen.

2.9 Vertrauensniveau und Prüftiefe

Für die Erreichung der Vertrauensniveaus *normal*, *substantiell* oder *hoch* sind unterschiedliche Prüftiefen erforderlich. Diese werden in der unten stehenden Tabelle beschrieben. Hat der Verfahrensbetreiber kein anvisiertes Vertrauensniveau angegeben, kann der Prüfer die Vorgehensweise (top-down / bottom-up) und die damit verbundene initiale Prüftiefe für das konkrete Verfahren nach eigenem Ermessen selbst festlegen.

Anstelle von Umsetzungsprüfungen oder aktiven Tests können (ganz oder teilweise) auch bereits vorhandene geeignete und vom BSI anerkannte Zertifizierungen treten.

Vertrauensniveau	Prüftiefe
normal	**Dokumentenprüfung** – Alle Anforderungen werden auf Basis der verfügbaren Dokumentation geprüft. Im Prüfbericht sind Referenzen auf die inspizierten Dokumentenstellen aufzuführen. Beispiele für zu prüfende Dokumentation sind Sicherheitskonzept, Systembeschreibung, Schnittstellendefinition, Handbücher oder auch bereits erfolgte Sicherheitsuntersuchungen oder Zertifizierungen einzelner Komponenten. Bei Bedarf ist die Prüftiefe selektiv (d.h. für einzelne Anforderungen) um eine Umsetzungsprüfung zu erweitern. Dies ist insbesondere dann der Fall, wenn nach der Dokumentenprüfung von einem konkreten Verdacht ausgegangen werden muss, dass das Verfahren bereits mit einem „*enhanced basic*“ Angriffspotential kompromittiert werden kann.
substantiell	**Umsetzungsprüfung** – Zusätzlich zur Dokumentenprüfung ist für jede Anforderung auch die Umsetzung („Implementierung“) in der Praxis zu prüfen. Dabei ist insbesondere auf die Übereinstimmung zwischen dokumentierter Information und konkreter Umsetzung zu achten. Für die Umsetzungsprüfung sollte sich der Prüfer die für eine Anforderung relevanten Aspekte beschreiben lassen und muss die jeweilige Umsetzung selbst in Augenschein nehmen. Im Prüfbericht sind sowohl Gesprächspartner und inspizierte Aspekte des Verfahrens aufzuführen, als auch die Beobachtungen im Rahmen der Prüfaktivität zu beschreiben. Bei Bedarf ist die Prüftiefe selektiv (d.h. für einzelne Anforderungen) um unabhängige Tests zu erweitern. Dies ist insbesondere dann der Fall, wenn nach der Dokumentenprüfung oder Umsetzungsprüfung von einem konkreten Verdacht ausgegangen werden muss, dass das Verfahren bereits mit einem „*moderate*“ Angriffspotential kompromittiert werden kann.
hoch	**Unabhängige Tests** – Zusätzlich zur Dokumenten- und Umsetzungsprüfung sind unabhängige Tests (insbesondere auch konkrete Angriffsszenarien) für das Verfahren durchzuführen. Hierzu ist dem Prüfer eine entsprechende Testmöglichkeit zur Verfügung zu stellen. Die durchgeführten Prüfaktivitäten sind im Prüfbericht zu dokumentieren.

Vertrauensniveau	Prüftiefe
	Die Art und Weise der unabhängigen Tests sollte sich zum Beispiel an den Common Criteria und insbesondere der [CEM] orientieren.

3 Inspektionsvorschriften für generische Anforderungen aus [PrüfB/TR-03107]

Dieses Kapitel beinhaltet diejenigen Anforderungen aus [TR-03107-1] und die zugehörigen Inspektionsvorschriften, welche mechanismenübergreifend gelten und in allen Prüfberichten berücksichtigt sein müssen.

Die in diesem Kapitel genannten Referenzen beziehen sich, falls nicht anderweitig erwähnt, auf die Abschnitte von [TR-03107-1]. *Kursiv* formatierte Anforderungen sind aus der [TR-03107-1] zitiert.

3.1 Generische Anforderung G1: Identitätsprüfung nach [TR-03147]

Referenz: 3.2.1 Identitätsprüfung

Anforderung: Die Identitätsprüfung wurde gemäß den Anforderungen von [TR-03147] bewertet.

Auswertungsvorschrift: Eine Bewertung gemäß [TR-03147] muss erfolgt sein. Das Endergebnis der Bewertung wird direkt übernommen. Falls keine Bewertung vorliegt, ist das Vertrauensniveau *normal* nicht erreichbar.

Normal	Substantiell	Hoch
Die Prüfung gemäß [TR-03147] resultiert im Niveau *normal*	Die Prüfung gemäß [TR-03147] resultiert im Niveau *substantiell*	Die Prüfung gemäß [TR-03147] resultiert im Niveau *hoch*

Tabelle 1: Vertrauensniveaus der generischen Anforderung G1

3.2 Generische Anforderung G2: Ausgabe nur an berechtigte Inhaber

Referenz: 3.2.2 Ausgabe der Authentisierungsmittel

Anforderung: *Es muss sichergestellt werden, dass Authentisierungsmittel nur an den berechtigten Inhaber ausgegeben werden.*

Auswertungsvorschrift: Aus der Antwort bzw. der Prüfobjektbeschreibung muss ersichtlich sein, dass der Verfahrensbetreiber Maßnahmen getroffen hat, durch welche die Ausgabe der Authentisierungsmittel nur an den jeweils berechtigten Inhaber erfolgt. Zu diesen Maßnahmen kann beispielsweise das persönliche Aushändigen, der Versand an eine registrierte Anschrift oder auch die durch den Inhaber selbst vorgenommene Generierung des Authentisierungsmittels gehören.

Wenn der Verfahrensbetreiber die Authentisierungsmittel nicht selbst ausgibt, sondern beim Benutzer bereits vorhandene verwendet, dann muss die Zuordnung bzw. Personalisierung sicher erfolgen. Es müssen Maßnahmen getroffen werden, die das Authentisierungsmittel zweifelsfrei an den berechtigten Inhaber binden.

Normal	Substantiell	Hoch
Das Prüfobjekt beinhaltet Vorkehrungen, damit die Ausgabe nur an den berechtigen Inhaber erfolgt. *Beispiele:* *- Zustellung durch reguläre Postsendung.*	*Wie normal* *Beispiele:* *- Zustellung durch reguläre Postsendung und getrennte Zustellung eines Aktivierungsfaktors* *- Zustellung durch persönliche Abholung (oder persönliches Einschreiben).*	*Wie normal* *Beispiel:* *- Zustellung durch persönliche Abholung (oder persönliches Einschreiben) und getrennte Zustellung eines Aktivierungsfaktors durch reguläre Postsendung.*

Tabelle 2: Vertrauensniveaus der generischen Anforderung G2

3.3 Generische Anforderung G3: Explizite Aktivierung

Referenz: 3.2.2 Ausgabe der Authentisierungsmittel

Anforderung: *Für das Vertrauensniveau hoch ist eine explizite Aktivierung der Authentisierungsmittel durch den Inhaber notwendig. Die Aktivierung muss so gestaltet sein, dass sie nur durch den berechtigten Inhaber erfolgt bzw. dieser zuverlässig eine unberechtigte Aktivierung erkennen kann.*

Hinweis: Nur relevant, falls das Vertrauensniveau *hoch* angestrebt wird.

Auswertungsvorschrift: Für mindestens eines der Authentisierungsmittel ist eine explizite Aktivierung erforderlich. Die sichere Zustellung alleine reicht für das Niveau *hoch* nicht aus. Die Aktivierungsmethode muss plausibel dargestellt sein, insbesondere auch im Hinblick auf die klare Erkennbarkeit einer bereits erfolgten unberechtigten Aktivierung.

Sollten die Angaben des Verfahrensbetreibers unklar sein, kann der Prüfer das Ablaufdiagramm des Enrolments analysieren. Typischerweise sollte in diesem markiert sein, ab welchem Zeitpunkt der Einsatz des Authentisierungsmittels möglich ist. Diesem muss eine Aktion des Inhabers zwecks Freischaltung vorausgehen. Eine bereits vorausgegangene Freischaltung muss klar erkennbar sein.

Der Prüfer muss praktisch nachvollziehen können, dass das Authentisierungsmittel sich ohne eine explizite Aktivierung nicht nutzen lässt.

Normal	Substantiell	Hoch
-	-	Explizite Aktivierung ist vorgesehen und wird forciert.

Tabelle 3: Vertrauensniveaus der generischen Anforderung G3

3.4 Generische Anforderung G4: Geschäftsbedingungen und Verhaltensregeln

Referenz: 3.2.3 Informationen für den Inhaber

Anforderung: *Dem Inhaber der Authentisierungsmittel müssen in geeigneter Weise die Geschäftsbedingungen sowie notwendige Verhaltensregeln zum Umgang mit den Authentisierungsmitteln übermittelt werden.*

Auswertungsvorschrift: Der Prüfer muss feststellen, ob dem Inhaber der Authentisierungsmittel die Geschäftsbedingungen sowie notwendige Verhaltensregeln zum Umgang mit den Authentisierungsmitteln in geeigneter Weise übermittelt werden. Geeignet ist in diesem Zusammenhang beispielsweise eine Darstellung auf der Webseite des Dienstes. Die Inhalte müssen klar dem Dienst zugeordnet werden können.

Alternativ ist eine Übermittlung mittels eines anderen Übertragungsweges, beispielsweise per E-Mail, PDF-Download oder auf postalischem Wege, denkbar. In solchen Fällen muss immer eine Referenz auf den Dienst (beispielsweise durch das Nennen der URL) vorhanden sein, sodass eine Zuordnung für den Authentisierungsmittelinhaber klar erkennbar ist.

Normal	Substantiell	Hoch
Geschäftsbedingungen und Verhaltensregeln werden in geeigneter Weise übermittelt	*Wie normal*	*Wie normal*

Tabelle 4: Vertrauensniveaus der generischen Anforderung G4

3.5 Generische Anforderung G5: Änderungen der Geschäftsbedingungen

Referenz: 3.2.3 Informationen für den Inhaber

Anforderung: *Dem Inhaber der Authentisierungsmittel müssen in geeigneter Weise die Geschäftsbedingungen sowie notwendige Verhaltensregeln zum Umgang mit den Authentisierungsmitteln übermittelt werden. Wenn sich die Geschäftsbedingungen oder notwendigen Verhaltensregeln ändern, müssen alle betroffenen Stellen und insbesondere der Authentisierungsmittelinhaber geeignet über die Änderungen informiert werden.*

Auswertungsvorschrift: Der Prüfer muss evaluieren, wie alle betroffenen Stellen und die Authentisierungsmittelinhaber über die Änderungen im Umgang mit den Authentisierungsmitteln oder den notwendigen Verhaltensregeln informiert werden. Die Prozessbeschreibung des Verfahrensbetreibers muss hierbei vollständig sein und geeignet darstellen, wie die Informationen übermittelt werden. Für jeden Empfängertypen (Authentisierungsmittelinhaber oder Stelle) können hierbei unterschiedliche Mechanismen zum Einsatz kommen. Der Prüfer muss sicherstellen, dass sämtliche relevante Stellen einschließlich Authentisierungsmittelinhaber informiert werden.

Normal	Substantiell	Hoch
Die Änderungen werden in geeigneter Weise übermittelt	*Wie normal*	*Wie normal*

Tabelle 5: Vertrauensniveaus der generischen Anforderung G5

3.6 Generische Anforderung G6: Sicherheit des Authentisierungsprotokolls

Referenz*: 3.3.2 Authentisierungsprotokoll*

Anforderung*: Das Authentisierungsprotokoll muss gegen Angreifer mit Angriffspotential gemäß Abschnitt 3.1 sicher sein.*

Auswertungsvorschrift: Der Prüfer muss evaluieren, gegen welches Angriffspotential das Authentisierungsprotokoll geschützt ist. Als Bewertungsgrundlage können hier insbesondere Zertifizierungen des Produktes dienen. Sollten keine Zertifizierungen vorliegen, muss der Prüfer evaluieren, ob geeignete Zertifizierungsprogramme für diesen Typ existieren. Ist dies der Fall und würde hieraus eine Bewertung der Widerstandsfähigkeit gegenüber Angreifern mit den genannten Angriffspotentialen ermöglicht, so muss der Verfahrensbetreiber darauf hingewiesen werden. Grundsätzlich wird eine Zertifizierung empfohlen, alternativ kann der Verfahrensbetreiber auch einen anderen geeigneten und glaubwürdigen Nachweis einreichen. Die Bewertung erfolgt anhand der Zertifizierung oder des erbrachten Nachweises.

Falls keine Zertifizierung vorliegt und auch keine weiteren Sicherheitsnachweise existieren, muss der Prüfer die Bewertung selbstständig anhand der Dokumentation durchführen.

Falls Sicherheitsbeweise existieren, sollten diese für die Ermittlung des Angriffspotentials herangezogen werden.

Zusätzliche Auswertungshinweise für *substantiell***:** neben der Überprüfung der Angaben des Verfahrensbetreibers muss der Prüfer die Implementierung des Protokolls begutachten. Die relevanten Aspekte des Protokolls soll er sich vom Verfahrensbetreiber zeigen und erklären lassen. Anhand dieser Analyse soll ersichtlich sein, dass das Prüfobjekt gegen das Angriffspotential *moderate* geschützt ist. Darüber hinaus wird es empfohlen, eine Zertifizierung durchführen zu lassen.

Zusätzliche Auswertungshinweise für *hoch***:** das Vertrauensniveau *hoch* ist nur mit einer Zertifizierung erreichbar, die belegt dass das Prüfobjekt gegen das Angriffspotential *high* geschützt ist.

Normal	Substantiell	Hoch
Geschützt gegen das Angriffspotential *enhanced-basic*	Geschützt gegen das Angriffspotential *moderate*	Geschützt gegen das Angriffspotential *high*

Tabelle 6: Vertrauensniveaus der generischen Anforderung G6

3.7 Generische Anforderung G7: Forward Secrecy

Referenz: 3.3.2 Authentisierungsprotokoll

Anforderung: *Sofern für einen Mechanismus die Vertraulichkeit ein Sicherheitsziel ist, so sollen kryptographische Verfahren eingesetzt werden, die Vorwärtssicherheit (Forward Secrecy) bieten.*

Auswertungsvorschrift: Der Verfahrensbetreiber muss angeben, für welche Kanäle Forward Secrecy benötigt wird. Dies gilt mindestens für all diejenigen Kanäle, auf welchen vertrauliche Daten übertragen werden.

Sollte der Verfahrensbetreiber keine Angaben machen oder diese unvollständig wirken, muss der Prüfer sich die im Prüfobjekt zum Einsatz kommende Kryptografie ansehen. Für jeden Kanal, auf dem vertrauliche Daten (z. B. Identitätsattribute des Nutzers) übertragen werden, müssen Ciphersuites vorhanden sein, welche Forward Secrecy (z. B. ephemerale Schlüssel) bieten und verwendet werden, sofern von der Gegenstelle unterstützt.

Normal	Substantiell	Hoch
Forward Secrecy ist für alle relevanten Kanäle unterstützt	*Wie normal*	*Wie normal*

Tabelle 7: Vertrauensniveaus der generischen Anforderung G7

3.8 Generische Anforderung G8: Dynamisches Authentisierungsprotokoll

Referenz: 3.3.2 Authentisierungsprotokoll

Anforderung: *Für die Vertrauensniveaus substantiell und hoch muss das Authentisierungsprotokoll dynamisch sein, d.h. das Verfahren muss dazu geeignet sein nachzuweisen, dass sich die Authentisierungsmittel im Augenblick der Authentisierung unter Kontrolle des Inhabers befinden. Dieser Nachweis muss für jede Authentisierung neu erzeugt werden.*

Hinweis: Nur relevant, falls die Vertrauensniveaus *substantiell* oder *hoch* angestrebt werden.

Auswertungsvorschrift: Es ist nicht ausreichend, den Authentisierungsschlüssel hinreichend abzusichern. Zusätzlich soll der Prüfer darauf achten, dass das Authentisierungsprotokoll den Schlüssel schützt (z. B. Gegen Replay). Hierbei muss der Prüfer relevante Stellen der Implementierung begutachten. Diese sollen mit dem Verfahrensbetreiber besprochen werden.

Die Analyse muss die Verwendung dynamischer Elemente nachvollziehbar darstellen. Es muss ersichtlich sein, welche Elemente dynamisch generiert werden und dass dies ausschließlich auf expliziten Wunsch des Inhabers erfolgt. Hierfür ist in der Regel eine Authentisierung des Nutzers an dem das dynamische Element generierenden Gerät notwendig. Die dynamischen Elemente werden zudem so eingesetzt, dass das Risiko einer Man-in-the-middle oder Replay Attacke minimiert wird.

Sollte der Verfahrensbetreiber ein Ablaufdiagramm der Authentisierung zur Verfügung stellen, muss in diesem ersichtlich sein, welches Element die dynamische Komponente des Protokolllaufs darstellt. Üblicherweise handelt es sich hier um Zufallszahlen wie Noncen oder dynamisch generierte Session-IDs. Darüber hinaus muss im Diagramm ersichtlich sein, dass vor dem Übermitteln der Authentisierungsdaten vom Sys-

tem des Inhabers in Richtung des Dienstes oder des Authentisierungsmittelbetreibers in jedem Fall eine Interaktion des Inhabers zwecks Freischaltung des Vorgangs erfolgt sein muss.

Das Erzeugen eines frischen Zufallswertes für jeden Vorgang kann in der Regel nicht aus dem Ablaufdiagramm entnommen werden. Hierfür sind gegebenenfalls Hinweise in der allgemeinen Beschreibung des Prüfobjekts oder in den Angaben des Verfahrensbetreibers zu finden. Je nach Verfahrensart können Zertifizierungen möglicherweise ebenfalls Hinweise liefern.

Zusätzliche Auswertungshinweise für *hoch*: Zusätzlich zur Umsetzungsprüfung soll der Prüfer Sicherheitstests durchführen. Dabei soll er zweifelsfrei ermitteln, dass das Authentisierungsprotokoll dynamische Elemente nutzt, die effektiv gegen Man-in-the-middle und Replay Attacken schützen.

Normal	Substantiell	Hoch
-	• Das Authentisierungsprotokoll ist dynamisch • Das Authentisierungsmittel befindet sich bei jeder Authentisierung nachgewiesen unter Kontrolle des rechtmäßigen Inhabers	*Wie substantiell*

Tabelle 8: Vertrauensniveaus der generischen Anforderung G8

3.9 Generische Anforderung G9: Sperrung

Referenz: 3.4 Rückruf/Sperrung, 3.4.1 Sperrung

Anforderung: *Im Falle der Kompromittierung von Authentisierungsmitteln muss es dem Inhaber möglich sein, die Authentisierungsmittel zu sperren;*

Für alle Vertrauensniveaus muss der Rückruf bzw. Sperrung von Authentisierungsmitteln durch den Inhaber möglich sein.

Grundsätzlich sollte eine effektive Sperrung so schnell wie möglich erfolgen (umgehend), die im Folgenden genannten Fristen sind als Minimalanforderungen zu verstehen.

Auswertungsvorschrift: Der Verfahrensbetreiber hat genaue Angaben zu allen unterstützten Sperrmöglichkeiten der Authentisierungsmittel gemacht. Jedes verwendete Authentisierungsmittel muss individuell innerhalb der in Tabelle 9 geforderten Fristen sperrbar sein.

Sollte der Diensteanbieter Sperrmöglichkeiten mit und ohne Authentisierungsmittel unterstützen (z. B. Self-Service respektive Hotline), so ist für die Auswertung vom Szenario ohne Authentisierungsmittel auszugehen. Wenn z. B. eine Sperrung über Self-Service jederzeit möglich ist, über die Hotline aber nur während der üblichen Geschäftszeiten, so ist für die Auswertung nur die Variante über die Hotline zu berücksichtigen.

Die Anforderung „Sperrstelle allgemein bekannt“ für das Niveau *hoch* kann beispielsweise erfüllt werden, indem die Sperrstelle geeignet auf der Seite des Dienstes verlinkt ist.

Zusätzliche Auswertungshinweise für *hoch*: Der Prüfer soll den Ablauf des Sperrvorgangs praktisch nachvollziehen. Hierbei soll er auf die Dauer der Sperrvorgänge achten. Falls für diesen Zweck ein Testkonto verwendet wird, soll es sich nicht signifikant vom Konto eines echten Benutzers unterschieden.

Normal	Substantiell	Hoch
• Effektive Sperrung eines Authentisierungsmittels erfolgt spätestens 24 Stunden nach der	• Effektive Sperrung eines Authentisierungsmittels erfolgt spätestens 12 Stunden nach	• Effektive Sperrung eines Authentisierungsmittels erfolgt spätestens 1 Stunde nach der

Sperrmeldung durch den Inhaber • Sperrung während der üblichen Geschäftszeiten	der Sperrmeldung durch den Inhaber • Sperrung jederzeit möglich	Sperrmeldung durch den Inhaber • Sperrung jederzeit möglich • Sperrstelle allgemein bekannt

Tabelle 9: Vertrauensniveaus der generischen Anforderung G9

3.10 Generische Anforderung G10: Übermittlung der Sperrmeldung

Referenz: 3.4.1 Sperrung

Anforderung: *Die Möglichkeit zur Übermittlung der Sperrmeldung muss über öffentliche Kommunikationswege verfügbar sein und den Inhabern des Authentisierungsmittels in geeigneter Weise bekannt gemacht werden.*

Auswertungsvorschrift: Der Prüfer muss sich davon überzeugen, dass für die Übermittlung der Sperrmeldung öffentliche Kommunikationswege benutzt werden können, und diese dem Inhaber auf geeignete Weise bekannt gemacht wurden. Für den Sperrmechanismus ist beispielsweise die Nennung einer konkreten Sperr-URL oder einer Sperr-Hotline möglich. Die Information an den Authentisierungsmittelinhaber kann über einen beliebigen Kanal erfolgen (z. B. Website, E-Mail oder Brief). Unabhängig vom Medium muss jedoch stets ein Bezug zum Dienst vorhanden sein.

Normal	Substantiell	Hoch
• Kommunikationswege für die Sperrmeldung sind öffentlich • Kommunikationswege wurden dem Inhaber bekannt gemacht	*Wie normal*	*Wie normal*

Tabelle 10: Vertrauensniveaus der generischen Anforderung G10

3.11 Generische Anforderung G11: Attributsänderung

Referenz: 3.4 Rückruf/Sperrung, 3.2.1 Identitätsprüfung

Anforderung: *Ein Rückruf von Authentisierungsmitteln ist auch dann notwendig, wenn die authentisierten Identitätsattribute nicht mehr gültig sind (z. B. Namensänderung) oder der Inhaber nicht mehr zum Besitz berechtigt ist.*

Sowohl für externe als auch interne Attribute muss festgelegt sein, inwiefern deren Gültigkeit erlischt, wenn sich die zugrunde liegende nachgewiesene Identität der Entität ändert.

Auswertungsvorschrift: Der Prüfer muss kontrollieren, dass der Verfahrensbetreiber in der Lage ist Identitätsattribute zu sperren, falls diese nicht mehr gültig sind. Hierbei sind folgende Aspekte zu beachten:

1. Der Verfahrensbetreiber hat Angaben dazu gemacht, auf welche Art und Weise er die Änderungen entgegennimmt. Hierbei kann es sich beispielsweise um eine eigene Schnittstelle (API) handeln.
2. Es muss eine Liste aller durch den Dienst erfassten Identitätsattribute vorliegen, in welcher markiert ist, welche davon den minimalen konstanten Datensatz für eine Identität darstellen.
3. Sollten sich die zum minimalen konstanten Datensatz gehörenden Attribute ändern oder der Inhaber anderweitig die Berechtigung zum Besitz des Authentisierungsmittels verlieren, muss der Verfahrensbetreiber automatisiert den Prozess zu dessen Sperrung initiieren.

Normal	Substantiell	Hoch

Der Dienst ist in der Lage die Änderung der Identitätsattribute zu verarbeiten und kann die damit verknüpften Authentisierungsmittel daraufhin sperren.	*Wie normal*	*Wie normal*

Tabelle 11: Vertrauensniveaus der generischen Anforderung G11

3.12 Generische Anforderung G12: Absicherung von Kommunikationsbeziehungen

Referenz: 3.6 Absicherung von Kommunikationsbeziehungen

Anforderung: *Diverse Anforderungen aus Abschnitt 3.6 aus [TR-03107-1] „Absicherung von Kommunikationsbeziehungen“.*

Für das Vertrauensniveau normal ist eine Absicherung der Kommunikation zwischen den beteiligten Stellen auf Transportebene ausreichend.

Für die Vertrauensniveaus substantiell und hoch ist eine Ende-zu-Ende-Beziehung zwischen den beteiligten Stellen notwendig.

Auswertungsvorschrift: Um mindestens das Vertrauensniveau *normal* zu erreichen, sollte der im Verfahren verwendete Authentisierungskanal abgesichert sein. Je nach anvisiertem Vertrauensniveau muss der Prüfer verifizieren, dass die Authentisierung über einen sicheren Kanal verläuft.

Die Angaben des Verfahrensbetreibers legen dar, dass sämtliche Kommunikationswege geeignet gesichert sind. Die Anforderungen der Vertrauensniveaus sind Tabelle 12 zu entnehmen. Sollten mehrere Kommunikationskanäle (z. B. alle vom Verfahrensbetreiber benannten URLs) verwendet werden, gilt das Minimumsprinzip: das Vertrauensniveau des am schwächsten gesicherten Kanals wird als Ergebnis übernommen.

Zusätzliche Auswertungshinweise für *substantiell*: Der Verfahrensbetreiber soll die Konfiguration der Kommunikationskanäle zwischen den beteiligten Stellen darlegen. Hieraus soll hervorgehen, dass für jeden Kommunikationspartner eine Ende-zu-Ende-Beziehung etabliert wird.

Zusätzliche Auswertungshinweise für *hoch*: Der Prüfer muss die Kommunikationskanäle praktisch untersuchen. Dabei soll er anhand der Verbindungen nachvollziehen können, wie diese aufgebaut sind und die übertragenen Daten schützen.

Normal	Substantiell	Hoch
Absicherung der Kommunikation zwischen den beteiligten Stellen auf Transportebene	Ende-zu-Ende-Beziehung zwischen den beteiligten Stellen	*Wie substantiell*

Tabelle 12: Vertrauensniveaus der generischen Anforderung G12

3.13 Generische Anforderung G13: Kryptographie

Referenz: 3.7 Kryptographie

Anforderung: *Für verschiedene Mechanismen werden konkrete kryptographische Anforderungen in den verschiedenen Teilen der [TR-03116] festgelegt, die jeweils in den Beschreibungen der Mechanismen referenziert werden. Sofern die [TR-03116] für einen Mechanismus keine Vorgaben enthält, so sind die Anforderungen aus [TR-02102] einzuhalten.*

Auswertungsvorschrift: Der Prüfer muss sich vergewissern, dass alle kryptographischen Anforderungen entsprechend den genannten Technischen Richtlinien für alle Kanäle umgesetzt sind. Die Reihenfolge der

Auswertung entspricht hierbei der in der Anforderung angegebenen, sprich die Vorgaben der [TR-03116] haben Vorrang vor den Vorgaben der [TR-02102]. Die Auswertung erfolgt auch im Hinblick auf die Gesamtheit aller Kanäle anhand des Minimumsprinzips, sodass die Bewertung dem Vertrauensniveau des am schwächsten gesicherten Kanals entspricht. Die Vorgaben zu TLS aus der [TR-03116] sollten anhand der [TR-03116-TS] überprüft werden. Für Testergebnisse zu Vorgaben aus Teil 4 der [TR-03116] kann zudem die [TLS-Checkliste] verwendet werden.

Normal	Substantiell	Hoch
Kryptographische Anforderungen werden eingehalten.	*Wie normal*	*Wie normal*

Tabelle 13: Vertrauensniveaus der generischen Anforderung G13

3.14 Generische Anforderung G14: Speicherung privater Schlüssel

Referenz: 3.7.1 Schlüsselspeicherung

Anforderung: *Private kryptographische Schlüssel aller Entitäten eines Authentisierungssystems (einschließlich des Inhabers von Authentisierungsmitteln) müssen sicher, das heißt vertraulich, gespeichert werden. Dies setzt voraus, dass der private Schlüssel gegen Kopieren geschützt ist und die Verwendung des Schlüssels durch Unberechtigte verhindert wird.*

Auswertungsvorschrift: Der Prüfer muss feststellen, ob die privaten kryptographischen Schlüssel ausreichend sicher gespeichert sind. Auslesen, Kopieren oder unberechtigtes Nutzen darf nicht möglich sein. Sollten die Angaben des Verfahrensbetreibers hierfür nicht ausreichend sein, muss der Prüfer in der Prüfobjektbeschreibung sämtliche vertrauliche Schlüssel verwendende Komponenten begutachten. Für die Bewertung ist entscheidend, dass die Schlüssel durch geeignete Mechanismen und Maßnahmen geschützt sind. Der Schutz der Vertraulichkeit kann, je nach verwendetem Authentisierungsmittel, unterschiedlich gestaltet sein. Grundsätzlich kann zwischen zwei Arten der Aufbewahrung unterschieden werden:

- Der Schlüssel selbst ist, nach einer geeigneten Freischaltung durch den Authentisierungsmittelinhaber, zugänglich. Für die Freischaltung eignen sich beispielsweise die Faktoren Wissen oder Biometrie. In diesem Zustand ist der Schlüssel nicht mehr vor dem Kopieren beziehungsweise der Einsichtnahme geschützt, sodass eine Speicherung in nicht-flüchtigem Speicher zu keinem Zeitpunkt erfolgen darf.
- Der Schlüssel ist in einer speziellen, sicheren Hardware gespeichert oder liegt in einem nicht durch normale Prozesse zugänglichen Speicherbereich des eingesetzten Gerätes. Er verlässt diesen geschützten Bereich nie, sondern generiert direkt innerhalb seiner geschützten Umgebung die benötigten Signaturen oder Ciphertexte.

Die zweite der beiden Varianten bietet einen besseren Schutz, da Angreifer bei der ersten Variante das Zeitfenster der Freischaltung des Schlüssels zu dessen Duplikation nutzen könnten. Für Niveau *substantiell* können Schlüssel, welche nicht auf Seite des Authentisierungsmittelinhabers, sondern beim Verfahrensbetreiber beziehungsweise dessen Infrastruktur gespeichert werden, auch durch geeignete organisatorische Maßnahmen wie ein ISMS geschützt werden. Für Niveau *hoch* ist für die Speicherung von Schlüsseln des Verfahrensbetreibers nur die zweite Variante zulässig.

Geeignete Hardware für das Niveau *hoch* stellen insbesondere auch Common Criteria auf mindestens Assurance Level EAL 4 / *hohes* Angriffspotential nach einem geeigneten Schutzprofil zertifizierte Chipkarten oder HSMs dar. Bereits vorhandene Zertifikate sollen bei der Prüfung berücksichtigt werden.

Die Anforderungen für die Vertrauensniveaus sind in Tabelle 14 festgehalten.

Zusätzliche Auswertungshinweise für *hoch*: Das Vertrauensniveau *hoch* ist nur zu erreichen, wenn der Verfahrensbetreiber zertifizierte Hardware verwendet. Der Prüfer muss sich überzeugen, dass die Zertifizierung Common Criteria auf mindestens Assurance Level EAL 4 / *hohes* Angriffspotential entspricht.

In einer sicheren Einsatzumgebung entsprechend [ISO27001] ist es ausreichend, wenn die Hardware gegen das Angriffspotential *moderate* geschützt ist. Hierbei muss der Verfahrensbetreiber anhand einer Zertifizierung belegen, dass die Einsatzumgebung den Vorgaben entspricht.

Normal	Substantiell	Hoch
Private Schlüssel sind sicher gespeichert	Die Schlüssel sind in geeigneter geschützter Hardware gespeichert. Schlüssel, die auf Seiten des Verfahrensbetreibers gespeichert werden, verlassen die geschützte Hardware auch nach Freischaltung nicht. Alternativ ist für die Schlüssel des Verfahrensbetreibers zulässig, dass sie ausschließlich in einer geschützten Umgebung (entsprechend [ISO27001]) gespeichert und verwendet werden, die durch eine vertrauenswürdige Stelle betrieben wird.	• Die Schlüssel sind in geeigneter Hardware gespeichert, welche gegen ein *hohes* Angriffspotential geschützt ist oder • Falls die Hardware in einer geschützten Umgebung (entsprechend [ISO27001]) durch eine vertrauenswürdige Stelle [...] betrieben wird, ist eine Resistenz gegen das Angriffspotential *moderate* ausreichend

Tabelle 14: Vertrauensniveaus der generischen Anforderung G14

3.15 Generische Anforderung G15: Speicherung öffentlicher Schlüssel

Referenz: 3.7.1 Schlüsselspeicherung

Anforderung: *[...] müssen öffentliche Schlüssel, die für die Authentifizierung genutzt werden, sicher, also gegen Manipulation geschützt, gespeichert werden.*

Auswertungsvorschrift: Die Antwort des Verfahrensbetreibers muss eine ausreichend gegen Manipulation gesicherte Aufbewahrung der öffentlichen Schlüssel nachvollziehbar darstellen. Der Prüfer muss sich anhand der Prüfobjektbeschreibung vergewissern, dass die öffentlichen Schlüssel nicht durch Angreifer mit Zugriff auf die Infrastruktur des Betreibers manipuliert werden können. Bei der Bewertung muss der Prüfer sowohl interne als auch externe Angreifer als Bedrohung berücksichtigen. Eine reine Sicherung der Systeme nach außen hin durch Firewalls und regelmäßige Patches reicht demnach nicht aus. Es muss auch sichergestellt sein, dass nur berechtigtes Personal Zugriff auf die Schlüsselspeicher hat. Empfehlenswert ist der Einsatz spezieller kryptografischer Hardware für alle Sicherheitsniveaus.

Geeignete Hardware für das Niveau *hoch* stellen beispielsweise auch Common Criteria auf Assurance Level EAL 4 / *hohes* Angriffspotential nach einem geeigneten Schutzprofil zertifizierte Chipkarten oder HSMs dar.

Die Anforderungen für die Vertrauensniveaus sind in Tabelle 15 festgehalten.

Zusätzliche Auswertungshinweise für *hoch*: Die Auswertung richtet sich nach Abschnitt 3.14.

Normal	Substantiell	Hoch
Die öffentlichen Schlüssel sind manipulationssicher gespeichert	*Wie normal*	• Die Schlüssel sind manipulationssicher, z. B. in geeigneter Hardware, gespeichert, welche gegen ein *hohes* Angriffspotential geschützt ist *oder*

		• Falls die Hardware in einer geschützten Umgebung (entsprechend [ISO27001]) durch eine vertrauenswürdige Stelle [...] betrieben wird, ist eine Resistenz gegen das Angriffspotential *moderate* ausreichend

Tabelle 15: Vertrauensniveaus der generischen Anforderung G15

3.16 Generische Anforderung G16: Agilität

Referenz: 3.7.2 Agilität

Anforderung: *Die kryptographischen Verfahren müssen so gestaltet werden, dass sie neuen kryptographischen Erkenntnissen angepasst werden können.*

Auswertungsvorschrift: Aus der Antwort des Verfahrensbetreibers muss ersichtlich sein, dass für jede zur kryptografischen Absicherung verwendeten Komponente des Prüfobjekts Konfigurationsmöglichkeiten vorgesehen sind. Dies schließt insbesondere die Konfigurierbarkeit künftig zu erwartender notwendiger Schlüssellängen und den Einsatz anderer Algorithmen ein, sodass in angemessener Zeit auf aktuelle Entwicklungen reagiert werden kann.

Bei der Auswertung der Antworten bezüglich Kryptografiebibliotheken ist es beispielsweise wichtig, dass diese bereits mehrere Algorithmen und verschiedene Schlüssellängen unterstützen, da es ansonsten zu hohen Verzögerungen bei der Integration kommen würde. Ausnahmen hiervon müssen durch den Verfahrensbetreiber begründet sein, beispielsweise weitere Maßnahmen, die trotzdem die Sicherheit der kryptographischen Verfahren gewährleisten.

Normal	Substantiell	Hoch
Die Anpassung der kryptographischen Verfahren ist möglich	*Wie normal*	*Wie normal*

Tabelle 16: Vertrauensniveaus der generischen Anforderung G16

3.17 Generische Anforderung G17: Nutzerumgebung

Referenz: 3.8 Anforderungen an die Nutzerumgebung

Anforderung: *Es muss sichergestellt werden, dass die Mechanismen mit entsprechend den Empfehlungen [des BSI für Bürger zur Absicherung des lokalen Endgeräts] konfigurierten Rechnern verwendbar sind, Mechanismen dürfen keine Anforderungen stellen, die den Empfehlungen des BSI [für Bürger zur Absicherung des lokalen Rechners] widersprechen.*

Auswertungsvorschrift: Die Antwort des Verfahrensbetreibers muss nachvollziehbar darstellen, dass der Verfahrensbetreiber keine Anforderungen aufstellt, die den Empfehlungen des BSI widersprechen oder diese abschwächen. Die aktuellen Empfehlungen können z. B. hier eingesehen werden: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/empfehlungen_node.html.

Die Empfehlungen berücksichtigen z. B. eine Firewall oder aktuellen Virenschutz auf dem Benutzerrechner.

Sollte der Verfahrensbetreiber als Antwort auf diese Frage notwendige Abweichungen benennen, so ist das Verfahren nicht für den Einsatz im E-Government geeignet.

Normal	Substantiell	Hoch
Das Verfahren stellt keine Anfor-	*Wie normal*	*Wie normal*

derungen, die den Empfehlungen des BSI für Bürger zur Absicherung des lokalen Rechners widersprechen		

Tabelle 17: Vertrauensniveaus der generischen Anforderung G17

3.18 Generische Anforderung G18: Eindeutige Inhaberidentifizierung

Referenz: 4 Authentisierungsverfahren

Anforderung: *Authentisierungsverfahren müssen den Inhaber der Authentisierungsmittel gegenüber der Gegenstelle eindeutig identifizieren (üblicherweise durch die Registrierung einer eindeutigen Kennung des Authentisierungsmittels bei der Gegenstelle).*

Auswertungsvorschrift: Aus der Antwort des Verfahrensbetreibers muss eindeutig ersichtlich sein, wie die Verknüpfung realisiert ist. Insbesondere muss daraus hervorgehen, dass eine Zuordnung zu einem anderen Account nicht möglich ist, sprich jedes Authentisierungsmittel nur eindeutig für diesen Dienst verwendet werden kann[2].

Normal	Substantiell	Hoch
Das Prüfobjekt identifiziert den Inhaber eindeutig	*Wie normal*	*Wie normal*

Tabelle 18: Vertrauensniveaus der generischen Anforderung G18

3.19 Generische Anforderung G19: Geheimhaltung der Nutzerkennung

Referenz: 4 Authentisierungsverfahren

Anforderung: *Das Authentisierungsverfahren muss einerseits diese Kennung der Gegenstelle gegenüber entsprechend der Anforderungen des jeweiligen Vertrauensniveaus nachweisen, Dritten darf die Kennung aus Datenschutzgründen aber nicht bekannt werden.*

Auswertungsvorschrift: Der Prüfer muss sicherstellen, dass die Nutzerkennung gegenüber Dritten ausreichend geschützt ist. Dies bedeutet insbesondere, dass sie nicht aus anderen Daten des Nutzers abgeleitet werden kann. Eine Ausnahme stellen hier frei wählbare oder auf E-Mail-Adressen basierende Logins dar, da beide Arten außerhalb der Kontrolle des Authentisierungsdienstes liegen.

Normal	Substantiell	Hoch
Die Nutzerkennung ist gegenüber Dritten geschützt	*Wie normal*	*Wie normal*

Tabelle 19: Vertrauensniveaus der generischen Anforderung G19

3.20 Generische Anforderung G20: Dienstbindung an den Sitzungskontext

Referenz: 6.2.3 Bindung der Identifizierung an den Sitzungskontext

Anforderung: *Als Bestandteil des Aufbaus eines Sitzungskontextes muss sichergestellt werden, dass die Identifizierungen des Dienstes an diese Sitzung gebunden werden. Dies umfasst, dass die Identität eindeutig einer be-*

[2] Token, welche die Login-Daten anhand eines Seeds generieren, sind hier nicht betroffen, da erst die Kombination aus Generator und Initialisierungswert ein Authentisierungsmittel darstellt.

stimmten Session und nicht lediglich einem bestimmten Kommunikationsendpunkt zugeordnet werden muss und auch nur dort gültig sein darf. Für die Vertrauensniveaus substantiell/hoch muss diese Bindung über geeignete technische/kryptographische Mechanismen erfolgen, etwa kryptographisch sichere Session-Identifier/-Cookies.

Auswertungsvorschrift: Der Prüfer muss evaluieren, wie der Dienst an den Sitzungskontext gebunden wird. Sollten die Angaben des Verfahrensbetreibers unklar sein, kann zur Bewertung dieses Punktes das Ablaufdiagramm der Authentisierung herangezogen werden.

Zusätzliche Auswertungshinweise für *substantiell*: Die Auswertung richtet sich nach Abschnitt 3.21.

Zusätzliche Auswertungshinweise für *hoch*: Die Auswertung richtet sich nach Abschnitt 3.21.

Normal	Substantiell	Hoch
Identifizierungen des Dienstes sind organisatorisch an die Sitzung gebunden	• Identifizierungen des Dienstes sind an die Sitzung gebunden • Die Bindung erfolgt über sichere technische/kryptographische Mechanismen	*Wie substantiell*

Tabelle 20: Vertrauensniveaus der generischen Anforderung G20

3.21 Generische Anforderung G21: Nutzerbindung an den Sitzungskontext

Referenz: 5.2.3 Bindung der Identifizierung an den Sitzungskontext

Anforderung: *Die übertragene Identität muss an den Sitzungskontext gebunden werden. Dies bedeutet unter anderem, dass die Identität einer Person eindeutig einer bestimmten Session und nicht lediglich einem bestimmten Kommunikationsendpunkt zugeordnet werden muss und auch nur dort gültig sein darf. Für die Vertrauensniveaus substantiell/hoch muss diese Bindung über geeignete technische/kryptographische Mechanismen erfolgen.*

Auswertungsvorschrift: Der Prüfer muss verifizieren, wie die Bindung der Identifizierung an den Sitzungskontext erfolgt. Für *normal* ist Transportverschlüsselung ausreichend, innerhalb welcher die Identität übertragen wird. Eine organisatorische Bindung zwischen einzelnen Kommunikationssessions und der Identität ist möglich.

Sollten die Antworten des Verfahrensbetreibers unklar bleiben, muss der Prüfer diesen Punkt anhand des Ablaufdiagramms der Authentisierung ermitteln.

Zusätzliche Auswertungshinweise für *substantiell*: Der Verfahrensbetreiber muss die Implementierung der Bindung an die Sitzung darlegen. Es muss ersichtlich sein, dass die Mechanismen hierbei ausreichend sichere kryptographische Algorithmen einsetzen. Mindestens mittelbar muss eine Beziehung zwischen der Identität sowie der Sitzung entstehen, d.h. das kryptografische Verfahren muss geeignete Attribute eines vorausgegangenen Identifizierungsvorgangs mit dem kryptographisch abgesicherten Sitzungskontext verknüpfen. Diese Bindung soll dynamisch für jede Sitzung etabliert werden.

Zusätzliche Auswertungshinweise für *hoch*: Zusätzlich zur Umsetzungsprüfung soll der Prüfer Sicherheitstests durchführen. Dabei soll er praktisch nachvollziehen können, wie die Bindung an den Sitzungskontext erfolgt und dass diese kryptographisch stark ist.

Normal	Substantiell	Hoch
Die übertragene Identität ist organisatorisch an den Sitzungskon-	• Die übertragene Identität ist an den Sitzungskontext ge-	*Wie substantiell*

text gebunden	bunden • Die Bindung erfolgt über sichere technische/kryptographische Mechanismen	

Tabelle 21: Vertrauensniveaus der generischen Anforderung G21

3.22 Generische Anforderung G22: Übermittlung der Identitätsattribute

Referenz: 5.2.4 Vertraulichkeit der Identitätsattribute

Anforderung: *Es muss sichergestellt sein, dass Identitätsattribute erst nach erfolgter Freigabe durch die Person übermittelt werden.*

Hinweis: Diese Anforderung ist nur insofern relevant, als datenschutzrechtlich relevante ID-Attribute übertragen werden.

Auswertungsvorschrift: Der Prüfer muss evaluieren, in welchem Prozessschritt Identitätsattribute übermittelt werden. Sollten die Angaben des Verfahrensbetreibers unklar sein, kann zur Bewertung dieses Punktes das Ablaufdiagramm der Authentisierung herangezogen werden. Aus diesem muss ersichtlich sein, dass vor der Übertragung eine explizite Freigabe durch den Inhaber erfolgt. Je nach Prüfobjekt kann es hierbei auch notwendig sein, dass der Inhaber sich mit einem oder mehreren Authentisierungsmitteln erneut authentisiert.

Normal	Substantiell	Hoch
Identitätsattribute werden erst nach erfolgter Freigabe durch die Person übermittelt	*Wie normal*	*Wie normal*

Tabelle 22: Vertrauensniveaus der generischen Anforderung G22

3.23 Generische Anforderung G23: Identifizierung des Dienstes

Referenz: 5.2.2 Identifizierung des Dienstanbieters, 5.2.4 Vertraulichkeit der Identitätsattribute

Anforderung: *Eine vorhergehende Identifizierung des Dienstes (und damit verbunden der Aufbau einer sicheren Verbindung) ist Voraussetzung für die nachfolgenden Kriterien und muss daher mindestens mit dem angestrebten Vertrauensniveau der Identifizierung einer Person erfolgen;*

Die Vertraulichkeit der Identitätsattribute einer Person setzt eine Identifizierung des empfangenden Dienstanbieters auf gleichem Vertrauensniveau wie die Identifizierung der Person voraus.

Auswertungsvorschrift: Der Prüfer muss evaluieren, ob eine vorhergehende Identifizierung des Dienstes stattfindet, und ob diese ausreichend ist. Hierfür gelten die Anforderungen aus Tabelle 23.

Die einzige Möglichkeit, den Dienst zu identifizieren, besteht in der Verifikation der URL und des TLS-Zertifikats des Dienstes. Hierbei muss der Prüfer evaluieren, dass die Anforderungen aus den Abschnitten 3.12 und 3.20 für den Dienst erfüllt sind.

Zusätzliche Auswertungshinweise für *substantiell*: Der Prüfer muss sich die verwendeten TLS-Zertifikate anschauen. Diese eignen sich, um das Prüfobjekt zweifelsfrei zu identifizieren.

Zusätzliche Auswertungshinweise für *hoch*: Für dieses Vertrauensniveau ist es erforderlich, den Verbindungsaufbau zum Prüfobjekt praktisch zu untersuchen. Insbesondere muss darauf geachtet werden, dass keine TLS-Warnungen ausgegeben werden.

Normal	Substantiell	Hoch

Die Identifizierung des Dienstes findet mindestens auf Vertrauensniveau *normal* statt	Die Identifizierung des Dienstes findet mindestens auf Vertrauensniveau *substantiell* statt	Die Identifizierung des Dienstes findet mindestens auf Vertrauensniveau *hoch* statt

Tabelle 23: Vertrauensniveaus der generischen Anforderung G23

3.24 Generische Anforderung G24: Multi-Faktor

Referenz: 3.3.1.4 Zwei-Faktor-Authentifizierung

Anforderung: *Zur Erreichung des Vertrauensniveaus substantiell ist grundsätzlich die Nutzung von zwei Faktoren zur Absicherung der Authentisierungsmittel notwendig, die die alleinige Kontrolle des Nutzers über seine Authentisierungsmittel sicherstellen. Dabei müssen die beiden Faktoren unterschiedlichen Kategorien angehören.*

Hinweis: Nur relevant, falls die Vertrauensniveaus *substantiell* oder *hoch* angestrebt werden.

Auswertungsvorschrift: Aus der Beschreibung des Prüfobjekts geht hervor, dass mehrere Faktoren aus unterschiedlichen Kategorien verwendet werden. Diese sind in der Lage, unterschiedlichen Angriffsszenarien standhalten zu können. Siehe Abschnitt 3.25 für den Schutz der Authentisierungsmittel z. B. gegen Duplizierung oder Manipulation durch Angreifer .

Normal	Substantiell	Hoch
-	• Das Prüfobjekt nutzt eine Kombination mehrerer Faktoren aus unterschiedlichen Kategorien •	• *Wie substantiell* •

Tabelle 24: Vertrauensniveaus der generischen Anforderung G24

3.25 Generische Anforderung G25: Widerstandsfähigkeit des Authentisierungsmittels

Referenz: 3.3.1 Authentisierungsmittel

Anforderung: *Die Authentisierungsmittel müssen so gestaltet werden, dass der berechtigte Inhaber sie gegen Missbrauch durch Dritte mit Angriffspotential gemäß Abschnitt 3.1 schützen kann.*

Für Vertrauensniveau hoch müssen die Authentisierungsmittel gegen Duplizierung und Manipulation durch Angreifer mit hohem Angriffspotential (siehe Abschnitt 3.1) geschützt sein

Auswertungsvorschrift: Aus den Antworten des Verfahrensbetreibers bzw. den Zertifizierungen der Authentisierungsmittel ist ersichtlich, dass die Resistenz den Vorgaben aus Tabelle 25 entspricht. Die Bewertung erfolgt gemäß dem höchsten erreichten Einzelniveau aus allen zum Einsatz kommenden Authentisierungsmitteln. Dies gilt allerdings nur, wenn alle Authentisierungsmittel für die Authentisierung benötigt werden (eine UND-Verknüpfung) und die Sicherheit eines Authentisierungsmittels nicht von der Sicherheit eines anderen abhängig ist.

Zusätzliche Auswertungshinweise für *substantiell***:** Der Verfahrensbetreiber ist verpflichtet die Sicherheitsdetails für Authentisierungsmittel darzulegen. Zusätzlich muss der Prüfer die Implementierung untersuchen. Die Analyse soll ergeben, dass die Sicherheitsmechanismen gegen Duplizierung und Manipulation durch Angreifer mit Angriffspotential *moderate* schützen.

Zusätzliche Auswertungshinweise für *hoch*: Das Vertrauensniveau *hoch* ist nur erreichbar, wenn der Verfahrensbetreiber über eine entsprechende Zertifizierung verfügt. Diese soll belegen, dass das Authentisierungsmittel gegen einen Angreifer mit dem Angriffspotential *high* nach [CEM] geschützt ist.

Normal	Substantiell	Hoch
Geschützt gegen das Angriffspotential *enhanced-basic*	Geschützt gegen das Angriffspotential *moderate*	Geschützt gegen das Angriffspotential *high*

Tabelle 25: Vertrauensniveaus der generischen Anforderung G25

4 Inspektionsvorschriften für prüfobjektspezifische Anforderungen aus [PrüfB/TR-03107]

Dieses Kapitel beinhaltet diejenigen Anforderungen aus [TR-03107-1] und die zugehörigen Inspektionsvorschriften, welche nur für bestimmte Mechanismen wichtig sind. Diese sind zu funktionalen Modulen zusammengefasst, welche in Tabelle 26 gelistet sind. Die dritte Spalte dieser Tabelle beschreibt die Bedingung, unter der das jeweilige Modul für die Prüfung relevant ist.

Modul	Abschnitt in diesem Dokument	Anwendbarkeitskriterium
Stellen	4.1	An dem Prüfobjekt sind externe Stellen beteiligt.
Authentisierungsmittel Besitz	4.2	Das Prüfobjekt unterstützt die Authentisierung mit dem Authentisierungsmittel Besitz.
Authentisierungsmittel Wissen	4.3	Das Prüfobjekt unterstützt die Authentisierung mit dem Authentisierungsmittel Wissen.
Authentisierungsmittel Biometrie	4.4	Das Prüfobjekt unterstützt die Authentisierung mit dem Authentisierungsmittel Biometrie.
Multi-Faktor Authentisierung	4.5	Das Prüfobjekt unterstützt die Authentisierung mit mindestens Zwei-Faktor Authentisierung.
Authentisierungsmittel eID	4.6	Das Prüfobjekt unterstützt die Authentisierung mit dem Authentisierungsmittel eID.
Authentisierungsmittel Softwaretoken	4.7	Das Prüfobjekt unterstützt die Authentisierung mit dem Authentisierungsmittel Softwaretoken.
Authentisierungsmittel OTP	4.8	Das Prüfobjekt unterstützt die Authentisierung mit dem Authentisierungsmittel One-Time-Password.
Authentisierungsmittel smsTAN	4.9	Das Prüfobjekt unterstützt die Authentisierung mit dem Authentisierungsmittel smsTAN.
Reaktivierung	4.10	Das Prüfobjekt unterstützt die Reaktivierung der Authentisierungsmittel nach einer Sperrung.

Tabelle 26: Auflistung der Module

Die in diesem Kapitel genannten Referenzen beziehen sich, falls nicht anderweitig erwähnt, auf die Abschnitte von [TR-03107-1]. *Kursiv* formatierte Anforderungen sind aus der [TR-03107-1] zitiert.

4.1 Anforderungskatalog zu Stellen

4.1.1 Spezifische Anforderung S1: Stellen

Referenz: 3.5 Vertrauenswürdigkeit von Stellen

Anforderung: *Bei den meisten Mechanismen übernehmen – neben dem Inhaber der Authentisierungsmittel und der vertrauenden Entität – weitere Stellen für die Sicherheit des Mechanismus relevante Aufgaben, zum Beispiel Enrolment, Identitätsprüfung und Ausgabe der Authentisierungsmittel (Abschnitt 3.2), Sicherung von Kommunikationsbeziehungen (Abschnitt 3.6) oder Speicherung von Daten. Auch Identitätsprovider sind Stellen in diesem Sinne.*

Alle Stellen müssen

- *Behörden oder juristische Personen sein und rechtlich befugt sein, die jeweilige Aufgabe wahrzunehmen;*
- *für ihre jeweiligen wahrgenommen Aufgaben ein Regelwerk aufstellen und dieses einhalten;*
- *organisatorisch und technisch in der Lage sein, die Aufgaben auf Basis des Regelwerks wahrzunehmen;*
- *genügend Ressourcen für die Erfüllung der Aufgaben und ggf. die Übernahme der sich aus den Aufgaben ergebende Haftung haben; und*
- *ein Informationssicherheitsmanagementsystem auf Basis etablierter Standards (z. B. IT-Grundschutz [BSI100-2] oder [ISO27001]) nutzen.*

Auswertungsvorschrift: Die Antworten des Verfahrensbetreibers müssen den in Tabelle 27 genannten Kriterien genügen.

Zusätzliche Auswertungshinweise für *hoch***:** Es ist eine Zertifizierung erforderlich, die das Sicherheitsniveau *hoch* gemäß [BSI100-2] attestiert. Werden keine entsprechenden Nachweise erbracht, kann maximal das Sicherheitsniveau *substantiell* erreicht werden.

Normal	Substantiell	Hoch
• Die Stelle ist eine Behörde oder juristische Person und ist rechtlich befugt, die jeweilige Aufgabe wahrzunehmen • Die Stelle stellt für ihre jeweiligen wahrgenommen Aufgaben ein Regelwerk auf und hält dieses ein • Die Stelle ist organisatorisch und technisch in der Lage, die Aufgaben auf Basis des Regelwerks wahrzunehmen • Die Stelle hat genügend Ressourcen für die Erfüllung der Aufgaben und ggf. die Übernahme der sich aus den Aufgaben ergebener Haftung • Falls die Stelle zur Erfüllung Ihrer Aufgaben auf externe Dritte zurückgreift, sind diese dem eigentlichen Dienst bekannt und erreichen mindestens das gleiche Vertrauensniveau	*Zusätzlich zu normal:* • Die Erstellung und Pflege eines Sicherheitskonzeptes sowie eine zugehörige regelmäßige Auditierung mit Testat nach IT-Grundschutz [BSI100-2] oder nach [ISO27001] sind verpflichtend. Der Audit muss durch eine neutrale Instanz (zum Beispiel ein anerkannter Auditor) erfolgen • Das Sicherheitskonzept und der Audit müssen alle durch die Stelle wahrgenommen Aufgaben und die Einhaltung der zugeordneten Schutzziele umfassen • Sofern für die durch die Stelle wahrgenommenen Aufgaben Technische Richtlinien des BSI (z. B. [TR-03145] für Certification Authorities), Normen oder anderer Stand der Technik für die Überprüfung zur Verfügung stehen, so sind diese einzuhalten	*Zusätzlich zu substantiell*: • Das Zertifikat nach IT-Grundschutz [BSI100-2] attestiert der Stelle das Erreichen des Niveaus *hoch* bzw. das Zertifikat nach [ISO27001] attestiert der Stelle das Erreichen eines entsprechenden Sicherheitsniveaus

Tabelle 27: Vertrauensniveaus der spezifischen Anforderung S1

4.2 Anforderungskatalog zum Authentisierungsmittel Besitz

Wegen den Anforderungen an das Auslesen, Kopieren oder unberechtigtes Nutzen eines Authentisierungsmittels, gilt ein Softwaretoken im Allgemeinen nicht als Besitz. Nur bei geeigneter Umsetzung kann er die-

ser Kategorie zugeordnet werden. Diese Umsetzung soll wirksame Sicherheitsmaßnahmen gegen Auslesen, Kopieren und unberechtigtes Nutzen vorsehen.

4.2.1 Spezifische Anforderung B1: Ausgabe des Tokens

Referenz: 3.2.2 Ausgabe der Authentisierungsmittel

Anforderung: *Die Ausgabe eines auf Besitz basierenden Sicherungsmittels muss so erfolgen, dass der berechtigte Inhaber nach Erhalt erkennen kann, ob das Sicherungsmittel unberechtigt benutzt wurde [...]*

Auswertungsvorschrift: Aus den Angaben des Verfahrensbetreibers muss hervorgehen, auf welche Art und Weise der Inhaber erkennen kann, dass der Besitz bereits verwendet wurde.

Zusätzlich muss aus der Antwort insbesondere auch hervorgehen, auf welche Art und Weise der Inhaber darüber informiert wird, wie er den Missbrauch erkennen kann.

Normal	Substantiell	Hoch
Der Besitzer kann unberechtigte Benutzung erkennen	*Wie normal*	*Wie normal*

Tabelle 28: Vertrauensniveaus der spezifischen Anforderung B1

4.2.2 Spezifische Anforderung B2: Anforderungen an den Token

Referenz: 3.3.1 Authentisierungsmittel, Tabelle 3: Eigenschaften von Authentisierungsfaktoren

Anforderung: Anforderungen aus Tabelle 3 in [TR-03107-1]: Eigenschaften von Authentisierungsfaktoren

Hinweis: Wie in Abschnitt 4.2 erwähnt, kann unter besonderen Voraussetzungen auch ein Softwaretoken zum Besitz gezählt werden. In diesem Fall sind nicht alle Anforderungen aus diesem Teil anwendbar. Diese sind entsprechend gekennzeichnet und bei der Auswertung zu ignorieren.

Auswertungsvorschrift: Der Prüfer muss anhand der Antworten des Verfahrensbetreibers kontrollieren, dass alle Anforderungen an den Besitz erfüllt sind. Insbesondere müssen folgende Punkte zweifelsfrei geklärt werden:

- Der Besitz ist ein physikalischer Token unter physischer Kontrolle des Inhabers (Nicht für Softwaretoken anwendbar, in diesem Fall ist *hoch* nicht erreichbar.)

  Dies wird in der Regel durch eine explizite Freischaltung durch einen weiteren Faktor unmittelbar vor der Verwendung des Besitzes sichergestellt. Alternativ ist auch eine Freischaltung durch den Inhaber in Form eines die Transaktionsinformationen beinhaltenden Ja / Nein – Dialogs möglich

- Der Token ist nicht kopierbar (Nicht für Softwaretoken anwendbar)

  Es darf nicht möglich sein, eine Kopie des Tokens anzufertigen, welche durch das Prüfobjekt als legitimes Authentisierungsmittel für den Inhaber anerkannt wird. Dies bedeutet insbesondere, dass der Prüfer sich davon überzeugen muss, dass auch bei teilweisen Kopien des Tokens keine wesentlichen Teile kopiert werden können. Hierzu zählt beispielsweise die Extraktion von Schlüsselmaterial aus Hardware-Token

- Der Inhaber wird darauf hingewiesen, dass der Token nicht weitergegeben werden darf

  Der Hinweis muss an einer für den Inhaber ersichtlichen Stelle platziert sein, beispielsweise im Registrierungsverfahren oder prominent bei den Handlungsempfehlungen. Ein „Verstecken“ des Hinweises, beispielsweise in den Allgemeinen Geschäftsbedingungen, ist nicht ausreichend

- Der Inhaber wird darauf hingewiesen, dass der Token nur zum vorgesehenen Zweck der Authentisierung verwendet werden darf. In besonderen Fällen, wo der Token z. B. von Beginn an für mehrere Einsatzzwecke konzipiert wurde, ist es zulässig ihn auch für diese zu benutzen. Der Einsatz soll jedoch auf möglichst

wenige, klar definierte Funktionen beschränkt werden. Wichtig ist, dass die Sicherheit des Tokens dabei nicht gefährdet ist.

Siehe vorigen Punkt.

- Der legitime Inhaber kann Verlust des Besitzes erkennen, ggf. implementiert das Verfahren zusätzlich eine entsprechende Missbrauchserkennung

  Für das Verfahren muss es möglich sein, den Verlust des Besitzes zu erkennen bzw. zu prüfen. D.h. es muss einen Weg geben festzustellen, ob der Inhaber den Authentisierungstoken noch besitzt. Dies kann der Vertrauensdienst z. B. auch durch geeignete Nachfragen bei dem Inhaber feststellen.

- Der Token kann über ein eindeutiges Merkmal gesperrt werden.

  Der Token muss eine eindeutige ID aufweisen und diese muss bei der Sperrung herangezogen werden. Diese ID sollte von derjenigen des Inhabers selbst abweichen, damit im Falle einer Sperrung kein neuer Account angelegt werden muss.

Normal	Substantiell	Hoch
Alle Anforderungen erfüllt	*Wie normal*	*Wie normal*, mit Softwaretoken nicht erreichbar

Tabelle 29: Vertrauensniveaus der spezifischen Anforderung B2

4.2.3 Spezifische Anforderung B3: Besondere Anforderungen für das Vertrauensniveau *hoch*

Referenz: 3.3.1.1 Besitz

Anforderung: *Für das Vertrauensniveau hoch muss der Token auch gegen Veränderung (Manipulation) durch Angreifer mit hohem Angriffspotential geschützt sein. Darüber hinaus muss der Inhaber sicherstellen können, dass der Besitztoken nur für eine intendierte Authentisierung aktiviert wird.*

Hinweis: Nur relevant, falls das Vertrauensniveau *hoch* angestrebt wird.

Auswertungsvorschrift: Der Prüfer muss evaluieren, ob ausreichender Schutz gegen Angreifer mit *hohem* Angriffspotential gegeben ist (siehe auch Abschnitt 3.25). Grundlage hierfür sind Zertifizierungen oder gleichwertige Prüfungen für den verwendeten Faktor Besitz.

Aus der Antwort des Verfahrensbetreibers muss darüber hinaus ersichtlich sein, dass eine unbeabsichtigte (z. B. unwissentliche oder versehentliche) Aktivierung des Besitzes nicht möglich ist. Dies muss für den Prüfer praktisch nachvollziehbar sein.

Normal	Substantiell	Hoch
Nicht relevant für *normal*	Nicht relevant für *substantiell*	• Der Token ist gegen Veränderung (Manipulation) durch Angreifer mit *hohem* Angriffspotential geschützt • Aktivierung des Tokens für eine Authentisierung ist erkennbar

Tabelle 30: Vertrauensniveaus der spezifischen Anforderung B3

4.3 Anforderungskatalog zum Authentisierungsmittel Wissen

4.3.1 Spezifische Anforderung W1: Ausgabe des Wissens

Referenz: 3.2.2 Ausgabe der Authentisierungsmittel

Anforderung: *Die Ausgabe von wissensbasierten Sicherungsmitteln muss so erfolgen, dass der Inhaber unberechtigte Kenntnisnahme erkennen kann (Unversehrtheit des „PIN-Briefes“).*

Auswertungsvorschrift: Aus der Antwort des Verfahrensbetreibers ist ersichtlich, auf welche Art und Weise eine unberechtigte Kenntnisnahme klar erkenntlich ist und auch, wie das entsprechende Vorgehen an den rechtmäßigen Besitzer kommuniziert wird. Es muss für den Inhaber möglich sein, anhand von diesen Anweisungen zweifelsfrei festzustellen, ob eine unberechtigte Kenntnisnahme stattgefunden hat. Bei einem PIN-Brief kann beispielsweise darauf hingewiesen werden, dass der Inhaber bei einem beschädigten Umschlag Ersatz anfordern soll.

Falls eine unberechtigte Kenntnisnahme des Wissens festgestellt wird, müssen Schritte unternommen werden um (weiteren) Missbrauch zu verhindern. Benutzer müssen explizit über die dazu auf ihrer Seite notwendigen Schritte hingewiesen werden. Zum Beispiel sollte der Hinweis gegeben werden, dass der Verfahrensbetreiber informiert wird und dass das Authentisierungsmittel nicht benutzbar ist.

Normal	Substantiell	Hoch
Der Besitzer kann unberechtigte Kenntnisnahme erkennen	*Wie normal*	*Wie normal*

Tabelle 31: Vertrauensniveaus der spezifischen Anforderung W1

4.3.2 Spezifische Anforderung W2: Anforderungen an das Wissen

Referenz: 3.3.1 Authentisierungsmittel, Tabelle 3: Eigenschaften von Authentisierungsfaktoren

Anforderung: Anforderungen aus Tabelle 3 in [TR-03107-1]: Eigenschaften von Authentisierungsfaktoren

Auswertungsvorschrift: Der Prüfer muss anhand der Antworten des Verfahrensbetreibers kontrollieren, dass alle Anforderungen an einen Faktor Wissen erfüllt sind. Insbesondere müssen folgende Punkte zweifelsfrei geklärt werden:

- Das Wissen ist nur dem berechtigten Inhaber und verifizierenden Entität bekannt

  Der Prüfer muss sicherstellen, dass:

  - ...das Wissen niemals ungesichert übertragen oder gespeichert wird
  - ...die Mitarbeiter und Dienstleister des Verfahrensbetreibers ebenfalls keinen Zugriff auf die ungesicherten Daten erhalten können
- Der Inhaber wird darauf hingewiesen, dass das Wissen nicht weitergegeben werden darf
  - Der Hinweis muss gut sichtbar platziert sein, beispielsweise als Teil des Registrierungsprozesses
- Der Inhaber wird darauf hingewiesen, dass das Wissen nur zum vorgesehenen Zweck der Authentisierung verwendet werden darf
  - Der Inhaber wird darauf hingewiesen, dass der gleiche Wissens-Token nicht für andere Dienste verwendet werden soll
- Der Inhaber wird darauf hingewiesen, dass er den Wissens-Token nicht aufschreiben oder in der Cloud speichern soll. Abweichungen sind nur zulässig, wenn sie nicht gegen die Regelung M 2.11 aus [BSI-GS] verstoßen.

- Das Verfahren verfügt über eine Missbrauchserkennung. Es ist also in der Lage zu erkennen, dass das Wissen möglicherweise von einer unberechtigten Person unbefugt verwendet wird. Weiterhin ist es in der Lage durch heuristische Methoden auffallende Abweichungen vom Normalverhalten zu detektieren. Ein Beispiel von solchen Abweichungen ist häufiger Zugriff aus weit entfernten geographischen Orten oder häufige Anfragen von einer verdächtigen IP
- Bei zu häufigen Authentisierungsversuchen, die über das übliche Maß hinausgehen, oder bei sonstigem Missbrauchsverdacht kann das entsprechende Konto bzw. Besitz mindestens vorübergehend gesperrt werden
- Als Ersatz für einen gesperrten Wissenstoken ist es möglich, ein neues Passwort bzw. eine neue PIN zu setzen. D. h. der Token lässt sich bei Bedarf ändern, um das gesperrte Wissen abzulösen.

Normal	Substantiell	Hoch
Alle Anforderungen erfüllt	*Wie normal*	*Wie normal*

Tabelle 32: Vertrauensniveaus der spezifischen Anforderung W2

4.3.3 Spezifische Anforderung W3: Passwortgebrauch

Referenz: 3.3.1.2 Wissen

Anforderung: *Bei Nutzung von Wissen als alleinigem Sicherungsfaktor sind die Anforderungen aus Maßnahme M 2.11 „Regelung des Passwortgebrauchs“ der IT-Grundschutz-Kataloge des BSI (siehe [BSI-GS]) einzuhalten.*

Hinweis: Diese Anforderung gilt nur für Passwort-basierte Sicherungsfaktoren.

Auswertungsvorschrift: Der Prüfer muss die Anforderungen von [BSI-GS] in der jeweils aktuellen Fassung feststellen. Siehe hierzu auch „ORP.4.A8 Regelung des Passwortgebrauchs“ in [BSI-GSK].

Anschließend muss er überprüfen, dass die Anforderungen des Verfahrensbetreibers an Wissen den Anforderungen von [BSI-GS] entsprechen.

Normal	Substantiell	Hoch
Die Anforderungen aus [BSI-GS] werden eingehalten	Nicht erreichbar	Nicht erreichbar

Tabelle 33: Vertrauensniveaus der spezifischen Anforderung W3

4.3.4 Spezifische Anforderung W4: Passwortentropie

Referenz: 3.3.1.2 Wissen

Anforderung: *Bei Verwendung eines Fehlbedienungszählers, der maximal drei Versuche, eine PIN zu raten zulässt, sollte eine PIN mindestens 4 (Vertrauensniveau normal), 5 (Vertrauensniveau substantiell) bzw. 6 (Vertrauensniveau hoch) dezimale Stellen haben (vgl. [AIS 20/31]).*

Auswertungsvorschrift: Der Prüfer muss die Entropie bzw. Resilienz des Passworts feststellen. Bei vorhandenem Fehlbedienungszähler ist die Berechnungsvorschrift: P := (Anzahl Versuche) / (Anzahl erlaubter Zeichen) ^ (Anzahl Stellen)

Normal	Substantiell	Hoch
0,003% <= P < 0,03%	0,0003% <= P < 0,003%	P < 0,0003%

Tabelle 34: Vertrauensniveaus der spezifischen Anforderung W4

Ist kein Fehlbedienungszähler vorhanden, so kann Vertrauensniveau *hoch* nicht erreicht werden.

Vertrauensniveau *substantiell* kann ohne Fehlbedienungszahler nur erreicht werden, wenn bei der Passwortprüfung ein anderer wirksamer Schutz gegen Brute-Force Angriffe umgesetzt ist. Abschnitt 4.7.1 enthält spezifischere Anforderungen für die Verwendung von Softwaretoken.

4.4 Anforderungskatalog zum Authentisierungsmittel Biometrie

4.4.1 Spezifische Anforderung Bio1: Anforderungen an die Biometrie

Referenz: 3.3.1 Authentisierungsmittel, Tabelle 3: Eigenschaften von Authentisierungsfaktoren

Anforderung: Anforderungen aus Tabelle 3 in [TR-03107-1]: Eigenschaften von Authentisierungsfaktoren

Auswertungsvorschrift: Der Prüfer muss anhand der Antworten des Verfahrensbetreibers kontrollieren, dass alle Anforderungen an die Biometrie erfüllt sind. Insbesondere müssen folgende Punkte zweifelsfrei geklärt werden:

- Das Merkmal soll den Inhaber zweifelsfrei identifizieren. D.h. insbesondere sollten auch Verwechselungen zwischen verschiedenen Menschen ausgeschlossen sein, wenn sie ähnliche Charakteristiken aufweisen
- Lebenderkennung ist implementiert
- Der Inhaber wird darauf hingewiesen, dass das biometrische Merkmal nur zum vorgesehenen Zweck der Authentisierung verwendet werden darf. Innerhalb eines Verfahrens darf das biometrische Merkmal nicht mehrfach verwendet werden (z. B. nicht zur Authentisierung und zur Transaktionsfreigabe; oder nicht zur Geräteentsperrung und Authentisierung innerhalb eines Verfahrens)
- Das Verfahren sollte über eine Missbrauchserkennung verfügen. Es ist also in der Lage zu erkennen, dass das biometrische Merkmal möglicherweise von einer unberechtigten Person unbefugt verwendet wird. Weiterhin können z. B. durch heuristische Methoden auffallende Abweichungen vom Normalverhalten detektiert werden.
- Bei häufigen Wiederholungen oder bei Missbrauchsverdacht kann das entsprechende Konto bzw. Besitz gesperrt werden. Bei mehrfach fehlgeschlagenen Wiederholungen innerhalb kurzer Zeit muss mindestens eine temporäre Sperrung des biometrischen Faktors erfolgen
- Nach Sperrung eines Merkmals durch Missbrauch ist das Enrolment und die Nutzung eines anderen Merkmals zulässig

Normal	Substantiell	Hoch
Alle Anforderungen erfüllt. Lebenderkennung ist geschützt gegen Angriffspotential *enhanced-basic*.	*Wie normal*, Lebenderkennung ist geschützt gegen Angriffspotential *moderate*.	*Wie normal*, Lebenderkennung ist geschützt gegen Angriffspotential *high*.

Tabelle 35: Vertrauensniveaus der spezifischen Anforderung Bio1

Zur Bewertung der Sicherheit von Biometrie als ein Authentisierungsfaktor auf Mobilgeräten hat das BSI *Presentation Attacks* bei Gesichts- und Fingerabdruckerkennung untersucht.

Mechanismen, die auf einem zweidimensionalen Bildabgleich beruhen, haben sich als nicht geeignet für Vertrauensniveau *substantiell* oder *hoch* herausgestellt. Die dreidimensionale Gesichtserkennung mit sogenannter „TrueDepth-Technologie / FaceID“, die teilweise auf Apple-Mobilgeräten implementiert ist, erscheint mit Blick auf Presentation Attacks bis auf weiteres für das Vertrauensniveau *substantiell* vertretbar. Zu beachten ist jedoch, dass Personen in enger Verwandtschaft (z.B. Geschwister oder Eltern/Kinder) in manchen Fällen eine falsch-positive Authentisierung gelingen kann. Sofern FaceID für Vertrauensniveau *substantiell* eingesetzt werden soll, muss vor der Aktivierung ein deutlicher Warnhinweis erfolgen, dass gegenüber einer ausschließlichen Absicherung mittels PIN zusätzlich das Risiko besteht, dass auch nahen biologischen Verwandten eine illegitime Entsperrung gelingen kann.

Fingerabdruckerkennung auf Mobilgeräten ist regelmäßig nicht als biometrischer Faktor für Vertrauensniveau *substantiell* oder *hoch* geeignet, da regelmäßig kein geeignet wirksamer *Presentation Attack Detection* (PAD) Mechanismus vorhanden ist.

4.4.2 Spezifische Anforderung Bio2: Sicherheit Biometrie

Referenz: 3.3.1.3 Biometrie

Anforderung: *Die Erfolgswahrscheinlichkeit für eine Überwindung der biometrischen Erkennung, ausgedrückt durch False Acceptance Rate, darf nicht wesentlich schlechter als die entsprechenden Vorgaben für den Sicherungsfaktor Wissen sein.*

Auswertungsvorschrift: Der Prüfer muss verifizieren, dass die FAR die zulässigen Werte nicht wesentlich überschreitet.

Als Orientierungshilfe bei der Bewertung muss der Prüfer die Schwellwerte des Faktors „Wissen“ heranziehen:

- *normal*: 0,003% <= FAR < 0,03%
- *substantiell*: 0,0003% <= FAR < 0,003%
- *hoch*: FAR <= 0,0003%

Biometrische Authentifizierung darf nur in Kombination mit dem Sicherungsfaktor Besitz eingesetzt werden. Alleinige Nutzung der Biometrie ist nicht hinreichend für das Erreichen des Niveaus *normal*.

Normal	Substantiell	Hoch
Die False Acceptance Rate ist nicht wesentlich schlechter als der in der Orientierungshilfe für n*ormal* angegebene Schwellwert	Die False Acceptance Rate ist nicht wesentlich schlechter als der in der Orientierungshilfe für *substantiell* angegebene Schwellwert	Die False Acceptance Rate ist nicht wesentlich schlechter als der in der Orientierungshilfe für *hoch* angegebene Schwellwert

Tabelle 36: Vertrauensniveaus der spezifischen Anforderung Bio2

4.5 Anforderungskatalog zu Multi-Faktor Authentisierung

Hinweis: Nur relevant, falls die Vertrauensniveaus *substantiell* oder *hoch* angestrebt werden.

4.5.1 Spezifische Anforderung MF1: Verknüpfung Sicherungsfaktoren

Referenz: 3.3.1.2 Wissen

Anforderung: *Bei Nutzung von Wissen in Kombination mit Besitz müssen beide Sicherungsfaktoren miteinander verknüpft sein, zum Beispiel die Benutzung einer PIN zur Freischaltung einer Chipkarte.*

Hinweis: Nur relevant, falls Wissen in Kombination mit Besitz verwendet wird. Sonst ist die Anforderung nicht anwendbar.

Auswertungsvorschrift: Der Prüfer muss kontrollieren, dass die beiden Sicherungsfaktoren miteinander verknüpft sind. Es muss ersichtlich sein (z. B. aus dem Ablaufdiagramm), dass der Einsatz des Besitzes zeitlich stets nach dem Freischalten durch das Wissen erfolgt.

Normal	Substantiell	Hoch
Nicht relevant für *normal*	*Die beiden Sicherungsfaktoren sind miteinander verknüpft*	*Wie substantiell*

Tabelle 37: Vertrauensniveaus der spezifischen Anforderung MF1

4.5.2 Spezifische Anforderung MF2: Fehlschlagen eines Faktors

Referenz: 3.3.1.4 Zwei-Faktor-Authentisierung

Anforderung: *[...] darf ein Angreifer das Fehlschlagen eines Authentisierungsversuches nicht einem einzelnen Authentisierungsfaktor zuordnen können.*

Auswertungsvorschrift: Aus der Antwort des Verfahrensbetreibers muss hervorgehen, dass das Fehlschlagen nicht einem einzelnen Faktor zugeordnet werden kann.

Sollte die Antwort auf diese Frage unklar ausfallen, kann der Prüfer das Ablaufdiagramm der Authentisierung heranziehen. Um eine Zuordenbarkeit zu vermeiden, müssen insbesondere folgende Punkte beachtet werden:

1. Das Authentisierungsverfahren selbst darf den Faktor nicht benennen
2. Das Feedback über den Fehlschlag der Authentisierung darf nicht unmittelbar nach Verwendung des gescheiterten Faktors erfolgen, sondern erst nach der Eingabe aller Faktoren.

   Beispiel: Ein Authentisierungsverfahren verwendet Benutzername und Passwort in Kombination mit einem OTP-Generator. Legitime Nutzer melden sich zunächst mit ersterem an und bestätigen das Login mit letzterem. In einem solchen Authentisierungsverfahren darf einem Angreifer nicht direkt nach Eingabe eines falschen Passworts angezeigt werden, dass dieses falsch war. Stattdessen muss er dennoch zur Eingabe des OTP aufgefordert werden. Erst im Anschluss darauf wird der Loginversuch als gescheitert gemeldet, auch wenn das OTP korrekt war.

Normal	Substantiell	Hoch
Nicht relevant für *normal*	*Ein Angreifer kann nicht erkennen welcher Sicherungsfaktor fehlgeschlagen ist*	*Wie substantiell*

Tabelle 38: Vertrauensniveaus der spezifischen Anforderung MF2

4.5.3 Spezifische Anforderung MF3: Resistenz beider Faktoren

Referenz: 3.3.1.4 Zwei-Faktor-Authentisierung

Anforderung: *[...] dürfen nicht beide Faktoren gemeinsam durch einen einzelnen Angriff auf die Nutzerumgebung angreifbar sein.*

Auswertungsvorschrift: Anhand der Angaben des Verfahrensbetreibers muss ersichtlich sein, dass die Sicherungsfaktoren so gespeichert und verwendet werden, dass ein einzelner Angriff auf die Nutzerumgebung nicht zu einer Kompromittierung mehrerer Faktoren führt. Dabei sind auch die Anweisungen an den Nutzer, die Faktoren entsprechend sicher zu behandeln, zu berücksichtigen.

Normal	Substantiell	Hoch
Nicht relevant für *normal*	Einzelne Angriffe wirken sich nicht auf die Sicherheit von mehr als einem einzelnen Faktor aus	*Wie substantiell*

Tabelle 39: Vertrauensniveaus der spezifischen Anforderung MF3

4.5.4 Generische Anforderung MF4: Ausgabe über getrennte Übermittlungswege

Referenz: 3.2.2 Ausgabe der Authentisierungsmittel

Anforderung: *Die Ausgabe für die Vertrauensniveaus substantiell/hoch muss so erfolgen, dass die beiden Sicherungsfaktoren [...] auf verschiedenen Übermittlungswegen ausgegeben werden. Diese Anforderung kann auch dadurch erfüllt werden, in dem die beiden Faktoren zeitlich getrennt auf gleichem Wege übermittelt werden, sofern sichergestellt ist, dass der erste Faktor den Inhaber erreicht hat, bevor der zweite übermittelt wird.*

Hinweis: Nicht relevant für Faktoren, die vom Nutzer selbst lokal generiert werden.

Auswertungsvorschrift: Die Trennung der Ausgabekanäle muss verständlich dargestellt sein. Dabei muss der Prüfer darauf achten, dass in der Darstellung entweder vollständig getrennte Kanäle (Verbindungen zwischen den Entitäten) verwendet werden, oder eine hinreichende zeitliche Verzögerung umgesetzt ist.

Normal	Substantiell	Hoch
Nicht relevant für *normal*	Es werden getrennte Kanäle verwendet. Die Trennung kann auch zeitlich erfolgen.	*Wie substantiell*

Tabelle 40: Vertrauensniveaus der generischen Anforderung MF4

4.6 Anforderungskatalog zum Authentisierungsmittel eID

4.6.1 Spezifische Anforderung eID1: eID-Funktion

Referenz: 4.1 Elektronischer Identitätsnachweis

Anforderung: *Der elektronische Identitätsnachweis [...] ist für die Authentisierung auf hohem Vertrauensniveau geeignet. Dies gilt auch bei Einsatz eines Pseudonyms (dienste- und kartenspezifische Kennung).*

Auswertungsvorschrift: Der Prüfer muss kontrollieren, ob das Prüfobjekt den elektronischen Identitätsnachweis verwendet. Der Einsatz des Pseudonyms (dienste- und kartenspezifische Kennung) für die Authentisierung stellt dabei kein Hindernis dar.

Normal	Substantiell	Hoch
Die eID-Funktion wird verwendet	*Wie normal*	*Wie normal*

Tabelle 41: Vertrauensniveaus der spezifischen Anforderung eID1

4.7 Anforderungskatalog zum Authentisierungsmittel Softwaretoken

4.7.1 Spezifische Anforderung SW1: Schlüsselspeicherung

Referenz: 4.2 Kryptographische Token

Anforderung: *Es gelten die Anforderungen aus Abschnitt 3.7 [„Kryptographie“]. Die privaten kryptographischen Schlüssel dürfen nicht außerhalb des Tokens vorliegen (kein Key-Backup oder Key-Escrow).*

Auswertungsvorschrift: Der Prüfer muss evaluieren, dass keine Speicherung der kryptografischen Schlüssel außerhalb des Tokens vorgesehen ist und der Inhaber auch auf diesen Umstand hingewiesen wird. Auch wenn es eine technische Möglichkeit zum Extrahieren des Schlüssels gibt (z. B. ein PKCS#12 Container), soll davon kein Gebrauch gemacht werden.

Zusätzliche Auswertungshinweise für *substantiell***:**

Es muss eine Schlüsselableitungsfunktion verwendet werden, die gleichzeitig signifikanten Rechenaufwand und Speicherplatz erfordert. Als Übergangsregelung für bereits vor 2019 bestehende Verfahren ist es ausnahmsweise bis maximal Ende 2022 auch zulässig, wenn nur eine Komponente, also Rechenaufwand oder Speicherplatz, signifikant beansprucht wird.

Das Verfahren muss den Nutzer deutlich wahrnehmbar darauf verpflichten, keine leicht zu erratenden Passwörter („Trivialpasswörter“) zu wählen. Ferner muss das System leicht zugängliche Hilfestellungen bieten, starke Passwörter zu wählen. Die Passwortentropie muss einen zuverlässigen Schutz vor möglichen Brute-Force Angriffen gewährleisten. Mit Stand 2018 sind dazu folgende Mindestanforderungen zu erfüllen:

- Das Schlüsselmaterial muss auf dem Computersystem mindestens durch Softwaremechanismen vor Kopieren oder Export geschützt sein. Weitere Schutzmechanismen wie, z. B. Windows Zertifikatsspeicher oder macOS Schlüsselbunds sollten verwendet werden.
- Das Computersystem, auf dem der Token gespeichert ist, sollte ausschließlich durch den Token-Inhaber genutzt werden. Es dürfen nur vorab definierte und eingeschränkte Nutzergruppen Zugriff auf das Computersystem haben. Das Speichern auf Computersystemen, die möglicherweise auch für Unbekannte zugänglich sind (z. B. einer öffentlichen Cloud) ist nicht zulässig.
- Die Passwortentropie (ggf. zusammen mit weiteren Maßnahmen, z. B. Iteration Count zur Verlangsamung von Brute-Force Suchen) muss gewährleisten, dass ein Angreifer mindestens 2^{64} Hashoperationen durchführen muss um im Falle der Mindestpasswortentropie alle möglichen Passwörter zu durchsuchen. Bei einer effektiven Passwortentropie von mindestens 50 Bit ergibt sich damit beispielsweise ein Iteration count von mindestens 2^{14} (= 16.348).
- Für jedes Jahr, über das der Token über 2018 hinaus gültig sein soll, verdoppelt sich die mindestens geforderte Anzahl an Hashoperationen. D. h. für Token die bis 2019 verwendet werden sollen ist erhöht sich die oben genannte Mindestanforderung auf 2^{65} Hashoperationen, bei Gültikeit bis 2020 auf 2^{66} Hashoperationen, bei Gültigkeit bis 2021 auf 2^{67} Hashoperationen usw.
- Für das Hashing von Passwörtern sollten nur *memory-hard* Hashfunktionen eingesetzt werden um verbesserten Schutz vor Angriffen unter Nutzung von GPUs zu bieten.

Ohne diese zusätzlichen Voraussetzungen ist eine Passwortentropie von 50 Bit nicht ausreichend.

Normal	Substantiell	Hoch
Kryptographische Schlüssel liegen nicht außerhalb des Tokens vor	*Zusätzlich zu normal:* • Der Token muss durch Softwaremechanismen und eingeschränkte Nutzergruppen vor unbefugten Zugriff geschützt sein. • Es müssen starke Passwörter mit hinreichender Entropie verwendet werden.	Nicht erreichbar

Tabelle 42: Vertrauensniveaus der spezifischen Anforderung SW1

4.7.2 Spezifische Anforderung SW2: Erzeugung und Löschung der Schlüssel

Referenz: 4.2 Kryptographische Token

Anforderung: *Sofern Schlüssel außerhalb des Tokens erzeugt werden, so muss dies in einer sicheren Umgebung erfolgen und die außerhalb des Tokens vorliegenden privaten Schlüssel [müssen] vor Auslieferung des Tokens gelöscht werden.*

Hinweis: Diese Anforderung ist nur dann relevant, wenn der Token nicht durch den Inhaber bzw. dessen Hardware selbst generiert wird.

Auswertungsvorschrift: Anhand der Angaben des Verfahrensbetreibers muss ersichtlich sein, wo das Schlüsselmaterial erzeugt wird. Sollte es beim Dienst und außerhalb des Tokens stattfinden, so muss eine Löschung vor der Auslieferung erfolgen. Der Verfahrensbetreiber soll daher angeben, zu welchem Zeitpunkt das Löschen des Schlüsselmaterials erfolgt. Im Idealfall geschieht dies unmittelbar nach Generierung des Tokens, spätestens aber vor dessen Auslieferung.

Normal	Substantiell	Hoch
• Die Schlüssel werden in einer sicheren Umgebung erzeugt. • Die Schlüssel werden vor Auslieferung gelöscht	*Wie normal*	Nicht erreichbar

Tabelle 43: Vertrauensniveaus der spezifischen Anforderung SW2

4.8 Anforderungskatalog zum Authentisierungsmittel OTP

4.8.1 Spezifische Anforderung OTP1: TANs

Referenz: 4.3 One-Time-Passwords

Anforderung: Diverse Anforderungen aus Abschnitt 4.3 von [TR-03107-1]

Das Vertrauensniveau hoch kann grundsätzlich nur mit TAN-Verfahren erreicht werden, bei denen wesentliche Vorgangsdaten in die Erzeugung der TAN eingehen und dem Nutzer unabhängig von der primären Verbindung zwischen Bürger und vertrauenden Entität angezeigt werden.

Hinweis: Das smsTAN-Verfahren wird im eigenen Abschnitt 4.9 betrachtet.

Auswertungsvorschrift: Der Prüfer muss feststellen, welches TAN-Verfahren zur Anwendung kommt. Die erreichbaren Niveaus sind entsprechend in der Tabelle 44 festgehalten.

Bei smsTAN ist auch das Erreichen des Niveaus *substantiell* unter Umständen möglich. Die notwendige Voraussetzung hierfür ist eine „echte“ Kanaltrennung, d. h. es müssen zwei physikalisch verschiedene Geräte für die Authentisierung und SMS-Empfang verwendet werden.

Zusätzliche Auswertungshinweise für *hoch*: Zusätzlich muss der Prüfer feststellen, wie TANs generiert werden. Hierfür gelten jeweils die Kriterien aus Tabelle 44.

Normal	Substantiell	Hoch
• Es werden die TAN-Verfahren smsTAN, pushTAN sowie chipTAN eingesetzt. Eine statische iTAN-Liste ist auch noch zulässig. Weitere Verfahren sind nur dann zugelassen, wenn sie das Sicherheitsniveau der genannten nicht unterschreiten	• Es sind die TAN-Verfahren pushTAN sowie chipTAN erlaubt. Weitere Verfahren sind nur dann zugelassen, wenn sie das Sicherheitsniveau der genannten nicht unterschreiten	• Nur mit den TAN-Verfahren pushTAN oder chipTAN erreichbar • Wesentliche Vorgangsdaten gehen in die Erzeugung der TAN ein • Die Vorgangsdaten werden dem Nutzer unabhängig von der primären Verbindung zwischen Bürger und vertrauenden Entität angezeigt

		• Das Verfahren setzt eine Zwei-Faktor-Authentisierung um

Tabelle 44: Vertrauensniveaus der spezifischen Anforderung OTP1

4.8.2 Spezifische Anforderung OTP2: TAN-Generatoren

Referenz: 4.3.4 TAN-Generatoren

Anforderung: *Der TAN-Generator muss individuell sein, d. h. Generatoren unterschiedlicher Inhaber sind nicht gegeneinander austauschbar;*

Der Generator (Faktor Besitz, z. B. eine Chipkarte) ist zur Erzeugung der TAN durch eine PIN oder Ähnliches (Faktor Wissen) geschützt.

Hinweis: Nur relevant, falls die Vertrauensniveaus *substantiell* oder *hoch* angestrebt werden.

Hinweis: Nicht anwendbar, falls keine TAN-Generatoren zum Einsatz kommen.

Auswertungsvorschrift: Anhand der Antworten des Verfahrensbetreibers ist ersichtlich, dass die eingesetzten TAN-Generatoren personalisiert sind. Dieses Kriterium ist auch erfüllbar, indem der eigentliche Generator mit einem weiteren Element, beispielsweise der Bankkarte, kombiniert werden muss.

Ein Zugriff auf die TAN-Generierung darf nur nach einer unmittelbar zuvor erfolgen Freischaltung durch einen weiteren Faktor möglich sein. Sollten die Antworten des Verfahrensbetreibers diesbezüglich unklar sein, kann der Prüfer dies auch dem Ablaufdiagramm der Authentisierung entnehmen.

Der Prüfer muss sich überzeugen, dass sich die Generatoren unterschiedlicher Inhaber nicht austauschen lassen. Es soll also nicht möglich sein, den TAN-Generator eines anderen Inhabers für die Anmeldung zu verwenden.

Normal	Substantiell	Hoch
Nicht relevant für *normal*	• TAN-Generator ist individuell • Erzeugen der TAN ist durch Sicherungsfaktor Wissen geschützt	*Wie substantiell*

Tabelle 45: Vertrauensniveaus der spezifischen Anforderung OTP2

4.9 Anforderungskatalog zum Authentisierungsmittel smsTAN

4.9.1 Spezifische Anforderung sms1: Registrierung der SIM

Referenz: 4.3.2 smsTAN

Anforderung: *Die Registrierung der SIM-Karte (bzw. genauer der Telefonnummer) auf das Konto des Bürgers bei der Behörde erfolgt in Verbindung mit einer Identifizierung des Bürgers mindestens auf Vertrauensniveau substantiell [...].*

Auswertungsvorschrift: Anhand des Prüfberichtes gemäß [TR-03147] muss ersichtlich sein, dass die Identifizierung des Bürgers mindestens auf dem Niveau *substantiell* erfolgt ist. Für Vertrauensniveau *normal* gilt die Anforderung analog. Falls keine Bewertung vorliegt, ist das Niveau *normal* nicht erreichbar.

Normal	Substantiell	Hoch

Registrierung ist auf Vertrauensniveau *normal* erfolgt	Registrierung ist auf Vertrauensniveau *substantiell* erfolgt	Nicht erreichbar

Tabelle 46: Vertrauensniveaus der spezifischen Anforderung sms1

4.9.2 Spezifische Anforderung sms2: Displaysperre

Referenz: 4.3.2 smsTAN

Anforderung: *Das smsTAN-Verfahren bildet eine Zwei-Faktor-Authentisierung über die Telefonnummer (Faktor Besitz) und den Zugangscode (PIN, Geste – Faktor Wissen) des Mobiltelefons. Daher darf das Verfahren nur mit Mobiltelefonen benutzt werden, die einen eingeschalteten und wirksamen Mechanismus zur Zugangssperre haben. Alternativ kann die smsTAN in Verbindung mit einem anderen wissensbasierten Faktor eingesetzt werden, wobei Abschnitt 3.3.1.4 zu beachten ist.*

Hinweis: Nur relevant, falls das Vertrauensniveau *substantiell* angestrebt wird.

Auswertungsvorschrift: Die Antwort des Verfahrensbetreibers muss verständlich darlegen, auf welche Art und Weise dem Inhaber kommuniziert wird, dass er eine Bildschirmsperre auf seinem für den Empfang der TANs genutzten Gerät aktivieren muss.

Wenn das technische forcieren der Bildschirmsperre nicht ohne weiteres möglich ist, muss stattdessen stets ein weiterer Faktor Wissen für dieses Verfahren verwendet werden. Welcher dies ist, muss aus der Antwort des Verfahrensbetreibers hervorgehen. Alternativ kann der Prüfer es dem Ablaufdiagramm entnehmen.

Normal	Substantiell	Hoch
-	• Der Inhaber wird darauf hingewiesen, dass er die Bildschirmsperre einschalten soll • Wenn die Bildschirmsperre technisch nicht durchsetzbar ist, wird ein weiterer Faktor Wissen mit dem smsTAN-Verfahren kombiniert	Nicht erreichbar

Tabelle 47: Vertrauensniveaus der spezifischen Anforderung sms2

4.9.3 Spezifische Anforderung sms3: Getrennter Kanal

Referenz: 4.3.2 smsTAN

Anforderung: *Die primäre Verbindung zwischen Bürger und Behörde (d.h. die eigentliche Transaktion) erfolgt nicht über das Mobiltelefon, sondern über ein separates Endgerät und ein anderes Netzwerk.*

Hinweis: Nur relevant, falls das Vertrauensniveau *substantiell* angestrebt wird.

Auswertungsvorschrift: Die Antwort des Verfahrensbetreibers muss darstellen, wie die Kanaltrennung forciert wird. Beispiele sind hierfür die Einschränkung auf bestimmte eSIMs oder das Aushändigen eines Feature-Phones, welches mit einer fest verbauten SIM ausgestattet ist. Mit einer normalen SIM-Karte aus dem freien Verkauf, welche in einem Smartphone verwendet werden kann, ist eine rein technische Erfüllung dieses Kriteriums nicht möglich.

Es ist auch möglich, dass der Vertrauensdienst den Inhaber darauf hin weist, dass für die Transaktion und den Empfang der smsTAN unterschiedliche Geräte und Netzwerke verwendet werden sollen. Ein entsprechender Hinweis muss an einer für den Inhaber ersichtlichen Stelle platziert sein, beispielsweise im Registrierungsverfahren oder prominent bei den Handlungsempfehlungen. Die Kenntnisnahme muss durch den

Nutzer bestätigt werden. Ein „Verstecken“ des Hinweises, beispielsweise in den Allgemeinen Geschäftsbedingungen, ist nicht ausreichend. Der Inhaber hat dementsprechend auf die Kanaltrennung zu achten.

Normal	Substantiell	Hoch
Nicht relevant für *normal*	• E-Government Vorgang läuft über ein anderes Gerät und Netzwerk, als Authentisierung ab • Der Inhaber wird auf die Kanaltrennung explizit hingewiesen	Nicht erreichbar

Tabelle 48: Vertrauensniveaus der spezifischen Anforderung sms3

4.10 Anforderungskatalog zur Reaktivierung

4.10.1 Spezifische Anforderung R1: Identifizierung

Referenz: 3.4.2 Reaktivierung

Anforderung: *Für eine Rücknahme einer Sperrung – sofern vom System unterstützt – muss eine Identifizierung des Inhabers eines Authentisierungsmittels mindestens auf dem Vertrauensniveau des Authentisierungssystems erfolgen.*

Auswertungsvorschrift: Aus der Antwort des Verfahrensbetreibers geht hervor, dass die Reaktivierung nur nach einer erneuten Identitätsprüfung des Inhabers möglich ist. Somit wird an dieser Stelle das Ergebnis der Prüfung gemäß [TR-03147] übernommen. Falls keine Bewertung vorliegt, ist das Niveau *normal* nicht erreichbar.

Normal	Substantiell	Hoch
Die Prüfung gemäß [TR-03147] resultiert im Niveau n*ormal*	Die Prüfung gemäß [TR-03147] resultiert im Niveau s*ubstantiell*	Die Prüfung gemäß [TR-03147] resultiert im Niveau *hoch*

Tabelle 49: Vertrauensniveaus der spezifischen Anforderung R1

4.10.2 Spezifische Anforderung R2: Kompromittierung

Referenz: 3.4.2 Reaktivierung

Anforderung: *Es muss sichergestellt sein, dass die Sicherheit der Authentisierungsmittel nicht kompromittiert wurde.*

Auswertungsvorschrift: Der Prüfer muss kontrollieren, dass wirksame Mechanismen eingesetzt werden, die sicherstellen, dass die Sicherheit der Authentisierungsmittel nicht kompromittiert wurde. Für kopierbare Authentisierungsmittel ist dies grundsätzlich nicht der Fall, da die Einmaligkeit nicht garantiert werden kann.

Für nicht kopierbare Authentisierungsmittel muss sichergestellt sein, dass ihre Verwendung von den Systemen des Dienstes wiedererkannt und protokolliert wird. Das Verfahren soll in der Lage sein zu erkennen, wenn ein Authentisierungsmittel seit seiner Suspendierung verwendet worden ist (unabhängig davon, ob der Dienst die Authentisierung annimmt oder nicht). Diese Erkenntnis soll in die Entscheidung über die Reaktivierung einfließen. Bei einer festgestellten Verwendung soll von einer Kompromittierung ausgegangen werden und das Authentisierungsmittel darf nicht reaktiviert werden.

Normal	Substantiell	Hoch
Nur nicht kompromittierte Authentisierungsmittel werden reaktiviert	*Wie normal*	*Wie normal*

Tabelle 50: Vertrauensniveaus der spezifischen Anforderung R2

Literaturverzeichnis

[AIS 20/31] BSI: AIS 20/31 -- A proposal for: Functionality classes for random number generators

[BSI-GS] BSI: IT-Grundschutz-Kataloge, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[BSI-GSK] BSI: IT-Grundschutz-Kompendium, Bausteine, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/bausteine_node.html

[BSI100-2] BSI: BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise

[CEM] CCMB: Common Criteria and Common Evaluation Methodology Version 3.1

[ISO27001] ISO/IEC: ISO/IEC 27001: Information technology -- Security techniques -- Information security management systems -- Requirements

[PrüfB/TR-03107] BSI: Ergebnisse der Prüfung gemäß TR-03107-1

[TLS-Checkliste] BSI: TLS nach TR-03116-4, Checkliste für Diensteanbieter

[TR-02102] BSI: Technische Richtlinie TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen

[TR-03107-1] BSI: Technische Richtlinie TR-03107-1, Elektronische Identitäten und Vertrauensdienste im E-Government

[TR-03107-1] BSI: Technische Richtlinie TR-03107, Elektronische Identitäten und Vertrauensdienste im E-Government

[TR-03116] BSI: Technische Richtlinie TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung

[TR-03116-TS] BSI: Technical Guideline TR-03116-TS, TLS Test-Specification

[TR-03145] BSI: Technische Richtlinie TR-03145, Secure CA Operation

[TR-03147] BSI: Technische Richtlinie TR-03147, Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen