Bundesamt
für Sicherheit in der
Informationstechnik

Ergebnisse der Prüfung gemäß TR-03107-1 in Version 1.1.1

Produkt XY

Version des Prüfberichtes: 0.15

Gemäß Prüfberichtsschema in Version: 1.05
11.12.2020

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 Kriterien sollen es ermöglichen, diese Verfahren zu definierten Vertrauensniveaus zuzuordnen. Dafür werden unterschiedliche Kriterien betrachtet, die generisch oder spezifisch für einen bestimmten Prozess sind. Im Rahmen des Prüfverfahrens wurden die relevanten Kriterien auf das in diesem Dokument betrachtete Prüfobjekt angewendet und die Ergebnisse ausgewertet. Eine maßgebliche Rolle spielen hierbei die Angaben des Verfahrensbetreibers sowie Zertifizierungen, welche im Rahmen der Prüfung herangezogen wurden und als Grundlage der Bewertung dienen.

Der vorliegende Prüfbericht gliedert sich in mehrere Abschnitte, welche sich jeweils mit den unterschiedlichen zu dem Prüfobjekt gehörenden Komponenten befassen. Er beinhaltet und bewertet nur diejenigen Anforderungen der [TR-03107-1], welche auch tatsächlich für das zu analysierende Prüfobjekt relevant sind. Weiterhin werden nur Authentisierungs- und Identifizierungsprozesse im E-Government betrachtet. Prozesse zum Zweck der Abgabe einer Willenserklärung oder zur Dokumentenübermittlung werden hier nicht berücksichtigt. Dies stellt jedoch keine Einschränkung hinsichtlich der zu betrachtenden „Mechanismen / Funktionen“ oder „Kriterien“ gemäß der [TR-03107-1] dar. Als Identifizierung wird in diesem Dokument sowohl die Identifizierung von Personen, als auch von Diensteanbietern verstanden.

Sämtliche Referenzen in diesem Dokument beziehen sich, soweit nicht anderweitig erwähnt, auf die zugrunde liegende Version der [TR-03107-1]. Die Bewertungsgrundlage für die hier dokumentierten Ergebnisse stellt, neben dieser Technischen Richtlinie selbst, insbesondere auch [Bew/TR-03107] in der zugehörigen Version dar.

2 Beschreibung des Authentisierungsverfahrens

Dieser Prüfbericht bezieht sich auf eine konkrete Ausprägung des analysierten Verfahrens. Dies bedeutet, dass das Ergebnis einen eindeutigen Bezug zu einem bestimmten Prüfobjekt (Authentisierungsverfahren in einer bestimmten Konfiguration mitsamt dem zugehörigen E-Government-Onlinedienst) eines bestimmten Betreibers hat. Insbesondere sind die Ergebnisse nicht notwendigerweise auf andere Ausprägungen des Authentisierungsverfahrens, z. B. andere Versionsnummern oder Konfigurationen, übertragbar. Die untersuchte Konstellation ist in diesem Kapitel eindeutig festgehalten.

2.1 Allgemeine Angaben

Hier werden die allgemeinen Angaben zum Prüfobjekt aufgeführt. Die Prüfung bezieht sich ausschließlich auf folgendes Authentisierungsverfahren:

- Angaben zum Verfahrensbetreiber

- Kontaktdaten des technischen Ansprechpartners auf Seiten des Verfahrensbetreibers

- Name und Versionsnummer des Prüfobjekts

- Auflistung aller Module des Prüfobjekts mit Namen und Version

2.2 Zertifizierungen

Falls das Prüfobjekt oder von diesem verwendete Bestandteile bereits zertifiziert wurden (Common Criteria, ISO, IT-Grundschutz, Technische Richtlinien, Pentests etc.), sind diese Zertifizierungen im Folgenden aufgeführt.

- Das Produkt besitzt folgende Zertifizierungen

2.3 URLs bzw. Online-Verfügbarkeit

Die Prüfung bezieht sich auf ein Prüfobjekt, welches den Nutzern Zugriff auf Dienste im E-Government-Bereich anbietet und besitzt dementsprechend Onlineschnittstellen, die bei der Prüfung zu berücksichtigen sind. Im Folgenden sind sämtliche URLs angeben, welche dabei benutzt werden.

- Das Produkt steht unter folgenden URLs zur Verfügung

2.4 Angestrebtes Vertrauensniveau

Bitte legen Sie fest, für welches Vertrauensniveau Sie eine Prüfung Ihres Verfahrens anvisieren. Ohne Angaben kann das höchstmögliche Vertrauensniveau in der Prüfung ermittelt werden. Dies kann allerdings erheblichen zeitlichen und organisatorischen Zusatzaufwand verursachen.

normal [ ]

substantiell [ ]

hoch [ ]

2.5 Auflistung der eingesetzten Protokolle

Bei einem Authentisierungsverfahren kommen meistens mehrere Protokolle zum Einsatz (z. B. TLS, SAML, Kerberos etc.). Um einen Überblick über die relevanten Protokolle zu geben, listen Sie bitte diese auf. Bitte ergänzen Sie nach Möglichkeit entsprechende Zusatzinformationen (z. B. SAML mit WebSSO-Profil).

- Das Produkt verwendet folgende Protokolle

_____
_____
_____
_____
_____

2.6 Festlegung des Authentisierungsmittels

Falls Ihr Authentisierungsverfahren mehrere Authentisierungsmittel unterstützt (z. B. Benutzername/Passwort, Softwaretoken und Hardwaretoken), muss hier eine Festlegung getroffen werden, welches Mittel als Grundlage für die Bewertung gelten soll. Eine Feststellung des Sicherheitsniveaus bezieht sich dann genau auf dieses bestimmte Authentisierungsmittel. Sollten mehrere Authentisierungsmittel bewertet werden, so müssen separate Vertrauensniveaubewertungen durchgeführt werden.

- Die Vertrauensniveaubewertung bezieht sich auf folgendes Authentisierungsmittel

_____

2.7 Anwendbarkeit der Module

Für die Feststellung des Vertrauensniveaus werden unterschiedliche Aspekte des Authentisierungsverfahrens betrachtet, die in mehrere spezifische Module unterteilt sind. Meistens sind nicht alle diese Aspekte auf ein bestimmtes Authentisierungsverfahren anwendbar. So ist z. B. das Modul zum Authentisierungsmittel Biometrie nur dann relevant, wenn Biometrie tatsächlich für die Authentisierung zum Einsatz kommt. Andernfalls muss dieses Modul ausgeblendet werden.

In diesem Abschnitt soll die Anwendbarkeit von spezifischen Modulen auf das Prüfobjekt beschrieben werden. Dabei soll klar ersichtlich sein, warum ein bestimmtes Modul anwendbar oder nicht anwendbar ist. Die nicht anwendbaren Module bleiben dann bei der Prüfung unberücksichtigt. Zu beachten ist, dass die generischen Anforderungen so definiert sind, dass sie grundsätzlich immer anwendbar sind. Die Entscheidung betrifft daher nur spezifische Module.

Modul	Anwendbarkeit	Begründung
Stellen		
Authentisierungsmittel Besitz		
Authentisierungsmittel Wissen		
Authentisierungsmittel Biometrie		
Multi-Faktor Authentisierung		
Authentisierungsmittel eID		
Authentisierungsmittel Softwaretoken		
Authentisierungsmittel OTP		
Authentisierungsmittel smsTAN		
Reaktivierung		

Tabelle 1: Anwendbarkeit von Modulen

2.8 Zeitraum der Prüfung

Die Prüfung fand vom TT.MM.JJJJ bis zum TT.MM.JJJJ statt.

2.9 Annahmen

Folgende Annahmen gelten für die in diesem Prüfbericht beschriebenen Ergebnisse.

ID	Annahme
A.1	

3 Generischer Anforderungskatalog

Dieses Kapitel beinhaltet mechanismenübergreifende Anforderungen, welche für sämtliche Verfahren relevant sind.

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

Referenz: 3.2.1 Identitätsprüfung

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

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.

Bewertung:

Begründung:

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 von Authentisierungsmitteln in geeigneter Weise bekannt gemacht werden.*

Bewertung:

Begründung:

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.

Bewertung:

Begründung:

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.

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

3.16 Generische Anforderung G16: Agilität

Referenz: 3.7.2 Agilität

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

Bewertung:

Begründung:

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* Endgeräts*] widersprechen.*

Bewertung:

Begründung:

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).*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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 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, etwa kryptographisch sichere Session-Identifier/-Cookies.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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

Bewertung:

Begründung:

4 Prüfobjektspezifische Module

Dieses Kapitel beinhaltet diejenigen spezifischen Anforderungen aus [TR-03107-1], welche für das Prüfobjekt relevant sind.

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.*

Sämtliche 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.

Bewertung:

Begründung:

4.2 Anforderungskatalog zum Authentisierungsmittel Besitz

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 [...]*

Bewertung:

Begründung:

4.2.2 Spezifische Anforderung B2: Anforderungen an den Token

Referenz: 3.3.1 Authentisierungsmittel

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

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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“)*

Bewertung:

Begründung:

4.3.2 Spezifische Anforderung W2: Anforderungen an das Wissen

Referenz: 3.3.1 Authentisierungsmittel

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

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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]).*

Bewertung:

Begründung:

4.4 Anforderungskatalog zum Authentisierungsmittel Biometrie

4.4.1 Spezifische Anforderung Bio1: Anforderungen an die Biometrie

Referenz: 3.3.1 Authentisierungsmittel

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

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

4.5 Anforderungskatalog zu Multi-Faktor Authentisierung

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.*

Bewertung:

Begründung:

4.5.2 Spezifische Anforderung MF2: Fehlschlagen eines Faktors

Referenz: 3.3.1.4 Zwei-Faktor-Authentisierung

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

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

4.5.4 Spezifische 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.*

Bewertung:

Begründung:

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 des Pseudonyms (dienste- und kartenspezifische Kennung).*

Bewertung:

Begründung:

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).*

Bewertung:

Begründung:

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 vor Auslieferung des Tokens gelöscht werden.*

Bewertung:

Begründung:

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.

Bewertung:

Begründung:

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.

Bewertung:

Begründung:

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 [...].*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

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.*

Bewertung:

Begründung:

5 Ergebnis der Prüfung

Dieses Kapitel beinhaltet das Ergebnis der Prüfung sowie etwaige Anmerkungen und Auflagen, welche bei der Bewertung zu beachten sind. Die Bewertung ist anhand einer Zusammenfassung aller Teilbewertungen vorzunehmen.

5.1 Vertrauensniveau des Prüfobjekts

Das Prüfobjekt hat folgendes Vertrauensniveau erreicht: _____

5.2 Begründung

Das Vertrauensniveau wird wie folgt begründet: _____

6 Informationen zu den Prüfern

Die Prüfung wurde durch die im Folgenden benannten Prüfer durchgeführt. Diese bestätigen durch ihre Unterschrift die Richtigkeit der im Dokument festgehaltenen Angaben.

1. Prüfer

Name:

Vorname:

Anschrift:

Unterschrift: _____

2. Prüfer

Name:

Vorname:

Anschrift:

Unterschrift: _____

7 Anhang

7.1 Fragebogen zur allgemeinen Beschreibung des Authentisierungsverfahrens

Dieser Prüfbericht bezieht sich auf eine konkrete Ausprägung des analysierten Authentisierungsverfahrens (nachfolgend Prüfobjekt). Dies bedeutet, dass das Ergebnis einen eindeutigen Bezug zu einem bestimmten Authentisierungsverfahren in einer bestimmten Konfiguration mitsamt dem zugehörigen E-Government-Onlinedienst hat. Insbesondere sind die Ergebnisse nicht notwendigerweise auf anderen Ausprägungen des Verfahrens, z. B. andere Versionsnummern oder Konfigurationen, übertragbar.

In diesem Fragebogen soll Ihr Authentisierungsverfahren eindeutig identifiziert werden. Die korrekte und ausführliche Beantwortung der Fragen ist essentiell, um weitere Nachfragen zu vermeiden. Um die Prüfung schnellstmöglich durchführen zu können, sollten Sie einen konkreten Ansprechpartner benennen, der für eine korrekte und zeitnahe Beantwortung der Fragen während der Prüfung zur Verfügung steht.

7.1.1 Allgemeine Angaben

Zur Prüfung wird folgendes Authentisierungsverfahren angemeldet:

- Angaben zum Verfahrensbetreiber

  _____

- Kontaktdaten des technischen Ansprechpartners

  _____

- Name und Versionsnummer des Prüfobjekts (falls zutreffend)

  _____

- Falls das Prüfobjekt aus mehreren Komponenten besteht, listen Sie bitte alle verwendeten Module hier auf

  _____
  _____
  _____
  _____
  _____

7.1.2 Zertifizierungen

Falls das Prüfobjekt oder von diesem verwendete Bestandteile bereits zertifiziert wurden (Pentests, ISO, etc.), tragen Sie diese bitte im Folgendem ein. Fügen Sie Ihrer Antwort bitte die entsprechenden Nachweise bei.

- Das Produkt besitzt folgende Zertifizierungen

  _____
  _____
  _____
  _____
  _____

7.1.3 URLs bzw. Online-Verfügbarkeit

Die Prüfung bezieht sich auf ein Prüfobjekt, welches den Nutzern Zugriff auf Dienste im E-Government-Bereich anbietet und besitzt dementsprechend Onlineschnittstellen, die bei der Prüfung zu berücksichtigen sind. Bitte geben Sie sämtliche verwendeten URLs hier an. Falls es bei der Authentisierung zur Kommunikation mit externen Serverbetreibern kommt, geben sie bitte jeweils auch den jeweiligen Kommunikationspartner an. Beispiel: *https://egov.meindienst.de (Adresse für Nutzer), https://oauth.dienstleister.de (Adresse des Authentisierungsfaktors x)*

- Das Produkt steht unter folgenden URLs zur Verfügung

_____
_____
_____
_____
_____

7.1.4 Allgemeine Beschreibung des Prüfobjekts

Bitte liefern Sie eine Übersicht über das Prüfobjekt und seine Komponenten. Hierbei ist, neben einer textuellen Beschreibung, auch ein Ablaufdiagramm der drei Funktionen Enrolment, Authentisierung und Revozierung wichtig. Welche Mechanismen gemäß [TR-03107-1] werden dabei genutzt? Welche Authentisierungsfaktoren kommen in Ihrem Authentisierungsverfahren zum Einsatz?

7.1.5 Angestrebtes Vertrauensniveau

Bitte legen Sie fest, für welches Vertrauensniveau Sie eine Prüfung Ihres Verfahrens anvisieren. Ohne Angaben kann das höchstmögliche Vertrauensniveau in der Prüfung ermittelt werden. Dies kann allerdings erheblichen zeitlichen und organisatorischen Zusatzaufwand verursachen.

normal [ ]

substantiell [ ]

hoch [ ]

7.1.6 Auflistung der eingesetzten Protokolle

Bei einem Authentisierungsverfahren kommen meistens mehrere Protokolle zum Einsatz (z. B. TLS, SAML, Kerberos etc.). Um einen Überblick über die relevanten Protokolle zu geben, listen Sie bitte diese auf. Bitte ergänzen Sie nach Möglichkeit entsprechende Zusatzinformationen (z. B. SAML mit WebSSO-Profil).

- Das Produkt verwendet folgende Protokolle

_____
_____
_____
_____
_____

7.1.7 Festlegung des Authentisierungsmittels

Falls Ihr Authentisierungsverfahren mehrere Authentisierungsmittel unterstützt (z. B. Benutzername/Passwort, Softwaretoken und Hardwaretoken), muss hier eine Festlegung getroffen werden, welches Mittel als Grundlage für die Bewertung gelten soll. Eine Feststellung des Sicherheitsniveaus bezieht sich dann genau auf dieses bestimmte Authentisierungsmittel. Sollten mehrere Authentisierungsmittel bewertet werden, so müssen separate Vertrauensniveaubewertungen durchgeführt werden.

- Die Vertrauensniveaubewertung bezieht sich auf folgendes Authentisierungsmittel

_____

7.1.8 Nutzung von externen Stellen

Die [TR-03107-1] berücksichtigt neben dem Inhaber des Authentisierungsmittels und der vertrauenden Entität auch weitere externe Stellen, die z. B. für Enrolment, Identitätsprüfung, Ausgabe der Authentisierungsmittel, Sicherung von Kommunikationsbeziehungen oder Speicherung von Daten zuständig sein können. Diese Stellen müssen vom Hersteller identifiziert und benannt werden. Im weiteren Verlauf der Vertrauensniveaufeststellung werden hierzu gesonderte Fragen gestellt.

Bitte benennen Sie daher hier alle Stellen, die im Sinne der [TR-03107-1] relevant sind.

7.1.9 Reaktivierung

Die [TR-03107-1] stellt besondere Anforderungen an die Rücknahme einer Sperrung. Sollte eine Rücknahme möglich sein, werden auch entsprechende Fragen für die Bewertung gestellt. Geben Sie bitte an, ob eine Reaktivierung in Ihrem Produkt vorgesehen ist.

Reaktivierung ist vorgesehen [ ]

Reaktivierung ist nicht vorgesehen [ ]

7.2 Prüfobjektbezogener Fragenkatalog

Die Bewertung wird anhand der folgenden Fragen vorgenommen.

7.2.1 Generische Fragen

ID	Frage
G1 3.1	Liegt für die Identitätsprüfung eine Bewertung gemäß [TR-03147] vor? Wie lautet ggf. das Endergebnis dieser Bewertung?
G2 3.2	Mit welchen Verfahren wird sichergestellt, dass verwendete Authentisierungsmittel nur an die dafür berechtigten Nutzer ausgegeben werden? Falls keine Ausgabe des Authentisierungsmittels seitens des Prüflings erfolgt, sondern stattdessen ein beim Benutzer bereits vorhandenes Authentisierungsmittel verwendet wird, wie erfolgt die Bindung des Authentisierungsmittels an den Nutzer?
G3 3.3	*Nur relevant, falls das Vertrauensniveau hoch angestrebt wird* Ist eine explizite Aktivierung eines oder mehrerer der Authentisierungsmittel erforderlich? Falls ja, wie ist diese Aktivierung jeweils ausgestaltet?

G4 3.4	Wie werden dem Authentisierungsmittelinhaber Geschäftsbedingungen sowie notwendige Verhaltensregeln zum Umgang mit den Authentisierungsmitteln übermittelt?
G5 3.5	Wie werden alle betroffenen Stellen und Authentisierungsmittelinhaber über Änderungen im Umgang mit den Authentisierungsmitteln oder notwendigen Verhaltensregeln informiert? Bitte benennen Sie dabei insbesondere, ob die Benachrichtigung aktiv erfolgt, oder die Stellen sich selbst regelmäßig informieren müssen.
G6 3.6	Gegen welches Angriffspotential (*enhanced-basic*, *moderate* oder *high* gemäß [CC] / [CEM]) ist das eingesetzte Authentisierungsprotokoll geschützt? Wurden für kryptographische Verfahren entsprechende Sicherheitsbeweise durchgeführt?
	Wenn keine Nachweise zum Schutzniveau vorliegen, muss eine Beschreibung des Authentisierungsprotokolls zur Verfügung gestellt werden. Diese soll ausreichend detailliert sein, damit der Prüfer eine Einschätzung selbstständig vornehmen kann. Z. B. können hierfür weitere Dokumente angegeben werden, die das Authentisierungsprotokoll technisch beschreiben. Sollten zudem noch Sicherheitsbeweise existieren, so sollen diese ebenfalls angegeben werden.
G7 3.7	Welche der eingesetzten Mechanismen / Protokolle verwenden Forward Secrecy? Legen Sie ggf. dar, ob Forward Secrecy garantiert oder nur optional ist.
G8 3.8	*Nur relevant, falls Vertrauensniveau substantiell oder hoch angestrebt wird* Wie kann das von Ihnen eingesetzte Authentisierungsprotokoll nachweisen, dass sich die Authentisierungsmittel im Augenblick der Authentisierung unter Kontrolle des Nutzers befinden? Wird dieser Nachweis für jede Authentisierung neu erzeugt?
G9 3.9	Wie kann ein Nutzer sein Authentisierungsmittel bei Bedarf (z. B. im Falle der Kompromittierung oder Verlust) sperren? Bitte machen Sie eine genaue Angabe zu allen vorgesehenen Sperrmöglichkeiten. Ist für die Sperrung das Authentisierungsmittel erforderlich (z. B. für das Anmelden am Self-Service)?
	Wie viel Zeit wird für eine effektive Sperrung eines Authentisierungsmittels nach der Sperrmeldung durch den Nutzer maximal benötigt? Nach [TR-03107-1], „*eine Sperrung ist effektiv zu dem Zeitpunkt, an dem die Sperrinformation für vertrauende Entitäten zur Verfügung steht.*“
	Bitte wählen Sie, zu welchen Zeiten die Sperrung durch den Nutzer möglich ist: • [ ] während der üblichen Geschäftszeiten (bitte Zeiten angeben) • [ ] jederzeit • [ ] jederzeit und allgemein bekannt (z. B. unmittelbar auf der Online-Präsenz des Dienstes ersichtlich)

G10 3.10	Wie werden die Möglichkeiten zur Übermittlung der Sperrmeldung den Nutzern von Authentisierungsmitteln bekannt gemacht? Mit Hilfe von welchen öffentlichen Kommunikationswegen werden die Sperrmöglichkeiten bekannt gemacht?
G11 3.11	Wie erlangt der Vertrauensdienst Kenntnis davon, dass der Nutzer nicht mehr zum Besitz des Authentisierungsmittels berechtigt ist oder sich seine relevanten / authentisierten Identitätsattribute ändern?
	Welche Identitätsattribute werden zu einer Identität erfasst? Bitte geben Sie eine Liste mit allen durch den Dienst erfassten Identitätsattributen und markieren Sie dabei, welche davon den minimalen konstanten Datensatz für eine Identität darstellen.
	Was passiert, wenn sich mindestens eines der Identitätsattribute ändert, das zum minimalen konstanten Datensatz gehört?
G12 3.12	Wie ist die Kommunikation zwischen den beteiligten Stellen gesichert? Bitte die Protokolle benennen, z. B. TLS mit oder ohne Client-Authentisierung
G13 3.13	Erläutern Sie die kryptographischen Mechanismen, Algorithmen, Schlüssellängen, Cipher Suites etc., die Sie einsetzen. Listen Sie diese nach Schnittstellen (URL angeben) bzw. Kommunikationsbeziehungen und auf allen Ebenen (Transport/Inhalt) eingesetzten kryptografischen Mechanismen gegliedert auf. Sofern die Verfahren gemäß Technischen Richtlinien des BSI formuliert sind, geben Sie diese zusätzlich an und schlüsseln Sie die Algorithmen in vergleichbarer Weise auf.
G14 3.14	Wie werden die privaten kryptographischen Schlüssel aller Entitäten gespeichert? Benennen Sie hierbei insbesondere auch die relevanten Zertifizierungen der verwendeten Komponenten.
	Wie wird sichergestellt, dass Auslesen, Kopieren oder unberechtigtes Nutzen von privaten Schlüsseln nicht möglich ist?
	Werden einzelne, zur Aufbewahrung privater Schlüssel genutzte Komponenten in geschützten Umgebungen (entsprechend [ISO27001]) betrieben? Falls ja, geben Sie bitte an, welche Komponenten dies sind und in welcher Umgebung sich diese jeweils befinden.
G15 3.15	Wie werden die öffentlichen Schlüssel, die für die Authentifizierung genutzt werden, gegen Manipulation geschützt? Benennen Sie hierbei insbesondere auch die relevanten Zertifizierungen der zur Aufbewahrung genutzten Komponenten.

	Werden einzelne, zur Aufbewahrung öffentlicher Schlüssel genutzte Komponenten in geschützten Umgebungen (entsprechend [ISO27001]) betrieben? Falls ja, geben Sie bitte an welche Komponenten dies sind und in welcher Umgebung sich diese jeweils befinden.
G16 3.16	Bitte beschreiben Sie in wie fern Ihr Authentisierungsverfahren modularisiert und konfigurierbar ist, sodass die kryptographischen Verfahren neuen kryptographischen Erkenntnissen angepasst werden können (z. B. Austausch von Schlüsseln, Austausch kryptographischer Primitiven und die Erhöhung von Schlüssellängen)? Bitte listen Sie auf, welche Parameter genau angepasst werden können (TLS Version, Cipher Suites, Elliptische Kurven, Hashalgorithmen, Schlüssellängen, xmlenc, xmldsig etc.). Sollten Sie externe Kryptografiebibliotheken einsetzen, listen Sie diese hier bitte auf.
G17 3.17	Gibt es spezielle Anforderungen an die Client-Systeme der Nutzer, welche Technischen Richtlinien oder Empfehlungen des BSI widersprechen (insbesondere den unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/empfehlungen_node.html bereitgestellten Empfehlungen)? Bitte benennen Sie sämtliche notwendige Abweichungen. Benennen Sie bitte weiterhin, welche Empfehlungen des BSI dabei berücksichtigt wurden (z. B. aktive Firewall, aktueller Virusscanner, letzte Sicherheitsupdates etc.)
G18 3.18	Wird der Inhaber des Authentisierungsmittels gegenüber dem Diensteanbieter eindeutig identifiziert? Falls ja, wie ist die Eindeutigkeit sichergestellt?
G19 3.19	Falls bei Ihrem Verfahren eine eindeutige Kennung verwendet wird, wie wird diese geschützt, sodass diese gegenüber Dritten nicht zugänglich ist?
G20 3.20	Wie wird sichergestellt, dass die Identifizierungen des Dienstes eindeutig einer bestimmten Session zugeordnet werden und auch nur dort gültig sind? Über welche organisatorische/technische/kryptographische Mechanismen findet die Bindung statt? Beschreiben Sie diese (inklusive Algorithmen, Schlüssellängen etc.).
G21 3.21	Wie findet die Bindung der übertragenen Identität bzw. eines vorangegangenen Identifizierungsprozesses an den Sitzungskontext statt? Wird die Identität einer Person eindeutig einer bestimmten Session zugeordnet? Wie wird sichergestellt, dass sie auch nur dort gültig ist? Über welche technische/kryptographische Mechanismen findet die Bindung statt? Beschreiben Sie diese (inklusive Algorithmen, Schlüssellängen etc.).
G22 3.22	*Nur relevant, falls datenschutzrechtlich relevante ID-Attribute übertragen werden.* Wie wird sichergestellt, dass Identitätsattribute erst nach erfolgter Freigabe durch den Nutzer übermittelt werden?

G23 3.23	Wie erfolgt eine Identifizierung des Dienstes gegenüber dem Nutzer bevor sich dieser authentisiert?
G25 3.25	Gegen welches Angriffspotential (*enhanced-basic*, *moderate* oder *high* gemäß [CC] / [CEM]) sind die eingesetzten Authentisierungsmittel geschützt? Bitte für jedes zum Einsatz kommende Authentisierungsmittel benennen und begründen.

Tabelle 2: Generische Fragen

7.2.2 Fragen zu Stellen

<table>
<tr><th>ID</th><th>Frage</th></tr>
<tr><td>S1

4.1.1</td><td>Bitte benennen Sie alle weiteren Stellen, die mit folgenden Aufgaben in Ihrem Authentisierungsverfahren betraut sind:
• Enrolment
• Identitätsprüfung
• Ausgabe der Authentisierungsmittel
• Sicherung von Kommunikationsbeziehungen
• Speicherung von Daten
• Andere relevanten Stellen
Bitte beachten Sie, dass für die Beantwortung dieser Frage nur externe Stellen relevant sind, also solche, die nicht dem Vertrauensdienstanbieter selbst angehören.
<table>
<tr><th>ID</th><th>Stelle</th></tr>
<tr><td>1</td><td></td></tr>
</table>
</td></tr>
</table>

	Bitte für jede der genannten Stellen, für welche die jeweilige Aussage zutrifft, die ihr zugeordnete ID eintragen: • Die Stelle ist eine Behörde oder juristische Person _____ • Die Stelle ist rechtlich befugt, ihre Aufgabe wahrzunehmen _____ • Die Stelle stellt für ihre Aufgabe ein Regelwerk auf und hält dieses ein. Bitte benennen Sie das Dokument und die aktuell gültige Versionsnummer. Besteht seitens der Stelle die Möglichkeit, dem Prüfer Einsicht in das Dokument zu gewähren (ggf. in gekürzter Form)? _____ • Die Stelle ist organisatorisch und technisch in der Lage, ihre Aufgaben auf Basis des Regelwerks wahrzunehmen _____ • Sämtliche anwendbare Technischen Richtlinien des BSI und relevante Standards werden durch die Stelle eingehalten. Dies betrifft insbesondere die Einhaltung der Vorgaben von [TR-02102] / [TR-03116] sowie die anwendbaren Module des IT-Grundschutzes _____ • Die Stelle hat genügend Ressourcen für die Erfüllung ihrer Aufgaben und ggf. für die Übernahme der sich aus den Aufgaben ergebender Haftung _____ • Die Stelle greift zur Erfüllung Ihrer Aufgaben auf externe Dritte zurück. Sind diese Dritten dem eigentlichen Dienst bekannt und erreichen sie mindestens das gleiche Vertrauensniveau? _____ • Die Stelle ist gemäß IT-Grundschutz [BSI100-2] oder [ISO27001] zertifiziert. Die Zertifizierung erstreckt sich über sämtliche für die Tätigkeit in Ihrem Authentisierungsverfahren relevanten Systeme und Komponenten _____ • Falls die Stelle nicht selbst eine Behörde ist: ist sie behördlich für die wahrgenommene Aufgabe nach geltenden Gesetzen / Prozessen anerkannt? Durch welche Behörde? _____

Tabelle 3: Fragen zu Stellen

7.2.3 Fragen zum Authentisierungsmittel Besitz

ID	Frage
B1 4.2.1	Wie kann der berechtigte Inhaber nach Erhalt erkennen, ob das Sicherungsmittel unberechtigt benutzt wurde?
B2 4.2.2	*Nicht relevant für Softwaretoken* Wie wird die Einmaligkeit und Nicht-Kopierbarkeit des Besitzes sichergestellt?
	Wie wird der Inhaber darauf hingewiesen, dass er den Besitz nicht weitergeben darf?
	Nicht relevant für Softwaretoken Wie wird verifiziert, ob der Besitz unter physischer Kontrolle des Inhabers ist?
	Wie wird der Inhaber darauf hingewiesen, dass der Besitz nur zur Authentisierung genutzt werden darf?
	Wie wird ein Verlust des Besitzes erkannt?
	Ist eine Missbrauchserkennung realisiert? Falls ja: wie?
	Ist eine Sperrung über ein eindeutiges Merkmal des Besitzes möglich? Falls ja: wie?
	Ist die Ausstellung eines neuen Besitztokens als Ersatz für ein gesperrtes Authentisierungsmittel möglich?
B3 4.2.3	*Nur relevant, falls das Vertrauensniveau hoch angestrebt wird* Wie kann der Inhaber des Authentisierungsmittels sicherstellen, dass der Besitztoken nur für eine intendierte Authentisierung aktiviert wird?

Tabelle 4: Fragen zum Authentisierungsmittel Besitz

7.2.4 Fragen zum Authentisierungsmittel Wissen

ID	Frage
W1 4.3.1	Wie kann der berechtigte Inhaber nach Erhalt erkennen, ob das Sicherungsmittel unberechtigt von einem Dritten eingesehen wurde?

	Wie werden diese Erkennungsmerkmale für eine unberechtigte Kenntnisnahme an den Inhaber kommuniziert?
	Wie wird der Inhaber über die auf seiner Seite notwendigen Schritte hingewiesen, falls eine unberechtigte Kenntnisnahme des Wissens festgestellt wird?
W2 4.3.2	Wie wird sichergestellt, dass das Wissen nur dem Inhaber und ggf. der verifizierenden Entität bekannt ist?
	Wird das Wissen zu irgendeinem Zeitpunkt ungesichert übertragen oder gespeichert?
	Können die Mitarbeiter oder Dienstleister des Verfahrensbetreibers einen Zugriff auf ungesichertes Wissen erhalten?
	Wie wird der Inhaber darauf hingewiesen, dass das Wissen nicht weitergegeben werden darf?
	Wie wird der Inhaber darauf hingewiesen, dass das Wissen nur zur Authentisierung genutzt werden darf?
	Wie wird der Inhaber darauf hingewiesen, dass der gleiche Wissens-Token nicht noch für andere Dienste verwendet werden darf?
	Wird der Inhaber darauf hingewiesen, dass er den Wissens-Token nicht aufschreiben oder in der Cloud speichern soll? Gibt es besondere Ausnahmen, die erlauben, das Wissen aufzuschreiben?
	Ist eine Missbrauchserkennung realisiert? Falls ja, wie?
	Ist Sperren des zugehörigen Accounts (bei entfernter Verifikation durch Server) bzw. Besitzes (bei lokaler Verifikation durch Besitztoken) bei Missbrauchsverdacht möglich?
	Ist Setzen eines neuen Passworts / einer neuen PIN als Ersatz für gesperrtes Passwort / PIN möglich?
W3 4.3.3	*Diese Anforderung gilt nur für Passwort-basierte Sicherungsfaktoren.* Nur bei Nutzung von Wissen als alleinigem Sicherungsfaktor: Wie sind die Anforderungen aus Maßnahme M 2.11 „Regelung des Passwortgebrauchs“ der IT-Grundschutz-Kataloge des BSI (siehe [BSI-GS]) auf Diensteseite umgesetzt? Wie werden die durch den Nutzer beeinflussbaren Regelungen forciert?

W4 4.3.4	Ist ein Fehlbedienungszähler implementiert? Wie viele Versuche lässt er zu? Wie viele Stellen hat das Passwort/die PIN mindestens? Welcher Zeichensatz ist erlaubt?
	Wenn kein Fehlbedienungszähler vorhanden ist, welcher andere wirksamer Schutz ist gegen Brute-Force Angriffe implementiert?

Tabelle 5: Fragen zum Authentisierungsmittel Wissen

7.2.5 Fragen zum Authentisierungsmittel Biometrie

ID	Frage
Bio1 4.4.1	Wird Lebenderkennung bei Authentisierung durchgeführt? Falls ja, wie?
	Wird das biometrische Merkmal ausschließlich für die Authentisierung verwendet?
	Ist eine Missbrauchserkennung realisiert? Falls ja, wie?
	Ist Sperren des zugehörigen Accounts (bei entfernter Verifikation durch Server) bzw. Besitzes (bei lokaler Verifikation durch Besitztoken) möglich?
	Wie ist eine Registrierung und Nutzung eines anderen biometrischen Merkmals als Ersatz für ein gesperrtes Merkmal realisiert?
Bio2 4.4.2	Bitte benennen Sie die ermittelte False Acceptance Rate. Wie wurden diese ermittelt?

Tabelle 6: Fragen zum Authentisierungsmittel Biometrie

7.2.6 Fragen zur Multi-Faktor Authentisierung

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

ID	Frage
MF1 4.5.1	*Nur relevant, falls Wissen in Kombination mit Besitz verwendet wird. Sonst ist die Frage nicht anwendbar.* Wie sind die Sicherungsfaktoren miteinander verknüpft?
MF2 4.5.2	Wie wird sichergestellt, dass das Fehlschlagen eines Authentisierungsversuchs nicht einem einzelnen Authentisierungsfaktor zugeordnet werden kann?
MF3	Wie wird verhindert, dass bei einem einzelnen Angriff auf die Nutzerumgebung das gesamte Verfahren kompromittiert werden kann? Bitte berücksichtigen Sie bei Ihrer Antwort sowohl die Aufbe-

4.5.3	wahrung der Faktoren, als auch deren Einsatz während des Authentisierungsvorgangs.
MF4 4.5.4	Auf welchen Übermittlungswegen werden dem Nutzer die Authentisierungsmittel bereitgestellt? Bitte für jedes Authentisierungsmittel einzeln benennen.

Tabelle 7: Fragen zur Multi-Faktor Authentisierung

7.2.7 Fragen zum Authentisierungsmittel eID

ID	Frage
eID1 4.6.1	Auf welche Art und Weise wird die eID-Funktion in Ihrem Prüfobjekt genutzt? Ist die Verwendung der eID-Funktion für jeden einzelnen Authentisierungsvorgang vorgesehen?

Tabelle 8: Fragen zum Authentisierungsmittel eID

7.2.8 Fragen zum Authentisierungsmittel Softwaretoken

ID	Frage
SW1 4.7.1	Liegen die privaten kryptographischen Schlüssel auch außerhalb des Tokens vor (beispielsweise für Key-Backup oder Key-Escrow)?
	Wird der Nutzer darauf hingewiesen, dass er diese auch bei gegebenen technischen Möglichkeiten nicht extrahieren darf?
	Welche Schlüsselableitungsfunktion wurde implementiert, um Brute-Force Angriffe abzuwehren? Welchen Rechenaufwand und Speicherplatz erfordert diese?
	Wie werden die Benutzer verpflichtet, keine leicht zu erratenden Passwörter („Trivialpasswörter“) zu wählen? Bietet das System Hilfestellungen wie starke Passwörter gewählt werden können?
	Wenn der Token auf dem Computersystem gespeichert wird, wie ist er vor Kopieren oder Export geschützt (z. B. Windows Zertifikatsspeicher, macOS Schlüsselbund)?
	Werden bestimmte Anforderungen an die Nutzergruppen gestellt, die den Zugriff auf das Computersystem regeln?

ID	Frage
SW2 4.7.2	In welcher Umgebung wird das Schlüsselmaterial erzeugt? Sollte die Erzeugung außerhalb des Tokens erfolgen, wann werden die vorliegenden privaten Schlüssel gelöscht?

Tabelle 9: Fragen zum Authentisierungsmittel Softwaretoken

7.2.9 Fragen zum Authentisierungsmittel OTP

ID	Frage
OTP1 4.8.1	Wie werden die TANs generiert? Bitte beschreiben Sie insbesondere, wie und welche Vorgangsdaten in die Erzeugung der TAN eingehen. Wie werden diese dem Inhaber angezeigt?
OTP2 4.8.2	*Nur relevant, falls die Vertrauensniveaus substantiell oder hoch angestrebt werden* *Nicht anwendbar, falls keine TAN-Generatoren zum Einsatz kommen.* Falls TAN-Generatoren eingesetzt werden (z. B. ChipTAN): Sind diese individuell? D.h. wie lässt sich sicherstellen, dass die Generatoren unterschiedlicher Inhaber nicht gegeneinander austauschbar sind? Wie ist die Erzeugung der TAN geschützt (bspw. durch eine PIN)?

Tabelle 10: Fragen zum Authentisierungsmittel OTP

7.2.10 Fragen zum Authentisierungsmittel smsTAN

ID	Frage
sms2 4.9.2	*Nur relevant, falls das Vertrauensniveau substantiell angestrebt wird* Wie wird dem Benutzer mitgeteilt, dass das Prüfobjekt nur mit Mobiltelefonen benutzt werden darf, die einen eingeschalteten und wirksamen Mechanismus zur Zugangssperre haben? Wird ein weiterer Faktor Wissen zusätzlich eingesetzt?
sms3 4.9.3	*Nur relevant, falls das Vertrauensniveau substantiell angestrebt wird* Wie wird sichergestellt, dass die primäre Verbindung zwischen Bürger und Behörde (d.h. die eigentliche Transaktion) nicht über das Mobiltelefon erfolgt, sondern über ein separates Endgerät und ein anderes Netzwerk? Wie wird dem Nutzer diese Notwendigkeit signalisiert?

Tabelle 11: Fragen zum Authentisierungsmittel smsTAN

7.2.11 Fragen zur Reaktivierung

ID	Frage
R1 4.10.1	Wie findet die Identifizierung des Inhabers eines Authentisierungsmittels für eine Rücknahme einer Sperrung statt?
R2 4.10.2	Wie wird sichergestellt, dass die Sicherheit der Authentisierungsmittel vor oder während einer Sperrung nicht kompromittiert wurde?

Tabelle 12: Fragen zur Reaktivierung

Literaturverzeichnis

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

[Bew/TR-03107] BSI: Bewertung von Authentisierungslösungen gemäß TR-03107: Anwendungs- und Vorgehensbeschreibung Version 0.6

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

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

[CC] CCRA: Common Criteria for Information Technology Security Evaluation 3.1

[CEM] CCMB: Common Methodologyfor Information TechnologySecurity Evaluation

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

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

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

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

[TR-03116] BSI: Technische Richtlinie TR-03116, Kryptographische Vorgaben für Projekte der Bundesregierung

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