Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

# Produktzertifizierung: Programm Beschleunigte Sicherheitszertifizierung (BSZ)

BSZ-Produkte

Version 2.1 vom 01.07.2024

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0)800 274 1000
E-Mail: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

# Änderungshistorie

| *Version* | *Datum* | *Name/Org-Einheit* | *Beschreibung* |
|---|---|---|---|
| 1.0 | 27.08.2021 | Referat SZ 33 | Erstausgabe der BSZ-Produkte |
| 1.1 | 01.02.2022 | Referat SZ 33 | Revision<br>• Austausch Dokumentenübersicht<br>• Änderung VB-Produkte *BSZ-NESAS* in VB-Produkte.PD<br>• Geschlechtergerechte Sprache<br>• Aufteilung des Ablaufs nach der Zertifizierungsentscheidung<br>• Änderung zur Meldung von Evaluierungsergebnissen an den Antragsteller<br>• Änderungen zur Beratung durch Prüfstellen |
| 1.2 | 01.05.2023 | Referat SZ 33 | Revision<br>• Zwei Stichpunkte in Hilfsmittel und eine Aufgabe für Antragsteller in Tabelle 1 ergänzt<br>• Überarbeitung Kapitel 5.2 und Anpassung in Unterabschnitt 3.3.1.3 für die Einführung OpenPGP als Verschlüsselungsverfahren für Kommunikation und Dokumentenaustausch<br>• Kapitel 5.6. (Kontaktregel zur Zertifizierungsstelle) hinzugefügt<br>• Redaktionelle Änderungen<br>• Kommunikation Schwachstellenmeldungen in Abschnitt 3.3.3 eingefügt<br>• Mechanismus zur Unparteilichkeit als Abschnitt 5.1.2 eingefügt<br>• Konkretisierung zu Updatepflicht bei Schwachstellen<br>• Aufteilung der 5 Prozessschritte aus Kapitel 3.3 in 3 Phasen |
| 2.0 | 01.11.2023 | Referat SZ 33 | Revision<br>• Unterabschnitt 3.3.1.2 Ergänzung SBOM<br>• EN 17640 [FiT CEM] als grundlegende Evaluierungsmethodologie eingeführt<br>• Geltungsbereich Highspeed Konnektor (HSK) für die Telematikinfrastruktur hinzugefügt |

| *Version* | *Datum* | *Name/Org-Einheit* | *Beschreibung* |
|---|---|---|---|
| 2.1 | 01.07.2024 | Referat SZ 33 | Revision<br>• Geltungsbereichs Komponenten im HAN des SMGW hinzugefügt<br>• Verweise auf deutsche Version der AIS B Dokumente aktualisiert |

*Tabelle 1: Änderungshistorie*

# Inhalt

# 1 Einleitung

Die Zertifizierung eines Produkts wird auf Veranlassung des Herstellers, der Vertreiberin bzw. des Vertreibers oder der Entwicklerin bzw. des Entwicklers von IT-Produkten durchgeführt.

Dieses Dokument richtet sich daher in erster Linie an alle Antragsteller für ein IT-Sicherheitszertifikat im Programm Beschleunigte Sicherheitszertifizierung (BSZ).

## 1.1 Zielsetzung und Eingliederung des Programms

Dieses Dokument beinhaltet detaillierte Anforderungen und Informationen als Ergänzung zum Dokument „Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleitungen“ [VB-Produkte.PD] für den Fall, dass sich der Antragsteller entschieden hat, eine Beschleunigte Sicherheitszertifizierung durchführen zu lassen. Hier findet man alle Informationen zur Durchführung des Verfahrens.

Eine Prüfstelle kann einen Hersteller auf Grundlage dieser Unterlagen zur Vorbereitung über den Ablauf eines Verfahrens informieren.

Es werden konkret die Aufgaben benannt, die berücksichtigt werden müssen, um den Regelungen und Anforderungen zum Verfahren gerecht zu werden. An den entsprechenden Stellen im Dokument wird z. B. auf Formulare oder andere Hilfsmittel hingewiesen, die besonders bei einer Erstzertifizierung hilfreich sind.

Die Beschreibung der verschiedenen Dokumentenkategorien befindet sich in der übergeordneten [VB-Produkte.PD].

Das Dokument „Verzeichnisse“ [Verzeichnisse] gibt einen Überblick über alle benötigten Hilfs- und Informationsquellen (Literaturverzeichnis) und enthält ein Stichwort- und Abkürzungsverzeichnis (Glossar).

# 2 Zertifizierungsprogramm

Dieses Programm beschreibt die Beschleunigte Sicherheitszertifizierung von IT-Produkten durch das BSI.

## 2.1 Beschleunigte Sicherheitszertifizierung von IT-Produkten

Die Beschleunigte Sicherheitszertifizierung (BSZ) im BSI stellt einen schlanken Ansatz zur Zertifizierung von IT-Produkten dar. Ziel der BSZ ist es, durch die Vermeidung von Formalismen und Kommunikationsschleifen und die Konzentration auf Prüfungen durch hochqualifizierte Experten die Dauer der einzelnen Zertifizierungsverfahren relativ gering und insbesondere planbar zu gestalten. Die BSZ setzt dazu die europäische Norm EN 17640 „Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte“ [FiT CEM] mit der Vertrauenswürdigkeitsstufe „hoch“ um. Das Verfahren ist vergleichbar mit dem französischen Zertifizierungsprogramm der CSPN (Certification de Sécurité de Premier Niveau) und es besteht ein Abkommen zur gegenseitigen Anerkennung der IT-Sicherheitszertifikate zwischen dem BSI und der französischen ANSSI (Agence nationale de la sécurité des systèmes d'information)[1]. Eine weitere europäische multilaterale Harmonisierung und Anerkennung von Zertifikaten im FiT CEM-Schema ist ein erklärtes Ziel.

### 2.1.1 Generelle Aspekte der Beschleunigten Sicherheitszertifizierung

Kern des Verfahrens sind vier Prüftätigkeiten, deren Reihenfolge aber nicht festgelegt ist: Prüfung der Installationsdokumentation, Prüfung der Konformität, Penetrationstesten und Bewertung der Implementierung kryptographischer Algorithmen. Der Umfang der Gesamtprüfdauer hängt von der Komplexität des IT-Produkts ab. Er wird im Rahmen der Auftaktbesprechung ermittelt und liegt grundsätzlich im Bereich von 15 bis 60 Personentagen bei Erstverfahren. Bei Wiederholungen, wie z. B. einer Rezertifizierung, kann der Zeitaufwand deutlich geringer sein, wobei die genaue Verteilung auf die einzelnen Prüftätigkeiten der Prüfstelle obliegt.

Für bestimmte Verfahrensschritte, Prüftätigkeiten oder Geltungsbereiche kann es zusätzliche Anforderungen geben. Diese werden in Anwendungshinweisen und Interpretationen zum Schema (AIS) als separate Dokumente von der Zertifizierungsstelle des BSI veröffentlicht. Themen der AIS-Dokumente sind z. B. Leitfäden zur Unterstützung der Antragsteller für die Bereitstellung der Nachweise wie das Dokument der Sicherheitsvorgaben, sowie verschiedene verfahrensbezogene Regelungen. Zur Abgrenzung von den AIS der BSZ zu anderen Zertifizierungsverfahren, wie z. B. (siehe [CC-Produkte]) sind die AIS für die Beschleunigte Sicherheitszertifizierung in dem Nummernkreis „B#“ organisiert, wobei # die laufende Nummer der AIS ist.

Die genannten Dokumente sowie weitere Informationen können von der Webseite des BSI im Themenbereich „Zertifizierung und Anerkennung“, Rubrik „Zertifizierung von Produkten“ abgerufen werden. Sie sind in den jeweiligen Evaluierungs- und Zertifizierungsverfahren entsprechend ihrer Einstufung (z. B. als Leitfaden oder verbindlich) anzuwenden.

Neben den Regularien muss eine Zertifizierung durch das BSI die Vorgaben des [BSIG] einhalten. Daraus resultiert ein Zertifizierungsvorbehalt bei öffentlichem Interesse nach § 9 Abs. 4 S.2 BSIG etwa, wenn sicherheitspolitische Interessen der Bundesrepublik Deutschland einer Zertifizierung entgegenstehen. Die Prüfung eines Zertifizierungsvorbehaltes erfolgt grundsätzlich vor Annahme eines Zertifizierungsantrages und abschließend vor der Erteilung eines Zertifikates.

Bezüglich der kryptographischen Algorithmen und Funktionen sind Rahmenbedingungen in spezifischen Vorgaben für den Geltungsbereich oder in der AIS B2 verankert und werden zu Beginn eines Antragsverfahrens festgelegt. Für die Auswahl von kryptographischen Algorithmen gilt der SOG-IS Kryptokatalog [SOGIS-ACM]. Eine Verwendung schwächerer oder proprietärer Algorithmen ist in der Regel nicht möglich.

[1] Mutual Recognition Agreement of Cybersecurity Evaluation Certificates issued under a Fixed-time Certification Process, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/BSZ/Abkommen_Anerkennung_ANSSI_BSI.pdf

Sofern kryptographische Protokolle nicht im Katalog enthalten sind, müssen sie dem Stand der Technik entsprechen und als sicher gelten.

Die formale Gültigkeit eines IT-Sicherheitszertifikates im Programm Beschleunige Sicherheitszertifizierung ist aufgrund des Technologiefortschritts grundsätzlich auf maximal zwei Jahre zeitlich befristet (siehe Abschnitt 5.4.2).

### 2.1.2 Produkte und Sicherheitsvorgaben

Bei der Beschleunigten Sicherheitszertifizierung wird das zu zertifizierende IT-Produkt grundsätzlich in einer bei Kunden häufig eingesetzten Konfiguration betrachtet (siehe Kapitel 3.2). Damit wird die Vergleichbarkeit von verschiedenen Beschleunigten Sicherheitszertifikaten für einen Produkttyp verbessert, dem Endkunden der Einsatz der zertifizierten Version erleichtert und gleichzeitig der Prozess der Produktzertifizierung effizienter gestaltet.

Das zu prüfende Produkt wird im Rahmen einer Beschleunigten Sicherheitszertifizierung als Evaluierungsgegenstand bezeichnet (engl. Target of Evaluation, TOE). Die Antragsteller beschreiben den TOE, dessen Sicherheitsfunktionen und die typische Einsatzumgebung in dem Dokument Sicherheitsvorgaben (engl. Security Target, ST). Das Dokument hat die zentrale Bedeutung für die Zielsetzung und Durchführung des Verfahrens. In diesem wird neben der Identifikation und Abgrenzung des TOE, das Sicherheitsproblem in Form von Angreifern, Werten, Annahmen und Bedrohungen für die Sicherheitsleistung des TOE begründet. Die Sicherheitsvorgaben sind nicht nur die Grundlage der Zertifizierung, sondern richten sich auch an Nutzerinnen und Nutzer des zertifizierten Produkts. Dazu soll es in natürlicher Sprache und verständlich für die typische Nutzergruppe sein. Details zur Erstellung von Sicherheitsvorgaben sind im Dokument [AIS B1] erläutert. Die Sicherheitsvorgaben werden im Falle eines erfolgreichen Abschlusses der Zertifizierung auf der Website der Zertifizierungsstelle veröffentlicht. Hierzu reicht der Antragsteller eine barrierefreie und von Metadaten, Versionstabellen, Änderungshinweisen und anderen Herstellereingaben bereinigte Version des Dokumentes ein.

Um einen Mindeststandard von Sicherheitsleistungen zu gewährleisten, muss der TOE die Mindestanforderungen bezüglich der Sicherheitsleitungen im jeweiligen Geltungsbereich erfüllen.

Nachbesserungen am TOE während des Verfahrens sind bei der Beschleunigten Sicherheitszertifizierung nicht vorgesehen und bedürfen im Einzelfall der Genehmigung durch die Zertifizierungsstelle.

## 2.2 Geltungsbereiche der BSZ

Die Beschleunigte Sicherheitszertifizierung erfolgt grundsätzlich nur in Geltungsbereichen, die von der Zertifizierungsstelle des BSI definiert wurden. Ausnahmen bedingen einen höheren Aufwand (insbesondere zum Aufbau des benötigten Fachwissens) und bedürfen der expliziten Zustimmung der Zertifizierungsstelle. Der gewünschte Geltungsbereich ist im Antrag anzugeben. Die Zertifizierung ist teilweise an Geltungsbereich spezifische Anforderungen geknüpft. Hiernach sind die nachfolgenden Geltungsbereiche definiert.

### 2.2.1 Geltungsbereich Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte

Dieser Geltungsbereich umfasst eine große Bandbreite von Produkten, die über Netzwerkschnittstellen mit der Außenwelt kommunizieren. Beispiele für typische Produkte hier sind

- IP basierte Netzwerk-Router,
- eingebettete und vernetzte industrielle Steuerungsgeräte,
- mobile Handhelds für Spezialaufgaben.

In diesem Geltungsbereich gelten die folgenden Anforderungsdokumente in der jeweils aktuellen Version:

- AIS B1, Anforderungen an ST und IAR
- AIS B2, Anforderungen an die Evaluierung kryptographischer Mechanismen gemäß BSZ

- AIS B3, Anforderungen an die Benutzeranleitung
- AIS B4, Anforderungen an die Evaluierung gemäß BSZ
- AIS B5, Anleitung zur Bestimmung des Aufwands für eine BSZ-Evaluierung
- AIS B6, Anforderungen an einen TOE

### 2.2.2 Geltungsbereich Highspeed Konnektor (HSK) für die Telematikinfrastruktur

Ein HSK ist eine performante und skalierbare Lösung für die Anbindung an die Telematikinfrastruktur des deutschen Gesundheitswesens (TI) und die Nutzung ihrer Anwendungen. Zertifikate in diesem Geltungsbereich sind ausschließlich für den Zulassungsprozess von Highspeed Konnektoren bei der gematik GmbH gedacht.

In diesem Geltungsbereich gelten die folgenden Anforderungsdokumente in der jeweils aktuellen Version:

- AIS B1, Anforderungen an ST und IAR
- AIS B2, Anforderungen an die Evaluierung kryptographischer Mechanismen gemäß BSZ
- AIS B3, Anforderungen an die Benutzeranleitung
- AIS B4, Anforderungen an die Evaluierung gemäß BSZ
- AIS B6, Anforderungen an einen TOE
- AIS B7, Verbindliche Anforderungen an einen Highspeed-Konnektor

### 2.2.3 Geltungsbereich Komponenten im HAN des SMGW

Dieser Geltungsbereich umfasst die Produkte im Home-Area-Netzwerk (HAN) des Smart-Meter-Gateway (SMGW), die nach der TR-03109-5 Kommunikationsadapter ihre IT-Sicherheit durch ein BSZ-Zertifikat nachweisen müssen.

In diesem Geltungsbereich gelten die folgenden Anforderungsdokumente in der jeweils aktuellen Version:

- AIS B1, Anforderungen an ST und IAR
- AIS B2, Anforderungen an die Evaluierung kryptographischer Mechanismen gemäß BSZ
- AIS B3, Anforderungen an die Benutzeranleitung
- AIS B4, Anforderungen an die Evaluierung gemäß BSZ
- AIS B5, Anleitung zur Bestimmung des Aufwands für eine BSZ-Evaluierung
- AIS B8, Requirements for evaluation according to the BSZ in the GB “Komponenten im HAN des SMGW”

# 3 Verfahren zur Zertifizierung

## 3.1 Beteiligte Stellen an einer Zertifizierung

Am Gesamtprozess der Zertifizierung sind drei Stellen beteiligt:

**Antragsteller**
ist ein Hersteller, Vertreiberin bzw. Vertreiber oder Entwicklerin bzw. Entwickler von IT-Produkten, die ein Zertifikat für ein IT-Produkt erlangen möchten.

**Die Prüfstelle**
wird von dem Antragsteller mit der Evaluierung des IT Produkts beauftragt. Dazu muss die Prüfstelle für den entsprechenden Geltungsbereich durch das BSI anerkannt sein. Die Zertifizierungsstelle des BSI hat den anerkannten Prüfstellen zur Durchführung von Evaluierungen verwaltungsrechtliche Nebenbestimmungen auferlegt. Dazu gehören auch Nebenbestimmungen, die die Sicherheit der Prüfstelle betreffen. Die Regelungen und Prozesse der Prüfstelle stellen sicher, dass die Vertraulichkeit in der Prüfstelle gewahrt ist. Die Befugnis für die Mitarbeiterinnen und Mitarbeiter der Prüfstelle bezieht sich jeweils auf bestimmte Technologien, Produktgruppen und Prüfaspekte. Für die Prüfstellenanerkennung ist es mit Zustimmung der Zertifizierungsstelle möglich, dass eine Prüfstelle, die sich im Anerkennungsprozess befindet, diese Rolle übernimmt, um ihre Eignung nachzuweisen.

**Die Zertifizierungsstelle des BSI:**
Die Mitarbeiterinnen und Mitarbeiter der Zertifizierungsstelle nehmen die von der Prüfstelle durchgeführte Evaluierung ab und fordern, falls notwendig, Nachprüfungen ein. Auf dieser Grundlage wird die Zertifizierungsentscheidung gefällt und ein entsprechender Bescheid ergeht dem Antragsteller.

## 3.2 Prüf- bzw. Evaluierungsgegenstand (TOE)

Die Prüfung und Bewertung wird als Evaluierung bezeichnet. Das zu prüfende Produkt wird daher im Rahmen einer Beschleunigten Sicherheitszertifizierung als Evaluierungsgegenstand bezeichnet (engl. Target of Evaluation, TOE). Neben der Festlegung des TOE (logisch und physische Abgrenzung und Identifizierung) wird zu Beginn eines Verfahrens in dem jeweiligen Dokument Sicherheitsvorgaben (engl. Security Target, ST) auch die beim Kunden häufig eingesetzte Konfiguration festgelegt und sichergestellt, dass sämtliche Sicherheitsfunktionalität auch testbar ist.

Zu dem TOE gehören auch die Handbücher, die auch in elektronischer Form vorliegen können. Insbesondere die ggf. notwendigen Schritte, die zur sicheren Konfiguration, d.h. Zustand gemäß ST, müssen darin beschrieben sein. Dies kann auch durch eine extra Konfigurationsanleitung (engl. Secure User Guidance, SUG) erfolgen.

Eine wesentliche Bedingung ist, dass die am Ende des Verfahrens im Zertifikat zu bestätigenden Sicherheitseigenschaften im Zusammenhang mit der Wahrung von Vertraulichkeit, Verfügbarkeit, Integrität oder Authentizität von zu schützenden Werten (engl. Assets) stehen, und dies zu Beginn in den verfahrensindividuellen Sicherheitsvorgaben festgelegt ist. Ferner müssen die Handbücher zweifelsfrei darlegen, wie der TOE in den zertifizierten Zustand gebracht wird. Schließlich muss der TOE den Updateprozess absichern.

## 3.3 Zertifizierungsprozess als Phasenmodell

Die Beschleunigte Sicherheitszertifizierung ist in drei Phasen, insgesamt fünf Prozessschritte aufgeteilt:

1. Vorbereitungs- und Antragsphase
2. Evaluierungsphase
    1. Auftaktbesprechung
    2. Evaluierung
    3. Abschlussinterview
3. Zertifizierungsphase

### 3.3.1 Vorbereitungs- und Antragsphase

Wenn ein Produkt mittels der Beschleunigten Sicherheitszertifizierung zertifiziert werden soll, ist der erste Schritt für einen potentiellen Antragsteller zu überprüfen, ob das Produkt die grundlegenden Anforderungen aus Abschnitt 2.1.2 erfüllt. Informationen zu Geltungsbereichen und Anforderungen an Produkte sind auf der Webseite www.bsi.bund.de/bsz bereitgestellt. Falls weitere Informationen benötigt werden, können diese bei der Zertifizierungsstelle des BSI erfragt werden.

Der nächste Schritt ist das Erstellen der Sicherheitsvorgaben und weiterer für den Zertifizierungsprozess benötigter Dokumente (siehe Unterabschnitt 3.3.1.2). Diese werden zum Teil zusammen mit dem Antragsformular (siehe Unterabschnitt 3.3.1.3) bei Antragstellung eingereicht und an die beauftragte Prüfstelle übergeben.

Die Prüfstelle überprüft die Dokumente und auf deren Basis den TOE, ob dieser sich grundsätzlich für ein BSZ-Verfahren eignet. Außerdem schätzt die Prüfstelle den Evaluierungsaufwand und überprüft, ob Ressourcen und Fähigkeiten für das angestrebte BSZ-Verfahren vorhanden und verfügbar sind. Basierend darauf wird ein Zeitplan für die Evaluierung erstellt.

Nach der Rückmeldung der Prüfstelle, dass der TOE zusammen mit den Dokumenten für ein BSZ-Verfahren geeignet ist, stellt der Antragsteller den Antrag auf eine Beschleunigte Sicherheitszertifizierung bei der Zertifizierungsstelle. Der Antrag wird anschließend formal und inhaltlich von der Zertifizierungsstelle geprüft.

Typischer Ablauf im Einzelnen:

| *Aufgaben Antragsteller/Hersteller* | *Hilfsmittel* | *Aufgaben Prüfstelle* | *Aufgaben Zertifizierungsstelle* |
|---|---|---|---|
| • TOE auf Zertifizierbarkeit prüfen<br>• ST und weitere Dokumente erstellen (siehe Unterabschnitt 3.3.1.2)<br>• Zusammenstellung von Kryptounterlagen<br>• Vertrag mit Prüfstelle schließen<br>• Antrag beim BSI stellen<br>• Anm.: Der Antragsteller sollte auch einen PGP-Schlüssel bereitstellen | • jeweils gültige AIS B Dokumente<br>• BSZ-EP<br>• Antragsformular<br>• öffentlicher PGP-Schlüssel der Zertifizierungs-stelle des BSI (auf der Webseite verfügbar) | • Vertrag mit Hersteller<br>• Eignungsprüfung von ST, TOE und weiterer Dokumente<br>• Bei Reevaluierung oder Rezertifizierung: Bewertung des Impact Analysis Reports (IAR)<br>• Aufwandsschätzung vornehmen<br>• Interne Planung vornehmen<br>• Analyse der Unabhängigkeit und Unparteilichkeit erstellen | • Ggf. Informations-gespräch zum Verfahren<br>• Bereitstellung von Informationen, z. B. auf www.bsi.bund.de/bsz<br>• Antrag prüfen |

*Tabelle 2: Aufgaben für die Vorbereitung und Antragstellung einer Zertifizierung im Programm BSZ*

### 3.3.1.1 Verkürzte Evaluierung bei Wiederholung des BSZ-Verfahrens

Wenn ein Produkt bereits ein BSZ-Verfahren durchlaufen hat, ist es möglich den Evaluierungsaufwand zu reduzieren (siehe Kapitel 4.2). In solchen Fällen ist eine Änderungsbeschreibung mit Auswirkungsanalyse (engl. Impact Analysis Report, IAR) verpflichtend. Ob und wie stark der Aufwand reduziert werden kann, wird im Einzelfall von der Zertifizierungsstelle unter Berücksichtigung der Empfehlung der Prüfstelle entschieden. Dies hängt nicht nur von der Art und Umfang möglicher Änderungen des Produkts ab, sondern auch davon, ob Evaluationsergebnisse aus den Vorverfahren übernommen werden. Es wird zwischen Rezertifizierung und Reevaluierung unterschieden. Bei der Rezertifizierung wurde das Produkt im Vorverfahren erfolgreich zertifiziert. Anders die Reevaluierung, bei dieser wurde das Vorverfahren mit einem negativen Ergebnis beurteilt.

Grundsätzlich ist eine Voraussetzung für eine verkürzte Rezertifizierung bzw. Reevaluierung, dass die Evaluierung durch die gleiche Prüfstelle und die gleichen Evaluatoren wie im vorherigen Verfahren durchgeführt wird. Abweichungen davon müssen begründet und durch die Zertifizierungsstelle genehmigt werden.

### 3.3.1.2 Antragstellereingaben

Für die Evaluierung im Rahmen der Zertifizierung eines IT-Produkts werden immer folgende Dokumente und Informationen verlangt:

- das Dokument Sicherheitsvorgaben (ST) (siehe Dokument [AIS B1]),
- einen abstrakten Überblick über die Architektur (z. B. welches Betriebssystem, welche zentralen Softwarekomponenten)
- eine Software Bill of Materials (SBOM) (siehe Dokument [AIS B1]),
- eine kurze technische Erläuterung, wie der Aktualisierungsmechanismus funktioniert,
- die gemäß Dokument [AIS B2] für die Kryptoanalyse benötigte Dokumentation bzw. Quell-/Pseudocode,
- eine Liste, in der grundsätzlich die Konformität zu den einzelnen Mindestanforderungen im jeweiligen Geltungsbereich bestätigt wird,

- eine Anleitung, wie der TOE in den zu zertifizierenden Zustand gebracht wird. Diese Anleitung (SUG) (siehe Dokument [AIS B3]) muss im Falle der erfolgreichen Zertifizierung dem TOE beigefügt werden.

Falls es sich bei dem Produkt um ein eingebettetes System (eng. Embedded System) handelt, werden zusätzlich folgende Gegenstände und Dienste verlangt:

- 3 TOEs inklusive der typischen Anleitungen und Handbücher (die Anzahl kann in einzelnen Geltungsbereichen abweichen, die am Ende der Evaluierung zerstört sein können,
- falls der TOE eine bestimmte Umgebung zur Funktion benötigt, sind diese für die Dauer der Evaluation bereitzustellen,
- grundsätzlich eine entschlüsselte Firmware.

Falls es sich bei dem Produkt um eine Softwareanwendung oder ein Produkt in einer virtualisierten Umgebung handelt, werden zusätzliche Eingaben und Informationen verlangt:

- das Installationspaket der Softwareanwendung/ der virtualisierten Umgebung,
- Spezifikation zu Hardware- und Softwareumgebung sowie Beschreibung von deren Abhängigkeiten (vgl. [AIS B6], Kapitel 3.5),
- eine Kompatibilitätsbeschreibung für unterschiedliche Hard- und Softwareumgebungen (vgl. [AIS B6], Kapitel 3.5).

Für die Evaluierung im Rahmen der Reevaluierung oder Rezertifizierung eines IT-Produkts werden zusätzlich folgende Dokumente und Informationen verlangt:

- eine Änderungsbeschreibung mit Auswirkungsanalyse (engl. Impact Analysis Report, IAR),
- ggf. gegenüber dem Vorverfahren aktualisierte Dokumente und Handbücher mit Änderungsverfolgung.

Bei Verfahren im Rahmen der Prüfstellenanerkennung muss der Antragsteller alle oben genannten Dokumente, Informationen, Gegenstände und ggf. auch Zugang zu Diensten, sofern nicht sowieso vorgesehen, auch der Zertifizierungsstelle zur Verfügung zu stellen, damit dort zur Qualitätssicherung des Verfahrens eine (ggf. stark verkürzte) parallele Evaluation bei Bedarf stattfinden kann.

#### 3.3.1.3 Antragsformular

Das Antragsformular erfordert Angaben, die für den Start des Verfahrens und seine Abwicklung benötigt werden. Das Formular steht auf der Internetseite des BSI unter www.bsi.bund.de/bsz zur Verfügung und enthält Erklärungen und Hinweise, die für das Ausfüllen behilflich sind.

Das Antragsformular bezieht sich ausschließlich auf die Beschleunigte Sicherheitszertifizierung eines IT-Produkts. Es enthält die Optionen für Erstzertifizierung, Rezertifizierung und Reevaluierung.

Im Antrag müssen Kontaktdaten für Anfragen bezüglich der Produktsicherheit angegeben werden. Die Kontaktdaten direkter Ansprechpartnerinnen und Ansprechpartner werden ausschließlich für die Kommunikation zwischen Zertifizierungsstelle und Antragstellern verwendet. Dazu muss zusätzlich noch eine spezifische, nicht personenbezogene E-Mail-Adresse angegeben werden, die bei positivem Ausgang des Verfahrens mit dem Zertifizierungsreport veröffentlicht wird, da die Angabe personenspezifischer Kontaktdaten für die Veröffentlichung nicht vorgesehen ist.

Weitere Anlagen sind

- die Sicherheitsvorgaben (engl. Security Target, ST),
- eine Liste der im TOE implementierten kryptographischen Mechanismen,
- das Handbuch zur sicheren Benutzung (engl. Secure User Guidance, SUG),
- Bedienungsanleitungen und Handbücher und
- für den Geltungsbereich „Highspeed-Konnektor“ die Einwilligungserklärung zur Einbeziehung der gematik.

Alle in Unterabschnitt 3.3.1.2 geforderten Dokumente kann die Zertifizierungsstelle, wenn für die Antragsbearbeitung notwendig, anfordern. Die Anlage Sicherheitsvorgaben wird bei Zertifikatserteilung auf der Website des BSI veröffentlicht. Weitere Informationen zur Veröffentlichung von Zertifizierungsunterlagen befinden sich in Kapitel 6.1.Wird ein Antrag auf Produktzertifizierung nicht durch den Hersteller, sondern durch einen Sponsor oder Vertreiber des Produkts gestellt, muss dem Antrag eine schriftliche Erklärung des Herstellers beigefügt werden, dass die Mitwirkung im Verfahren und die Bereitstellung der erforderlichen Produktnachweise sichergestellt ist.

Werden prüfungsrelevante Produktteile oder Nachweise durch Dritte entwickelt oder bereitgestellt oder verfügt der Antragsteller nicht über die Rechte an allen prüfungsrelevanten Nachweisen oder Teilen, so muss deren Mitwirkung sichergestellt werden. Dazu muss eine Erklärung der dritten Parteien vorgelegt werden, die die Mitwirkung im Verfahren bestätigt. Ein Beispiel hierfür kann sein, wenn ein Teil des TOE zugekauft wurde und der Antragsteller selbst nicht die Rechte an den Unterlagen hat, die für die Evaluierung erforderlich sind. Das Erklärungsschreiben muss die Organisation, die ihre Mitwirkung erklärt, eindeutig benennen und darlegen, auf welche Bestandteile des Produkts sich diese Erklärung bezieht.

Bei Rezertifizierung oder Reevaluierung des gleichen TOE ist die Änderungsbeschreibung mit Auswirkungsanalyse (engl. Impact Analysis Report, IAR) erforderlich. Im IAR werden sicherheitsrelevante Änderungen beschrieben. Diese Darlegung ist für die Wiederverwendbarkeit von früheren Prüfergebnissen erforderlich und ermöglicht folgend die Deltaplanung. Der Zertifizierungsantrag muss handschriftlich unterzeichnet werden und einen Firmenstempel enthalten. Er ist in schriftlicher Form zu leiten an:

Bundesamt für Sicherheit in der Informationstechnik
Referate SZ33– Zertifizierungsstelle
Postfach 20 03 63
53133 Bonn

Der Antrag kann vorab zusammen mit den notwendigen Anlagen per verschlüsselter E-Mail an bsz@bsi.bund.de gesendet werden. Die Anlagen sind grundsätzlich in elektronischer Form einzureichen. Auf der Internetseite des BSI steht dafür ein öffentlicher PGP-Schlüssel für das o.g. BSZ-Postfach zur Verfügung. Weitere Informationen zur elektronischen Dokumentenübertragung finden sich in Kapitel 5.2.

Die Prüfstelle stellt die für die Auftaktbesprechung benötigten Informationen, wie im Dokument [AIS B4] beschrieben, der Zertifizierungsstelle in elektronischer Form zur Verfügung.

Die Rahmenbedingungen zum Verfahren gemäß Kapitel 5.3 [VB-Produkte.PD], speziell zur Ablehnung eines Antrages, finden Anwendung.

## 3.3.2 Evaluierungsphase

### 3.3.2.1 Auftaktbesprechung

Die Auftaktbesprechung hat das Ziel, eine solide Grundlage für das Zertifizierungsverfahren zu legen, so dass die nachfolgende Evaluierung möglichst ohne Zeitverzug beginnen und das Verfahren planmäßig durchgeführt werden kann.

Grundsätzlich findet diese frühestens 10 Werktage nach Eingang der Sicherheitsvorgaben (ST) und aller weiteren Antragstellerdokumente durch die Antragstellerin bzw. den Antragsteller und 5 Werktage nach Eingang der Präsentationsvorlage durch die Prüfstelle im BSI statt. Es nehmen alle am Verfahren beteiligten Parteien, d. h. Antragsteller, Prüfstelle und Zertifizierungsstelle, teil.

Insbesondere sollen:

- Information zu den Sicherheitsanforderungen und der Konzeption des TOE vermittelt werden,
- die Sicherheitsvorgaben, insbesondere die zu betrachtende Konfiguration des TOE, final abgestimmt werden,
- die kryptographischen Verfahren erörtert werden,

- alle inhaltlichen und verfahrenstechnischen Fragen abgestimmt werden,
- die Evaluierungsplanung, inklusive Evaluierungsaufwand (Anzahl der anzusetzenden Evaluierungstage) abgestimmt werden,
- die weitere Zeitplanung zur Durchführung der Evaluierung und des Verfahrens abgestimmt werden und
- mögliche Hindernisse, soweit nicht schon in der Vorbereitung des Verfahrens (3.3.1) geschehen, identifiziert und Lösungsmöglichkeiten eruiert werden.

Im Falle einer Rezertifizierung oder Reevaluierung ist die Abstimmung zur Änderungsbeschreibung mit Auswirkungsanalyse (IAR) ein zentraler Punkt.

Typischer Ablauf im Einzelnen:

| ***Aufgaben Antragsteller/Hersteller*** | ***Hilfsmittel*** | ***Aufgaben Prüfstelle*** | ***Aufgaben Zertifizierungsstelle*** |
|---|---|---|---|
| • Bereitstellung notwendiger Informationen | • jeweils gültige AIS B Dokumente<br>• BSZ-Auftakt-Agenda-Vorlage<br>• BSZ-EP | • Vorstellung von ST und TOE<br>• bei Reevaluierung oder Rezertifizierung Vorstellung und Bewertung des IAR<br>• Vorstellung und Abstimmung des Testaufwands<br>• Abstimmung des Zeitaufwands und der zeitlichen Rahmenplanung<br>• Abstimmung der Konfiguration des TOE<br>• Abstimmen der kryptographischen Evaluierung<br>• Abstimmung offener Punkte | • Freigabe der TOE-Konfiguration<br>• Freigabe des Prüfaufwands<br>• Klärung offener Fragen<br>• Hinweise zum Testverlauf, z. B. bestimmte Testansätze, Kryptoprüfung |

*Tabelle 3: Die Auftaktbesprechung*

### 3.3.2.2 Evaluierung

Das Evaluierungs- und Zertifizierungskonzept basiert auf einer strengen Arbeitsteilung zwischen dem Antragsteller, den Evaluatorinnen bzw. Evaluatoren und dem Leiter bzw. der Leiterin des Evaluationsprojektes in der Prüfstelle, der zugewiesenen Zertifiziererin bzw. dem Zertifizierer und ggf. den benannten Prüfbegleitern für spezielle Prüfaspekte in der Zertifizierungsstelle. Um eine effiziente Prüfung zu ermöglichen, erfolgt in der Regel während der Evaluierungsphase keine weitere Kommunikation zwischen den Parteien. Evaluierungsergebnisse dürfen erst nach der finalen Bewertung des TOE und Abnahme des ETR mit dem Antragsteller oder Hersteller geteilt werden. Es ist der Prüfstelle ausdrücklich nicht gestattet, ihre Bewertung zwischenzeitlich gefundener Schwachstellen mit dem Antragsteller oder Hersteller abzustimmen.

In folgenden Situationen ist eine Kommunikation während der Evaluierungsphase zulässig bzw. erforderlich:

- Soweit für die Evaluierung erforderlich, kann die Prüfstelle technische Sachverhalte beim Antragsteller erfragen. Rückfragen von Seiten des Antragstellers (z. B. zum Sachstand) sind nicht erlaubt.
- Die Prüfstelle darf den Antragsteller über kurze Statusmeldungen bezüglich der Einhaltung des abgestimmten Zeitplans informieren. Bei sich abzeichnenden Verzögerungen gegenüber dem vereinbarten Zeitplan sind die anderen Parteien umgehend zu informieren.
- Bei wichtigen Befunden informiert die Prüfstelle die Zertifizierungsstelle umgehend. Nach Prüfung des Befundes entscheidet die Zertifizierungsstelle, ob sie den Antragsteller informiert bzw. durch die Prüfstelle informieren lässt. Ein Befund gilt hierbei als wichtig, wenn er mindestens eines der folgenden Kriterien erfüllt:
    - Der Befund stellt aus Sicht der Prüfstelle ein erhebliches Sicherheitsrisiko mit in der Praxis realistischen Angriffsszenarien eines bereits im Verkauf bzw. Einsatz befindlichen Produkts dar.
    - Der Befund stellt aus Sicht der Prüfstelle eine erhebliche Abweichung bzw. Schwachstelle dar, die eine Zertifizierung verhindert und dadurch eine erhebliche Veränderung am Produkt erfordert.

Die Evaluierung erfolgt nach den Vorgaben im Dokument der [AIS B4]. Die Prüfstelle ist angehalten, den zu Beginn des Verfahrens vereinbarten Zeitplan einzuhalten. Die Prüfstelle dokumentiert den im Rahmen der Evaluierung gefundenen Ergänzungsbedarf, die Fehler und Inkonsistenzen in den eingereichten Dokumenten sowie die am TOE festgestellten Schwachstellen und Abweichungen im Evaluierungsreport (engl. Evaluation Technical Report, ETR). Zusätzlich wird eine Bewertung der Befunde vorgenommen und zusammen mit einem Gesamturteil inklusive Zertifizierungsempfehlung im ETR dokumentiert.

Typischer Ablauf im Einzelnen:

| ***Aufgaben Antragsteller/Hersteller*** | ***Hilfsmittel*** | ***Aufgaben Prüfstelle*** | ***Aufgaben Zertifizierungsstelle*** |
|---|---|---|---|
| • Bereitstellung des TOE (Anzahl je nach Produkttyp und Geltungsbereichs)<br>• Bereitstellung unverschlüsselter Firmware<br>• Bereitstellung notwendiger Zusatz-Hard- & Software<br>• Ggf. Klärung von Rückfragen für die Installation von Infrastruktur | • AIS B3<br>• AIS B4 | **Prüfeinrichtung**<br>• Einrichtung des TOE gemäß SUG in der Prüfkonfiguration | • keine |
| • Ggf. beantworten von Rückfragen der Prüfstelle | • jeweils gültige AIS B Dokumente<br>• BSZ-ETR-Vorlage | **Evaluierung:**<br>• Entwicklung und Pflege der Prüfstrategie und Testplanung<br>• Ausführen der Evaluierung mit Konformitäts- und Penetrationstests<br>• Dokumentation der Ergebnisse | • keine |

| *Aufgaben Antragsteller/Hersteller* | *Hilfsmittel* | *Aufgaben Prüfstelle* | *Aufgaben Zertifizierungsstelle* |
|---|---|---|---|
| • keine | • AIS B4<br>• BSZ-ETR-Vorlage | **Berichte:**<br>• Erstellen des ETR<br>• Übersenden ETR an BSI-Zertifizierungsstelle<br>• Aktualisieren des ETR basierend auf Kommentierung durch BSI-Zertifizierungsstelle | • Prüfen des ETR<br>• Kommentierung des ETR |

*Tabelle 4: Aufgaben während der Evaluierung*

#### 3.3.2.3 Abschlussinterview

Zur Beurteilung der durch die Prüfstelle durchgeführten Evaluation wird ein Interview mit der Prüfstelle durchgeführt. In diesem Interview stellt die Prüfstelle ihr Vorgehen während Evaluation im Detail vor, präsentiert die Ergebnisse und nimmt eine detaillierte Bewertung der Ergebnisse vor. Die Zertifizierungsstelle hinterfragt kritisch das Vorgehen der Prüfstelle, um festzustellen, ob die durchgeführte Evaluation ausreichend für eine abschließende Bewertung des Evaluierungsgegenstandes ist. Außerdem hinterfragt die Zertifizierungsstelle die Bewertung der Ergebnisse und trifft die finale Zertifizierungsentscheidung.

Falls die Zertifizierungsstelle feststellt, dass es noch offene Fragen gibt, die durch zusätzliche Tests mit geringen Aufwand geklärt werden können, kann sie diese nachfordern. Der Umfang der zusätzlichen Tests ist begrenzt und diese sollen nur erfolgen, wenn sie zwingend notwendig für die Zertifizierungsentscheidung sind.

Typischer Ablauf im Einzelnen:

| *Aufgaben Antragsteller/Hersteller* | *Hilfsmittel* | *Aufgaben Prüfstelle* | *Aufgaben Zertifizierungsstelle* |
|---|---|---|---|
| • Keine | • AIS B4<br>• BSZ-ETR-Vorlage | • Vorstellung der Evaluierungsergebnisse<br>• Verteidigung der Prüfstrategie<br>• Unterstützung bei der Beurteilung der Befunde<br>• Beantwortung von Rückfragen<br>• Aktualisierung des ETR<br>• Ggf. (minimale) Nachevaluationen | • Kritische Bewertung von:<br>  • Ergebnissen<br>  • Strategien<br>  • Expertenauswahl<br>  • Beurteilung der Befunde<br>• Feststellung finale Einschätzung der Befunde<br>• Entscheidung zur Annahme des ETR |

*Tabelle 5: Aufgaben im Abschlussinterview*

### 3.3.3 Zertifizierungsphase

Nach der finalen Bewertung des TOE vervollständigt die Zertifizierungsstelle die Verfahrensunterlagen und informiert den Antragsteller über die Entscheidung. Es folgt die formale Anhörung des Antragstellers mit 14 tägiger Frist. Danach wird der Zertifizierungsbescheid versandt.

Bei positiver Entscheidung bezüglich der Zertifizierung wird die Zertifikatsurkunde und der Zertifizierungsreport angefertigt und zusammen mit dem Zertifizierungsbescheid an den Antragsteller

versandt. Nach Ablauf der Widerspruchsfrist und mit Zustimmung des Antragstellers wird Zertifikat und Zertifizierungsreport auf der BSI Webseite veröffentlicht.

Typischer Ablauf bei positiver Entscheidung im Einzelnen:

| ***Aufgaben Antragsteller/Hersteller*** | ***Hilfsmittel*** | ***Aufgaben Prüfstelle*** | ***Aufgaben Zertifizierungsstelle*** |
|---|---|---|---|
| • Keine | • BSZ-EP<br>• BSZ-ETR-Vorlage | • Abgenommenen ETR signieren und der Zertifizierungsstelle vorlegen | • Vollständigkeit des signierten Prüfberichts überprüfen |
| • Ggf. Entwurf des Zertifizierungsreports kommentieren<br>• Ggf. auf formale Anhörung reagieren *(Verkürzt Frist bis zur Zertifikatserteilung)* | • Keine | • Ggf. Entwurf des Zertifizierungsreportes kommentieren | • Zertifikatsurkunde, Zertifizierungsreport und Zertifizierungs-bescheid erstellen<br>• Ggf. Entwurf des Zertifizierungsreports zur Kommentierung versenden<br>• Formale Anhörung des Antragstellers zu Nebenbestimmungen und Auflagen im Bescheid *(Frist 14 Tage)*<br>• Postalische Zustellung von Zertifizierungs-bescheid und Zertifizierungsreport an den Antragsteller. *(Widerspruchsfrist 1 Monat oder Widerspruchs-verzichtserklärung)* |
| • Empfangsbestätigung an BSI senden<br>• 4 Wochen Zeit, schriftlich Widerspruch gegen die Zertifizierung-sentscheidung bei der Zertifizierungsstelle einzulegen. *(Bei Verzicht auf Widerspruch verkürzt sich die Frist zur Veröffentlichung)* | • Zeichen-ordnung | • keine | • Ggf. Widerspruch bearbeiten<br>• Nach Ablauf der Widerspruchsfrist ist der Bescheid bestandskräftig.<br>• Veröffentlichung des Zertifikats sowie des Zertifizierungsreports<br>• Postalischer Versand der Zertifikatsurkunde<br>• Wenn gewünscht Zertifizierungszeichen bereitstellen |
| • Aufwände des Verfahrens (Gebühren und Auslagen) dem BSI | • BMIBGebV | • Keine | • Kostenbescheid an Antragsteller versenden |

| *Aufgaben Antragsteller/Hersteller* | *Hilfsmittel* | *Aufgaben Prüfstelle* | *Aufgaben Zertifizierungsstelle* |
|---|---|---|---|
| erstatten (siehe Kapitel 5.5) | | | |
| • Alle evaluierungs-relevanten Nachweise und das evaluierte Produkt für den Zeitraum der Gültigkeit des Zertifikates plus 3 weitere Jahre archivieren | • Keine | • Alle evaluierungs-relevanten Nachweise archivieren<br>• Den TOE zur Archivierung dem Antragsteller aushändigen (es sei denn, es gibt eine andere Vereinbarung).<br>• Weitere Prüfunterlagen gemäß interner Regelungen oder vertraglichen Vereinbarung mit dem Antragsteller archivieren. | • Alle zertifizierungs-relevanten Nachweise archivieren |
| • Einhaltung der Nebenbestimmungen im Bescheid und der Regelungen der Zeichenordnung | • Zeichen-ordnung | • Keine | • Wenn relevant: Bearbeitung von Nachlieferungen aus Nebenbestimmungen |
| • Überwachung des Produkts auf mögliche Schwachstellen, siehe Abschnitt 5.4.3 | • Keine | • Keine | • Überwachung des Produkts auf mögliche Schwachstellen, siehe Abschnitt 5.4.3 |

*Tabelle 6: Aufgaben zum Abschluss des Verfahrens bei positiver Entscheidung*

Typischer Ablauf bei negativer Entscheidung im Einzelnen:

| *Aufgaben Antragsteller/Hersteller* | *Hilfsmittel* | *Aufgaben Prüfstelle* | *Aufgaben Zertifizierungsstelle* |
|---|---|---|---|
| • keine | • BSZ-EP<br>• BSZ-ETR-Vorlage | • Abgenommenen Prüfbericht signiert der Zertifizierungsstelle vorlegen | • Vollständigkeit des signierten Prüfberichts überprüfen |
| • Ggf. auf formale Anhörung reagieren | • Keine | • Keine | • Negativbescheid nach formaler Anhörung |
| • 4 Wochen Zeit, schriftlich Widerspruch gegen die Zertifizier-ungsentscheidung bei der Zertifizierungsstelle einzulegen. | • Keine | • Keine | • Ggf. Bearbeitung Widerspruch<br>• Nach Ablauf der Widerspruchsfrist ist der Bescheid bestandskräftig. |
| • Aufwände des Verfahrens (Gebühren und Auslagen) dem BSI erstatten (siehe Kapitel 5.5) | • BMIBGebV | • Keine | • Kostenbescheid an Antragsteller schicken |

| *Aufgaben Antragsteller/Hersteller* | *Hilfsmittel* | *Aufgaben Prüfstelle* | *Aufgaben Zertifizierungsstelle* |
|---|---|---|---|
| • Keine | • Keine | • Alle evaluierungs-relevanten Nachweise archivieren<br>• Den TOE zur Archivierung dem Antragsteller aus-händigen (es sei denn, es gibt eine andere Vereinbarung)<br>• Weitere Prüfunterlagen gemäß interner Regelungen oder vertraglichen Verein-barung mit dem Antragsteller archivieren | • Alle verfahrens-relevanten Nachweise archivieren |

*Tabelle 7: Aufgaben zum Abschluss des Verfahrens bei negativer Entscheidung*

#### 3.3.3.1 Abschlussdokumente

Der bei positivem Abschluss der Evaluierung von der Zertifizierungsstelle erstellte Zertifizierungsreport enthält neben einer sicherheitstechnischen Beschreibung des Produkts u. a. ausgewählte Angaben zum Ergebnis der Evaluierung, Hinweise und Auflagen zur Benutzung des zertifizierten Gegenstandes sowie Angaben zur Eignung der implementierten kryptographischen Mechanismen aus Sicht des BSI.

Weiterhin wird bestätigt, dass die Evaluierung nach den anerkannten Verfahren durchgeführt wurde, und dass die in den Sicherheitsvorgaben spezifizierten Sicherheitsanforderungen hinsichtlich Funktionalität und Prüfumfang erfüllt werden. Hinweise und Auflagen an den Anwender sind im Report enthalten, die für den Einsatz des Produkts in der zertifizierten Konfiguration einzuhalten sind.

Falls der Antragsteller der Veröffentlichung des Zertifizierungsreports nicht zustimmt oder widerspricht, kann mit dem Zertifikat nicht geworben werden.

Das Dokument Sicherheitsvorgaben ist als Anlage zum Zertifizierungsreport Teil der Veröffentlichung des Zertifizierungsergebnisses.

Der Zertifizierungsbescheid nebst etwaiger Nebenstimmungen und Auflagen gibt die finale Zertifizierungsentscheidung der Zertifizierungsstelle wieder.

Das Zertifikat und der Zertifizierungsreport können in deutscher oder englischer Sprache erstellt werden. Maßgeblich ist i. d. R. die für das Dokument Sicherheitsvorgaben vom Antragsteller gewählte Sprache. Falls der ETR nicht auf Deutsch vorliegt, kann die Zertifizierungsstelle eine deutsche Zusammenfassung der wichtigsten Punkte des ETR von der Prüfstelle verlangen. Falls die Sicherheitsvorgaben nicht auf Deutsch vorliegen, kann das BSI eine Übersetzung verlangen.

# 4 Aufrechterhaltung einer Zertifizierung

## 4.1 Aufrechterhaltung der Vertrauenswürdigkeit

Ein Zertifikat wird für eine bestimmte evaluierte Produktversion eines TOE erteilt. Daher gilt das erteilte Zertifikat nicht für die geänderte Version des TOE. Damit der geänderte TOE als zertifiziert deklariert werden kann, ist eine Rezertifizierung unter Berücksichtigung der jeweiligen Änderungen und der jeweils aktuellen Angriffstechniken erforderlich.

## 4.2 Rezertifizierung

Der grundsätzliche Ablauf einer Rezertifizierung ist wie bei einem Erstverfahren, bei geringen Änderungen und der gleichen Prüfstelle wie bei der Erstzertifizierung ist jedoch eine Verringerung des Testaufwandes möglich. Die Angriffsresistenz wird nach dem jeweils aktuellen Stand der Technik vollständig neu bewertet und die aktuelle Gültigkeit kryptographischer Algorithmen und Parameter berücksichtigt.

Antragsteller müssen eine Änderungsbeschreibung mit Auswirkungsanalyse (IAR, siehe Dokument [AIS B1]) dem Zertifizierungsantrag beifügen. Auf dieser Basis entscheidet die Zertifizierungsstelle unter Hinzuziehung der Prüfstelle über die erforderliche Änderung (Reduktion) des Testaufwands.

Auf Basis der Änderungen am Produkt (IAR) und den Herstellernachweisen wird zwischen Zertifizierungsstelle und Prüfstelle im Rahmen der Auftaktbesprechung festgelegt, welchen Umfang die Evaluierung hat, welche Prüfschritte erneut durchgeführt werden müssen, bzw. welche früheren Prüfergebnisse wiederverwendbar sind.

Diese Regelungen gelten auch analog für eine Reevaluierung, falls vorher eine vollständige Evaluierung mit negativem Ergebnis erfolgte.

Nach positivem Abschluss der Evaluierung werden die technischen Ergebnisse durch die Zertifizierungsstelle in einem aktualisierten Zertifizierungsreport dokumentiert und ein neues Zertifikat erteilt.

Die formale Gültigkeit eines Zertifikats sowie die sicherheitstechnische Bewertung des Produkts wird im Rahmen einer Rezertifizierung entsprechend angepasst.

# 5 Spezielle Rahmenbedingungen

## 5.1 Grundlage für die Zertifizierung

### 5.1.1 Nationale Zertifizierungspolitik für die Sicherheitszertifizierung von IT-Produkten durch das BSI

Die Dienstleistung der Beschleunigten Sicherheitszertifizierung von IT-Produkten durch das BSI wird als Antragsverfahren angeboten. Eine Zertifizierung kann erfolgen, wenn festgestellt wird, dass die jeweiligen Prüfvorschriften erfüllt sind und dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen (§ 9, Abs.4 Nr. 2 BSIG). Die Prüfung nach § 9, Abs.4 Nr. 2 BSIG erfolgt bei Antragsannahme jedoch vorbehaltlich einer abschließenden Entscheidung zum Zeitpunkt der Unterzeichnung eines Zertifizierungsbescheides und des Zertifikates.

Grundsätzlich sind die technischen Mindestanforderungen gemäß dem Dokument der [AIS B6] zu erfüllen.

Weitere aktuelle oder produkttypspezifische Informationen finden sich auf der Internetseite des BSI unter www.bsi.bund.de/bsz.

### 5.1.2 Mechanismus zur Sicherung der Unparteilichkeit

Gemäß DIN EN ISO/IEC 17065 ist die Zertifizierungsstelle verpflichtet, sich einen Mechanismus zur Sicherung der Unparteilichkeit zu erlassen. Im Programm der Beschleunigten Sicherheitszertifizierung von IT-Produkten wird die Unparteilichkeit der Zertifizierungsstelle durch folgenden Mechanismus gewährleistet:

Die Zertifizierungsstelle stellt durch Rotieren der Zertifiziererinnen und Zertifizierer für konkrete Prüfstellen bzw. Antragsteller sicher, dass keine festen Beziehungen zwischen den Zertifiziererinnen und Zertifizierern und Prüfstellen bzw. Antragstellern entstehen. In regelmäßigen stichprobenartigen Verfahrensaudits durch den Prozesseigner BSZ und das Qualitätsmanagement des BSI wird das unparteiliche Handeln aller Beteiligten überwacht und potenzielle Anhaltspunkte für Parteilichkeit und Einflussnahme konsequent verfolgt.

## 5.2 Vertraulichkeit und Dokumentenaustausch

Der Dokumentenaustausch zwischen Antragsteller, Prüfstelle und Zertifizierungsstelle erfolgt i. d. R. auf elektronischem Wege per verschlüsselter E-Mail. Dazu wird OpenPGP entsprechend der Empfehlungen aus TR-02102-1 eingesetzt. Für die Übermittlung des Antrags und der weiteren notwendigen Einreichungen sind die Antragsteller und Antragstellerinnen angehalten den unter den Antragsformularen verfügbaren öffentlichen Schlüssel für die Übermittlung an die E-Mailadresse: bsz@bsi.bund.de zu verwenden. Für den weiteren Austausch im Verfahren wird ein separater verfahrensbezogener OpenPGP-Schlüssel von der Zertifizierungsstelle erstellt und der Prüfstelle per E-Mail für die weitere Kommunikation im Verfahren bereitgestellt.

Für Dokumente, die in Papierform an das BSI geschickt werden oder die per Kurierversand direkt an der Pforte des BSI abgegeben werden, sowie für bereitgestellte DVD/CDs gelten die Regelungen im übergeordneten Dokument [VB-Produkte.PD].

## 5.3 Rahmenbedingungen zum Verfahren

### 5.3.1 Evaluierungs- und Zeitplanung

In der Auftaktbesprechung stellt die Prüfstelle das geplante Vorgehen während der Evaluierung, den geplanten Zeitaufwand und ihre Zeitplanung vor. Die Zertifizierungsstelle kann die Planung u. a. ablehnen, wenn sie unvollständig ist, kein Einvernehmen über die Planung erzielt werden kann oder wenn die Fachkompetenz der Prüfstelle nicht hinreichend nachgewiesen ist. Die Prüfstelle verpflichtet sich, Abweichungen von der vereinbarten Zeitplanung den anderen Beteiligten umgehend mitzuteilen.

### 5.3.2 Evaluierungsvertrag

Da eine durch das BSI nach § 9 Abs. 6 BSIG i. V. m. § 19 ff. BSI-ZertV anerkannte Prüfstelle zur Einhaltung der Vorgaben des Zertifizierungsschemas verpflichtet ist, darf der Evaluierungsvertrag keine der sachgerechten Evaluierung und Prüfbegleitung hinderlichen Regelungen enthalten, insbesondere keine Regelungen, die eine Informationsweitergabe zu Erkenntnissen aus der Evaluierung an die Zertifizierungsstelle behindern könnte. Der Vertrag muss berücksichtigen, dass sich im Auftaktbesprechung oder im laufenden Verfahren neue oder zusätzliche Sachverhalte (z. B. zusätzliche Penetrationstests, Korrekturen und Ergänzungen zum Prüfbericht wie von der Zertifizierungsstelle als erforderlich betrachtet, Workshops) ergeben können, welche die Evaluierungsaufwände beeinflussen.

### 5.3.3 Hilfestellungen und Beratung von Antragstellern und Herstellern

Bei der Erstellung der für die Zertifizierung erforderlichen Dokumente, kann der Antragsteller Beratungsleistungen z. B. bei anerkannten BSZ-Prüfstellen unabhängig von der Evaluierung beauftragen. Diese darf jedoch nicht in die Evaluierung eingebunden sein, um die Unabhängigkeit und Objektivität der Evaluierung nicht zu gefährden.

Die für die Evaluierung innerhalb des BSZ-Verfahrens vorgesehene Prüfstelle kann und soll die Dokumente bereits vor Antragstellung prüfen (siehe Dokument [AIS B4]). Hierbei ist zu beachten, dass als Rückmeldung nur eine reine Mängelliste ohne Hinweise zur Behebung der Mängel an den Antragsteller übergeben werden darf. Die Unabhängigkeit und Objektivität der Evaluierung muss gewährleistet bleiben.

Eine Ausnahme bildet hier die im Dokument [AIS B1] beschriebene Auflistung der kryptographischen Mechanismen (Algorithmen und Kommunikationsprotokolle). Hier kann die Prüfstelle basierend auf Informationen von Antragsteller oder Hersteller bei der Erstellung unterstützen. Zu beachten ist, dass die Unterstützung auf die Zusammenstellung der Liste begrenzt ist und die Unabhängigkeit und Objektivität der Evaluierung gewährleistet bleiben muss. Die Unterstützung bei Erstellung der Auflistung der kryptographischen Mechanismen ist gegenüber der Zertifizierungsstelle anzugeben.

Die für die Evaluierung innerhalb des BSZ-Verfahrens vorgesehene Prüfstelle kann den TOE bereits vor Antragstellung einer technischen Prüfung mit geringer Prüftiefe und ohne tiefgehende Tests der Sicherheitsfunktionen unterziehen. Hierbei ist das Ziel festzustellen, ob das TOE überhaupt die technische Mindestreife hat, um ein BSZ-Verfahren mit Erfolgsaussichten zu beginnen. Diese Prüfung ist kein Teil der Beschleunigten Sicherheitszertifizierung, insbesondere nicht der Evaluierungsphase. Es ist zu beachten, dass als Rückmeldung nur eine reine Mängelliste ohne Hinweise zur Behebung der Mängel an den Antragsteller übergeben werden darf. Eine solche technische Vorprüfung ist bei Antragstellung gegenüber der Zertifizierungsstelle anzugeben. Die Zertifizierungsstelle kann bei Bedarf Auskunft über Art und Umfang der Vorprüfung und der Rückmeldung verlangen. Die Unabhängigkeit und Objektivität der Evaluierung muss gewährleistet bleiben.

Die Prüfstelle muss gegenüber Zertifizierungsstelle ihre Unabhängigkeit von Antragsteller und Hersteller darlegen und ihre Unparteilichkeit versichern. Eine entsprechende Erklärung muss durch den Antragsteller bei Antragstellung eingereicht werden. Hilfestellungen und Prüfungen vor der Antragstellung durch die Prüfstelle müssen in der Erklärung angegeben werden.

### 5.3.4 Gültigkeit von Standards und Interpretationen

Mit der offiziellen Annahme eines Zertifizierungsantrages werden die relevanten Versionen der Prüfkriterien und Interpretationen (AIS) im Rahmen einer Auftaktbesprechung festgelegt. Ein Übergang auf neuere Versionen ist in gegenseitiger Abstimmung während des laufenden Verfahrens möglich.

AIS, die sich auf Angriffstechniken beziehen, müssen immer in der aktuell gültigen Version angewandt werden. Die Zertifizierungsstelle entscheidet hierzu im Einzelfall über die Anwendung der relevanten neuen Interpretationen.

Technische Richtlinien, internationale Vorgaben aus Anerkennungsabkommen und Algorithmenkatalogen, die nicht von der Zertifizierungsstelle verantwortet werden, finden grundsätzlich in der zum Zeitpunkt des Auftaktgesprächs gültigen Fassung Anwendung.

Die Einbeziehung kryptographischer Verfahren kann zusätzliche Begutachtungen durch das BSI einschließen. Das BSI kann die Einbeziehung kryptographischer Verfahren verweigern, insbesondere wenn ein öffentliches Interesse vorliegt, Fragen der nationalen Sicherheit betroffen sind oder proprietäre Algorithmen verwendet werden, zu denen keine hinreichende Sicherheitsaussage des BSI vorliegen.

### 5.3.5 Zertifizierungsnummer

Die Zertifizierungsnummer wird bei positivem Bescheid des Zertifizierungsantrages erteilt und wird zur eindeutigen Kennzeichnung der Zertifikatsunterlagen verwendet.

## 5.4 Rahmenbedingungen zur Aufrechterhaltung eines BSZ-Zertifikates

### 5.4.1 Gültigkeit

Ein Produktzertifikat bezieht sich nur auf die angegebene Version des evaluierten Produkts und wenn alle Auflagen hinsichtlich der Generierung, der Konfiguration und des Einsatzes des Produkts beachtet werden und das Produkt in der Einsatzumgebung betrieben wird, die im Zertifizierungsreport und in den Sicherheitsvorgaben beschrieben ist.

Ein Zertifikat bestätigt die Vertrauenswürdigkeit des Produkts gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da Angriffe mit neuen oder weiterentwickelten Methoden nach Erteilung möglich sind, wird der Antragsteller über Nebenbestimmungen verpflichtet, für die Zertifikatslaufzeit ein aktives Schwachstellenmanagement für das zertifizierte Produkt zu betreiben (siehe Abschnitt 5.4.3).

Auflagen für die Anwenderin oder Anwender ergeben sich aus dem Zertifizierungsreport und den evaluierten Handbüchern, inklusive SUG, falls vorhanden.

Angaben zur Einsatzumgebung des Produkts ergeben sich aus dem Zertifizierungsreport und aus den Sicherheitsvorgaben.

Auflagen für den Zertifikatsinhaber ergeben sich aus dem Zertifizierungsbescheid.

### 5.4.2 Zeitliche Befristung

Die Zertifizierungsstelle muss gemäß der rechtlichen Grundlage die formale Gültigkeit eines Zertifikates für die jeweiligen Geltungsbereiche der Zertifizierung zeitlich befristen. Dennoch bezieht sich die inhaltlich-technische Zertifikatsaussage zur Vertrauenswürdigkeit auf den Zeitpunkt der Ausstellung, da eine Vorhersage der Angriffsresistenz in die Zukunft schwierig ist und individuell sehr unterschiedlich sein kann. Die Gültigkeit der Laufzeit verwendeter kryptographischer Algorithmen oder Parameter abhängig vom Einsatzbereich des Produkts kann sich auf die Festlegung der formalen zeitlichen Befristung des Zertifikates auswirken. Dies ist im Zertifizierungsreport vermerkt.

Die inhaltlich-technische Zertifikatsaussage zur Vertrauenswürdigkeit ist auf den Zeitpunkt der Ausstellung des Zertifikates bezogen. Die formale Gültigkeit eines IT-Sicherheitszertifikates ist aufgrund des Technologiefortschritts grundsätzlich auf maximal zwei Jahre zeitlich befristet. Abweichende Fälle können aufgrund besonderer rechtlicher Rahmenbedingungen für bestimmte Produkttypen festgelegt werden.

### 5.4.3 Schwachstellenmanagement und Bereitstellung von Updates

Die Inhaberin oder der Inhaber eines IT-Sicherheitszertifikates nach BSZ ist verpflichtet, für die Laufzeit des Zertifikats ein aktives Schwachstellenmanagement für das zertifizierte Produkt zu betreiben. Dieses umfasst mindestens:

- das Bereitstellen einer Kontaktstelle, über die Endnutzerinnen oder Endnutzer Schwachstellen melden können,
- das aktive und fortwährende Überprüfen des Produkts auf Schwachstellen (z. B. durch Überwachung einschlägiger Schwachstellendatenbanken, die Bewertung und Behandlung gemeldeter Schwachstellen),
- das unverzügliche Informieren der Zertifizierungsstelle über bekannt gewordene Schwachstellen im zertifizierten Produkt,
- das zeitnahe Bereitstellen geeigneter Updates zur Behebung der bekannt gewordenen Schwachstellen über einen festgelegten, dem Endnutzer zugänglichen Distributionskanal (z. B. eine Download-Seite),
- das Informieren der Endnutzerinnen oder Endnutzer über die Verfügbarkeit von neuen Sicherheitsupdates (z. B. über einen Newsletter oder einen Change Log).

Bei Bekanntwerden von ausnutzbaren Schwachstellen erfolgt die Rücknahme bzw. Widerruf gem. §§ 48, 49 VwVfG des Zertifikats, wenn die Voraussetzungen für die Zertifizierung nicht (mehr) vorliegen. Das BSI empfiehlt Zertifikatinhaberinnen bzw. Zertifikatinhabern daher dringend, eine aktualisierte und schwachstellenbereinigte Produktversion zeitnah einer Rezertifizierung zu unterziehen.

Ebenso erfolgt die Rücknahme bzw. Widerruf gem. §§ 48, 49 VwVfG des Zertifikats, wenn der Inhaber eines IT-Sicherheitszertifikates nach BSZ seiner Verpflichtung nicht nachkommt, ein Schwachstellen-management wie oben beschrieben zu betreiben.

## 5.5 Kosten

Das BSI stellt dem Antragsteller eine Rechnung auf Basis der (BMIBGebV) in Rechnung. Dabei wird nach Aufwand abgerechnet. Die beratenden Vorgespräche mit dem BSI vor Antragstellung sind kostenfrei.

Die Abrechnung, der bei der Prüfstelle anfallenden Evaluierungskosten wird zwischen Antragsteller und Prüfstelle vertraglich vereinbart. Der Aufwand für die Evaluierung hängt von der Komplexität des TOE und dem Produkttyp ab und kann nicht pauschal beziffert werden. Die Prüfstellen können auf Anfrage Schätzwerte angeben oder erstellen entsprechende Angebote.

## 5.6 Kontakt zur Zertifizierungsstelle

Erster Ansprechpartner oder Ansprechpartnerin bei laufenden Zertifizierungsverfahren ist die zugewiesene Zertifiziererin oder der zugewiesene Zertifizierer. Die Kontaktdaten sind dem jeweiligen Schreiben zur Aufnahme des Verfahrens zu entnehmen.

Übergeordnete Fragen zur Zertifizierung oder zu den Prüfkriterien können adressiert werden an:

• E-Mail: bsz@bsi.bund.de oder an

• Organisationseinheit: referat-sz33@bsi.bund.de.

Telefonisch kann bei Nichterreichen der Zertifiziererin oder des Zertifizierers auch die zentrale Rufnummer des BSI - Telefon: +49 (0)800 274 1000 mit Nennung vom Zertifizierungsreferat SZ 33 oder das Geschäftszimmer SZ kontaktiert werden.

Dokumente zur Zertifizierung müssen an die zentrale E-Mail-Adresse: bsz@bsi.bund.de gesendet werden. Ein PGP-Schlüssel steht auf der Internetseite des BSI in der Rubrik Themen „Zertifizierung und Anerkennung /Zertifizierung von Produkten /Beschleunigte Sicherheitszertifizierung“ zur Verfügung.

# 6 Veröffentlichung der Zertifizierung

## 6.1 Veröffentlichung durch das BSI

Informationen zu zertifizierten Produkten werden vom BSI in folgenden, regelmäßig aktualisierten Publikationen veröffentlicht.

- BSI-Forum (Organ des BSI in der Zeitschrift KES): In dieser Publikation wird der Inhalt eines seit der letzten Ausgabe der Zeitschrift neu erteilten Zertifikates zusammenfassend dargestellt.
- Rubrik „Zertifizierung und Anerkennung“ auf den Internetseiten des BSI: Hier werden in Form von Übersichtslisten Zertifikate nach Produkttypen gegliedert aufgelistet und das Zertifikat, der Zertifizierungsreport, etwaige Ergänzungen und die Sicherheitsvorgaben (ST) zum Download angeboten. Die Sicherheitsvorgaben als Antragstellerdokument müssen den Vorgaben gemäß AIS B1 folgen.

Widerruft der Antragsteller schriftlich gegenüber dem BSI die im Antrag gemachte Zustimmung zur Veröffentlichung des Zertifizierungsergebnisses, erfolgt keine Nennung in den genannten Publikationen. In diesem Fall fällt das Zertifikat auch nicht unter die internationalen Anerkennungsvereinbarungen. Auch darf dann nicht mit dem Zertifizierungszeichen für das Produkt geworben werden.

# 7 Referenzen und Glossar [Verzeichnisse]

Das Dokument Verzeichnisse als Nachschlagewerk für Interessenten und Beteiligte an Zertifizierungs- und Anerkennungsverfahren [Verzeichnisse] gibt einen Überblick über alle benötigten Anforderungen, Quellen und Hilfsmittel mit einem Glossar- und Abkürzungsverzeichnis.

Die Listen im Bereich der Anforderungen, Quellen und Hilfsmittel sind als Stammliste zu verstehen und decken für sämtliche Anforderungen und Dokumente die Information über aktuelle Quellenhinweise ab.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Verzeichnisse_Nachschlagewerk.pdf?__blob=publicationFile&v=41.