Bundesamt
für Sicherheit in der
Informationstechnik

Anerkennung: Programm zur Anerkennung als Prüfstelle im Bereich Common Criteria

CC-Prüfstellen

Version 1.3 vom 19.03.2020

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-111
E-Mail: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	20.07.2015	Anerkennungsstelle S 25	Erstausgabe ersetzt „BSI 7125“ und das entsprechende Kapitel aus dem alten „Prog-Stellen“
1.0.1	08.08.2016	QMB D	Austausch der Abbildung 1: Zertifizierungs- und Anerkennungsprogramme (Dokumentenübersicht)
1.0.2	20.12.2016	QMB D	Austausch der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramm)
1.1	01.08.2017	Anerkennungsstelle D 25	Revision: • Ergänzung / Klarstellung zur Unabhängigkeit und Unparteilichkeit der Prüfstelle und der Evaluatoren und Überarbeitung Vorlage Unabhängigkeitserklärung • Klarstellung zu Aufgaben der Prüfstelle bei Verfahrensvarianten • Überarbeitung Technische Domänen • Anforderungen zur Meldung erfahrener Evaluatoren (neu) • Kap. 2.2 und 7.1 Aktualisierung wegen SOG-IS Anforderungen • Kap. 4.1.1 Ergänzung zu Unabhängigkeit und Unparteilichkeit • Kap. 4.1 Detaillierung der Anforderungen im Evaluierungs-Ablauf • Kap. 5.1 Ergänzung bzgl. Verfügbarkeit bei Audits, Unterbeauftragung und Nutzung externer Tools
1.2	02.07.2018	Anerkennungsstelle D 25	Revision: • Austausch der Abbildung 1: Zertifizierungs- und Anerkennungsprogramme (Dokumentenübersicht) • Klärung Ziel des Dokumentes • Klarstellungen zum Ablauf der Evaluierung und von Voraussetzungen und Randbedingungen • Ergänzungen zu Tools • Ergänzung zu Workshops • Änderung zu formalen Unterschriften • Änderungen bzgl. der neu erschienenen 17025 (Version, Begriff Unabhängigkeit und Unparteilichkeit)
1.3	19.03.2020	Anerkennungsstelle SZ 12	Revision: • Austausch der Abbildung 1: Zertifizierungs- und Anerkennungsprogramme (Dokumentenübersicht) • Begrifflichkeiten geändert:

Version	Datum	Name	Beschreibung
			Anforderungsdokumente sind Programme (insbesondere im Titel und in Kap. 2 „Anerkennungsprogramm“) • Hinweis zum RSS-Feed und auf das Dokument [CC-Evaluatoren] in Kap. 2 „Anerkennungsprogramm, • Workshops bei Zertifizierungsverfahren in Kap. 5.4 „Arbeitstreffen mit den Prüfstellen “, • weitere redaktionelle Anpassungen.

Inhaltsverzeichnis

Änderungshistorie ... 3
1 Einleitung ... 7
1.1 Zielsetzung des Dokuments CC-Prüfstellen ... 7
1.2 Eingliederung in die Dokumentenstruktur ... 8
2 Anerkennungsprogramm ... 9
2.1 Common Criteria (CC) ... 9
2.2 Common Criteria Technical Domains (Technische Domänen) ... 9
2.2.1 Smartcards and Similar Devices ... 10
2.2.2 Hardware and Security Boxes ... 10
2.3 Information Technology Security Evaluation Criteria (ITSEC) ... 10
3 Verfahren zur Anerkennung von CC-Prüfstellen ... 11
3.1 Zusätzlich notwendige Unterlagen zur Beantragung ... 11
3.2 Spezielle Informationen zur Systembegutachtung ... 11
3.2.1 Durchführung der Fachbegutachtungen ... 11
3.2.2 Durchführung der Begutachtung des Informationssicherheitsmanagementsystems ... 12
4 Aufrechterhaltung der Anerkennung ... 14
4.1 Anforderungen an den Ablauf der Evaluierung im Rahmen der Zertifizierung von Produkten, Schutzprofilen und Standorten ... 14
4.1.1 Aufgaben in der Vorbereitungsphase einer Produktevaluierung ... 14
4.1.2 Aufgaben in der Evaluierungsphase eines Produktes ... 18
4.1.3 Aufgaben in der Zertifizierungsphase eines Produktes ... 21
4.2 Fachbegutachtungen ... 22
4.3 Reanerkennung ... 22
5 Spezielle Rahmenbedingungen ... 23
5.1 Weitere Regelungen zur Zusammenarbeit ... 23
5.2 Unabhängigkeit und Unparteilichkeit der Prüfstelle und der jeweiligen Evaluatoren ... 25
5.3 Meldung weiterer CC-Evaluatoren ... 26
5.4 Arbeitstreffen mit den Prüfstellen ... 26
5.4.1 Arbeitstreffen (Workshops) innerhalb von Zertifizierungsverfahren ... 26
5.5 Verfahren bei Mängeln in der Evaluierung ... 27
6 Referenzen und Glossar ... 29
7 Weitere Hilfsmittel ... 30
7.1 Vorlage „Evaluierungsplan“ ... 30
7.2 Vorlage für Unabhängigkeits- und Unparteilichkeitserklärung der Prüfstelle als Anlage zum Evaluierungsplan ... 33

Abbildungsverzeichnis

Abbildung 1: Zertifizierungs- und Anerkennungsprogramme (Dokumentenübersicht) ... 8

Tabellenverzeichnis

Tabelle 1: Aufgaben bei der Fachbegutachtung ... 12

Tabelle 2: Aufgaben bei der Begutachtung des Informationssicherheitsmanagementsystems....13
Tabelle 3: Aufgaben in der Vorbereitungsphase einer Produktevaluierung....17
Tabelle 4: Aufgaben in der Evaluierungsphase eines Produktes....20
Tabelle 5: Aufgaben in der Zertifizierungsphase eines Produktes....21

1 Einleitung

Die Anerkennung einer Prüfstelle[1] wird auf Veranlassung des Inhabers oder der Geschäftsleitung einer Stelle durchgeführt.

Anerkannt werden Stellen, die von natürlichen oder juristischen Personen des Privatrechts betrieben werden. Hinsichtlich staatlicher Prüfstellen gelten ggf. abweichende Regelungen.

1.1 Zielsetzung des Dokuments CC-Prüfstellen

Dieses Dokument beinhaltet verpflichtende Anforderungen und weitere wichtige Informationen und Regelungen als Ergänzung zur übergeordneten „Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern“ [VB-Stellen]. Es richtet sich insbesondere an die Antragsteller, die sich dafür entschieden haben, eine Anerkennung im Bereich der Common Criteria (CC) (oder der Information Technology Security Evaluation Criteria (ITSEC)) durchführen zu lassen.

Es werden die speziellen Anforderungen mit detaillierten Hinweisen zu Verfahrensabläufen benannt, die ein Antragsteller berücksichtigen muss. An den entsprechenden Stellen im Dokument wird z.B. auf Formulare oder weitere Hilfsmittel hingewiesen, die insbesondere bei einer Erstanerkennung hilfreich sind.

1 Englischer Begriff bzw. Abkürzung "Evaluation Facility" or "IT-Security Evaluation Facility", ITSEF

1.2 Eingliederung in die Dokumentenstruktur

Einen Überblick über die zur Verfügung stehenden Dokumente sowie die Zertifizierungs- und Anerkennungsprogramme gibt die folgende Abbildung. Alle Dokumente stellen Informationen zielgruppenorientiert zur Verfügung.

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

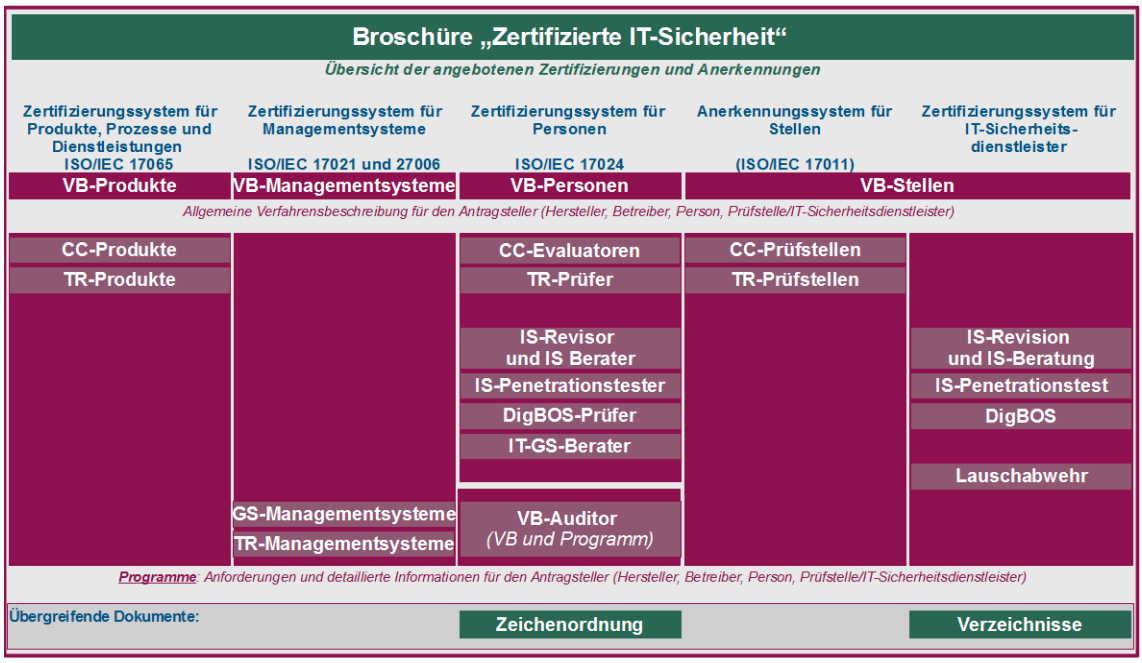

Abbildung 1: Zertifizierungs- und Anerkennungsprogramme (Dokumentenübersicht)

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

2 Anerkennungsprogramm

Das Anerkennungsprogramm beschreibt die folgenden Anerkennungsmöglichkeiten:

1) Anerkennung als Prüfstelle für Common Criteria (CC[2]).
2) Anerkennung als Prüfstelle für Common Criteria Technical Domains:
    1) Smartcards and Similar Devices
    2) Hardware and Security Boxes.
3) Ankerkennung als Prüfstelle Information Technology Security Evaluation Criteria [ITSEC].

Es besteht die Möglichkeit über einen RSS-Feed über Aktualisierungen informiert zu werden. Der RSS-Feed kann über die BSI Webseite abonniert werden.

Prüfstellen müssen die Anforderungen der DIN EN ISO/IEC 17025 [ISO 17025] einhalten sowie über die erforderliche Fachkompetenz im entsprechenden Programm verfügen.

Weiter müssen die Anforderungen des CCRA- und SOG-IS-MRA-Abkommens [CCRA], [SOG-IS-MRA] national vollständig umgesetzt werden.

Zudem muss das Informationssicherheitsmanagementsystem (ISMS) der Prüfstellen dem Dokument „Anforderungen an die Sicherheit von Stellen“ [AS-Stellen] entsprechen, wobei die Sicherheitsanforderungen als mindestens „hoch“ anzusetzen sind.

2.1 Common Criteria (CC)

Die „Common Criteria for Information Technology Security Evaluation (CC)“ stellen die international anerkannten Kriterien zur Prüfung und Bewertung der Sicherheit von IT-Produkten dar. Sie sind für die Bewertung der Sicherheitseigenschaften praktisch aller informationstechnischer Produkte geeignet. CC-Evaluierungen dürfen nur von CC-Evaluatoren durchgeführt werden, deren Fachkompetenz im Rahmen einer Kompetenzfeststellung beim BSI festgestellt wurde. Die Anforderungen an die Fachkompetenz des CC-Evaluators sind im Dokument „CC-Evaluatoren“ [CC-Evaluatoren] detailliert beschrieben. Zusätzlich muss die anerkannte Stelle die technischen Fachkompetenzen in den technischen Fachbereichen, in denen CC-Evaluierungstätigkeiten angeboten werden, nach dem Stand der Technik vorhalten und nachweisen. Diese Fachkompetenzen beziehen sich sowohl auf die Produkttechnologien als auch die Prüfmethoden.

Bei einer Erstanerkennung muss die Prüfstelle ihre Kompetenz durch eine erfolgreiche Probeevaluierung eines fiktiven Produktes (Prüfbaustein) nachweisen. Es müssen alle benannten CC-Evaluatoren gleichermaßen an der Evaluierung aktiv mitwirken.

2.2 Common Criteria Technical Domains (Technische Domänen)

Für bestimmte technische Bereiche ist eine im Rahmen des SOG-IS-Abkommens [SOG-IS-MRA] höherwertige Anerkennung nach definierten Technischen Domänen mit besonderen Rahmenbedingungen vorgesehen.

Voraussetzung für die Anerkennung der Stelle in einer Technischen Domäne ist die Anerkennung als Prüfstelle nach Common Criteria (CC) unter Berücksichtigung aller CC Assurance Komponenten aller EAL-Stufen, die im Anerkennungsbereich einer Technischen Domäne liegen.

2 Die Abkürzung CC schließt alle im Dokument [Verzeichnis] genannten Versionen der Common Criteria als auch den zugehörigen ISO Standard ISO 15408 ein. Gleiches gilt bzgl der Abkürzung CEM und dem ISO Standard ISO 18045

Derzeit sind die Technischen Domänen „Smartcards and Similar Devices“ und „Hardware Devices with Security Boxes“ definiert. Allgemeine Informationen und begleitende Dokumente zu den Technischen Domänen sind auf der SOG-IS-Internetseite [SOG-IS] erhältlich.

Die Prüfstelle muss mindestens zwei Personen beschäftigen, deren Fachkompetenz vom BSI festgestellt wurde. Die Anforderungen an die Fachkompetenz des CC-Evaluators sind im Dokument „CC-Evaluatoren“ [CC-Evaluatoren] detailliert beschrieben.

Die notwendigen Kompetenzen und Anforderungen sind umfassend in den offiziellen SOG-IS-Dokumenten Joint Interpretation Library Minimum ITSEF Requirements for Security Evaluations [SC&SD ITSEF Req; SecBoxes ITSEF Req], die für die jeweilige Technische Domäne gelten, geregelt und müssen umgesetzt und durch die Prüfstelle erfüllt werden.

2.2.1 Smartcards and Similar Devices

Bei den „Smartcards and Similar Devices“ sind wesentliche Sicherheitsfunktionalitäten des Evaluierungsgegenstands von Hardwareeigenschaften und den Sicherheitseigenschaften der spezifisch implementierten Embedded Software auf der Ebene des Mikrochips abhängig. Typischerweise muss verhindert werden, dass ein Angreifer, der physischen Zugriff auf ein solches Produkt besitzt,

- Kenntnis von darauf gespeicherten geheimen Informationen (z.B. kryptographischen Schlüsseln) erlangen bzw.
- Sicherheitsdienste (z.B. Authentisierungsprüfungen) manipulieren kann.

Bei der Evaluierung müssen alle für Smartcards und ähnliche Produkte spezifischen Angriffsmethoden betrachtet werden, auch solche, die besondere Kompetenzen, Einrichtungen oder Ressourcen benötigten. Die Besonderheit liegt darin, dass unterschiedliche Hersteller eine Rolle spielen und unterschiedliche Hardware, Betriebssysteme oder Anwendungen einfließen.

2.2.2 Hardware and Security Boxes

Bei den „Hardware and Security Boxes“ sind signifikante Sicherheitsfunktionalitäten des Evaluierungsgegenstandes (EVG)s von der Hardware, den verwendeten Bauteilen, den Leiterplatten und dem Gehäusedesign abhängig. Insbesondere ist auch die physische Gehäusesicherheit von Bedeutung. Darüber hinaus verfügen Produkte dieses Typs über komplexe Betriebssysteme und vielfältige Schnittstellen zu IT-Netzwerken und externen Geräten. Bei der Evaluierung müssen alle Angriffsmethoden in Bezug auf Gehäuse, Hardware und Embedded Software nach dem jeweils aktuellen Stand der Technik betrachtet werden, auch solche, die besondere Kompetenzen, Einrichtungen oder Ressourcen benötigen.

2.3 Information Technology Security Evaluation Criteria (ITSEC)

Die Information Technology Security Evaluation Criteria (ITSEC) bieten eine Skala für eine abgestufte Bewertung der Wirksamkeit, d.h. der Fähigkeit des IT-Produktes, den angenommenen Bedrohungen zu widerstehen. Die Abstufung bei der Wirksamkeit reicht von niedrig über mittel bis hoch. Zum anderen wird die nachgewiesene Qualität nach einer sechsstufigen Bewertungsskala angegeben (E1 als niedrigste Stufe bis E6 als höchste Stufe für die Korrektheit). Die Stufen beziehen sich auf die Prüftiefe und die Prüfmethoden.

Die Prüfstelle muss mindestens zwei Personen beschäftigen, deren Fachkompetenz vom BSI festgestellt wurde. ITSEC-Evaluierungen dürfen nur von ITSEC-Evaluatoren durchgeführt werden, deren Fachkompetenz im Rahmen einer Kompetenzfeststellung beim BSI festgestellt wurde.

Eine Erstanerkennung für den Standard ITSEC wird nicht mehr durchgeführt, da es sich hierbei um ein auslaufendes Kriterienwerk handelt. Die Aufrechterhaltung bestehender ITSEC-Anerkennungen werden im Einzelfall abgestimmt.

3 Verfahren zur Anerkennung von CC-Prüfstellen

3.1 Zusätzlich notwendige Unterlagen zur Beantragung

Notwendige Unterlagen zur Beantragung der Anerkennung sind in der Verfahrensbeschreibung [VB-Stellen] beschrieben. Folgende zusätzliche Unterlagen müssen dem Antrag auf Anerkennung beigefügt werden:

- Systemdokumentation Informationssicherheitsmanagement:
  Dokumentation des Informationssicherheitsmanagementsystems (inkl. Netztopologie) und materieller Sicherheit (inkl. Lageplan der Räumlichkeiten).
- Stellungnahme zum Informationssicherheitsmanagement:
  Eine schriftliche Stellungnahme zu allen Einzelaspekten der „Anforderungen an die Sicherheit von Prüfstellen“ mit den Informationen darüber, durch welche Maßnahmen der Antragsteller die Einzelaspekte der Anforderungen erfüllt und an welchen Stellen in der ISMS-Dokumentation die Maßnahmen dokumentiert sind.

3.2 Spezielle Informationen zur Systembegutachtung

Bei der Systembegutachtung muss zur Erfüllung der DIN EN ISO/IEC 17025 grundsätzlich eine Fachbegutachtung erfolgen, um nachzuweisen, dass ausreichend Fachkompetenz vorhanden ist.

Bei einer Begutachtung des Informationssicherheitsmanagementsystems des IT-Sicherheitsdienstleisters auf Grundlage des Dokuments „Anforderungen an die Sicherheit von Stellen“ [AS-Stellen] werden konkretisierte Anforderungen der DIN EN ISO/IEC 17025 bezüglich der Sicherstellung der Vertraulichkeit, Verfügbarkeit und der Integrität überprüft.

3.2.1 Durchführung der Fachbegutachtungen

Bei einer erstmaligen Anerkennung einer CC-Prüfstelle wird die Kompetenz der Stelle und der beteiligten Evaluatoren an Hand eines geeigneten Evaluierungsverfahrens überprüft.

Schwerpunkt der Fachbegutachtung sind spezielle fachliche Anforderungen, die sich aus dem jeweiligen Programm ergeben.

Eine Fachbegutachtung kann unter anderem wie folgt durchgeführt werden, durch:

- Interviews mit Mitarbeitern,
- Begutachtung der technischen Ausstattung,
- Probeevaluierung eines Testobjekts.

In den Programmen der Technischen Domänen „Smartcards and Similiar Devices“ und „Hardware Devices and Security Boxes“ werden im Rahmen der Fachbegutachtung insbesondere folgende Aspekte begutachtet:

- Die Fachkenntnisse und Fähigkeiten der eingesetzten Mitarbeiter,
- Das Vorhandensein und die Nutzung notwendiger technischer Ausstattung.

Aufgaben der CC-Prüfstelle	**Hilfsmittel [Verzeichnisse]**	**Aufgaben Zertifizierungsstelle (BSI)**
• Die Prüfstelle muss bereits im Rahmen der Beantragung zur Anerkennung für jeden Bereich qualifizierte CC-Evaluatoren benennen und in	• CC-Evaluatoren	• Die Anerkennungsstelle bewertet die eingereichten Angaben und Nachweise. • Der Fachbegutachter legt

Aufgaben der CC-Prüfstelle	Hilfsmittel [Verzeichnisse]	Aufgaben Zertifizierungsstelle (BSI)
den Profilen darstellen, wodurch die Fachqualifikation gegeben ist.		den Kreis der zu interviewenden CC-Evaluatoren fest.
• Die Prüfstelle muss sicherstellen, dass die von der Anerkennungsstelle im Rahmen der Vorbereitung der Fachbegutachtung benannten Mitarbeiter am Begutachtungstermin vor Ort sind und interviewt werden können. • Zusätzlich muss die Prüfstelle sicherstellen, dass das Equipment, das im Programm erforderlich ist, und das Bedienen dieses Equipments vor Ort überprüft und begutachtet werden kann.	• Begutachtungsplan • Anforderungen aus SOG-IS Dokumenten: Joint Interpretation Library Minimum ITSEF Requirements for Security Evaluations of „Smartcards and similar Devices“ und „Hardware Devices with Security Boxes“.	• Die Fachbegutachter führen Interviews mit den CC-Evaluatoren und ggf. spezifischen Fachexperten der Prüfstelle durch, begutachtet die Ausrüstung und den Umgang damit. • Die Ergebnisse der Begutachtung werden im Abschlussgespräch erläutert und mit den Prüfstellenverantwortlichen besprochen.

Tabelle 1: Aufgaben bei der Fachbegutachtung

3.2.2 Durchführung der Begutachtung des Informationssicherheitsmanagementsystems

Im Rahmen der Systembegutachtung wird die Erfüllung der Anforderungen an das Informationssicherheitmanagementsystem überprüft. Die Anforderungen sind in dem nicht öffentlichen Dokument [AS-Stellen] beschrieben.

Die Prüfstelle hat folgende Pflichten:

Aufgaben der CC-Prüfstelle	Hilfsmittel [Verzeichnisse]	Aufgaben Anerkennungsstelle (BSI)
• Die Prüfstelle muss die Anforderungen an die Sicherheit von Prüfstellen erfüllen und anhand der dokumentierten Regelungen, Festlegungen und Prozesse belegen. Die Nachweise und Dokumentation müssen der Anerkennungsstelle bei der Beantragung vorgelegt werden (s. dazu Kapitel 3.1.).	• AS-Stellen	• Die Anerkennungsstelle bewertet die Unterlagen.
• Die Prüfstelle muss sicherstellen, dass an dem Begutachtungstermin die Fachverantwortlichen vor Ort befragt werden können und das Begutachterteam die Räumlichkeiten der Prüfstelle samt Serverräume und sonstigen relevanten Räume im Rah-	• Begutachtungsplan	• Das Begutachterteam begutachtet vor Ort die Maßnahmen und Prozesse, befragt die Fachverantwortlichen, führt eine Begehung der Räumlichkeiten der Prüfstelle sowie der für die Sicher-

Aufgaben der CC-Prüfstelle	Hilfsmittel [Verzeichnisse]	Aufgaben Anerkennungsstelle (BSI)
men der Begehung begutachten kann.		heit der Prüfstelle relevanten Räume und Gerätschaften durch. • Die Ergebnisse werden in dem Abschlussgespräch erläutert und besprochen.

Tabelle 2: Aufgaben bei der Begutachtung des Informationssicherheitsmanagementsystems

4 Aufrechterhaltung der Anerkennung

Zur Aufrechterhaltung der Anerkennung muss die Prüfstelle die nachfolgenden Anforderungen an die Abläufe der Evaluierung im Rahmen der Produktzertifizierung sowie zur Reanerkennung einhalten. Darüber hinaus sind die Anforderungen aus Kap. 5 „Spezielle Rahmenbedingungen“ einzuhalten.

4.1 Anforderungen an den Ablauf der Evaluierung im Rahmen der Zertifizierung von Produkten, Schutzprofilen und Standorten

Im Folgenden wird das Verfahren einer Produktzertifizierung mit den Aufgaben der CC-Prüfstelle dargestellt. Eine Schutzprofil- oder Standortzertifizierung erfolgt entsprechend unter Verwendung der dafür relevanten Prüfaspekte, Kriterien und Interpretationen. Zur Aufrechterhaltung einer Zertifizierung gibt es verkürzte Varianten der Zertifizierung, wie Rezertifizierung, Reassessment oder partielle ALC-Reevaluierung, bei denen die Prüfstelle mit Evaluierungstätigkeiten beteiligt ist und die folgenden Ausführungen ebenfalls entsprechend gelten. Details zu den Verfahren sind im Dokument [CC-Produkte] (Anforderungsdokument für den Antragsteller bzw. Hersteller zur [VB-Produkte]) beschrieben.

Einen Überblick über alle benötigten Hilfsmittel befindet sich im Dokument [Verzeichnisse].

4.1.1 Aufgaben in der Vorbereitungsphase einer Produktevaluierung

Aufgaben Prüfstelle	**Hilfsmittel [Verzeichnisse]**	**Aufgaben Antragsteller/ Hersteller**	**Aufgaben Zertifizierungs-stelle**
Informationen austauschen: • Hersteller / Antragsteller (insbesondere bei Erstzertifizierung) über das Verfahren zur Zertifizierung informieren. • Sich über das zu zertifizierende Produkt und den Hersteller informieren.	• VB-/CC-Produkte • individuell spezifische AIS-Dokumente	• Über Sicherheitseigenschaften, vorgesehene Einsatzumgebung und technische Eigenschaften des Produktes informieren.	
Voraussetzungen sichern: • Unparteilichkeit und Unabhängigkeit der Prüfstelle und aller zum Einsatz geplanten Evaluatoren prüfen und Erklärung gemäß Vorlage abgeben. • Evaluierungsvertrag mit dem Hersteller abschließen. Die Anforderungen an Rahmenbedingungen (s. Kap. 5) sind zu berücksichtigen. • Klärung der Abgrenzung „Collection of Developer Evidence“ zur Beratung. • Die Prüfstelle muss im Rahmen der Prüfung von Anfragen, Angeboten und Verträgen sicherstellen, dass die **Anforderungen, einschließlich der zu verwendenden Standard-**	• AIS 23 • AIS 42 • AIS und Methodologiedokumente • Vorlage Evaluierungsplan • ISO 17025	• Evaluierungsvertrag mit der Prüfstelle abschließen	

Aufgaben Prüfstelle	Hilfsmittel [Verzeichnisse]	Aufgaben Antragsteller/ Hersteller	Aufgaben Zertifizierungs-stelle
methoden, angemessen festgelegt, schriftlich niedergelegt und verstanden sind und die Prüfstelle über die Fähigkeit und die Mittel verfügt, die Anforderungen zu erfüllen. Es müssen auch zeitliche Aspekte berücksichtigt werden. *Die Prüfung der Fähigkeit sollte unter Beweis stellen, dass die Prüfstelle über die notwendigen materiellen Mittel, Personalmittel und Informationsmittel verfügt und dass die Evaluatoren über die Fertigkeiten und Erfahrungen verfügen, die für die Durchführung der betreffenden Evaluierung notwendig sind.* *Sollten während der Evaluierungsdurchführung weitere Methoden entwickelt werden, müssen diese mit dem Hersteller vereinbart, in einer Verfahrensanweisung, detailliert beschrieben und validiert werden.*			
Optional: **An Informationsgespräch teilnehmen**	• Broschüre • VB-Produkte • CC-Produkte	• Informationsgespräch führen.	• Informationsgespräch führen.
Bei Antragsstellung unterstützen: • Eine grobe Voranalyse (Vorevaluierung) der vorhandenen Produktdokumente durchführen und auf fehlende Teile hinweisen. • Unterstützung bei der Erstellung einer Übersicht der Entwicklungs- und Produktionsstandorte sowie einer Liste der im Produkt (in externen Schnittstellen und Protokollen) implementierten kryptografischen Mechanismen. • Bei geplanter Wiederverwendung von Prüfergebnissen aus anderen Zertifizierungsverfahren diese identifizieren und deren grundsätzliche Eignung, Aktualität, Verfügbarkeit und Vollständigkeit ermitteln.	• Antragsformular • CC-Produkte • AIS 1 • AIS 46 • AIS47 • AIS 42 • Kryptokatalog	• Technische Information und Nachweise zum Produkt bereitstellen und mit dem Antrag ans BSI schicken	• Antragseingang bestätigen. • Antrag und zugehörige Anlagen inhaltlich prüfen.
Security Target (ST) abstimmen: • Das Security Target begutachten (Vorevaluierung). • Ggf. Impact Analysis Report (IAR) berücksichtigen.	• AIS 41 / 47 • CC (Teile 1 und 2) • verwendete Protection Profiles (PP)	• Security Target erstellen. • Ggf. IAR bereitstellen.	• Grundsätzliche Zertifizierbarkeit aus technischer Sicht feststellen, vorbehaltlich des positiven Ab-

Aufgaben Prüfstelle	Hilfsmittel [Verzeichnisse]	Aufgaben Antragsteller/ Hersteller	Aufgaben Zertifizierungs-stelle
•	• ggf. AIS 38		schlusses der Evaluierung unter Berücksichtigung des STs und der rechtlichen Rahmenbedingungen.
Vorschlag eines Evaluierungs- und Meilensteinplans erstellen • Evaluierungsplan gemäß Vorlage erstellen • Prüfaspekte und Prüfberichte - bei ErstProdukteval: gemäß ST Claim - bei Reeval: gemäß ST und IAR Auswertung - bei Produkt-Reassesment: AVA, zzgl (*) - bei ALC-Reeval: ALC, zzgl (*) (*): bei begleitender ST oder Guidance Änderungen Prüfergebnis i.d.R. nicht per Einzelprüfbericht sondern per ETR Ergänzung dokumentieren - bei SiteEval / SiteZert: AST, ACL - bei PP-Eval: APE, ggf. ACE • Vorschlag der Zertifizierungsstelle zur Abstimmung zur Verfügung stellen • Rückmeldungen der Zertifizierungsstelle umsetzen *Typischer Ablauf bei Produkten (ALC i.d.R. parallel):* *1. ASE-Evaluierung* *2. ADV / AGD-Evaluierung, Input für Testkonzept (ATE_IND, AVA)* *3.ADV/AGD Workshop* [3] *4. Evaluierung ATE des Herstellers* *5. ATE/AVA-Evaluator- Testkonzepte erstellen* *6. ATE / AVA -Kick-off-Meeting*[4] *und Krypto Kick-off-Meeting* *7. ATE/AVA-Evaluierung und Evaluatoranalysen und -tests* *8.ATE/AVA Workshop* [5] *9. Wenn erforderlich Zusatzdokus wie ETR for Composition oder STAR Report erstellen* *10. Berichte Finalisieren*	• AIS 45 • AIS 14 / 47 • Vorlage Evaluierungsplan (s. Kap. 7.1)	• Terminplanung durchführen.	• Evaluierungsplanung abstimmen. • Terminplanung durchführen.

3 Im ADV/AGD Workshop werden typischerweise die Ergebnisse der Designevaluierung besprochen.
4 Im ATE / AVA-Kick-off.Meeting werden das Test- und Analysekonzept des Evaluators besprochen sowie insbesondere auch die geplanten Analysen und Tests zu kryptografischen Verfahren.
5 Im ATE / AVA Workshop werden die Ergebnisse der Evaluatortests und -Analysen zu ATE und AVA besprochen.

Aufgaben Prüfstelle	Hilfsmittel [Verzeichnisse]	Aufgaben Antragsteller/ Hersteller	Aufgaben Zertifizierungs-stelle
Am Kick-off-Meeting teilnehmen: • Erste ST-Begutachtungsergebnisse einbringen • Review der Angaben des Antragstellers zu Krypto und zu Standorten vorstellen • Evaluierungskonzept vorstellen • Zeitplanung vorstellen und abstimmen • Workshops zur Vorbereitung und zur Besprechung von Ergebnissen im Einvernehmen mit der Zertifizierungsstelle planen. Siehe dazu auch Kap. 5.4. • ST, Termin- und Evaluierungsplan beschließen.	• AIS 45 • fachliche AIS wie jeweils erforderlich • Kryptokatalog	• Am Kick-off-Meeting teilnehmen. • Evaluierungsvertrag prüfen und ggf. anpassen.	• Kick-off-Meeting organisieren und leiten.
Auf Start der Evaluierungsphase warten: • Evaluierungsvertrag mit abgestimmten Evaluierungsplan abgleichen und ggf. Vertrag anpassen. • Evaluierungsaktivitäten vorbereiten.			• Schreiben über den Start der Evaluierungsphase versenden.

Tabelle 3: Aufgaben in der Vorbereitungsphase einer Produktevaluierung

4.1.2 Aufgaben in der Evaluierungsphase eines Produktes

Aufgaben der Prüfstelle	Hilfsmittel [Verzeichnisse]	Aufgaben der Hersteller	Aufgaben der Zertifizierungsstelle
• **Optional:** An einer Schulung durch den Hersteller teilnehmen		• **Optional:** Schulung der Evaluatoren, Zertifizierer und Prüfbegleiter durchführen	• **Optional:** An einer Schulung durch den Hersteller teilnehmen
Evaluierung durchführen: • Evaluierungstätigkeiten zu den im ST geforderten Prüfaspekten unter Berücksichtigung der Prüfung zugrunde liegenden Sicherheitskriterien, der Methodologie und der AIS durchführen. • Prüfergebnisse inhaltlich nachvollziehbar dokumentieren und vollständig der Zertifizierungsstelle zur Verfügung stellen. • Einzelprüfberichte gemäß den Anforderungen an Aufteilung und Inhalt aus den zugehörigen AIS erstellen. • Wenn erforderlich ETR-for-Composition erstellen • Interne fachliche Qualitätssicherung der Prüfberichte durchführen, i.d.R. durch Projektleiter oder wo inhaltlich erforderlich kompetenten aber nicht am konkreten Verfahren beteiligten Evaluator. • Prüfbericht(e) mit ggf. relevanten Zusatzdokumenten an die Zertifizierungsstelle verschicken. • Kommentare der Zertifizierungsstelle in der jeweiligen Review-Protokolldatei beantworten, wo erforderlich Evaluierungsschritte und Prüfberichte ergänzen. • Vorbereitung der Workshops zur Evaluierung. *Entscheidungen in strittigen Fragen werden im Benehmen mit den Prüfstellen durch das BSI getroffen.* *Die vorläufig abgenommene Prüfberichte müssen ggf. ergänzt werden, wenn sich während der Evaluierung neue Erkenntnisse ergeben.* *Die Evaluierung ist beendet, wenn alle*	• CC • CEM • Supporting Documents • alle relevanten AIS • AIS 14; 19; 23; 38	• Herstellernachweise bereitstellen bzw. ggf. Zugang zu den Herstellernachweisen gewähren.	• Die Evaluierung durch Begutachtung und mit schriftlichen Kommentaren zu den Prüfberichten begleiten. • Prüfberichte vorläufig abnehmen und dies schriftlich bestätigen. • Entscheidungen in strittigen Fragen herbeiführen. • Prüfberichte final abnehmen und ETR anfordern.

Aufgaben der Prüfstelle	Hilfsmittel [Verzeichnisse]	Aufgaben der Hersteller	Aufgaben der Zertifizierungs-stelle
Prüfberichte final abgenommen sind.			
An Workshops zur Evaluierung teilnehmen: Mögliche Workshops zur: • Präsentation und Besprechung der Ergebnisse der Evaluierung des Produktdesigns, • Abstimmung der Testplanung, Testdurchführung und zur AVA-Vorbereitung (AVA-Kick-off-Meeting), • Kryptoevaluierung (Krypto-Kick-off-Meeting), • Präsentation von Test- und Analyseergebnissen, • Klärung von strittigen Fragen,etc. *Zur Konzeption und Zielsetzung von Workshops siehe Kap. 5.4*	• AIS 31; 46	• An Workshops zur Evaluierung teilnehmen.	• Workshops zur Evaluierung durchführen.
Tests bzw. Penetrationstests durchführen: • Analyse- und Testkonzepte sowie Umsetzungsplanung vorlegen. Bei Wiederverwendung früherer Tests deren Aktualität begründen. • Verfügbarkeit der notwendigen Testtools und bei höheren Stufen auch der Quellcodeanalysetools sicherstellen. Ggf. Toolumgebung des Entwicklers bei der Prüfstelle installieren. • Abstimmung der Testplanung, Testdurchführung und zu AVA-Analysen vor deren Durchführung mit der Zertifizierungsstelle (i.d.R. im Rahmen eines AVA-Kick-off-Meetings / Krypto-Kick-off-Meeting), • Durchführung der ATE und AVA Aktivitäten • Dokumentation der Ergebnisse und ggf. Präsentation von Test- und Analyseergebnissen im Workshop *Die Termine sind seitens der Prüfstelle rechtzeitig mit dem Zertifizierer abzustimmen (4-6 Wochen vor den Testterminen) oder sind bereits Bestandteil des abgestimmten Evaluierungsplans.* *Die Testdurchführung erfolgt grundsätzlich in der Prüfstelle, durch die Mitarbeiter der Prüfstelle und mit Hilfe von Werkzeugen der*			• Abstimmungen durchführen und ggf. an Testaktivitäten teilnehmen.

Aufgaben der Prüfstelle	Hilfsmittel [Verzeichnisse]	Aufgaben der Hersteller	Aufgaben der Zertifizierungs-stelle
Prüfstelle. Abweichungen sind mit dem Zertifizierer vorab abzustimmen! *Der Evaluator muss uneingeschränkten Zugang zu allen erforderlichen Werkzeugen haben und die Vertraulichkeit der Tätigkeiten und der Unterlagen muss gewahrt sein.*			
Ggf. Standort-Audits beim Hersteller vor Ort durchführen: • Die Auditplanung ist frühzeitig mit dem Zertifizierer abzustimmen. Dabei sind alle relevanten Standorte zu berücksichtigen. • Das Audit ist gemäß AIS vorzubereiten, durchzuführen und zu protokollieren. *ALC-Evaluierung und Audits können i.d.R. parallel zur Evaluierung nach den Klassen ADV/ AGD/ATE erfolgen.* *Die Wiederverwendung von Auditergebnissen aus anderen Zertifizierungsverfahren ist mit dem Zertifizierer vorab abzustimmen.* *Die Wiederverwendung von Ergebnissen aus einem Standortzertifikat ist gemäß AIS 47 durchzuführen. Wenn erforderlich STAR-Report zur Unterstützung der Wiederverwendung von Audits erstellen.*	• AIS 1 • AIS 47 • AIS 38	• Zutritt zum Standort ge-währen.	• Abstimmungen durchführen und ggf. an Standort-Audits teilnehmen. • Ggf. STAR ab-nehmen
Evaluierungsbericht (ETR) erstellen: • ST-lite prüfen wenn verfügbar. • ETR erstellen. • Durchführung der abschließenden inter-nen Qualitätssicherung der Prüfberichte und des ETR durch Qualitätsbeauftragten der Prüfstelle. • ETR mit ggf. relevanten Zusatzdokumenten an die Zertifizierungsstelle verschicken. • Kommentare in der Review-Protokolldatei beantworten und Nacharbeit durchführen. **Voraussetzung:** **Alle Prüfberichte sind vorläufig abgenommen.** *Die Teilprüfberichte sind als Anlage Bestandteil des zusammenfassenden ETR* *Mit der ETR-Abnahme ist die inhaltliche Voraussetzung für die Erteilung des Zertifikates gegeben.*	• AIS 19 / 47 • AIS 35		• ETR begutachten und ggf. kom-mentieren. • Ggf. ETR-for-Composition ab-nehmen • Formale Abnah-me des ETR durchführen. • Antragsteller und Prüfstelle über diese Ab-nahme informie-ren.

Tabelle 4: Aufgaben in der Evaluierungsphase eines Produktes

4.1.3 Aufgaben in der Zertifizierungsphase eines Produktes

Aufgaben der Prüfstelle	Hilfsmittel [Verzeichnisse]	Aufgaben der Hersteller	Aufgaben der Zertifizierungs-stelle
Abgenommene Prüfberichte dem BSI vorlegen: • Mit der handschriftlichen Unterschrift wird die inhaltliche Vollständigkeit und Richtigkeit der technischen Prüfergebnisse sowie die Qualitätssicherung der Prüfberichte und die Einhaltung der Verfahren bestätigt (siehe Vorlage Kap. 5.1). *Der Eingang dieser Unterlagen beim BSI ist eine Bedingung zur Erteilung des Zertifikats.*	• AIS 19 / 47		• Überprüfung der Vollständigkeit der Prüfberichte und Unterschriften
Ggf. Entwurf des Zertifizierungsreports kommentieren.			• Zertifizierungs-report und weitere zertifizierungsrelevante Unterlagen erstellen.
Alle evaluierungsrelevanten Nachweise archivieren: • Den Evaluierungsgegenstand zur Archivierung dem Antragsteller aushändigen (es sein denn, es gibt eine andere Vereinbarung). • Weitere Prüfunterlagen gemäß interner Regelungen oder vertraglichen Vereinbarung mit dem Antragsteller archivieren. *I.d.R. hat sich der Antragsteller mit dem Antrag verpflichtet, seine Evaluierungsnachweise und das zertifizierte Produkt (Prüfmuster) selbst zu archivieren.*			
Ggf. Feedbackgespräch mit Zertifizierungsstelle: • telefonisch oder F2F • Positives und Negatives aus dem Verfahren • Verbesserungsvorschläge zum Prozess			• Gespräch mit Prüfstelle

Tabelle 5: Aufgaben in der Zertifizierungsphase eines Produktes

4.2 Fachbegutachtungen

Im Rahmen der Anerkennung als Prüfstelle werden regelmäßig Fachbegutachtungen durch das BSI durchgeführt, um die Eignung der Prüfstelle und der Evaluatoren im betreffenden Bereich sicherzustellen zu überprüfen und eventuelle Abweichungen von den Anforderungen notwendigen Qualifizierungsbedarf zu erkennen.

Eine Fachbegutachtung erfolgt dabei mindestens alle 3 Jahre im Rahmen der Systembegutachtung (Erst- oder Reanerkennung). In den Programmen der Technischen Domänen „Smartcards and Similiar Devices“ und „Hardware Devices and Security Boxes“ werden nach SOG-IS-MRA mindestens alle 2 Jahre Fachbegutachtungen durchgeführt.

4.3 Reanerkennung

Eine Fachbegutachtung (Lizenzierung) durch eine Probeevaluierung findet bei einer Reanerkennung nicht statt, wenn die Prüfstelle in der Geltungsperiode der ablaufenden Anerkennung mindestens eine Evaluierung mit dem Ziel der Erteilung eines Deutschen IT-Sicherheitszertifikats mit einer Prüftiefe entsprechend EAL4 nach CC bzw. E3 nach ITSEC durchgeführt hat und die Zertifizierungsstelle des BSI die Fachkompetenz der Prüfstelle bestätigt.

Auf Antrag kann auch eine Reanerkennung ausgesprochen werden, wenn nur Verfahren kleinerer CC-EAL-Stufen durchgeführt wurden. Die Prüfstelle bekommt dann eine eingeschränkte Anerkennung für Verfahren bis zu den entsprechenden kleineren EAL-Stufen; eine Fachbegutachtung (Lizenzierung) ist dann ebenfalls nicht notwendig.

5 Spezielle Rahmenbedingungen

5.1 Weitere Regelungen zur Zusammenarbeit

1. Die Prüfstelle muss die prozessspezifischen Anforderungen und Abläufe der Produktzertifizierung einhalten und ist gegenüber der Produktzertifizierungsstelle verpflichtet, Auskünfte zum Ablauf und Inhalt laufender Evaluierungsverfahren zu erteilen. Die Prüfstelle muss die prozessspezifischen Anforderungen gemäß Kapitel 4.1 „Anforderungen an den Ablauf der Evaluierung im Rahmen der Zertifizierung von Produkten, Schutzprofilen und Standorten“ einhalten und ist gegenüber der Produktzertifizierungsstelle verpflichtet, Auskünfte zum Ablauf und Inhalt laufender Evaluierungsverfahren zu erteilen.
2. Sie teilt der Produktzertifizierungsstelle umgehend mit, wenn geplante Lieferungen von Prüfberichten nicht rechtzeitig erfolgen. Diese können zu verzögernden Ketteneffekten in der weiteren Bearbeitung des Verfahrens führen. Die Produktzertifizierungsstelle verlangt eine unaufgeforderte Anpassung und Neuabstimmung des Zeitplans unter Beteiligung des Antragstellers. Sollte dieser neue Zeitplan auf Nachfrage der Zertifizierungsstelle nicht zur Verfügung gestellt werden, kann eine zeitnahe Bearbeitung der Prüfergebnisse durch die Zertifizierungsstelle nicht erfolgen. Die Zertifizierungsstelle setzt den Antragsteller in Kenntnis und kann ein Mahn- und Aussetzungsverfahren einleiten.
3. Die Prüfstelle ist für die technische Korrektheit und für die wahrheitsgemäße Dokumentation ihrer Prüfergebnisse verantwortlich.
4. Die Archivierung des Evaluierungsgegenstandes nach Abschluss der Evaluierung erfolgt grundsätzlich nach Vorgaben der Zertifizierungsstelle des BSI unter Berücksichtigung der Stellungnahme des Herstellers. In der Regel erfolgt die Archivierung des Prüfgegenstands beim Hersteller.
5. Falls spezielle Mess- und Prüfeinrichtungsgegenstände oder Software für die Evaluierung/Prüfung verfügbar sind, dürfen nur die vom BSI für die jeweiligen Zwecke erlaubte Hard- oder Software verwendet werden. Das BSI wird dann der Prüfstelle die erforderliche Hard- oder Software (sofern verfügbar) inkl. der notwendigen Einweisung gebührenpflichtig zur Verfügung stellen, sofern die Bundesrepublik Deutschland ganz oder teilweise die Nutzungsrechte besitzt.
6. Bei der Erstellung und Überarbeitung von AIS sind die Prüfstellen verpflichtet, sich am Kommentierungsprozess zu beteiligen.
7. Die Prüfstelle muss für Fachbegutachtungen oder für Audits im Rahmen der Anerkennungsabkommen (VPA) den Begutachtern/Auditoren Einblick in Evaluierungsergebnisse und Prüfberichte ermöglichen. Die CC-Evaluatoren und Fachexperten der Prüfstelle müssen für Fachinterviews durch die Begutachter des BSI bzw. die Auditoren im VPA zur Verfügung stehen. Die Evaluierungsverträge mit Herstellern, Standortbetreibern bzw. PP-Erstellern müssen dies ohne spezifische Vertraulichkeitsvereinbarung (NDA) ermöglichen, da die Begutachter Mitarbeiter des BSI oder der Partnerbehörden in den Anerkennungsabkommen sind.
8. Ist eine Unterbeauftragung bestimmter Evaluatorentätigkeiten an eine externe Stelle vorgesehen, so sind neben den Regelungen aus [VB-Stellen] folgende Regelungen einzuhalten: für AVA-Evaluierungstätigkeiten ist nur eine partielle Unterbeauftragung zulässig, z.B. die Durchführung einer spezifischen Analyse. Gemeinsam zwischen mehreren anerkannten Prüfstellen des BSI aufgesetzten Evaluierungsprojekte werden im Einzelfall geregelt.
9. Die Verwendung von Testequipment außerhalb der Räumlichkeiten der Prüfstelle muss im Evaluierungsplan dargelegt und im Testplan präzisiert werden. Es müssen angemessene Sicherheits-maßnahmen zum Schutz des EVG, vertraulicher Informationen und des Know-Hows des Evaluators getroffen werden. Bei Verbleib des EVG oder von vertraulichen Unterlagen in der

externen Stelle, z.B. unbeaufsichtigt über Nacht, müssen angemessene Zusatzmaßnahmen zum Schutz getroffen werden. Wird die Testdurchführung am EVG z.B. aufgrund von Nicht-Verfügbarkeit der Tools, unterbrochen, so müssen Maßnahmen zur Sicherstellung und Neueinrichtung der verwendeten Konfiguration der Tools und des EVG getroffen werden. Der Evaluator ist verantwortlich für die Durchführung und für die Ergebnisse solcher extern durchgeführter Tests. Wird extern genutztes Testequipment durch Betriebspersonal (Operator) gesteuert, z.B. bei Bespoke Equipment, muss der Evaluator bei der Durchführung vor Ort dabei sein und das Betriebspersonal anweisen was wie zu tun ist. Der Evaluator muss dazu die notwendigen Kenntnisse zum jeweiligen EVG, zur Art des durchzuführenden Tests, zu den Tools und deren Verwendung mitbringen.

10. Da die Prüfstelle durch die Anerkennungsvereinbarung mit dem BSI zur Einhaltung den Vorgaben des Zertifizierungsschemas verpflichtet ist, darf der Evaluierungsvertrag keine, eine sachgerechte Evaluierung und Prüfbegleitung behindernden 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 Kick-off Meeting oder im laufenden Verfahren neue oder zusätzliche Sachverhalte (z. B. zusätzliche Penetrationstests, Wiederholungsaudit, Korrekturen und Ergänzungen zum Prüfbericht wie von der Zertifizierungsstelle als erforderlich betrachtet, Workshops) ergeben können, welche die Evaluierungsaufwände beeinflussen.

11. Bei der Aktualisierung und Ergänzung von Prüfberichten sind die inhaltlichen Änderungen kenntlich zu machen, z.B. in dem mit Änderungsmarkierungen gearbeitet wird. In den gelieferten pdf-Dokumente müssen die Änderungsmarkierungen sichtbar sein. Dies dient der Beschleunigung der Durchsicht beim Zertifizierer.

12. Prüfberichte enthalten die Namen aller an den im jeweiligen Bericht beteiligten Evaluatoren der Prüfstelle und unterstützenden Fachexperten der Prüfstelle oder ggf. beauftragten Experten. Prüfberichte zu Teilen der Evaluierung nach AIS 14 sind Anlage zur abschließenden ETR Summary nach AIS 19.

13. Die abschließende Fassung der ETR-Summary wird
    - von dem für das Evaluierungsprojekt verantwortlichen Projektleiter oder den Prüfstellenleiter mit dem bestimmten Wortlaut (siehe Fußnote) händisch unterzeichnet und
    - vom Qualitätsmanagementbeauftragten (QMB) der Prüfstelle mit dem bestimmten Wortlaut (siehe Fußnote) händisch unterzeichnet und
    dem BSI zugestellt. [6]
    Anmerkung: Die Unterzeichnung des Zertifikates kann erst nach Eingang des unterschriebenen ETR bei der Zertifizierungsstelle erfolgen.

6 **Wortlaut zur Unterschrift des Projektleiters / Prüfstellenleiters:**
"Alle an dieser Evaluierung beteiligten Personen sind in der wahrgenommenen Rolle angeführt. Die Unabhängigkeit und Unparteilichkeit der Evaluatoren war gewährleistet und sie hatten die für die Prüfung notwendigen Mittel / Ressourcen zur Verfügung. Die Prüfberichte geben die tatsächlichen Fakten und Ergebnisse wieder und sind durch keine anderen Sachverhalte als die zwischen Prüf- und Zertifizierungsstelle bestehenden beeinflusst."
bzw.:
"All persons involved in this evaluation are listed with the role they took. The independence of the evaluators had been ensured and they had all means and resources necessary for the evaluation performed available. The evaluation reports reflect the actual facts and results and are not being influenced by circumstances other than those defined between evaluation body and certification body."
Wortlaut zur Unterschrift QMB:
"Das Verfahren ist gemäß den im Rahmen der Anerkennung durch das BSI abgenommenen Prozessen der Prüfstelle durchgeführt und eventuelle Abweichungen sind individuell dokumentiert und werden von der Prüfstellenleitung verantwortet. Formale und inhaltliche QS wurde wie auf den Dokumenten vermerkt durchgeführt."
bzw.:
"The procedure has been performed according to the processes of the evaluation facility as approved by BSI within the ITSEF Approval and Licensing process. Potential deviations have been individually documented and the head of the ITSEF takes responsibility for this. Formal and content quality checks have been perfomed as indicated on the respective documents."

14. In vielen Fällen wird die Evaluierung auf mehrere Evaluatoren aufgeteilt und es werden für bestimmte Tätigkeiten Fachexperten hinzugezogen, z.B. für bestimmte Penetrationstests oder Analysen. Die Prozesse innerhalb der Prüfstelle müssen sicherstellen, dass ein hinreichender Informationsaustausch zwischen den beteiligten Personen ermöglicht und tatsächlich praktiziert wird und diese Personen Zugriff auf alle für sie relevanten Herstellernachweise und Prüfergebnisse haben, um ihre jeweilige eigene Aufgaben erfüllen zu können. Beispielsweise müssen die an AVA-Analysen und Pentests arbeitenden Personen detaillierte Kenntnisse von allen gem. CC für AVA zu berücksichtigenden Nachweisen haben und über alle als potentiell z.B. bei der ADV-Evaluierung erkannten Schwachstellen informiert werden. In vielen Fällen wird die Evaluierung auf mehrere Evaluatoren aufgeteilt und es werden für bestimmte Tätigkeiten Fachexperten hinzugezogen, z.B. für bestimmte Penetrationstests oder Analysen. Die Prozesse innerhalb der Prüfstelle müssen sicherstellen, dass ein hinreichender Informationsaustausch zwischen den beteiligten Personen ermöglicht und tatsächlich praktiziert wird und diese Personen Zugriff auf alle für sie relevanten Herstellernachweise und Prüfergebnisse haben, um ihre jeweilige eigene Aufgaben erfüllen zu können. Beispielsweise müssen die an AVA-Analysen und Pentests arbeitenden Personen detaillierte Kenntnisse von allen gem. CC für AVA zu berücksichtigenden Nachweisen haben und über alle als potentiell z.B. bei der ADV-Evaluierung erkannten Schwachstellen informiert werden.

5.2 Unabhängigkeit und Unparteilichkeit der Prüfstelle und der jeweiligen Evaluatoren

Die mit der Evaluierung beauftragte Prüfstelle und die an einer Evaluierung arbeitenden Personen müssen unabhängig sein und der Zertifizierungsstelle darüber eine auf die geplante Evaluierung bezogene Unabhängigkeitserklärung als Anlage zum Evaluierungsplan abgeben.

Wenn ein vorgesehener Evaluator, der Projektleiter oder ein anderer Mitarbeiter der Prüfstelle oder deren Vorgesetzter in einer Beziehung zum EVG-Hersteller, Standortbetreiber oder PP-Ersteller steht, welche einen Interessenskonflikt hervorrufen könnte, kann die Unabhängigkeit und Unparteilichkeit gefährdet sein. Eine solche Gefährdung kann z. B. bei folgenden Konstellationen auftreten:

1 Beratung des EVG-Herstellers, Standortbetreibers oder PP-Erstellers hinsichtlich des EVGs oder PPs (z. B. zum TOE/EVG-Konzept oder -Design),

2 Mitarbeit an der Entwicklung, Herstellung oder dem Vertrieb des EVGs, an der Konzeptionierung oder Umsetzung der Standortsicherheit oder an der Entwicklung des PPs sowie der für die Zertifizierung benötigten Nachweise des Herstellers, Standortbetreibers oder PP-Erstellers,

3 andere geschäftliche Verbindungen zwischen der Prüfstelle und dem EVG-Hersteller, Standortbetreiber oder PP-Erstellers (z. B. Beratung, Konzeptionierung, Entwicklungsbegleitung, Mutter/Tochter oder Schwester-Beziehung).

Die Feststellung der Unabhängigkeit und Unparteilichkeit durch das BSI ist Voraussetzung für die Annahme eines Zertifizierungsantrags.

Nicht zulässig sind:

1 Ein weisungsbefugter Vorgesetzter der Person, die Evaluierungstätigkeiten übernimmt, ist oder war an der Entwicklung, der Erstellung von Nachweisen und/oder Beratung zum zu evaluierenden Produkt/PP/Standort beteiligt.

   a Ein Mitarbeiter der Prüfstelle ist oder war an der Entwicklung, der Erstellung von Nachweisen und/oder Beratung zum zu evaluierenden Produkt/PP/Standort beteiligt und wird als Projektleiter oder Evaluator für die Evaluierung eingesetzt.

5.3 Meldung weiterer CC-Evaluatoren

Die Prüfstelle hat jederzeit die Möglichkeit, weitere CC-Evaluatoren als erfahrene, eingearbeitete CC-Evaluatoren dem BSI nachzumelden. Dazu ist die Fachkompetenz der Evaluatoren in Bezug auf die Technologiefelder und die CC-Prüfaspekte dem BSI durch Bereitstellung der Befugnismatrix, die sich aus dem jeweils abgearbeiteten und abgeschlossenen Einarbeitungsprogramm der Person ergeben hat, und ggf. weiterer Nachweise (z.B. Teilnahmebescheinigungen an Schulungen) nachzuweisen. Diese Nachweise werden seitens des BSI geprüft und bewertet. Sollte das BSI diese als nicht ausreichend erachten, so kann der Evaluator abgelehnt werden. Der jeweilige Evaluator darf nur in den Bereichen eingesetzt werden, die durch die Befugnismatrix abgedeckt sind.

Die Einarbeitung des CC-Evaluators erstreckt sich i.d.R. auf bestimmte CC-Prüfstufen. Es müssen mindestens die Prüfstufen EAL 1-EAL 4 sowie alle wesentlichen Aspekte der Common Criteria für diese Prüfstufen abgedeckt werden. Soll der Evaluator auch für höhere Prüfstufen eingesetzt werden, dann müssen auch diese abgedeckt sein. Ausnahmen in Einzelfällen von dieser Anforderung sind zu begründen. Im Rahmen der Einarbeitung müssen auch die ATE- und AVA-Prüfaspekte in besonderer Tiefe und Umfang berücksichtigt werden.Ebenso muss die Einarbeitung die Technologiefelder abdecken, für die der Evaluator die Befugnis erhält.

5.4 Arbeitstreffen mit den Prüfstellen

Auf Vorschlag des BSI oder einer Prüfstelle werden Arbeitssitzungen zu spezifischen Fragestellungen durchgeführt.

Hierunter fallen z. B.

- Prüfstellentreffen: Diskussionen zu den Kriterienwerken und zu Interpretationen, Änderungen des Zertifizierungsverfahrens, Schulung hinsichtlich spezieller Methoden und Werkzeuge,
- Workshops zum Qualitätsmanagement,
- Informationsaustausch zum Stand der Technik und zu Angriffsmethoden und Analysen,
- Spezifische Treffen z.B. zu Kryptothemen, zu Smartcard/Hardware-Themen, zur Evaluierung von Terminals.
- Arbeitstreffen (Workshops) innerhalb von Zertifizierungsverfahren

Die Anzahl solcher Arbeitssitzungen wird nach Dringlichkeit und fachlichen Erfordernissen festgelegt. Grundsätzlich sind maximal vier reguläre Prüfstellentreffen im Jahr vorgesehen. Die Prüfstellen sollten mit zumindest einem für das jeweilige Thema geeigneten Mitarbeiter vertreten sein.

5.4.1 Arbeitstreffen (Workshops) innerhalb von Zertifizierungsverfahren

Innerhalb von Zertifizierungsverfahren werden gemeinsame Workshops zwischen am Verfahren beteiligten Evaluatoren und ggf. Fachexperten der Prüfstelle, dem Zertifizierer und dem Fachexperten der Zertifizierungsstelle durchgeführt.

Das Ziel des Workshops ist, im direkten Gespräch den Prüfansatz, Prüfumfang und die Ergebnisse bzw. Kommentare des Zertifizierers zu verstehen, dem Klärungsbedarf möglichst effizient gerecht zu werden und damit die Abnahme der Prüfergebnisse zu beschleunigen. Von den beteiligten Evaluatoren wird erwartet, dass sie Fragen zum TOE, zur Evaluierung und zu den Ergebnissen erklären können. Die Effizienz der Klärung von Fachfragen kann verbessert sein, wenn die relevanten Fachleute seitens des Antragstellers am Workshop teilnehmen. Über die Teilnahme des Antragstellers entscheidet der zuständige Zertifizierer im Einzelfall.

Typische Workshopthemen sind:

- ADV-Ergebnisse und Testplanung,
- AVA-Kick-off,
- AVA-Krypto-Kick-off,
- AVA-Ergebnisse.

Der Meilensteinplan muss die jeweils geplanten Workshops berücksichtigen. Ad hoc Workshops zur Besprechung von Evaluierungsfragen können sowohl vom Evaluator als auch vom Zertifizierer jederzeit einberufen werden. Ergebnisse von Workshops und Gesprächen werden in Protokollnotizen festgehalten und sind Teil der Verfahrensakte. Protokollnotizen und Präsentationen von Workshops werden als Anlagen zum jeweiligen Prüfbericht genommen und entlasten damit die Ergebnisdokumentation im Prüfbericht. Alle Workshops und Gespräche sollen das schriftliche Kommentierungsverfahren entlasten und die Klärung der Sachfragen und der Abnahme beschleunigen.

5.5 Verfahren bei Mängeln in der Evaluierung

Mängel können in folgende Mängelarten eingeteilt werden:

- Terminplanung und -treue
- QS-Mängel
- Mangel an CC-Kenntnissen
- Mängel im Ablauf des Verfahrens
- Mangelnde Kenntnisse über den Evaluierungsgegenstand (EVG)/das Produkt

Fehler und/oder nicht nachvollziehbare Aspekte in einem Prüfbericht werden durch den Zertifizierer in einem Review-Protokoll oder im Protokoll eines Workshops festgehalten. Alle Mängel- bzw. Kommentierungspunkte müssen vom Evaluator nachgebessert bzw. beantwortet werden.

Eine Eskalation bei erheblichen Mängeln in der Prüfdokumentation wird in folgenden drei Eskalationsstufen ausgeführt:

- **1. Eskalationsstufe:**
  Bei einer hohen Zahl von Kommentierungen behält sich der Zertifizierer vor, das Review für den Einzelprüfbericht vorzeitig abzubrechen. Dies geschieht mit dem Hinweis, alle Prüfaspekte erneut mit der gebotenen Sorgfalt und geltenden Qualität zu wiederholen. Der Leiter der Zertifizierungsstelle wird hierüber informiert. Vor einem solchen Abbruch des Reviews ist jedoch ein Fachgespräch zwischen Prüfbegleiter und Evaluator obligatorisch, um offensichtliche Missverständnisse auszuschließen.
  Ist eine erste Nachbesserung/Kommentierungsrunde nicht zufriedenstellend erfolgt, wird eine zweite Review-Runde durchgeführt.
  Ist auch diese Nachbesserung/Kommentierungsrunde nicht zufriedenstellend und auch ein Fachgespräch nicht erfolgreich, erfolgt ggf. noch eine dritte Review-Runde oder das Verfahren geht in die nächste Eskalationsstufe über.
- **2. Eskalationsstufe:**
  Ist die Nachbesserung/Kommentierungsrunde nicht zufriedenstellend, wird in dieser Reviewrunde der Evaluator und der Leiter der Evaluierungsstelle zu einem Klärungsgespräch zur Zertifizierungsstelle unter Beteiligung des Leiters der Zertifizierungsstelle einberufen.
  Mängel werden dann noch einmal genauer diskutiert und abgeklärt. Erarbeitete Lösungen sind nach Abstimmung umzusetzen.
  Die Anerkennungsstelle wird informiert.

3. Eskalationsstufe:
Ist die nachfolgende Nachbesserung nicht zufriedenstellend, ist ein Abbruch des Prüfverfahrens dem

Antragsteller vorzuschlagen oder von der Zertifizierungsstelle einzuleiten.
Die Anerkennungsstelle wird im Rahmen ihrer Überwachungstätigkeit aktiv.

6 Referenzen und Glossar

Die Aufschlüsselung der referenzierten Dokumente und das Glossar befindet sich im Dokument „Verzeichnisse“ [Verzeichnisse].

7 Weitere Hilfsmittel

7.1 Vorlage „Evaluierungsplan“

- Cover Sheet (Lab specific including identification of document and author).
- Document History.
- Distribution List (i.e. ITSEF, sponsor/developer, certification body BSI).
- Introduction:
  - Brief outline of status and intention of this document,
  - Identifiers: (Identification of product to be evaluated; Identification of assurance package to be used; Identification of BSI, sponsor of evaluation, ITSEF),
  - Points of contact (Names and contact data of main persons (Project manager at ITSEF; at sponsor/developer; others).
- Evaluation basis (Names and version numbers of documents):
  - Criteria and methodology,
  - List of all relevant Scheme interpretations (AIS) including reference to international interpretations and guidelines (CCRA Supporting Documents; JIL Documents),
  - Additional interpretations and guidelines planned to be used,
  - Relevant governmental laws and ordinance (nationally e.g. for Smart Meters, eHealth), EU-Regulations (e.g. eIDAS, Digital Tachograph,...for tachograph), Technical Guidelines (e.g. on crypto algorithms).
- TOE Evaluation:
  - Description of TOE (Security functionality and features (in keywords), top level architecture, separation from environment), (i.e. reference to relevant chapters of the Security Target available but additions to be made for the TOE or Life Cycle if important for planning of tasks and outline of competences below)
  - Discussion of possible show stoppers for crypto parts, e.g.. proprietary algorithms
  - Reference to evaluation of previous versions of the product or site evaluations if reuse of results is planned:
    outline of differences in functionality, architecture, concepts (Note: reuse of previous evaluation results is only possible if specific references are outlined), reference to the applicants IAR, but additions to be made for the TOE or Life Cycle if important for planning)
    Listing of ALC evaluations or site certificates planned to be reused.
  - Tasks of ITSEF (planned and already performed) related to TOE or if reuse is planned to a similar device of the sponsor/developer:
    - outline of evaluation aspects (assurance components to be covered),
    - outline of consulting tasks of ITSEF personnel for evidence production, product development, developer site security,
  - Personnel assignment (names and roles resp. focus of individual tasks, including consulting tasks),
    - for Preparation phase (e.g. consulting for ST and evidence production),
    - for Evaluation phase (who is planned for what task),

- for Consulting along with the project
  Note: A declaration of independence by the head of the ITSEF for all members of the evaluation team is required, see chap. Fehler: Verweis nicht gefunden.

- Competence of the ITSEF and the assigned personnel:
  - For each assigned evaluator outline why he is competent to conduct his evaluation tasks and outline his experience and know-how related to type of TOE resp. technology / architecture / attack methods / the specific TOE in relation to the tasks planned for him.
    The following items are of specific interest:

    - experience with AVA tasks for analysis and penetration methods and tools as required.

    - experience with tasks if specific know-how is required (e.g.
      on semiformal languages, on formal methods and tools used,
      on the operating system (if part of the TOE),
      on the types of interfaces and protocols used by the TOE
      on domain separation concepts
      on the TOE implementation representation (SW, HW) and tools used
      on site security measures including network security,
      on side channel analysis, cryptography,
      on product life cycle, development concepts, (if relevant) chip/HW production process and specific type of sites)
      Note: a reference to specific parts of recently finalised BSI evaluation/certification project of a similar product is possible, but reference must be specific to the task considered.
  - In case the TOE is a new type of product for certification, outline of plan to build up the required competence e.g. plans for product and technology training, cooperation with other facilities.
  - If a junior evaluator is involved outline of plan to build up the required competence e.g. plans for training.
- Outline of tools to be used for evaluation tasks e.g. for ATE, AVA, source code review, formal methods,
  - Availability of required tools: at the ITSEF site, at developers sites, other sites; in case of usage of tools outside the ITSEF site outline how availability and confidentiality is ensured.
    Note: Details of test tools are typically specified in the test plan to be provided later.
- Preparation of Kick-off Meeting:
  - Outline briefly result of the ITSEFs initial assessment of the draft ST or reference to a comment file provided.
- Detailed evaluation work plan:
  - Evaluation approach (full evaluation / re-evaluation resp. Re-use of previous results / use of a composite approach / ....).
  - Definition of work packages.
  - Planning for work packages (order, what first, how to solve dependencies).
  - Reception Plan of sponsor/developer evidence (what when).
  - Site visit (list of sites and last visit used for a previous certification procedure, re-use, planned visits):
  - ADV Design review (what is planned at ITSEF site, what at developer site),
  - Testing (approach and plan): (can be shifted to a later phase in the project, but non-availability of tools can become a show stopper if not addressed early)

    - ATE independent testing at ITSEF, which support from the developer is required by the ITSEF for independent testing?

- Proposal for AVA-kick-off meeting, Pen Test planning (if already possible)): re-use from previous evaluations (if yes provide rationale).

  - Deliverables of ITSEF (to sponsor/developer; to BSI, to others) (i.e. observation reports, test plans, site visit checklist/protocols, intermediate evaluation reports, ETR,....).
  - Plan how ITSEF is prepared for updates required by the certifier.
  - Schedule (BSI Template for Milestoneplan should be used). Outline how support of certification tasks is managed (i.e. review of draft certification report).

- Miscellaneous
  - Formats and languages of developer evidence and documentation of evaluation results.
  - Document updates (how version numbering, marking of changes will be done).
  - Exchange of information (confidentiality -encryption tools used, keys).
  - Declaration of independence by head of ITSEF for all members of the evaluation team (according to template chap. Fehler: Verweis nicht gefunden).

7.2 Vorlage für Unabhängigkeits- und Unparteilichkeitserklärung der Prüfstelle als Anlage zum Evaluierungsplan

Angaben zur vorgesehenen Evaluierung:

- Name Antragsteller / EVG-Hersteller, Standortbetreiber oder PP-Ersteller: _____
- Bezeichnung des zu evaluierenden EVGs, Standortes oder PPs: _____
- Bezug zum Dokument „Evaluierungsplan“ (Kennzeichner, Datum, Version):_____

Angaben zur Unabhängigkeit und Unparteilichkeit:

- Ich erkläre, dass mir mit Ausnahme der nachfolgend genannten Verbindungen keine weiteren Verbindungen (gem. Kapitel 5.2 Satz 1 (Beratung) - 2 (Unterstützung bei Entwicklung)) der für die Durchführung der Evaluierung vorgesehenen Mitarbeiter der Prüfstelle (Namen gemäß o.g. Evaluierungsplanes) zum EVG-Hersteller, Standortbetreiber bzw. PP-Ersteller bekannt sind.

  Folgende Verbindungen bestehen von Mitarbeitern der Prüfstelle zum EVG-Hersteller, Standortbetreiber bzw PP-Ersteller: _____
  (bitte Verbindungen, z.B. Art und Umfang der Beratung oder Entwicklungsunterstützung erläutern und ggf. auf separater Anlage die Konstellation darlegen).
- Folgende Verbindungen (gem. Kapitel 5.2 Satz 3. bestehen zwischen der Prüfstelle und dem EVG-Hersteller, Standortbetreiber bzw. PP-Ersteller: _____
  (bitte Verbindungen erläutern und ggf. auf separater Anlage die Konstellation darlegen).
- Für den Fall, dass Personen der Prüfstelle gem. Kapitel 5.2 Satz 1-3 aktiv waren oder sind, gelten folgende Abhängigkeiten zu den benannten Evaluatoren: _____
  (z.B. Vorgesetztenverhältnisse, etc. bitte Verbindungen erläutern und ggf. auf separater Anlage die Konstellation darlegen).
- Es bestehen folgende Mutter/Tochter/Schwester- oder ähnliche Beziehungen zwischen Hersteller und Prüfstelle: _____
  (bitte Verbindungen erläutern und ggf. auf separater Anlage die Konstellation darlegen).

Ich sehe die Unabhängigkeit und die Unparteilichkeit der Prüfstelle trotz der o.g. Angaben nicht gefährdet, weil _____
(bitte begründen).

Ich verpflichte mich, Erkenntnisse, welche die hiermit erklärte Unabhängigkeit und Unparteilichkeit in Frage stellen könnten, der Zertifizierungsstelle des BSI unverzüglich mitzuteilen.

_____ _____

Ort, Datum Name und Unterschrift Leiter Prüfstelle