Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anerkennung: Programm zur Anerkennung als Prüfstelle im Bereich Common Criteria (CC)

CC-Prüfstellen

Version 1.6 vom 01.11.2024

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0)800 247 1000
E-Mail: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Änderungshistorie

Version	*Datum*	*Name/Org-Einheit*	*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 D25	Revision in 2017
1.2	02.07.2018	Anerkennungsstelle D25	Revision in 2018
1.3	19.03.2020	Anerkennungsstelle SZ 12	Revision in 2020
1.4	15.07.2021	Anerkennungsstelle SZ12	Revision: • Austausch der Abbildung 1: Zertifizierungs- und Anerkennungsprogramme (Dokumentenübersicht) • Ausgliederung der Informationen zum Ablauf der Evaluierung im Zertifizierungsverfahren, Regeln und Randbedingungen in ein separates Schemadokument CC-Evaluierungsprozess [CC-EP] • Anpassung des Links zum Sog-IS-MRA
1.5	31.03.2023	Anerkennungsstelle SZ12	Revision: • Ergänzung neues Kapitel 5.3.1 „CC-Spezialisten“
1.6	01.11.2024	Anerkennungsstelle S 21	Revision: • Entfernen der Abbildung 1 • Referenz VB-Stellen durch VB-Prüfstellen ersetzt • Anerkennung für ITSEC entfernt

Tabelle: Änderungshistorie

Inhalt

Tabellenverzeichnis

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 und Eingliederung des Programms

Dieses Dokument beinhaltet verpflichtende Anforderungen und weitere wichtige Informationen und Regelungen als Ergänzung zur übergeordneten „Verfahrensbeschreibung zur Anerkennung von Prüfstellen“ [VB-Prüfstellen]. Es richtet sich insbesondere an die Antragsteller, die sich dafür entschieden haben, eine Anerkennung als Prüfstelle im Bereich der Common Criteria (CC) 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.

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

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

Hinweis: Anerkennungen im Bereich Common Criteria gelten nur für die nationale CC-Zertifizierung, die am 31.01.2026 ausläuft und können daher nur noch bis zum 31.01.2026 erteilt werden. Für die Arbeit im Rahmen der europäischen CC-Zertifizierung ist eine Befugniserteilung gem. [VB-Befugnis] notwendig.

[1] Englischer Begriff bzw. Abkürzung „Evaluation Facility“ or „IT-Security Evaluation Facility“, ITSEF

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:
   a. Smartcards and Similar Devices
   b. Hardware Devices and Security Boxes.

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

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.

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.

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

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 benötigen. 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) 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.

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-Prüfstellen] 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 Fachbegutachtung

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 den Profilen darstellen, wodurch die Fachqualifikation gegeben ist.	• CC-Evaluatoren	• Die Anerkennungsstelle bewertet die eingereichten Angaben und Nachweise. • Der Fachbegutachter legt 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 Informationsmanagementsystems

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

Die Prüfstelle hat folgende Pflichten:

Aufgaben der CC-Prüfstelle	**Hilfsmittel [Verzeichnisse]**	**Aufgaben Zertifizierungsstelle (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 Rahmen der Begehung begutachten kann.	• Begutachtungsplan	• Das Begutachterteam begutachtet vor Ort die Maßnahmen und Prozesse, befragt die Fachverantwortlichen, führt eine Begehung der Räumlichkeiten der Prüfstelle sowie der für die Sicherheit der Prüfstelle relevanten Räume und Gerätschaften durch. • Die Ergebnisse werden in dem Abschlussgespräch erläutert und besprochen.

Tabelle 2: Aufgaben bei der Begutachtung des Informationsmanagementsystems

4 Aufrechterhaltung der Anerkennung

4.1 Vorgaben für das CC-Evaluierungsverfahren

Zur Aufrechterhaltung der Anerkennung muss die Prüfstelle die im Dokument [CC-EP] dargelegten Anforderungen an die Abläufe der Evaluierung im Rahmen der Zertifizierung nach Common Criteria sowie zur Reanerkennung einhalten. Darüber hinaus sind die Anforderungen aus Kap. 5 „Spezielle Rahmenbedingungen“ einzuhalten.

4.2 Fachbegutachtung

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

Fünf Monate vor Ablauf der Anerkennung muss ein erneuter Antrag auf Reanerkennung gestellt werden, damit gewährleistet werden kann, dass die Anerkennung lückenlos fortgeführt wird.

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 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. Bei der Erstellung und Überarbeitung von AIS sind die Prüfstellen verpflichtet, sich am Kommentierungsprozess zu beteiligen.
2. 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.
3. 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.
4. 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. Die Kompetenzmatrix der CC-Evaluatoren muss der Anerkennungsstelle immer aktuell vorliegen. Negative Änderungen oder das Ausscheiden eines Evaluators, die sich während eines Evaluierungsverfahrens ergeben, müssen bezogen auf die jeweils in einem Verfahren eingesetzten Evaluatoren unmittelbar dem zuständigen Zertifizierer mitgeteilt werden.

Weitere Regelungen zur Zusammenarbeit sind in dem Dokument CC-EP beschrieben.

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. Dazu ist die Erklärung durch den Prüfstellenleiter mit dem jeweiligen Evaluierungsplan abzugeben.

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. Zusätzlich lädt das BSI den Evaluator zu einem Interview ein, um die Fachkompetenz zu verifizieren (siehe CC-Evaluatoren). Der Evaluator darf nur nach positiver Entscheidung des BSI als erfahrener, eingearbeiteter Evaluator und 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.

5.3.1 CC-Spezialisten

Die Prüfstelle hat die Möglichkeit, Spezialisten für technische Spezialthemen, die im Rahmen einer Evaluierung relevant und erforderlich sind, bei der Anerkennungsstelle zu benennen und bei Bedarf entsprechend einzusetzen.

Die CC-Spezialisten müssen mit ihren Kompetenzen in der Befugnismatrix der Prüfstelle geführt werden.

Die mit der Evaluierung befassten CC-Spezialisten müssen die Anforderungen des Dokuments „Anforderungen an die Sicherheit von Stellen“ [AS-Stellen] (sofern für Personen zutreffend) erfüllen und arbeiten nach den selben Grundsätzen der Sorgfaltspflicht, der Vertraulichkeit, der Unvoreingenommenheit und Unparteilichkeit wie Evaluatoren.

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. Die jeweilig für das Thema zuständigen Evaluatoren des Projektes müssen an dem Workshop teilnehmen.

6 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.