Bundesamt
für Sicherheit in der
Informationstechnik

Produktzertifizierung: Programm IT-Sicherheitszertifizierung Common Critieria (CC)

CC-Produkte

Version 3.5 vom 19.03.2020

Common Criteria

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/Org.Einheit	Beschreibung
1.0	Februar 2005	ZertStelle Ref 322	Erstausgabe der BSI 7138
2.0	Oktober 2010	ZertStelle Ref 322	Neuausgabe der BSI 7138 aufgrund grundlegende Aktualisierung und Ergänzung
2.1	November 2012	ZertStelle Produkt Ref S 22	Revision der BSI 7138 aufgrund Korrekturen nach int./ext. Kommentierung und Aktualisierung
2.2	Februar 2014	ZertStelle Produkt Ref S 22	Revision der BSI 7138 aufgrund Aktualisierung zur internationalen Anerkennung, spezifischen Prozessaspekten, Maintenance.
3.0	10.07.2015	ZertStelle Produkt Ref S 22/ S 23	Neuausgabe Dokument CC-Produkte aufgrund Dokumentenumstrukturierung, inhaltlich als Fortschreibung der BSI 7138
3.1	02.08.2016	ZertStelle Produkt Ref D 22/ D 23	Revison
3.1.1	20.12.2016	ZertStelle Produkt Ref D 22/ D 23	Revison
3.2	24.05.2018	ZertStelle Produkt Ref D 22/ D 23	Revision: • Klarstellung zu Prozessvarianten Maintenance, Reassessment, Partielle ALC Re-Evauierung • Wegfall SigG-Bezug und Bestätigungsverfahren, • Aktualisierung zu Anerkennungsabkommen, • Aktualisierung zu Krypto.
3.3	26.03.2019	ZertStelle Produkt Ref D 22/ D 23	Revision: • Austausch der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramm) • Ergänzung STAR Report zur Unterstützung der Wiederverwendung von Auditergebnissen.
3.4	09.09.2019	QMB SZ	Revision aufgrund Abweichungen aus dem DAkkS-Audit 2019: • Austausch und Umbenennung der Abbildung 1: Zertifizierungs- und Anerkennungsprogramme (Dokumentenübersicht), • Konkretisierung bzgl. der Begrifflichkeiten Zertifizierungssystem und -programm insbesondere in den Kapiteln 1

Version	Datum	Name/Org.Einheit	Beschreibung
			„Einleitung“ und 2 „Zertifizierungsprogramm“.
3.5	19.03.2020	ZertStelle Produkt Ref SZ 21/ SZ 22	Revision: • BMI-KostV durch die BMI-GebV ersetzt • Kap.2.2 „Zertifizierung von Schutzprofilen (Protection Profiles)“Ergänzung zu PP-Zerti • Kap. 3.2.6 „Die Evaluierungsphase“ ergänzt bzgl negativer Beendigung des Verfahrens • Kap.5.5 „Kosten“: Ergänzung zu Kosten bei behördlichen Antragstellern • Kap. 5.6 „Kontakt zur ZertStelle“ ergänzt

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Die Zertifizierung eines Produktes wird auf Veranlassung des Herstellers, Vertreibers oder Entwicklers von IT-Produkten durchgeführt, die Zertifizierung eines Standortes i.d.R. auf Veranlassung des Standortbetreibers, die Zertifizierung eines Schutzprofils auf Veranlassung der Autoren oder Bedarfsträger.

Dieses Dokument richtet sich daher in erster Linie an alle Antragsteller für ein IT-Sicherheitszertifikat, aber ebenso auch an Autoren von Schutzprofilen, die diese auf Konformität mit den zugelassenen Versionen der Prüfkriterien hin zertifizieren lassen wollen sowie an Betreiber von Entwicklungs- und Produktionsstandorten, die diese zertifizieren lassen wollen.

1.1 Zielsetzung des Programms

Dieses Programm beinhaltet detaillierte Anforderungen und Informationen als Ergänzung zum Dokument „Verfahrensbeschreibung zur Zertifizierung von Produkten“ [VB-Produkte] für den Fall, dass sich der Antragsteller entschieden hat, eine Zertifizierung nach Common Criteria durchführen zu lassen. Der Antragsteller findet hier Informationen zur Durchführung des Verfahrens.

Eine Prüfstelle kann einen Hersteller auf Grundlage dieser Unterlagen zur Vorbereitung eines Verfahrens beraten.

Es werden konkret die Aufgaben benannt, die ein Antragsteller berücksichtigen muss, 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.

1.2 Eingliederung in die Dokumentenstruktur

Das Schaubild gibt einen Überblick über die zur Verfügung stehenden Dokumente der Konformitätsbewertung.

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

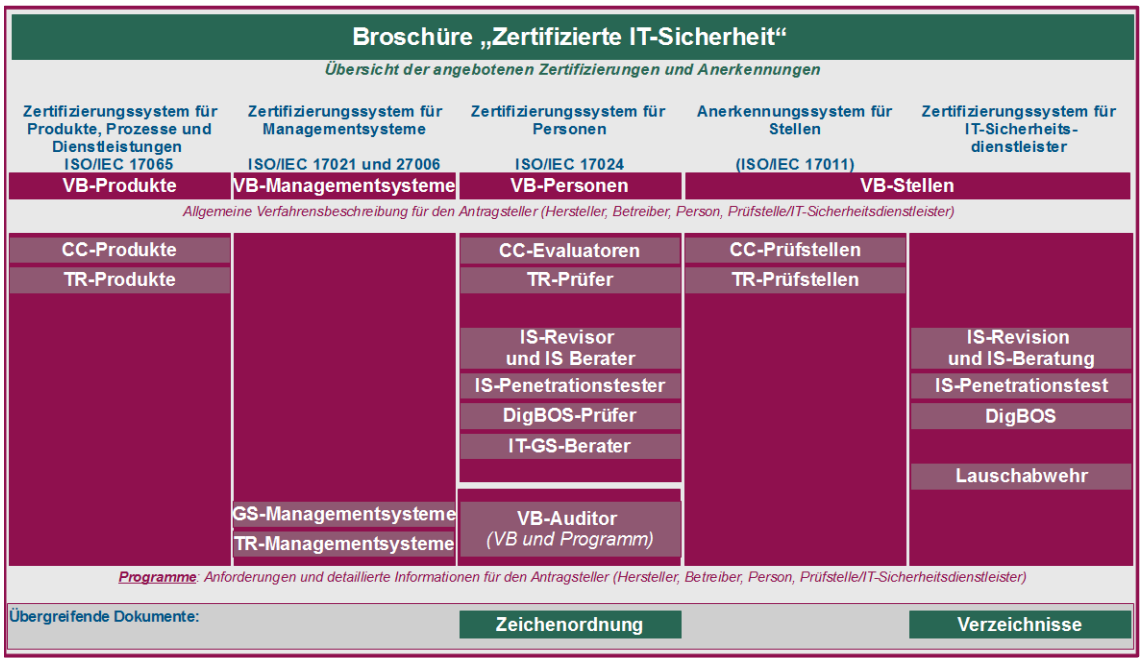

Abbildung 1: Zertifizierungs- und Anerkennungsprogramm (Dokumentenübersicht)

2 Zertifizierungsprogramm

Das Programm zur IT-Sicherheitszertifizierung beschreibt die folgenden Zertifizierungsmöglichkeiten:

1) Zertifizierung eines IT-Produktes nach den Common Criteria (CC[1]) und die ergänzenden Prozesse für die Zertifizierung eines Schutzprofils (Protection Profile, PP) und eines Standortes nach CC,
2) Zertifizierung eines IT-Produktes nach den Information Technology Security Evaluation Criteria [ITSEC].

Die für das Zertifizierungsprogramm notwendigen und aktuell gültigen Dokumente sind im Dokument [Verzeichnis] aufgelistet.

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

2.1 Zertifizierung der IT-Sicherheit von IT-Produkten nach Common Criteria (CC)

2.1.1 Generelle Aspekte der Zertifizierung nach CC

Die Common Criteria (CC) als Spezifikations- und Prüfstandard für IT-Sicherheitssprodukte entstanden in intensiver internationaler Zusammenarbeit und wurden auch in den ISO-Standard 15408 überführt.

Die CC gliedern sich in 3 Teile. Der Teil 1 stellt die Grundlagen der Kriterien dar und gibt einen Überblick über die Konzepte der CC. Die Teile 2 und 3 der Common Criteria sind Kataloge mit denen die Sicherheitsanforderungen an die Funktionalität und an die Vertrauenswürdigkeit (Assurance) eines Produktes strukturiert spezifiziert werden können. Sie bilden die Grundlage zur Festlegung des jeweils zu evaluierenden Produktumfanges und der Prüfmethoden und Prüftiefe. Sie sind in ihrer generischen Struktur für die Evaluierung von vielen unterschiedlichen IT-Produkten anwendbar.

Für die konsistente Anwendung der CC dient das Evaluationshandbuch „Common Evaluation Methodology (CEM)“ [CEM]. Es dient den Prüfstellen als Prüfanleitung und wurde auch in den ISO-Standard 18045 überführt.

Auf der Internetseite[2] des [CCRA] sind aktuelle Informationen zu den CC und CEM zu finden. Die aktuell gültige, sowie auch frühere Versionen der Kriterien, stehen dort zum Download bereit.

Die Anforderungen der Kriterienwerke sind mit dem Ziel, sie auf ein möglichst breites Produktspektrum anwenden zu können, generisch und stellenweise interpretierbar formuliert worden. Aus diesem Grund werden Anwendungshinweise und Interpretationen zum Schema (AIS) als separate Dokumente von der Zertifizierungsstelle des BSI veröffentlicht. Themen der AIS-Dokumente sind z. B. Evaluierungsanforderungen für Hardware und Smartcards, Anforderungen an Zufallszahlengeneratoren, Evaluierungsmethodik für höhere Prüfstufen, Entwicklung und Evaluierung formaler Sicherheitsmodelle, Leitfadendokumente zur Unterstützung der Antragsteller für die Bereitstellung der Nachweise, Interpretationen gültiger Vorgaben sowie verschiedene verfahrensbezogene Regelungen.

Die AIS-Dokumente schließen grundsätzlich die international abgestimmten Dokumente zur Anwendung der Kriterienwerke wie z. B. die Dokumente der Joint Interpretation Working Group (JIWG Supporting

1 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

2 http://www.commoncriteriaportal.org

Documents aus dem SOG-IS-Anerkennungsabkommen [SOGIS-MRA]) und die sogenannten CC Supporting Documents aus dem internationalen Anerkennungsabkommen CCRA ein.

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.

Zur Vereinfachung und zur Standardisierung von Produktzertifizierungen können sogenannte Protection Profiles (Schutzprofile) verwendet werden. In Schutzprofilen sind Sicherheitsanforderungen für Produktklassen als Quasi-Standard festgelegt. Sie ermöglichen daher, vergleichbare Sicherheitsvorgaben und damit vergleichbare Zertifikate für IT-Produkte zu erstellen.

Die unter dem Dach des europäischen SOG-IS-Anerkennungsabkommens organisierten Nationen erklären bestimmte Schutzprofile, die sie als Standard für den jeweiligen Technologiebereich ansehen, zu sogenannten SOG-IS Recommended PPs. Ebenso stellen auch die unter dem Dach des CC Anerkennungsabkommens (CCRA) entwickelten sogenannten Collaborative Protection Profiles (cPP) insbesondere für Produktklassen im Bereich der kommerziellen Standardprodukte („Commercial of the Shelf Products”) weitreichend abgestimmte Mindestanforderungen zur Anwendung in Produktzertifizierungsverfahren dar. Bei Ausschreibungen oder Beschaffungsprozessen kann ein Bedarfsträger auf ein jeweils im Technologiebereich relevantes Schutzprofil als Anforderung oder Mindestanforderung an die erforderlichen Produkte Bezug nehmen und ggf. darauf aufbauend individuelle Zusatzanforderungen bedarfsorientiert formulieren.

Neben den Regularien aus den Kriterien und den Anerkennungsabkommen muss eine Zertifizierung durch das BSI die Randbedingungen des [BSIG] einhalten. Daraus resultiert ein Zertifizierungsvorbehalt bei öffentlichem Interesse nach BSIG § 9, Abs. 4 (2), etwa wenn sicherheitspolitische Interessen der Bundesrepublik Deutschland einer Zertifizierung entgegenstehen. Im konkreten kann sich dies z. B. auf Hersteller, Produkte oder die Auswahl der kryptografischen Algorithmen und Funktionen und die diesbezügliche Evaluierungsmethodik beziehen. Die Prüfung eines Zertifizierungsvorbehaltes erfolgt im Einzelfall vor Annahme eines Zertifizierungsantrages und abschließend vor der Erteilung eines Zertifikates.

Bezüglich der kryptografischen Algorithmen und Funktionen sind Rahmenbedingungen in spezifischen Verfahrensvorgaben, in AIS 46 oder in Technischen Richtlinien des BSI verankert und werden zu Beginn eines Antragsverfahrens festgelegt. Für die Auswahl von kryptografischen Algorithmen gilt der SOG-IS Kryptokatalog [SOGIS-ACM], die Technische Richtlinie BSI [TR-03116] oder die Technische Richtlinie BSI [TR-02102]. Bei Verwendung schwächerer oder proprietärer Algorithmen erfolgt eine Entscheidung durch das BSI im Einzelfall, ob der jeweilige Algorithmus im Rahmen der Zertifizierung, ggf. unter Auflagen, akzeptiert werden kann. Bei Verwendung proprietärer Algorithmen als Teil des zu zertifizierenden Produktes ist mit erhöhtem Zeitaufwand für die Analyse der Eignung dieser Algorithmen und für die Evaluierung und Abnahme durch das BSI zu rechnen.

2.1.2 Zertifizierung von Produkten nach CC

Bei der Zertifizierung eines Produktes durch das BSI nach CC muss grundsätzlich ein vom BSI zertifiziertes oder als geeignet anerkanntes Schutzprofil zur Erstellung der für das Zertifizierungsverfahren geltenden Sicherheitsvorgabe angewendet werden. Damit wird die Vergleichbarkeit von verschiedenen Produktzertifikaten für einen Produkttyp verbessert und gleichzeitig der Prozess der Produktzertifizierung effizienter gestaltet. Ist für einen Produkttyp kein vom BSI als geeignet anerkanntes Schutzprofil verfügbar, so gestaltet sich die Vorbereitungsphase als wesentlich aufwendiger, da das BSI vor Aufnahme des Verfahrens im Einzelfall auf Basis der individuellen Produkt-spezifischen Sicherheitsvorgaben über die grundsätzliche Zertifizierbarkeit des Produktes entscheiden muss.

Schutzprofile stehen für verschiedene Produkttypen zur Verfügung. Vom BSI zertifizierte Schutzprofile sind auf der Internetseite des BSI veröffentlicht. Weitere Schutzprofile stehen auf der Internetseite des CCRA und des SOG-IS MRA zur Verfügung. Die Konformität eines zertifizierten Schutzprofils mit den CC wird im Rahmen des CCRA und des SOG-IS MRA unter den jeweiligen Nationen gegenseitig anerkannt. Die

inhaltliche Eignung eines Schutzprofils, das zur Durchführung einer bestimmten Produktzertifizierung verwendet werden soll, wird im Einzelfall geprüft. Die Verwendung nicht zertifizierter Schutzprofile ist nur in begründeten Ausnahmen möglich und verursacht Mehraufwände.

Neben den Anforderungen aus dem Schutzprofil können zusätzliche Funktionalitäten und grundsätzlich auch höhere Prüfanforderungen in einem Produktzertifizierungsverfahren berücksichtigt werden. Höhere Prüfanforderungen führen jedoch zu höheren Kosten- und Zeitaufwänden. Details zur Erstellung von Sicherheitsvorgaben sind in Teil 1 der CC und im dem Dokument AIS 41 „Guidelines for PPs and STs“ [AIS 41] erläutert.

Die Prüfkomponenten (Assurance Components) aus Teil 3 der CC werden i.d.R. gemäß der vordefinierten EAL-Stufen ausgewählt, ggf. ersetzt durch höherwertige Komponenten (Augmentierung). Bei Verwendung eines Schutzprofils sind die Komponenten durch das Schutzprofil festgelegt, können in begründeten Fällen aber auch durch höherwertige Komponenten ersetzt werden. Ausnahme ist die Anwendung eines cPP unter der Anerkennung des CCRA, wo exakt die im cPP festgelegten Komponenten zu verwenden sind.

2.1.3 Zertifizierung von Produkten in Technical Domains

Im europäischen Anerkennungsabkommen [SOG-IS MRA] und auch im internationalen Abkommen CCRA sind spezifische technische Bereiche (Technical Domains) festgelegt, in denen Zertifizierungsverfahren besonderen Anforderungen und Vorgaben genügen müssen.

Eine Technical Domain unter SOG-IS MRA spiegelt dabei eine IT-Produktfamilie, für die eine gemeinsame technische Evaluierungskompetenz notwendig ist, wider. Dies trifft insbesondere im Bereich der Schwachstellenanalyse zu. Darüber hinaus ist damit auch eine höherwertige Anerkennung (höher als EAL 4) von Zertifikaten unter besonderen Rahmenbedingungen geregelt. Derzeit sind die Technical Domains „Smartcards and Similar Devices” und „Hardware Devices with Security Boxes” definiert.

Im CCRA stellt eine Technical Domain einen Bereich dar, in dem eine internationale Technical Community (iTC) ein gemeinsames Schutzprofil (cPP) mit spezifischer Evaluierungsmethodologie als Verfeinerung der CEM entwickelt hat.

Querschnittthemen wie etwa die Evaluationsmethodologie für kryptografische Sicherheitsmechanismen werden in beiden Abkommen in jeweils separaten Arbeitsgruppe erarbeitet, um diese schließlich verbindlich vorzuschreiben.

Bei der Auswahl einer Prüfstelle ist darauf zu achten, dass die Stelle über die BSI-Anerkennung/Lizenzierung für die jeweilige Technical Domain verfügt.

2.1.3.1 Technical Domain „Smartcards and Similar Devices“

Diese Technical Domain aus dem SOG-IS MRA bezieht sich auf Smartcards und ähnliche Produkte, bei denen ein wesentlicher Teil der erforderlichen Sicherheitsfunktionalität von Eigenschaften der Hardware auf Chiplevel abhängt. Dazu zählen zum Beispiel Smartcard-Hardware/ICs, Smartcard-Produkte (Komposition aus Chip, Betriebssystem und Anwendung z.B. für Signaturkarten, Java Cards, Digitale-Tachograph-Karten, Gesundheitskarten), TPMs oder Chip-Sicherheitsmodule.

Bei Zertifizierung eines Produktes aus diesem Bereich unter der Anerkennung durch das SOG-IS MRA müssen die für diese Technical Domain gehörigen JIL Supporting Documents, in denen die Evaluierungsmethodologie der CEM technologiespezifisch verfeinert wird, angewendet werden. Diese Unterlagen sind Teil der AIS aber auch der Internetseite[3] des [SOGIS-MRA] der Rubrik Supporting Documents zu entnehmen.

3 http://www.sogisportal.eu

2.1.3.2 Technical Domain „Hardware Devices with Security Boxes“

Die Technical Domain „Hardware Devices with Security Boxes” bezieht sich auf Produkte, die aus diskreten Bauteilen auf einer oder mehreren Leiterplatten aufgebaut sind, wobei wesentliche Bestandteile der erforderlichen Sicherheitsfunktionalität von einer physischen Hardwareschutzhülle, die Gegenmaßnahmen gegen direkte physische Angriffe beinhaltet, erbracht werden (sog. Security Box). Dazu zählen zum Beispiel Payment Terminals, Tachograph Vehicle Units, Smart-Grid-Komponenten, Taxameter, Zugangskontroll-Terminals oder Hardwaresicherheitsmodule (HSM).

Bei Zertifizierung eines Produktes aus diesem Bereich unter der Anerkennung durch das SOG-IS MRA müssen die für diese Technical Domain gehörigen JIL Supporting Documents, in denen die Evaluierungsmethodologie der CEM technologiespezifisch verfeinert wird, angewendet werden. Diese Unterlagen sind Teil der AIS aber auch auf der Internetseite[4] des [SOGIS-MRA] der Rubrik Supporting Documents zu entnehmen.

2.1.3.3 Zertifizierung auf Grundlage von cPPs

Bei Zertifizierung eines Produktes nach einem cPP unter der Anerkennung durch das CCRA ist eine exakte Konformität mit dem cPP einzuhalten, d.h. die Sicherheitsvorgabe für das Produktzertifizierungsverfahren darf weder bei den funktionalen Sicherheitsanforderungen noch bei den Prüfanforderungen vom cPP abweichen, auch wenn das IT-Produkt mehr Sicherheitsleistung bietet.

Zusätzlich müssen die zu dem cPP zugehörigen CCRA Supporting Documents, in denen die Evaluierungsmethodologie der CEM technologiespezifisch verfeinert wird, angewendet werden. Diese Unterlagen sind auf der Internetseite[5] des [CCRA] der Rubrik Collaborative PPs zu entnehmen.

Über das cPP hinausgehende Sicherheitseigenschaften können in einem zweiten Zertifikat im Rahmen des gleichen Evaluationsverfahrens unter Ausnutzung der Re-Use-Prozesse erteilt werden. Dieses ist dann entweder nicht im CCRA anerkannt oder nicht konform zu dem cPP und bis EAL 2 im Rahmen des CCRA anerkannt.

2.2 Zertifizierung von Schutzprofilen (Protection Profiles)

Der Autor eines Schutzprofils ist i. d. R. eine Behörde, eine regulatorisch wirkende öffentliche Instanz, eine Organisation, die mit Standardisierung befasst ist, oder eine Anwenderorganisation, da es sich bei einem Schutzprofil um einen Standard für Sicherheitsanforderungen im Hinblick auf einen bestimmten Sicherheitsbedarf in einem Anwendungsbereich handelt, der bei einer späteren Produktzertifizierungen herangezogen werden soll. Einen Antrag auf Zertifizierung eines Schutzprofils durch das BSI kann daher grundsätzlich nur von solchen Organisationen gestellt werden.

Im Rahmen der Zertifizierung eines Schutzprofils wird dessen Konformität mit dem CC-Standard geprüft und bestätigt. Darüber hinaus prüft das BSI die Angemessenheit der Sicherheitsanforderungen für den beschriebenen Einsatzbereich der jeweiligen Produkte, u.a. die Anforderungen an kryptografische Funktionen und Algorithmen.

Die Prüfkomponenten für die Evaluierung eines Schutzprofils werden der Klasse APE aus Teil 3 der CC entnommen.

Eine implizite Zertifizierung von Schutzprofilen durch Anwendung in Produktzertifizierungsverfahren unter Berufung auf die Ähnlichkeit von ASE und APE ist nicht möglich.

4 http://www.sogisportal.eu

5 http://www.commoncriteriaportal.org

Da ein Schutzprofil übergeordnete Bedeutung in der Standardisierung hat, findet zur Zertifizierung eines Schutzprofils immer ein Vorgespräch mit der Zertifizierungsstelle statt. Darin wird unter Einbeziehung von Fachexperten der Inhalt des Schutzprofils besprochen und ggf. Randbedingungen und Restriktionen (z.B. zu Kryptoverfahren) erläutert.

2.3 Zertifizierung von Standorten (Site-Certification)

Zur Unterstützung späterer Produktzertifizierungen können Entwicklungs- und Produktionsstandorte für IT-Produkte separat nach Common Criteria evaluiert und zertifiziert werden. Der Betreiber eines solchen Standortes kann beim BSI einen Antrag auf Zertifizierung eines Standortes nach CC stellen. Ziel einer solchen Standortzertifizierung ist i. d. R. die separate Produkttyp bezogene Prüfung der Standortssicherheit, des Konfigurationsmanagements und der Annahme- und Lieferprozesse (ggf. auch Teilaspekte von Tools). Im Einzelnen wird dies in einer Standortsicherheitsvorgabe jeweils festgelegt. Die Ergebnisse sollen dann zur Wiederverwendung in späteren Zertifizierungsverfahren für IT-Produkte, die in diesem Standort entwickelt oder produziert werden, geeignet sein. Mit der Standortzertifizierung können Synergieeffekte bei Produktzertifizierungen erreicht werden, z. B. wenn verschiedene Produkte gleichen Typs und möglicherweise von verschiedenen Entwicklerfirmen in einem Standort produziert werden.

Bei der Evaluierung werden insbesondere auch die CC-Zusatzdokumente zur Standortzertifizierung angewendet (siehe auch zugehörige Anwendungshinweise und Interpretationen [AIS 47] und Supporting Document „Site-Certification“ [SupDoc-SC]). Zusätzlich findet auch das Supporting Document „Minimum Site Security Requirements“ (siehe [AIS 1]) Anwendung.

Für die Erteilung eines Standortzertifikates nach Common Criteria für einen Entwicklungs- oder Produktionsstandort für IT-Produkte ist mit der Beantragung des Zertifikates die Bereitstellung eines Dokumentes Standortsicherheitsvorgaben (Site Security Target (SST)) erforderlich. Darin werden Umfang und Tiefe der geplanten Zertifizierung nach den Anforderungen der CC [SupDoc-SC] sowie der zugehörigen [AIS 47] dargelegt.

Die Prüfkomponenten für die Evaluierung eines Standortes werden der Klasse ALC aus Teil 3 der CC mit den Ergänzungen und Verfeinerungen aus [SupDoc-SC] entnommen. Für die Evaluierung der Standortsicherheitsvorgabe wird die Klasse AST aus [SupDoc-SC] verwendet. Zur Unterstützung der Wiederverwendung des Zertifizierungsergebnisses in nachfolgenden Produktzertifizierungen sollte nach Abnahme des Prüfergebnisses der so genannte Site-Technical-Audit-Report (STAR) (siehe [AIS 1]) von der Prüfstelle erstellt werden. Dieser Report enthält über den Zertifizierungsreport und das SST hinausgehende Informationen für einen Produktevaluator.

2.4 Zertifizierung der IT-Sicherheit von Produkten nach Information Technology Security Evaluation Criteria (ITSEC)

Die europäischen Kriterien ITSEC [ITSEC] für die Evaluierung von IT-Produkten können im BSI Zertifizierungsschema nur noch in begründeten Ausnahmefällen angewendet werden, z. B. wenn Altverträge zwischen einem Bedarfsträger und einem Hersteller bestehen oder Gesetze und Verordnungen dies ausschließlich erfordern. Daher werden Neuanträge auf Zertifizierung nach ITSEC grundsätzlich nicht mehr angenommen. Im Folgenden wird nur auf CC Bezug genommen. ITSEC Anforderungen müssen im Einzelfall entsprechend abgeleitet werden.

2.5 Zertifizierung von Produkten nach Anforderungen aus EU-Verordnungen

2.5.1 VERORDNUNG (EU) Nr. 910/2014 (eIDAS-VO)[6]

Gemäß Vertrauensdienstegesetz (VDG) ist das Bundesamt für Sicherheit in der Informationstechnik die öffentliche Stelle gemäß Artikel 30 Absatz 1 der Verordnung (EU) Nr. 910/2014 sowie gemäß Artikel 39 Absatz 2 in Verbindung mit Artikel 30 Absatz 1 der Verordnung (EU) Nr. 910/2014. Die Zertifizierungsstelle des BSI nimmt diese Aufgabe wahr.

Nach der Verordnung Artikel 29 und 30 müssen qualifizierte elektronische Signaturerstellungseinheiten (QSCD) Anhang II der Vorordnung erfüllen und nach Artikel 30 (3) nach bestimmten Verfahren zertifiziert werden. Das bedeutendste Verfahren ist die Zertifizierung der QSCD nach Common Criteria unter Verwendung bestimmter CC-Schutzprofile. Diese sind im zugehörigen Durchführungsbeschluss[7] aufgelistet. Die Zertifizierung der QSCD muss bestätigen, das das Produkt konform zum jeweiligen Schutzprofil ist. Dazu wird das Schutzprofil zur Erstellung der Sicherheitsvorgaben herangezogen. Die Evaluierung und Zertifizierung erfolgt dann nach dem regulären Verfahren (siehe Kap. 3).

Alternativ dazu, ermöglicht die eIDAS Verordnung die Anwendung von einem anderen Verfahren, sofern dabei gleichwertige Sicherheitsniveaus angewendet werden und dieses Verfahren der Kommission mitteilt. wurde. Dieses Verfahren darf nur angewendet werden, wenn Normen im Sinne des Artikel 30 Abs. 3 a) nicht vorliegen oder ein Sicherheitsbewertungsverfahren im Sinne des Artikel 30 Abs. 3 a) im Gange ist. Als alternatives Prüfverfahren gilt hier derzeit z.B. die CC-Zertifizerung eines Produktes nach einem Schutzprofil der Serie EN 419221-x solange diese noch nicht direkt im Durchführungsbeschluss aufgelistet sind.

Die EU Kommission führt eine öffentliche Liste aller nach den Regularien der VO zertifizierten QSCD. Die Zertifizierungsstelle des BSI meldet nach Zertifizierung einer solchen QSCD die relevante Information an die EU Kommission.

2.5.2 VERORDNUNG (EU) Nr. 165/2014 (Digitaler Fahrtenschreiber)[8]

Nach der Verordnung muss die Sicherheit der Komponenten (Motion Sensor, Vehicle Unit, Tachograph Card, GNSS Module) durch eine Zertifizierung nachgewiesen werden. Im zugehörigen Durchführungsbeschluss [9] wird für die Zertifizierung auf die relevanten Schutzprofile verwiesen. Die Schutzprofile wurden durch die EU Kommission (JRC) erstellt und nach Common Criteria zertifiziert. Sie sind auf der Internetseite des BSI und auch auf der Internetseite des SOGIS Anerkennungsabkommens (www.sogisportal.eu) verfügbar.

6 VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

7 DURCHFÜHRUNGSBESCHLUSS (EU) 2016/650 DER KOMMISSION vom 25. April 2016 bzw. ggf. aktualisierte Fassung

8 VERORDNUNG (EU) Nr. 165/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 4. Februar 2014 über Fahrtenschreiber im Straßenverkehr, zur Aufhebung der Verordnung (EWG) Nr. 3821/85 des Rates über das Kontrollgerät im Straßenverkehr und zur Änderung der Verordnung (EG) Nr. 561/2006 des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Sozialvorschriften im Straßenverkehr

9 DURCHFÜHRUNGSVERORDNUNG (EU) 2016/799 DER KOMMISSION vom 18. März 2016 zur Durchführung der Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates zur Festlegung der Vorschriften über Bauart, Prüfung, Einbau, Betrieb und Reparatur von Fahrtenschreibern und ihren Komponenten bzw. ggf. aktualisierte Fassung

Die Zertifizierung der Komponenten des Fahrzeugschreibers muss bestätigen, das das Produkt konform zum jeweiligen Schutzprofil ist. Dazu wird das Schutzprofil zur Erstellung der Sicherheitsvorgaben herangezogen. Die Evaluierung und Zertifizierung erfolgt dann nach dem regulären Verfahren (siehe Kap. 3).

3 Verfahren zur Zertifizierung

3.1 Beteiligte Stellen an einer Zertifizierung

Am Gesamtprozess der Zertifizierung sind drei Stellen beteiligt:

1. Der Antragsteller (Hersteller, Sponsor oder Vertreiber eines IT-Produkts / Behörde oder Anwenderorganisation als Verfasser eines Schutzprofils / verantwortlicher Betreiber eines Entwicklungs- oder Produktionsstandortes).
2. Die vom Antragsteller ausgewählte und für das jeweilige Programm anerkannte Prüfstelle. Anhand der vom BSI veröffentlichten Liste der anerkannten Prüfstellen beauftragt der Antragsteller eine für das entsprechende Programm geeignete Prüfstelle mit der Durchführung der Evaluierung seines Produktes. Das BSI hat vertragliche Vereinbarungen bzw. verwaltungsrechtliche Nebenbestimmungen mit den anerkannten Prüfstellen zur Durchführung von Evaluierungen im Hinblick auf eine Zertifizierung durch das BSI. Die Regelungen und Prozesse der Prüfstelle stellen sicher, dass die Vertraulichkeit gewahrt ist. Die Befugnis für die Mitarbeiter der Prüfstelle bezieht sich jeweils auf bestimmte Technologien, Produktgruppen und Prüfaspekte.
3. Die Zertifizierungsstelle des BSI.
   Die Mitarbeiter der Zertifizierungsstelle begleiten die von der Prüfstelle durchgeführte Evaluierung. Zur personellen Unterstützung hat das BSI eine vertraglich vereinbarte Kooperation in der Prüfbegleitung mit dem Fraunhofer Institut FOKUS. Das dort eingerichtete „CertLab" kann vom BSI unterbeauftragt werden, eine bestimmte Prüfbegleitung im Rahmen eines Zertifizierungsverfahrens durchzuführen. Die Regelungen und Prozesse der Zertifizierungsstelle und die darauf abgestimmten Regelungen und Prozesse von CertLab in Verbindung mit der vertraglichen Regelung zwischen BSI und Fraunhofer FOKUS stellen sicher, dass die Vertraulichkeit gewahrt ist und Prüfbegleitungen bei CertLab vergleichbar mit denen beim BSI durchgeführt werden. Eine spezielle verfahrensbezogene Vertraulichkeitsvereinbarung (NDA) zwischen Antragsteller und Fraunhofer FOKUS (CertLab) ist auf Grund der Vertragsgestaltung mit dem BSI nicht erforderlich. Der Prüfbegleiter bei CertLab hat dieselbe Rolle und damit dieselben Aufgaben und Pflichten wie ein Prüfbegleiter im BSI. Er erhält genau so wie ein Prüfbegleiter des BSI alle für die Durchführung der Prüfbegleitung notwendigen Herstellernachweise und Prüfergebnisse. Die Befugnis für die Mitarbeiter des CertLab bezieht sich nur auf bestimmte Technologien und Produktgruppen und nur auf das jeweilige Zertifizierungsverfahren. Die Abnahme des abschließenden Evaluierungsberichtes und die Zertifizierung des Produktes erfolgt ausschließlich durch das BSI.

3.2 Prüf- bzw. Evaluierungsgegenstand (EVG, TOE)

Die Prüfung und Bewertung bezeichnet man als Evaluierung. Der Prüfgegenstand wird daher im Rahmen einer Zertifizierung nach CC als Evaluierungsgegenstand (EVG, engl. Target of Evaluation, TOE) bezeichnet. Neben der Festlegung des Evaluierungsgegenstandes (logisch und physische Abgrenzung und Identifizierung) wird zu Beginn eines Verfahrens in dem jeweiligen Dokument Sicherheitsvorgabe auch der Prüfumfang, d.h. die Auswahl der Prüfkomponenten aus Teil 3 der CC, festgelegt.

3.2.1 EVG bei Produktzertifizierungen

Bei Produktzertifizierungen handelt es sich bei dem EVG um ein IT-Produkt einschließlich der Anwendungshandbücher. Die CC-Version 3.1 definiert Target of Evaluation als: „set of software, firmware and/or hardware possibly accompanied by guidance“. Der zu prüfende EVG wird zu Beginn eines Zertifizierungsverfahrens vom Antragsteller im Dokument Sicherheitsvorgaben (Security Target, ST) auf das

Produkt bezogen definiert. Bei Verwendung eines Schutzprofils ist die logische und physische Abgrenzung des EVG durch das Schutzprofil vorbestimmt.

Es können Produkte unterschiedlichster Art evaluiert werden:

- Softwareprodukte (z. B. Betriebssysteme, Datenbanksysteme, Anwendungsprogramme, VPN-Software, Firewalls).
- Hardwareprodukte (z. B. Smartcard Integrated Circuits).
- Kombinationen aus Software und Hardware (z. B. Hardware einer Smartcard zusammen mit einem Betriebssystem und einer darauf befindlichen Anwendung, Embedded Devices wie z.B. Hardwaresicherheitsmodule, Kartenterminals).
- Kombinationen aus einzelnen Softwareprodukten.

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 (Assets) stehen, und dies zu Beginn in den verfahrensindividuellen Sicherheitsvorgaben festgelegt ist.

In Abhängigkeit vom Entwicklungsstadium des Produktes können verschiedene Arten der Evaluierung eines Produktes unterschieden werden. Eine Evaluierung kann:

1. entwicklungsbegleitend in den Phasen Produktentwurf- und Konzipierung, Implementierung, Prototyperstellung und Abnahme als Erstevaluierung und Zertifizierung erfolgen. Dabei werden Zug um Zug die notwendigen Prüfschritte durchgeführt, so dass das Zertifikat fast zeitgleich mit der Markteinführung vorliegen kann,
2. für eine bereits existierendes und im Markt befindliches Produkt erfolgen,
3. für ein weiterentwickeltes zertifiziertes Produkt als Deltaprozess erfolgen (Assurance-Continuity-Prozess, d. h.: Reevaluierung / Rezertifizierung oder Maintenance je nach Sicherheitsrelevanz der Änderungen.

Die Erfahrung hat gezeigt: Je früher im Entwicklungsstadium eines Produktes mit der Evaluierung und Zertifizierung begonnen wird, um so kostengünstiger und zeitsparender für den Hersteller kann das Verfahren durchgeführt werden. Abhängig vom jeweiligen Entwicklungsstadium des Produktes kann die Planung der Evaluierung und Zertifizierung individuell zwischen den beteiligten Stellen abgestimmt werden, um sie in den Entwicklungsprozess zu integrieren.

3.2.2 EVG bei Schutzprofilzertifizierung

Bei einer Schutzprofilzertifizierung ist der EVG das jeweilige Dokument Schutzprofil.

3.2.3 EVG bei Standortzertifizierung

Bei Standortzertifizierungen ist der EVG ein Entwicklungs- oder Produktionsstandort oder eine entsprechende Organisationseinheit, die bestimmte Dienste im Rahmen der Entwicklung oder Produktion eines nachfolgend zu zertifizierenden IT-Produktes bietet, in ihren festgelegten physischen, logischen und organisatorischen Grenzen. Die logische Abgrenzung beschreibt die Rolle, die der Standort im Lebenszyklus einer Produktentwicklung und Produktion spielt sowie die logische Abgrenzung innerhalb der IT-Systeme. Die physische Abgrenzung ist durch die relevanten Räumlichkeiten, den Ort und die Standorte der IT-Systeme gegeben. Innerhalb dieser Abgrenzungen werden Verfahren, Prozesse und Regeln geprüft und die Abhängigkeiten von Dritten Stellen (z.B. andere Standorte eines Herstellers, ein Lieferant oder eine IT-Dienstleister) ermittelt. Der zu prüfende Standort wird zu Beginn eines Standortzertifizierungsverfahrens vom Antragsteller im Dokument Standortsicherheitsvorgaben (Site Security Target, SST) definiert [AIS47].

Zum Zeitpunkt der Evaluierung und Zertifizierung eines Standortes nach CC müssen die physischen, logischen und organisatorischen Grenzen definiert sein und die Verfahren, Prozesse und Regeln, die zur Entwicklung bzw. Produktion eines nach CC zu zertifizierenden IT-Produktes oder den jeweiligen Produkttyp erforderlich sind, vor Ort implementiert und nachweisbar in ihrer Anwendung sein.

3.2.4 Zertifizierungsprozess als Phasenmodell

Die Erst- und Rezertifizierung von Produkten, Schutzprofilen und Standorten ist in 3 Phasen aufgeteilt, die Vorbereitungsphase, die Evaluierungsphase und die Zertifizierungsphase. Dies gilt auch für spezifische Prozesse wie einer Neubewertung / Re-Assessment der Angriffsresistenz (AVA) oder einer partiellen Evaluierung nur von Aspekten des Produktlebenszyklus (ALC).

Diese Prozessarten unterscheiden sich nicht im grundsätzlichen Ablauf, alle drei Hauptphasen werden durchlaufen, jedoch liegen Unterschiede in der Art der bereitzustellenden Nachweise durch den Antragsteller, in der Art und Umfang der angewandten Prüfkomponenten nach CC und in der Art der Zertifizierungsdokumente am Ende.

Bei einem Maintenance-Verfahren, das sicherheitsirrlevante Änderungen betrifft, ist Phase 2 (Evaluierung) nicht relevant.

3.2.5 Vorbereitungsphase

Aufgrund der Vorgaben der Sicherheitskriterien werden für die Evaluierung eines IT-Produktes oder eines Standortes in Abhängigkeit von der gewählten Prüftiefe bestimmte Nachweise vom Antragsteller verlangt. Bei Evaluierung eines IT-Produktes werden neben der Bereitstellung des Produktes bestimmte Nachweise zum Produktdesign, Handbücher und Testnachweise in dokumentierter Form benötigt. Umfang und Beschreibungstiefe dieser Informationen richten sich nach den jeweils verwendeten Prüfkomponenten aus den CC, die im Dokument Sicherheitsvorgaben festgelegt sind.

Für die Erstellung der Antragsunterlagen, insbesondere der Anlagen zum Zertifizierungsantrag, kann Beratungskompetenz aus dem Bereich der Prüfstellen hinzugezogen werden.

Das Dokument Sicherheitsvorgabe (Security Target) hat die zentrale Bedeutung für die Zielsetzung und Durchführung des Verfahrens. Darin wird neben der Identifikation und Abgrenzung des Evaluierungsgegenstandes das Sicherheitsproblem in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken, die Sicherheitsziele und die funktionalen Sicherheitsanforderungen festgelegt. Details zur Strukturierung des Security Target finden sich in CC Teil 1 und AIS 41.

Typischer Ablauf im Einzelnen:

Aufgaben Antragsteller/Hersteller	**Hilfsmittel (zusätzlich zu CC und CEM)**	**Aufgaben Prüfstelle**	**Aufgaben Zertifizierungs-stelle**
Informationen austauschen / Informationsgespräche führen: • Über Sicherheitseigenschaften, vorgesehene Einsatzumgebung und technische Eigenschaften des Produktes informieren. • Design-Konzept, Komplexität und Entwicklungsmethoden erläutern.	VB-/CC-Produkte individuell spezifische AIS-Dokumente CC-Schulung	• Über das Verfahren zur Zertifizierung informieren. • Sich über das zu zertifizierende Produkt und den Hersteller informieren.	• Darlegung des Prozesses und der Randbedingungen.

Aufgaben Antragsteller/Hersteller	Hilfsmittel (zusätzlich zu CC und CEM)	Aufgaben Prüfstelle	Aufgaben Zertifizierungs-stelle
Dokument Sicherheitsvorgaben (Security Target) erstellen.	ggf. PP AIS 41 AIS 46 AIS 47	• Evaluator kann erstes Assessment der Sicherheitsvorgaben durchführen und Rückmeldung geben.	
Prüfung auf Verfügbarkeit der erforderlichen Nachweise und Verwendbarkeit: • Absprache mit Prüfstelle, welche Nachweise in welcher Form erforderlich sind und welche Kriterien und unterstützende Dokumente heranzuziehen sind. • Ermittlung der relevanten Entwicklungs- und ggf. Produktionsstandorte sowie Dritthersteller, die Teile des EVG entwickeln oder produzieren. (bei Drittherstellern: Unterstützung des Antragstellers durch schriftliche Zusage der Dritthersteller ist erforderlich.) • Bei geplanter Wiederverwendung von Prüfergebnissen aus anderen Zertifizierungsverfahren deren grundsätzliche Eignung, Verfügbarkeit und Vollständigkeit ermitteln.	AIS 23 AIS 42	• beim "Readyness-Assessment" unterstützen, d.h. Analyse, welche Nachweise beim Hersteller bereits vorliegen bzw. noch erstellt oder ergänzt werden müssen. *Ebenso kann im Rahmen der Vorevaluierung eine erste Analyse der Sicherheitseigenschaften des Produktes erfolgen, um so grundsätzlichen Problemen bei der Evaluierung vorzubeugen.*	
Weitere Anlagen zum Antrag erstellen: • Kryptoliste, Übersicht Standorte, ggf. IAR (siehe Kap. 3.2.5.1).	AIS 46 (Krypto) ggf. AIS 38 (IAR)	• Evaluator kann erstes Assessment der Anlagen durchführen und Rückmeldung geben.	
Evaluierungsvertrag mit der Prüfstelle abschließen: *Der Evaluierungsvertrag regelt die Beauftragung der Prüfstelle zur Durchführung der Evaluierung.* • Bei der Erstellung des Zeitplanes mitwirken.	AIS 23 AIS 42 AIS und Methodologiedokumente gemäß Verzeichnis	• Evaluierungsvertrag abschließen. • Zeitplan zu Evaluierungstätigkeiten und der Lieferungen an die Zertifizierungsstelle mit dem Antragsteller vorbereiten. *Möglichst realistische Abschätzung des Evaluierungsaufwandes unter Berücksichtigung der Prüfvorgaben und von Erfahrungswerten.*	

Aufgaben Antragsteller/Hersteller	Hilfsmittel (zusätzlich zu CC und CEM)	Aufgaben Prüfstelle	Aufgaben Zertifizierungs-stelle
Zertifizierungsantrag stellen: • Anlagen zum Zertifizierungsantrag abschließend bearbeiten. • Zertifizierungsantrag gemäß Hinweisen im Antrag ausfüllen, mit Firmenstempel versehen und persönlich unterschreiben und mit den erforderlichen Anlagen an die Zertifizierungsstelle senden (Antrag in Papierform an das BSI, Anlagen vorzugsweise elektronisch). •	Antragsformular öff. PGP-Schlüssel der ZertStelle des BSI	• Evaluator kann erstes Assessment der Sicherheitsvorgaben und der Anlagen durchführen und Rückmeldung geben • Evaluierungsplan, mit Antragsteller abgestimmten Entwurf der Zeitplanung bereitstellen.	• Antragseingang bestätigen. • Antrag und zugehörige Anlagen inhaltlich prüfen. • Aussage zur grundsätzlichen Zertifizierbarkeit aus technischer Sicht treffen.
Security Target abstimmen: • Security Target unter Berücksichtigung von Kommentaren der Prüfstelle und der Zertifizierungsstelle aktualisieren. • Ggf. IAR finalisieren.	AIS 41 verw. PP	• Security Target begutachten und kommentieren. • Ggf. Impact Analysis Report (IAR) berücksichtigen.	• Grundsätzliche Zertifizierbarkeit aus technischer Sicht feststellen, vorbehaltlich des positiven Abschlusses der Evaluierung unter Berücksichtigung des Security Targets und der rechtlichen Rahmenbedingungen.
Vorschlag eines Evaluierungs- und Meilensteinplans erstellen: • Terminplanung durchführen.	AIS 45 Vorlage Evaluierungsplan	• Terminplanung durchführen. • Evaluierungsplan erstellen[10].	• Abstimmung des Evaluierungsplanes mit der Prüfstelle. • Abstimmung der Zeitplanung mit Antragsteller und Prüfstelle.
Kick-off-Meeting: • Am Kick-off-Meeting teilnehmen. • Evaluierungsvertrag prüfen und ggf. anpassen. (siehe Kap. 3.2.5.2).	AIS 45	• Am Kick-off-Meeting teilnehmen. • Security Target, Termin- und Evaluierungsplan beschließen. • Protokoll erstellen. Evaluierungsvertrag prüfen und ggf. anpassen.	• Kick-off-Meeting organisieren und leiten.

10 Der Evaluierungsplan enthält Angaben zur inhaltlichen Durchführung der Evaluierung, der anzuwendenden Kriterien und Interpretationen sowie zur zeitlichen Planung, ebenso eine Unabhängigkeits- und Unparteilichkeitserklärung. Er sollte möglichst auch schon auch Termine für Workshops zur Besprechung von Teilergebnissen, wie zu ADV, ATE, AVA und die geplanten Termine für Standortaudits beinhalten. Details zu Inhalten des Evaluierungsplan finden sich im Dokument [CC-Prüfstellen].

Aufgaben Antragsteller/Hersteller	Hilfsmittel (zusätzlich zu CC und CEM)	Aufgaben Prüfstelle	Aufgaben Zertifizierungs-stelle
Auf Start der Evaluierungsphase warten • Ggf. Evaluatoren und Zertifizierer / Prüfbegleiter schulen.		• Evaluierungsaktivitäten vorbereiten. • ggf. Vertrag anpassen.	• Schreiben über den Start der Evaluierungsphase versenden.[11]

Tabelle 1: Aufgaben in der Vorbereitungsphase

3.2.5.1 Antragsformulare

Die Antragsformulare erfragen Angaben, die für den Start des Verfahrens und seine Abwicklung benötigt werden. Die Formular stehen auf der Internetseite des BSI in der Rubrik „Zertifizierung und Anerkennung / Zertifizierung von Produkten / Zertifizierung nach CC / Anträge“ zur Verfügung. Die Formulare enthalten Erklärungen und Hinweise, die für das Ausfüllen behilflich sind.

Gesonderte Antragsformulare gibt es für:

1. die Zertifizierung von IT-Produkten:
   Dieses Formular bezieht sich ausschließlich auf die Zertifizierung eines IT-Produktes für die Optionen Erstzertifizierung und, bei Änderungen an einem bereits zertifizierten Produkt, auf eine Rezertifizierung oder Maintenance, je nach Sicherheitsrelevanz der Änderungen. Weiterhin gibt es die Option Re-Assessment (Neubewertung) eines bereits zertifizierten Produktes und die Option ALC-Reevaluierung bei Änderungen ausschließlich bei den Entwicklungs- und Produktionsstandorten.

   Wird ein Antrag auf Produktzertifizierung nicht durch den Hersteller, sondern durch einen Sponsor oder Vertreiber des Produktes 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 Produktes zugekauft wurde und der Antragsteller selbst nicht die Rechte an den Entwicklungsunterlagen hat, die für die angestrebte Prüfstufe erforderlich sind. Das Erklärungsschreiben muss darlegen: den Namen der Organisation, die ihre Mitwirkung erklärt, und auf welche Bestandteile des Gegenstandes der Zertifizierung sich diese Erklärung bezieht.

   Weitere Anlagen sind: das Dokument Sicherheitsvorgabe, eine Übersicht der Entwicklungs- und Produktionsstandorte, eine Liste der im Produkt (in externen Schnittstellen und Protokollen) implementierten kryptografischen Mechanismen.

   Bei Rezertifizierung oder Maintenance ist eine Änderungsbeschreibung mit sog. Auswirkungsanalyse (Impact Analysis Report (IAR), siehe AIS 38) zur Darlegung der Sicherheitsrelevanz der Änderungen und zur Planung der Wiederverwendbarkeit früherer Prüfergebnisse und Ermöglichung deiner Deltaplanung erforderlich.

11 Nach positivem Kick-off-Meeting offizielle Eröffnung des Verfahrens mit Vergabe der Zertifizierungsnummer und Benennung der Prüfbegleiter der Zertifizierungsstelle des BSI oder ggf. von CertLab. Das Verfahren wird in die öffentliche Liste (BSI-Webseite) der laufenden Zertifizierungsverfahren eingetragen, wenn der Antragsteller dies wünscht (Bezug: Zertifizierungsantrag).

2. die Zertifizierung von Schutzprofilen:
   Dieses Formular bezieht sich ausschließlich auf die Zertifizierung eines Schutzprofils für die Optionen Erstzertifizierung und, bei Änderungen an einem bereits zertifizierten Schutzprofil, auf eine Rezertifizierung oder Maintenance. Das Antragsformular zur Zertifizierung eines Schutzprofils kann unter zertdokus@bsi.bund.de angefordert werden.
3. die Zertifizierung von Standorten nach CC:
   Der Zertifizierungsantrag bezieht sich ausschließlich auf die Zertifizierung eines Entwicklungs- oder Produktionsstandortes für die Optionen Erstzertifizierung und, bei Änderungen an einem bereits zertifizierten Standort, auf eine Rezertifizierung oder Maintenance.

   Bei Standortzertifizierungen gehören zum Antrag verschiedene Anlagen wie z. B. das Dokument Standortsicherheitsvorgaben. Die Konzeption des Dokumentes Standortsicherheitsvorgaben ist in den im Antrag genannten Prüfgrundlagen definiert (siehe Dokument [AIS 47]).

   Bei Änderungen an einem bereits zertifizierten Standort muss ein IAR die Änderungen beschreiben und die Sicherheitsrelevanz erläutern.

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 SZ21/SZ22- Zertifizierungsstelle
Postfach 20 03 63
53133 Bonn

Vorab kann der Antrag per E-Mail gesendet werden an: zertdokus@bsi.bund.de. Die Anlagen sollten in elektronischer Form zugesendet werden. Auf der Internetseite des BSI ist dazu zu den Antragsformularen auch ein öffentlicher PGP-Schlüssel für das o.g. Postfach zertdokus verfügbar.

Die Prüfstelle stellt den Evaluierungs- und Zeitplan auf separatem Wege der Zertifizierungsstelle in elektronischer Form zur Verfügung.

3.2.5.2 Kick-off-Meeting

Das Kick-off-Meeting hat insbesondere das Ziel,

- Information zu den Sicherheitsanforderungen und der Konzeption des Evaluierungsgegenstandes zu vermitteln,
- die Sicherheitsvorgaben bei Produkt- und Standortverfahren abzustimmen,
- die Einbeziehung etwaiger Plattformzertifikate oder Standortzertifikate zu erörtern,
- die Einbeziehung kryptografischer Verfahren zu erörtern,
- die Dokumentenlage beim Antragsteller zu erörtern,
- die erforderlichen Standortaudits zu besprechen,
- die Evaluierungsplanung abzustimmen (inhaltlicher und verfahrenstechnischer Fragen),
- die vorgeschlagene Zeitplanung sowie Workshops abzustimmen.

3.2.6 Die Evaluierungsphase

Das Evaluierungs- und Zertifizierungskonzept basiert auf einer engen Kooperation zwischen den beteiligten Parteien Antragsteller, den zugewiesenen Evaluatoren und dem Leiter des Evaluationsprojektes in der Prüfstelle und dem zugewiesenen Zertifizierer und ggf. benannte Prüfbegleiter für spezielle Prüfaspekte in der Zertifizierungsstelle. Die Kommunikation erfolgt i. d. R. in schriftlicher Form (z. B. Dokumente, E-Mail,

Formschreiben) oder im laufenden Verfahren telefonisch (z. B. Status-Telefonkonferenzen, Klärung von kleineren Fachfragen, die nicht vertraulichkeitskritisch sind) oder in gemeinsamen Besprechungen.

Alle Beteiligten sind angehalten, den zu Beginn des Verfahrens vereinbarten Zeitplan möglichst einzuhalten. Bei sich abzeichnenden Verzögerungen sind die anderen Beteiligten zu informieren, um eine aktualisierte Verfahrensplanung neu abzustimmen.

Die Nachweise / Dokumentation, die der Antragsteller für die Evaluierung zur Verfügung stellen muss, liegen idealerweise bereits überwiegend als Design- und Testdokumentation im Entwicklungsprozess des Produktes bzw. als Prozessdokumentation der relevanten Standorte vor. Bestimmte Analysen, die die CC fordern, sind CC spezifisch, wie z.B. die Beschreibung der Sicherheitsarchitektur (ADV_ARC, Testabdeckungs- und tiefenanalysen (ATE_COV, ATE_DPT)). Die Erstellung dieser Unterlagen ist wegen ihrer Spezifika ggf. bei der Planung besonders zu berücksichtigen.

Bei der Erstellung und Dokumentation der für die Zertifizierung erforderlichen Nachweise, kann der Antragsteller Beratungsleistungen z. B. bei anerkannten CC-Prüfstellen unabhängig von der Evaluierung beauftragen. Dieses wird in vielen Fällen vom BSI auch ausdrücklich empfohlen, muss jedoch bestimmten Regeln wie personeller Trennung und Vermeidung von Abhängigkeiten genügen, um die Unabhängigkeit und Objektivität der Evaluierung nicht zu gefährden. Externe Berater müssen dabei jedoch direkt und intensiv mit den Entwicklern und Prozessverantwortlichen beim Hersteller zusammenarbeiten, um Inkonsistenzen zu vermeiden und sicherzustellen, dass auch der tatsächliche Sachverhalt zum Produkt oder zu den Prozessen berücksichtigt wird.

Im Rahmen der Evaluierung festgestellter Ergänzungsbedarf / Fehler / Inkonsistenzen an den Herstellernachweisen müssen geklärt und durch den Antragsteller behoben werden. Hierfür muss der Antragsteller Ressourcen und Prozesse bereitstellen. Ebenso sind Nachbesserungen am Produkt seitens des Antragstellers während des Verfahrens stets möglich, dies führt dann aber zur Wiederholung von Evaluierungsschritten.

Der Evaluator kann unter besonderen Rahmenbedingungen und in Abstimmung mit der Zertifizierungsstelle ergänzende erforderliche Produktnachweise aus verschiedenen Quellen zusammentragen, z. B. durch Interviews mit den Entwicklern ermitteln. Dies beschleunigt in besonderen Fällen den Evaluierungsprozess (siehe Konzept „Collection of Developer Evidence" [AIS 23]).

Bei Evaluierung eines Entwicklungs- oder Produktionsstandortes werden Beschreibungen der Prozesse, Verfahren und Regeln, die am jeweiligen Standort gelten, in dokumentierter Form benötigt. Umfang und Beschreibungstiefe dieser Informationen richten sich ebenfalls nach den jeweils verwendeten Prüfkomponenten aus den CC aus den Bereichen: CM capabilities - ALC_CMC, CM scope - ALC_CMS, Delivery - ALC_DEL, Development security - ALC_DVS, Life-cycle definition - ALC_LCD, Tools and techniques - ALC_TAT. Für die Bereitstellung der Unterlagen gelten sinngemäß dieselben Regeln, die für die Evaluierung von IT-Produkten genannt wurden. Entsprechend konzentrieren sich die Aufgaben der Prüfstelle auch neben der Evaluierung der Standortsicherheitsvorgabe auf die ALC-bezogenen Prüfaufgaben unter Verwendung der hierfür geltenden Hilfsmittel.

Die Rahmenbedingungen zum Verfahren gemäß Kapitel 5.3 [VB-Produkte], speziell zur Ablehnung eines Antrages oder negativen Bescheidung, finden Anwendung. Dies kann sich z.B. beziehen auf eine Verletzung der Unparteilichkeit, Nichterfüllung der Obliegenheiten des Antragstellers z.B. bei fehlenden Produktnachweisen oder wesentlichen Änderungen am Antrag oder am Zertifizierungsgegenstand.

Typischer Ablauf des Verfahrens:

Aufgaben Antragsteller/Hersteller	Hilfsmittel (zusätzlich zu CC und CEM)	Aufgaben Prüfstelle	Aufgaben Zertifizierungsstelle
Bereitstellungen zur Evaluierung im Produktverfahren: • Bereitstellung IT-Produkt an Prüfstelle und auf Anfrage an Zertifizierungsstelle. • Bereitstellung der prüfrelevanten Herstellernachweise zum Produkt gemäß SecurityTarget, CC/CEM und AIS. • Ggf. Nachbesserungen am EVG und an den Herstellernachweisen. • Ggf. Erforderliche Testwerkzeuge bereitstellen. • Zugang zu prüfrelevanten Standorten für Evaluator und Zertifizierer ermöglichen[12].	AIS 14 AIS 1 ggf. AIS 23 Alle für die Prüfung bzgl Technologie und Prüfaspekt erforderliche AIS und Supporting Documents	• Evaluierung durchführen und erforderliche Prüfdokumentation erstellen, die nach AIS 14 in Teilaspekte aufgeteilt ist. • Prüfergebnisse und Prüfberichte der Zertifizierungsstelle vollständig zur Verfügung stellen. • Kommentare und Nachforderungen bearbeiten. • Durchführung von Tests bzw. Penetrationstests bei Produkten. • Durchführung der Standortaudits beim Hersteller vor Ort. • Workshops mit der Zertifizierungsstelle zur effizienten Besprechung von Prüfberichten, Kommentaren des Zertifizierers und des Klärungsbedarfs des Evaluators. • Ablauf gemäß vereinbarter Planung[13]. • ggf. ETR-for Composition erstellen • ggf. STAR Reporte zu Standortaudits erstellen	• Evaluierung begleiten (Prüfbegleitung), um eine einheitliche Vorgehensweise und Methodik und vergleichbare Bewertungen sicherzustellen. • Prüfberichte bewerten und kommentieren. • Ggf. Tests bzw. Penetrationstests und Standortaudits vor Ort überwachen. • Workshops mit der Prüfstelle durchführen. • *Bei z.B. fehlenden oder unzureichenden Nachweisen des Antragstellers oder der Prüfstelle oder bei Verletzung der Unparteilichkeit kann ein Zertifizierungsverfahren durch die*
Bereitstellungen zur Evaluierung im Standortverfahren: • Bereitstellung der prüfrelevanten Herstellernachweise zum Standort gemäß Security Target, CC/CEM und AIS. • Ggf. Nachbesserungen an Prozessen und Maßnahmen am Standort und an den Herstellernachweisen. • Zugang zu prüfrele-	AIS 14 AIS 1 AIS 47 AIS 23		

12 Audits von Entwicklungs- und Produktionsstandorten sind z. B. in der Prüfklasse ALC ab einer bestimmten Prüftiefe/Evaluierungsstufe erforderlich. Ein vorhandenes Standortzertifikat kann in das Verfahren eingebunden werden und führt zu einer erheblichen Einsparung von Evaluierungsaufwänden für diesen Prüfaspekt.

13 Typischer Ablauf bei Produkten:
1. ASE-Evaluierung 2. ADV / AGD-Evaluierung 3.ADV/AGD Workshop1
4. Evaluierung ATE des Herstellers 5. ATE/AVA-Evaluator- Testkonzepte erstellen 6. ATE / AVA - Kick-off-Meeting1 7. ATE/AVA-Evaluierung und Evaluatoranalysen und -tests 8.ATE/AVA Workshop2
ALC-Evaluierung und Audits können i.d.R. parallel zur Evaluierung nach den Klassen ADV/AGD/ATE erfolgen

Aufgaben Antragsteller/Hersteller	Hilfsmittel (zusätzlich zu CC und CEM)	Aufgaben Prüfstelle	Aufgaben Zertifizierungsstelle
vanten Standorten für Evaluator und Zertifizierer ermöglichen.			*Zertifizierungsstelle nach Anhörung der Parteien abgebrochen oder mit negativem Ergebnis beendet werden.*
Bereitstellungen zur Evaluierung im PP-Verfahren: • Bereitstellung PP an Prüf- und Zertifizierungsstelle. • Ggf. Nachbesserungen am PP bereitstellen.	• AIS 14	• Evaluierung nach Klasse APE durchführen und erforderlichen Prüfbericht erstellen. • Kommentare und Nachforderungen bearbeiten.	• ggf. Abnahme ETR-for Composition • ggf. Abnahme STAR Reporte zu Standortaudits
Ggf. Teilnahme an Besprechungen und Workshops: • Ggf. die Teilnahme an Evaluierungsbesprechungen sowie Workshops zur Klärung von strittigen Fragen, Detailplanungen, Prüfergebnissen etc.		• Teilnahme an Evaluierungsbesprechungen und Workshops zum Verfahren, AVA-Meetings, etc. zur Präsentation von Prüfergebnissen und Klärung von Kommentaren der Zertifizierungsstelle.	• Workshops (z. B. ADV Workshop, ATE/ AVA-Kick-off Meeting) organisieren und Teilnahme zur Klärung von strittigen Fragen, Detailplanungen, Prüfergebnissen, etc.
(Optional) **Erstellung eines ST-Lite:** • Zur Veröffentlichung der Sicherheitsvorgaben im Zuge der Zertifizierung kann nach bestimmten Regeln (siehe AIS 35) eine reduzierte öffentliche Fassung der Sicherheitsvorgaben (ST-lite) erstellt werden.	AIS 35	• Prüfung ST-lite, wenn relevant.	• Abnahme ST-lite.
ETR-Abnahme durch BSI: *Damit sind die inhaltlichen Voraussetzungen für die Erteilung des Zertifikates gegeben.*	AIS 19	• Nach Abnahme der Einzelprüfberichte durch den Zertifizierer zusammenfassenden ETR erstellen. • Kommentare und Nachforderungen bearbeiten. • *Anm.: Die o.g. Teilprüfberichte sind als Anlage Bestandteil des zusammenfassenden ETR.*	• Prüfung, ggf. Kommentierung und formale Abnahme des ETR durchführen. • Antragsteller und Prüfstelle über diese Abnahme informieren.

Tabelle 2: Aufgaben in der Evaluierungsphase

3.2.7 Zertifizierungsphase

Aufgaben Antragsteller/Hersteller	Hilfsmittel (zusätzlich zu CC und CEM)	Aufgaben Prüfstelle	Aufgaben Zertifizierungs-stelle
Ggf. Mitwirkung bei der Erstellung des Zertifizierungsreports und Reaktion auf die Anhörung: • Ggf. den Entwurf des Zertifizierungsreportes kommentieren. • Ggf. Reaktion auf formale Anhörung.		• Kommentierung Entwurf des Zertifizierungsreportes.	**Zertifizierungsentscheidung treffen und Verfahren abschließen** **Bei positiver Zertifizierungsentscheidung :** Zertifikatsurkunde, Zertifizierungsreport und Zertifizierungsbescheid erstellen. Formale Anhörung des Antragstellers zu Nebenbestimmungen und Auflagen im Bescheid (Frist 14 Tage) und Erteilung Zertifikat. **Bei negativer Zertifizierungsentscheidung:** Negativbescheid nach formaler Anhörung. Postalische Zustellung von Bescheid, Zertifikat und Zertifizierungsreport an den Antragsteller. (Widerspruchsfrist 1 Monat oder Widerspruchverzichtserklärung). Wenn bei Produktzertifikaten gewünscht: Zertifizierungszeichen (Button) bereitstellen (rgb, cmyk).
Versand Empfangsbestätigung und ggf. Widerspruchsverzicht: • Empfangsbestätigung an BSI senden. • Widerspruchsverzicht ausstellen und an BSI senden, sonst 4 Wochen Zeit schriftlich Widerspruch gegen die Zertifizierungsentscheidung bei der Zertifizierungsstelle einzulegen. *(Bei Verzicht auf Widerspruch verkürzt sich die Frist zur Veröffentlichung.)*			• Ggf. Bearbeitung Widerspruch. *Nach Ablauf der Widerspruchsfrist ist der Bescheid bestandskräftig.* • Veröffentlichung des Ergebnisses der Zertifizierung sowie Zertifizierungsreport einschließlich der öffentlichen Fassung der Sicherheitsvorgaben, Standortsicherheitsvorgaben bzw. des zertifizierten Schutzprofils[14].

14 In den Fällen in denen das BSI das zertifizierte Schutzprofil nicht selbst veröffentlichen darf, z. B. wenn es von CEN / CENELEC oder ISO erstellt wurde, wird die genaue Bezugsquelle genannt.

Aufgaben Antragsteller/Hersteller	Hilfsmittel (zusätzlich zu CC und CEM)	Aufgaben Prüfstelle	Aufgaben Zertifizierungs-stelle
Kostenabrechnung durchführen: • Aufwände des Verfahrens (Gebühren und Auslagen) dem BSI erstatten (siehe Kap. 5.5).	BMI-GebV		• Kostenbescheid an Antragsteller schicken.
Archivierung durchführen: • Alle evaluierungsrelevanten Nachweise und das evaluierte Produkt für den Zeitraum der Gültigkeit des Zertifikates plus 3 Jahre archivieren.		• Alle evaluierungs-relevanten Nachweise archivieren.	• Alle zertifizierungsrelevanten Nachweise archivieren.
Einhaltung der Nebenbestimmungen im Bescheid und der Regelungen der Zeichenordnung.	Zeichenordnung		• Wenn relevant: Bearbeitung von Nachlieferungen aus Nebenbestimmungen.

Tabelle 3: Aufgaben in der Zertifizierungsphase

3.2.8 Abschlussdokumente

Der bei positivem Abschluss der Evaluierung vom BSI erstellte Zertifizierungsreport enthält neben einer sicherheitstechnischen Beschreibung des Produktes, Schutzprofils bzw. Standortes u.a. ausgewählte Angaben zum Ergebnis der Evaluierung, Hinweise und Auflagen zur Benutzung des zertifizierten Gegenstandes (Produkt, Schutzprofil, Standort) sowie bei Produktzertifikaten Angaben zur Eignung der implementierten kryptografischen Mechanismen aus Sicht des BSI.

Weiterhin wird bestätigt, dass die Evaluierung nach den anerkannten Verfahren und Kriterien 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 Produkte bzw. die Verwendung des Schutzprofils bzw. für die Nutzung des Standortes in der zertifizierten Konfiguration einzuhalten sind.

Falls der Antragsteller der Veröffentlichung des Zertifizierungsreports nicht zustimmt oder widerspricht, fällt das Zertifikat nicht unter die internationalen Anerkennungsvereinbarungen und wird vom BSI nicht in den entsprechenden öffentlichen Listen geführt.

Bei Produkt- und bei Standortzertifikaten ist das Dokument Sicherheitsvorgaben als Anlage zum Zertifizierungsreport Teil der Veröffentlichung des Zertifizierungsergebnisses. Der Antragsteller kann eine reduzierte öffentliche Fassung der vollständigen Sicherheitsvorgaben (ST-lite) nach den Regeln von [AIS 35] zur Verfügung stellen. Die öffentliche Fassung muss dazu vor Abschluss der Evaluierungsaktivitäten der Prüfstelle vorliegen und ist Teil der Abnahme durch die Zertifizierungsstelle.

Der Zertifizierungsbescheid stellt das im rechtlichen Sinne offizielle Votum der Zertifizierungsstelle dar und enthält Nebenbestimmungen und Auflagen, die durch den Antragsteller einzuhalten sind.

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.

Bei einer Zertifizierung nach eIDAS VO wird die Bundesnetzagentur gemäß der Regelungen des Vertrauensdienstegesetzes[15] informiert.

15 Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz) vom 18. Juli 2017 bzw. ggf. in der aktuellen Fassung

4 Aufrechterhaltung einer Zertifizierung

4.1 Aufrechterhaltung der Vertrauenswürdigkeit

Ein Zertifikat wird für eine bestimmte evaluierte Version eines Evaluierungsgegenstandes (Produktversion, PP-Version, bzw. bestimmter Stand der Prozesse und Regelungen am Standort) erteilt. Daher gilt das erteilte Zertifikat nicht für die geänderte Version des Evaluierungsgegenstandes. Damit der geänderte Evaluierungsgegenstand als zertifiziert deklarieren werden kann, ist eine Erneuerung des Zertifikates unter Berücksichtigung der jeweiligen Änderungen und der jeweils aktuellen Angriffstechniken erforderlich. Durch Analyse der Änderungen einerseits bzgl. sicherheitsrelevanter / sicherheitsirrelevanter Änderungen sowie Änderungen mit geringem / größerem Umfang kann entschieden werde, ob eine Rezertifizierung basierend auf einer Reevaluierung (sogenannter „major change“) oder ein und Maintenance-Prozess ohne Reevaluierung (sogenannter „minor change“) durchgeführt werden muss. Die Entscheidung über die erforderliche Wahl des Prozesses liegt bei der Zertifizierungsstelle. Die grundsätzliche Vorgehensweise und die Unterscheidungskriterien sind im Dokument „Assurance Continuity, CCRA Requirements“ [CC-AC] sowie in [AIS 38] beschrieben.

Durch Fortentwicklung der Angriffstechniken, bei Bekanntwerden neuer Schwachstellen einer Produkttechnologie oder bei Auslaufen der Gültigkeit von kryptografischen Algorithmen und Parametern „altert“ ein bestehendes Zertifikat oder kann sogar seine Gültigkeit verlieren. Zur Verifikation der Gültigkeit eines Zertifikates kann eine Neubewertung der Angriffsresistenz nach dem aktuellen Stand der Technik beantragt und durchgeführt werden (Neubewertung/Re-Assessment). Auch bei einem Zertifikat, bei dem explizit eine Neubewertung nach einer bestimmten Frist gefordert ist, kann diese Überprüfung durch eine Neubewertung (Re-Assessment) durchgeführt werden.

4.1.1 Rezertifizierung bei größerem Umfang der Änderungen

Der grundsätzliche Ablauf einer Rezertifizierung ist wie bei einem Erstverfahren, jedoch sind die Evaluierungstätigkeiten zunächst auf die Änderungen und deren Auswirkung auf die Sicherheit konzentriert. Die Angriffsresistenz bei Produktverfahren wird jedoch in jedem Fall nach dem jeweils aktuellen Stand der Technik vollständig neu bewertet (z. B. CC-Prüfaspekt AVA) und die aktuelle Gültigkeit kryptografischer Algorithmen und Parameter berücksichtigt.

Der Antragsteller beschreibt die Änderungen in einem Impact Analyse Report (IAR), der dem Zertifizierungsantrag beizufügen ist. Auf dieser Basis entscheidet die Zertifizierungsstelle, ggf. unter Hinzuziehung der Prüfstelle, über die erforderliche Wahl des Prozesses.

Auf Basis der Änderungen am Produkt und den Herstellernachweisen (IAR) wird zwischen Zertifizierungsstelle und Prüfstelle im Rahmen der Verfahrensplanung festgelegt, welchen Umfang die Reevaluierung hat, welche Prüfschritte erneut durchgeführt werden müssen, bzw. welche früheren Prüfergebnisse wiederverwendbar sind und damit zu welchen Prüfschritten aktualisierte Prüfberichte vorzulegen sind. Auch Audits der Entwicklungs- und Produktionsumgebung werden, falls sie älter als zwei Jahre sind, erneut durchgeführt.

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

Die formale Gültigkeit eines Zertifikat sowie die sicherheitstechnische Bewertung des Produktes wird im Rahmen einer Rezertifizierung erneuert.

4.1.2 Maintenance bei geringem Umfang der Änderungen

Für die Durchführung eines Maintenance-Prozesses muss die Analyse der Änderungen zu dem Schluss gekommen sein, dass es sich um einen „Minor Change" handelt. Die geänderten Herstellernachweise und Testergebnisse werden dann direkt durch die Zertifizierungsstelle begutachtet.

Bei Produktverfahren wird bei diesem Prozess die Angriffsresistenz des Produktes (Prüfaspekt AVA) jedoch nicht nach dem jeweils aktuellen Stand der Technik neu bewertet, sondern es gilt die Angriffsresistenz zum Zeitpunkt der erfolgten letzten Erst- oder Rezertifizierung oder der letzten Neubewertung.

Das jeweilige Ergebnis zu einem Maintenance-Verfahren kann auch Ergänzungen in Bezug auf die Auswahl oder die Gültigkeit kryptografischer Algorithmen und Parameter enthalten, z. B. wenn die relevanten Bezugsdokumente (i. d. R. Technische Richtlinien des BSI oder der jeweils relevante Katalog zugelassener kryptographischer Algorithmen) sich geändert haben.

Bei positiver Entscheidung wird das Ergebnis durch die Zertifizierungsstelle in einem Maintenance-Report als Ergänzung zum bestehenden Zertifizierungsreport dokumentiert.

Ein Maintenance-Prozess kann grundsätzlich bis zu 2 Jahre nach Ausstellung eines Zertifikates erfolgen. Danach ist eine Rezertifizierung oder eine Neubewertung (Re-Assessment) erforderlich.

Die formale Gültigkeit eines Zertifikat sowie die sicherheitstechnische Bewertung des Produktes wird im Rahmen dieses Verfahrens nicht erneuert.

4.1.3 **Partielle ALC-Reevaluierung**

Beziehen sich bei Produktzertifikaten die Änderungen lediglich auf die zum Prüfaspekt ALC (Lifecycle Support) relevanten Aspekte, so kann eine partielle ALC-Reevaluierung wie im CC Supporting Document [CC-AC] unter dem Begriff Subset-Evaluation beschrieben, durchgeführt werden. Dabei wird die Klasse ALC durch die Prüfstelle vollständig reevaluiert. In diesem Fall konzentriert sich die Reevaluierung auf die ALC-Klasse.

Typische ALC Änderungen sind z.B. Re-Auditierung von Standorten, Änderung in der Produktions- oder Lieferkette durch Hinzunahme oder Wegfall von Standorten, Änderungen in Auslieferungsprozessen, Änderungen im Konfigurationsmanagementsystem, Änderungen an Werkzeugen, die zur Produktion des TOE verwendet werden.

Die Angriffsresistenz des Produktes (Prüfaspekt AVA) wird dabei nicht nach dem jeweils aktuellen Stand der Technik neu bewertet, sondern es gilt die Angriffsresistenz zum Zeitpunkt der erfolgten letzten Erst- oder Rezertifizierung oder der letzten Neubewertung. Neben den direkten ALC-bezogenen Prüfunterlagen schließt die Evaluierung mit einem spezifisch ergänzten ETR ab. Aufgrund der Nicht-Aktualisierung des Prüfaspektes AVA wird das Ergebnis dieses Prozesses auch mit einem speziellen Maintenance-Report abgeschlossen und nicht mit einem neuen Zertifikat.

Eine Partielle ALC-Reevaluieerung kann grundsätzlich während des formalen Gültigkeitszeitraumes des zu Grunde liegenden Zertifikates erfolgen. Danach ist eine Rezertifizierung oder eine Neubewertung (Re-Assessment) erforderlich.

Die formale Gültigkeit eines Zertifikat sowie die sicherheitstechnische Bewertung des Produktes wird im Rahmen dieses Verfahrens nicht erneuert.

4.1.4 Re-Assessment Schwachstellenanalyse

Bei einer Neubewertung/Re-Assessment wird die zertifizierte Version eines Produktes einschließlich der nachträglich durch Maintenance hinzugefügten Versionen erneut einer aktuellen Schwachstellenanalyse und, falls erforderlich, Penetrationstests nach dem Stand der Technik durch die Prüfstelle unterzogen.

Ausgangspunkt ist die letzte durchgeführte Zertifizierung, Rezertifizierung oder das letzte Re-Assessment einschließlich aller erfolgten Maintenance-Verfahren. Aufgrund der Produktkenntnis erfolgt die Evaluierung durch die Prüfstelle, die die vorangegangene Evaluierung durchgeführt hat.

Der Umfang der Arbeiten wird zwischen Prüfstelle und Zertifizierungsstelle abgestimmt. Die Arbeiten sind auf den Prüfaspekt Schwachstellenanalyse (AVA) konzentriert. Eine Aktualisierung des Dokumentes zur Unterstützung von Kompositionsverfahren (ETR-for-Composite-Evaluation) ist ggf. ebenfalls zu erstellen. Neue oder verbesserte Angriffstechniken müssen berücksichtigt werden. Die aktuelle Gültigkeit kryptografischer Algorithmen und Parameter wird berücksichtigt. Ergeben sich neue oder ergänzte Auflagen zur Benutzung des Produktes werden die aktualisierten Handbücher oder die aktualisierten Sicherheitsvorgaben ebenfalls in die Evaluierung (AGD und ASE) einbezogen.

Bei einer Neubewertung zu einem Kompositionsverfahren müssen aktuelle Unterlagen aus der Plattformzertifizierung zur Verfügung stehen (ETR for Composition und Handbücher der Plattform), ggf. ist zuvor eine Neubewertung des Plattformzertifikates erforderlich. Das Dokument ETR for Composition der Plattform darf zum Zeitpunkt der Abnahme der Prüfergebnisse durch die Zertifizierungsstelle grundsätzlich jeweils nicht älter als 18 Monate sein (näheres siehe AIS 36).

Ergänzend wird die Gültigkeit der Audits der Entwicklungs- und Produktionsstandorte geprüft, wenn dieser Prüfaspekt Teil der Zertifizierung war und die Sicherheit der jeweiligen Standorte mitentscheidend ist für die Bewertung der Angriffsresistenz (Bsp: Bei Anforderungen an die Vertraulichkeit der Designunterlagen müssen die dafür relevanten Sicherheitsmaßnahmen noch gültig sein; Bei Anforderungen an die Verfügbarkeit evaluierter Prozesse z.B. zur Auslieferung oder zur Generierung oder Produktion des Produktes). Liegen die relevanten Audits länger als zweieinhalb Jahre zurück oder haben sich Änderungen ergeben, so müssen diese Prüfaspekte ebenfalls aktualisiert werden (ALC). In diesen Fall wird dann der Prozess der Rezertifizierung gewählt oder parallel eine Partielle ALC-Reevaluierung durchgeführt.

Zur Abstimmung der notwendigen Re-Assessment-Arbeiten wird zu Beginn ein AVA-Kickoff-Meeting durchgeführt. Der Antragsteller muss alle Herstellernachweise aus der vorangegangenen Zertifizierung und aus ggf. nachträglich durchgeführten Maintenance-Verfahren sowie das Produkt in allen zuvor zertifizierten Versionen und Konfigurationen zu Verfügung stellen, so wie die Prüfstelle es für die Arbeitsschritte benötigt. Die Prüfstelle führt dann die erforderlichen Evaluierungsarbeiten aus und stellt die relevanten Prüfberichte (AVA, ggf. ETR for Composition, ETR) der Zertifizierungsstelle zur Verfügung. Nach Abnahme der Berichte und positivem Ergebnis wird das Ergebnis durch die Zertifizierungsstelle in einem Reassessment-Report als Ergänzung zum bestehenden Zertifizierungsreport dokumentiert. Die formale Gültigkeit des Basiszertifikates wird im Rahmen dieses Verfahrens nicht erneuert.

Kann die Schwachstellenanalyse die diesbezügliche Anforderung aus den Sicherheitsvorgaben nicht bestätigen wird dem Antragsteller die aktuelle (ggf. niedrigere) Angriffsresistenz mitgeteilt und die Zertifizierungsstelle behält sich vor, das frühere Zertifikat zurückzuziehen.

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 Sicherheitszertifizierung von IT-Produkten nach Common Criteria 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 (BSIG § 9, Abs.4 (2)). Die Prüfung nach BSIG § 9, Abs.4 (2) erfolgt bei Antragsannahme jedoch vorbehaltlich einer abschließenden Entscheidung zum Zeitpunkt der Unterzeichnung eines Zertifizierungsbescheides und des Zertifikates.

Grundsätzlich müssen Zertifizierungsverfahren für IT-Produkte beim BSI unter Verwendung von Prüfvorschriften, z. B. Schutzprofilen, die vom BSI zertifiziert oder als geeignet anerkannt wurden, durchgeführt werden. Ist für einen Produkttyp kein vom BSI als geeignet anerkanntes Schutzprofil verfügbar, entscheidet das BSI vor Aufnahme des Verfahrens im Einzelfall auf Basis einer individuellen produktspezifischen Sicherheitsvorgabe über die grundsätzliche Zertifizierbarkeit.

Die Prüftiefe bzw. die Auswahl der Prüfkomponenten, die für ein Zertifizierungsverfahren zugelassen werden, richtet sich grundsätzlich nach den gültigen internationalen Vereinbarungen, den Möglichkeiten der Sicherheitskriterien und einem begründeten Bedarf von Bedarfsträgern, die z.B. auf Basis eines Risikomanagements für die Einsatzumgebung und Anwendung eines Produktes eine bestimmte Prüftiefe benötigen, oder sie resultieren aus Anforderungen aus nationalen IT-Sicherheitsprojekten, nationalen oder EU-Gesetze oder Vorschriften.

Die Verfahrensabwicklung kann innerhalb der Zertifizierungsstelle priorisiert werden, wenn ein besonderes öffentliches Interesse festgestellt wurde oder bei Produkten, die in nationalen IT-Infrastrukturen zum Einsatz kommen (bspw. elektronischer Reisepass und Personalausweis, öffentliches Gesundheitswesen, kritische Infrastrukturen des Bundes).

Die Verwendung von höherwertigen Prüfkomponenten erfordert die Verfügbarkeit einer spezifischen Evaluierungsmethodologie und eine erweiterte Prüfbegleitung durch die Zertifizierungsstelle. Die für eine erweiterte Prüfbegleitung notwendigen Ressourcen sind jedoch nicht immer verfügbar, wodurch es zu Verzögerung in der Bearbeitung kommen kann. Ebenso muss die Prüfstelle die relevanten Kompetenzen und den erforderlichen Anerkennungslevel vorab nachweisen.

Weitere aktuelle oder produkttypspezifische Informationen finden sich auf der Internetseite des BSI in der Rubrik „Zertifizierung und Anerkennung / Zertifizierung nach CC und ITSEC / Grundsätzliche Aussagen“.

5.1.2 Internationale Anerkennungsvereinbarungen

5.1.2.1 Grundsätzliche Regelungen für die Anerkennung von IT-Sicherheitszertifikaten durch das BSI

BSI Gesetz §9, Abs. 7 regelt, dass grundsätzlich Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union vom Bundesamt anerkannt werden, soweit sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen und die

Gleichwertigkeit vom Bundesamt festgestellt worden ist. Zur Ausgestaltung dieser Anforderung wurden internationale Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten ausgehandelt und von den entsprechenden Staaten unterzeichnet. Durch diese Abkommen wird weitestgehend die Mehrfachzertifizierung des gleichen Produktes in verschiedenen Staaten vermieden, wenn die IT-Sicherheitszertifikate auf den gemeinsamen Sicherheitskriterien beruhen. Diese Anerkennungsabkommen regeln grundsätzlich:

- wie das jeweilige Abkommen koordiniert und umgesetzt wird. Dafür ist jeweils ein Management-Komitee (wie das SOG-IS MC oder das CCRA MC) verantwortlich, dem verschiedene Arbeitsgruppen zuarbeiten. Durch die Zusammenarbeit in den verschiedenen Arbeitsgruppen ist ein kontinuierlicher Austausch von Informationen zwischen den unterzeichnenden Staaten sichergestellt.
- wie die Anerkennung und die gegenseitige Überwachung von nationalen Zertifizierungsstellen erfolgt,
- in welchen Vertrauenswürdigkeitsstufen (Prüftiefen, Prüfumfang) und technischen Bereichen die Anerkennung gilt und
- welche Einschränkungen bei der Anerkennung von Zertifikaten gelten, wenn diesen nationalen, internationalen oder EU-Gesetzen oder -Verordnungen entgegenstehen. Dies gilt insbesondere in Anwendungsbereich der nationalen Sicherheit.

Das BSI hat ein Abkommen zur Anerkennung von IT-Sicherheitszertifikaten in Europa für CC- und ITSEC-Zertifikate [SOGIS-MRA] und ein weltweites Abkommen [CCRA] zur Anerkennung von CC-Zertifikaten unterzeichnet. Zertifikate, die gemäß dieser Abkommen von anderen Stellen erteilt sind, werden bis zu den in den Abkommen genannten Prüfstufen grundsätzlich als einem BSI-Zertifikat gleichwertig anerkannt.

Die Anerkennung eines Zertifikates gemäß den genannten internationalen Vereinbarungen schließt die Anerkennung der Eignung ausgewählter kryptografischer Algorithmen und Funktionen und die Anerkennung von Prüfergebnisse zur Implementierung und zur Stärke von kryptografischen Algorithmen und Funktionen grundsätzlich nicht ein. Unter der Anerkennung gemäß [SOGIS-MRA] wird die Bewertung der Eignung und der Stärke kryptografischer Algorithmen und Funktionen anerkannt, sofern der unter SOGIS-MRA erstellte Kryptokatalog [SOGIS-ACM] zur Anwendung kommt. Ansonsten haben nationale Regelungen und Vorschriften Vorrang. Über Ausnahmen und den Umfang der erforderlichen Nachprüfung durch eine beim BSI anerkannte Prüfstelle oder das BSI selbst wird im Einzelfall entschieden. Die internationale Abstimmung dieser Anerkennungsfragen ist noch nicht abgeschlossen.

Die Anerkennung eines Zertifikates durch das BSI kann verwehrt werden, wenn der Anerkennung überwiegende öffentliche Interessen - insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland - entgegenstehen (BSIG §9, Abs. 4, 2.).

Standortzertifikate fallen grundsätzlich nicht unter die internationalen Anerkennungsabkommen, allerdings wird die Wiederverwendung der Ergebnisse einer Standortevaluierung in einer Produktevaluierung im Rahmen der Abkommen unterstützt. Im einzelnen entscheidet die mit der Einbindung befasste Produkzertifizierungsstelle über die Anerkennung des Zertifikats und Wiederverwendung der Ergebnisse. Die entsprechenden Evaluierungsergebnisse können daher im Einzelfall bei BSI-Zertifizierungsverfahren wiederverwendet werden. Zur Unterstützung der Wiederverwendung der Ergebnisse aus einer Standortzertifizierung in einer Produktzertifizierung dient der STAR Report, der i.d.R. mit dem Standortzertifikat erstellt und abgenommen wird.

Zertifikate, ausgestellt von anderen Zertifizierungsstellen, die nicht veröffentlicht wurden oder das entsprechende Logo nicht tragen, unterliegen grundsätzlich nicht der Anerkennung durch das BSI.

Das BSI erkennt IT-Sicherheitszertifikate, die nicht von anerkannten Zertifizierungsstellen z. B. aus dem CCRA oder SOG-IS MRA ausgestellt wurden, grundsätzlich nicht an.

Die formale Anerkennung eines Zertifikates durch das BSI ist explizit keine Zusicherung der Zertifizierungsstelle zur Verwendung des zertifizierten Produktes. Über die Verwendung von zertifizierten Produkten entscheiden die jeweiligen Bedarfsträger.

5.1.2.2 Das europäische Abkommen (SOG-IS MRA V3)

Das derzeit gültige europäische Abkommen ist im April 2010 in Kraft getreten. In diesem Abkommen ist eine Anerkennung von Zertifikaten für IT-Produkte auf Basis der Common Criteria bis zu bestimmten Vertrauenswürdigkeitsstufen (Evaluation Assurance Level (EAL)) festgelegt. Darüber hinaus gilt eine höherwertige Anerkennung für bestimmte technische Bereiche („Technical Domains“) unter besonderen Rahmenbedingungen:

- Im Abkommen wurde der technische Bereich „Smartcards and Similar Devices“ definiert. Die Anerkennung eines Zertifikates aus diesem Produktbereich erfordert den Nachweis der Verwendung der zugehörigen Unterstützungsdokumente („JIWG Supporting Documents“).
- Ein weiterer technischer Bereich wurde für „Hardware Devices with Security Boxes” definiert. Die Anerkennung eines Zertifikates aus diesem Produktbereich erfordert den Nachweis der Verwendung der zugehörigen Unterstützungs-dokumente („JIWG Supporting Documents“).

Abbildung 2: SOG-IS-Logo

Die Anerkennung bezieht sich im Einzelnen auf:

- Produktzertifikate nach CC für Vertrauenswürdigkeitskomponenten bis einschließlich der Stufe EAL 4 oder der Familie Fehlerbehebung (Flaw Remediation (ALC_FLR)),
- Produktzertifikate nach CC unter den Regelungen der jeweiligen technischen Bereiche ("Technical Domains") sofern das Zertifikat von einer für die Technical Domain anerkannten Zertifizierungsstelle erteilt wurde und
- CC-Zertifikate für Protection Profiles.

Zusätzlich werden Zertifikate für Schutzprofile auf Basis der Common Criteria anerkannt.

Aktuelle Details, JIWG Supporting Documents und eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen sind der Internetseite des BSI in der Rubrik Zertifizierung und Anerkennung / Zertifizierung von Produkten / Zertifizierung nach CC / Internationale Anerkennung, oder der Internetseite http://www.sogisportal.eu zu entnehmen.

Das SOG-IS-Logo mit entsprechendem Zusatztext kennzeichnet auf einem Zertifikat des BSI, ob und wie es unter diese Vereinbarung fällt. Beinhaltet ein Zertifikat, das nicht unter eine besondere Technical Domain fällt, Prüfkomponenten oberhalb der Stufe EAL 4 (CC) oder E3 niedrig (basic) (ITSEC), so werden nur die der Stufe EAL 4 bzw. E3 niedrig (basic) zugeordneten Prüfaussagen dieser Prüfkomponenten anerkannt.

5.1.2.3 Das internationale CC-Abkommen (CCRA)

Die internationale Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten auf Basis der CC (Common Criteria Recognition Arrangement [CCRA]) wurde am 8. September 2014 ratifiziert. Es bezieht sich auf:

- CC Zertifikate, die auf einem sog. Collaborative Protection Profile (cPP) (bei exakter Verwendung) basieren,
- Zertifikate für Vertrauenswürdigkeitskomponenten bis einschließlich der Stufe EAL 2 oder der Familie Fehlerbehebung (Flaw Remediation (ALC_FLR)) und
- Zertifikate für Protection Profiles und für Collaborative Protection Profiles (cPP).

Abbildung 3: CCRA-Logo

Aktuelle Details, CCRA Supporting Documents und eine aktuelle Liste der Unterzeichnerstaaten bzw. der anerkannten Zertifizierungsstellen sind der Internetseite des BSI in der Rubrik Zertifizierung und Anerkennung / Zertifizierung

von Produkten / Zertifizierung nach CC / Internationale Anerkennung, oder der Internetseite http://www.commoncriteriaportal.org zu entnehmen.

Durch das CCRA-Logo mit entsprechendem Zusatztext ist auf jedem Zertifikat des BSI gekennzeichnet, ob und wie ein Zertifikat unter diese Anerkennungsvereinbarung fällt. Beinhaltet ein Zertifikat Vertrauenswürdigkeitskomponenten oberhalb des Anerkennungslevels (cPP / EAL 2 / EAL 4 bei Heranziehung der Übergangsregeln), so erfolgt die Anerkennung der Evaluierungsergebnisse für diese Komponenten auf der jeweils oberen Grenze der Anerkennung nach CCRA-2014 bzw. CCRA-2000.

5.2 Vertraulichkeit und Dokumentenaustausch

Die Firmenpolitik des Antragstellers und die Praxis hinsichtlich der vertraulichen Handhabung oder Weitergabe der Unterlagen zum evaluierten Produkt an Dritte, die nicht der Überwachung durch die Zertifizierungsstelle unterliegen, hat Einfluss auf die Bewertung der Ausnutzbarkeit von potenziellen Schwachstellen im Rahmen der Evaluierung, da z. B. vom Hersteller veröffentlichte Informationen zum Produkt als verfügbar für einen Angreifer gelten und somit ggf. die Angreifbarkeit vereinfachen.

Quellcode von Produkten oder anderweitig hochsensible Designinformationen, die nach einer dokumentierten Sicherheitspolitik des Herstellers klassifiziert sind und die Entwicklungsumgebung nicht verlassen dürfen, können in bestimmten Fällen anstatt bei der Prüfstelle auch beim Antragsteller vor Ort, z.B. in der Entwicklungsumgebung, vom Evaluator und vom Zertifizierer begutachtet und analysiert werden. Dazu muss der Antragsteller gegenüber der Zertifizierungsstelle jeweils glaubhaft machen, dass einer Weitergabe der Unterlagen wesentliche Interessen des Antragstellers entgegenstehen. Bei dieser Vorgehensweise entstehen i.d.R. erhöhte Zeitaufwände und erhöhte Kostenaufwände für den Antragsteller.

Der Dokumentenaustausch zwischen Antragsteller, Prüfstelle und Zertifizierungsstelle erfolgt i. d. R. auf elektronischem Wege per verschlüsselter E-Mail. Das BSI bietet dazu das Verschlüsselungsprogramm Chiasmus an. Zwischen BSI und Prüfstelle ist die Verwendung dieses Programms verpflichtend. Der Antragsteller kann eine Lizenz dieses Programms beim BSI erwerben. Für den Antragsteller ist das Programm jedoch nicht verpflichtend. Verfügt der Antragsteller nicht über dieses Programm, werden die Herstellerdokumentation über die Prüfstelle an die Zertifizierungsstelle des BSI oder unter Verwendung von PGP an die Zertifizierungsstelle des BSI gesendet.

Die Lieferung von elektronischen Dokumenten zu einem Zertifizierungsverfahren muss an die E-Mail Adresse:

zertdokus@bsi.bund.de

erfolgen. Ein öffentlicher PGP Schlüssel für zertdokus ist auf der Internetseite des BSI bei den Antragsformularen verfügbar. Die Lieferung an persönliche BSI-Email Adressen von Zertifizierern erfolgt in der Regel zusätzlich in Kopie zur Kenntnis.

Für Dokumenten, 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].

5.3 Rahmenbedingungen zum Verfahren

5.3.1 Evaluierungsplan

Der Evaluierungsplan enthält Angaben zur inhaltlichen Durchführung der Evaluierung, der anzuwendenden Kriterien und Interpretationen sowie zur zeitlichen Planung, ebenso eine Unabhängigkeits- und Unparteilichkeitserklärung. Die Planung sollte auch Workshops zur Besprechung

von Teilergebnissen, wie zu ADV, ATE, AVA und die geplanten Termine für Standortaudits beinhalten. Die Zertifizierungsstelle kann Workshops vorschreiben, auch ad hoc bei Bedarf in laufenden Verfahren.

Die Zertifizierungsstelle kann einen Evaluierungsplan u. a. ablehnen, wenn er unvollständig ist, kein Einvernehmen über die Planung erzielt werden kann oder wenn die Fachkompetenz der Prüfstelle und der eingesetzten Evaluatoren nicht hinreichend nachgewiesen ist.

Die Beteiligten verpflichten sich, Abweichungen von der vereinbarten Zeitplanung den anderen Beteiligten mitzuteilen und den Zeitplan erneut abzustimmen. Regelmäßige Telefonkonferenzen zum Abgleich des Verfahrensstatus werden empfohlen.

5.3.2 Evaluierungsvertrag

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.

5.3.3 Gültigkeit von Standards und Interpretationen

Mit der offiziellen Annahme eines Zertifizierungsantrages werden die relevanten Versionen der Prüfkriterien und Interpretationen (AIS) i. d. R. im Rahmen eines Kick-off Meetings 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.

Die Common Criteria sind in der vom BSI als verbindlich veröffentlichten Version zu verwenden. Bei Verfügbarkeit einer neuen Version der Kriterien wird für laufende Verfahren eine Übergangszeit in Abhängigkeit vom Umfang der Änderungen gewährt.

Technische Richtlinien und Algorithmen Kataloge, die nicht von der Zertifizierungsstelle verantwortet werden, finden grundsätzlich in der zum Zeitpunkt der Abnahme des ETR gültigen Fassung Anwendung.

Die Einbeziehung kryptografischer Verfahren kann zusätzliche Begutachtungen durch das BSI einschließen. Das BSI kann die Einbeziehung kryptografischer 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 vorliegt.

5.3.4 Unterstützung von aufbauenden Folgeverfahren

Bei Produkten aus der Klasse „Smartcards and Similar Devices“ besteht das Konzept, eine auf einer erfolgten Zertifizierung eines Produktes (Platform Product) aufbauende Zertifizierung eines erweiterten Produktes (Composite Product) in einer bestimmten Form zu unterstützen. Damit wird sichergestellt, dass zum einen das Produkt- und Prüfstellen Know-How aus der Evaluierung der Plattform geschützt wird, zum anderen aber Evaluator und Zertifizierer des erweiterten Produktes ausreichend Informationen für die Gesamtbetrachtung erhalten.

In diesem Fall wird durch die Prüfstelle, die die Evaluierung der Plattform durchführt, ein Dokument „ETR for composite evaluation“ nach dem Konzept wie in [AIS 36] dargelegt im Rahmen der

Plattformevaluierung erstellt und von der Zertifizierungsstelle in die Abnahme der Evaluierung einbezogen und im Zertifizierungsreport der Plattform referenziert. Das jeweilige Dokument „ETR for composite evaluation“, die evaluierten Handbücher der Plattform, die vollständige Sicherheitsvorgabe sowie der Zertifizierungsreport müssen dem Evaluator und dem Zertifizierer des Kompositionsproduktes zur Verfügung gestellt werden. Ebenso ist auf Verlangen der Prüfstelle oder der Zertifizierungsstelle ein sog. Open Sample zur Unterstützung der Schwachstellenanalyse des Composite Product zur Verfügung zu stellen.

Das Konzept ist sowohl Prüfstellen übergreifend als auch international zwischen den relevanten Zertifizierungsstellen des SOG-IS MRA Anerkennungsabkommens anwendbar.

Die Übertragung dieses Modells auf andere Produkttypen muss im Einzelfall zwischen Prüfstelle und Zertifizierungsstelle abgestimmt werden.

5.3.5 Wiederverwendung von Prüfergebnissen bei Produktevaluierungen (Re-use)

Die Wiederverwendung von Prüfergebnissen der Evaluierung aus einem Produkt-Zertifizierungsverfahren (Basisverfahren) für ein anderes Produkt-Zertifizierungsverfahren (Folgeverfahren) von demselben Antragsteller ist grundsätzlich möglich. Es ist jedoch erforderlich, dass der Prüfstelle, die bestimmte Ergebnisse wiederverwenden möchte, die Prüfberichte des Basisverfahrens vorliegen. Nur so kann festgestellt und bewertet werden, was in welcher Form wiederverwendet werden kann. Typische Anwendung ist die Reevaluierung / Zertifizierung einer aktualisierten Version eines Produktes oder die Evaluierung / Zertifizierung ähnlicher Produkte eines Herstellers.

Für die Prüfstellen übergreifende Wiederverwendung von Ergebnissen der Evaluierung eines Entwicklungs- oder Produktionsstandortes eines Herstellers sind erweiterte Regelungen nach [AIS 38] unter besonderen Rahmenbedingungen innerhalb des nationalen Zertifizierungsschemas des BSI anzuwenden. Dieses Vorgehen kann z. B. dann erfolgen, wenn ein Standort für die Entwicklung oder Produktion mehrerer Produkte desselben Typs von einem Hersteller verwendet wird. Rückfragen zur wiederverwendeten Standortevaluierung erfolgen über die BSI Zertifizierungsstelle an die jeweilige Prüfstelle. Die Wiederverwendung von Ergebnissen eines Standortaudits, das in einem anderen Zertifizierungsschema unter SOG-IS MRA oder CCRA von einer dort lizenzierten fachlich geeigneten Prüfstelle durchgeführt wurde, ist möglich, wenn die relevanten Informationen (wie evaluierte Prozesse, Sicherheitskonzept, Schnittstellen) zu dem Standort und das Protokoll des Audits (oder ein abgestimmter Transferbericht, der sog. STAR Report) vorliegt und die Prüfstelle mit diesen Informationen eine vollständige Evaluierung nachweisen kann. Rückfragen erfolgen über die BSI Zertifizierungsstelle an die zuständige SOG-IS/CCRA Zertifizierungsstelle, die die dort zuständige Prüfstelle einbinden kann.

Vorliegende Standortzertifikate können bei Vorliegen o.g. relevanter Informationen, der Standortsicherheitsvorgabe und eines abgenommenen STAR Reportes unter Verifizierung der Umsetzung von Annahmen und Auflagen in die ALC Evaluierung bei einem Produktverfahren eingebunden werden (siehe AIS 47). Auch hier werden Rückfragen über die BSI Zertifizierungsstelle gelenkt.

Bei Kompositionszertifizierungen im Smartcard-Bereich erfolgt, aufbauend auf einer Plattformzertifizierung (z. B. für eine Chiphardware), eine Zertifizierung der Plattform mit zusätzlichen Produktteilen (z. B. Betriebssystem und Anwendung). Die Zertifizierungsergebnisse der Plattform können hierbei nur für einen bestimmten Zeitraum bei der Kompositionszertifizierung wiederverwendet werden. Bei Überschreitung dieser Frist (18 Monate) oder auch, wenn zwischenzeitlich relevante Angriffsszenarien auf die Plattform bekannt geworden sind, ist zunächst eine Neubewertung (Re-Assessment) der Angriffsresistenz der Plattform erforderlich. Näheres regeln die Anwendungshinweise und Interpretationen AIS 36. Dem Evaluator und dem Zertifizierer des Kompositionsproduktes muss das jeweilige Dokument „ETR for composite evaluation“, die evaluierten Handbücher, die vollständige Sicherheitsvorgabe sowie der Zertifizierungsreport der Plattform zur Verfügung stehen.

Andere Formen von Kompositionsevaluierungen sind z.B. nach CC unter Verwendung der Prüfklasse ACO für bestimmte Prüftiefen grundsätzlich möglich und müssen im Einzelfall abgestimmt werden oder individuelle Konzepte werden im Einzelfall abgestimmt.

Die Einbringung von Ergebnissen eines bestehenden Produktzertifikates, das von einer anderen nationalen Zertifizierungsstelle der CCRA oder SOG-IS MRA Nationen ausgestellt wurde, in ein darauf aufbauendes Zertifizierungsverfahren beim BSI, z. B. für eine Folgeversion des Produktes oder bei Vergrößerung des Funktionsumfanges ist grundsätzlich möglich, jedoch gelten spezifische Randbedingungen und Besonderheiten für die Bereitstellung der Nachweise, für die Anforderungen an die Prüfstelle und für die Durchführung der Evaluierung. Dies wird im Einzelfall durch die Zertifizierungsstelle des BSI festgelegt.

5.3.6 Zertifizierungsnummer

Die Zertifizierungsnummer ist die Vorgangskennung beim BSI; sie wird bei jedem Schriftwechsel zur Kennzeichnung von Dokumenten und des Zertifizierungsreports verwendet.

Produktzertifikat: BSI-DSZ-CC-nnnn-jjjj
(DSZ= Deutsches IT-Sicherheitszertifikat, CC= Angabe des Kriterienwerkes, nnnn = laufende Antragsnummer, jjjj = Jahr der Erteilung des Zertifikats (wird erst bei Erteilung des Zertifikats angefügt)).

Standortzertifikat: BSI-DSZ-CC-S-nnnn-jjjj
(DSZ= Deutsches IT-Sicherheitszertifikat, CC= Angabe des Kriterienwerkes, S=Standort, nnnn = laufende Antragsnummer, jjjj = Jahr der Erteilung des Zertifikats (wird erst bei Erteilung des Zertifikats angefügt)).

Zertifikate für Schutzprofil: BSI-CC-PP-nnnn-jjjj
(CC= Angabe des Kriterienwerkes, PP=Schutzprofil, nnnn = laufende Antragsnummer, jjjj = Jahr der Erteilung des Zertifikats (wird erst bei Erteilung des Zertifikats angefügt)).

Ergänzung durch Maintenanceverfahren:
Ergänzung der jeweiligen Zertifizierungsnummer um: -MA-kk (MA=Maintenance, kk=lfd. Nummer.

Ergänzung durch Neubewertung / Re-Assessment:
Ergänzung der jeweiligen Zertifizierungsnummer um: -RA-kk (RA=Re-Assessment, kk=lfd. Nummer.

Mögliche Ergänzung bei Rezertifizierung:
Ergänzung der jeweiligen Zertifizierungsnummer um eine Versionsnummer: BSI-DSZ-CC-nnnn-Vx-jjjj oder BSI-CC-PP-nnnn-Vx-jjjj (nnnn=bisherige laufende Antragsnummer, Vx=Versionskennung der Rezertifizierung, jjjj=Jahr der Rezertifizierung).

5.4 Rahmenbedingungen zur Aufrechterhaltung eines CC-Zertifikates

5.4.1 Gültigkeit und ihre Randbedingungen

Ein Produktzertifikat bezieht sich nur auf die angegebene Version des Produktes und wenn alle Auflagen hinsichtlich der Generierung, der Konfiguration und dem Einsatz des Produktes 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 Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da Angriffe mit neuen oder weiter entwickelten Methoden nach Erteilung möglich sind, besteht die Möglichkeit, die Widerstandsfähigkeit des Produktes im Rahmen des Assurance-Continuity-Programms des BSI regelmäßig überprüfen zu lassen (z. B. durch Rezertifizierung oder Neubewertung/Reassessment). Die Zertifizierungsstelle empfiehlt, regelmäßig (z. B. jährlich) oder entsprechend der Anforderungen aus dem Risikomanagement des Anwenders eine Einschätzung der

Widerstandsfähigkeit vornehmen zu lassen. Es kann Zertifikate geben, bei denen eine Verpflichtung zur Neubewertung nach einem bestimmten Zeitraum enthalten ist.

Bei Änderungen am Produkt kann die Gültigkeit eines Zertifikats auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller die Aufrechterhaltung der Vertrauenswürdigkeit (d. h. eine Rezertifizierung / Maintenance-Verfahren) in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen aufdeckt.

Auflagen für den Anwender ergeben sich aus dem Zertifizierungsreport und den evaluierten Handbüchern.

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

Auflagen für den Zertifikatsinhaber ergeben sich aus dem Zertifizierungsbescheid.

Der Anwender eines zertifizierten Produktes muss die mit dem Zertifikat zum Ausdruck gebrachten Ergebnisse, Randbedingungen und Auflagen in seinem Risikomanagementprozess berücksichtigen. Um die Fortentwicklung der Angriffsmethoden und -techniken zu berücksichtigen, sollte er ein Zeitintervall definieren, in dem eine Neubewertung des Produktes erforderlich ist und die Neubewertung vom Inhaber des Zertifikates über das Assurance-Continuity-Programm des BSI verlangen.

5.4.2 Zeitliche Befristung

Die Zertifizierungsstelle muss gemäß der rechtlichen Grundlagen die formale Gültigkeit eines Zertifikates für das jeweilige Zertifizierungsprogramm 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 kryptografischer Algorithmen oder Parameter abhängig vom Einsatzbereich des Produktes kann sich auf die Festlegung der formalen zeitlichen Befristung des Zertifikates auswirken. Dies ist im Zertifizierungsreport dann vermerkt.

5.4.2.1 Gültigkeit einer Produktzertifizierung

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 fünf Jahre zeitlich befristet. Abweichende Fälle können aufgrund besonderer rechtlicher Rahmenbedingungen für bestimmte Produkttypen festgelegt werden. Geht die Befristung über fünf Jahre hinaus, ist zur Aufrechterhaltung des Zertifikates ein regelmäßiges Re-Assessment, spätestens nach fünf Jahren, erfolgreich zu durchlaufen. In gesetzlich regulierten Bereichen können spezifische Regelungen für eine Neubewertung kürzer als nach 5 Jahren relevant sein. Wird eine zu einem Termin geforderte Neubewertung nicht durchgeführt, verliert das Zertifikat zu diesem Termin grundsätzlich seine Gültigkeit und wird archiviert.

Die zeitliche Befristung des Produktzertifikates hat keinen Einfluss auf etwaige kürzere Wiederverwendungsfristen bei auf einem Plattformzertifikat aufbauenden Zertifikaten (z.B. bei Smartcard-Kompositionsverfahren 18 Monate).

5.4.2.2 Gültigkeit einer Standortzertifizierung

Die formal Gültigkeit eines Standortzertifikates ist aufgrund sich fortentwickelnden Entwicklungs- und Produktionsmethoden zeitlich auf zwei Jahre zeitlich befristet.

5.4.2.3 Gültigkeit einer Schutzprofilzertifizierung

Die formale Gültigkeit eines Zertifikates für ein Schutzprofil ist zeitlich auf zehn Jahre befristet mit der Empfehlung, den technischen Inhalt des Schutzprofils entsprechend dem Fortschritt des Standes der Technik in dem Technologiebereich und in der angenommenen Einsatzumgebung des betrachteten Produkttyps, als auch entsprechend der Fortentwicklung der Evaluierungskriterien regelmäßig zu überprüfen. Diese Überprüfung sollte dann in eine Aktualisierung und Rezertifizierung des Schutzprofils münden. Typischerweise werden technische Standards alle fünf Jahre überprüft.

5.5 Kosten

Das BSI stellt dem Antragsteller Gebühren und Auslagen auf Basis der Gebührenverordnung des BMI [BMI-GebV] in Rechnung. Dabei handelt es sich bei Erstverfahren um Pauschalen in Abhängigkeit von der Komplexität des Verfahrens (nach CC EAL Stufe, Produktkomplexität) sowie Auslagen bei verfahrensbezogenen Dienstreisen der Prüfbegleiter. Bei Folgeverfahren (z. B. Rezertifizierung, Maintenance, Neubewertung) wird neben einer Grundpauschale 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 Produktes, dem Produkttyp und der beantragten Prüfstufe ab und kann nicht pauschal beziffert werden. Die Prüfstellen können auf Anfrage Schätzwerte angeben oder erstellen entsprechende Angebote.

Bei Antragstellung durch eine Behörde gelten besondere Regelungen, die im Einzelfall besprochen werden.

5.6 Kontakt zur Zertifizierungsstelle

Erster Ansprechpartner bei laufenden Zertifizierungsverfahren ist der zugewiesene Zertifizierer. Die Kontaktdaten sind dem jeweiligen Schreiben zur Aufnahme des Verfahrens (ID-Vergabe) zu entnehmen.

Übergeordnete Fragen zur Zertifizierung oder zu den Prüfkriterien können adressiert werden an zertifizierung@bsi.bund.de / Telefon: +49 (0)228 99 9582-111 oder an die Organisationseinheiten: referat-sz21@bsi.bund.de und referat-sz22@bsi.bund.de.

Telefonisch kann bei Nichterreichen des Zertifizierers die zentrale Rufnummer des BSI (Telefon: +49 (0)228 99 9582-0) mit Nennung des Zertifizerungsreferates SZ 21 oder SZ 22 oder Geschäftszimmer SZ kontaktiert werden.

Dokumente zur Zertifizierung müssen an die zentrale Adresse: zertdokus@bsi.bund.de gesendet werden. Ein pgp-Schlüssel steht auf der Internetseite des BSI in der Rubrik „Zertifizierung und Anerkennung / Zertifizierung von Produkten / Zertifizierung nach CC / Anträge“ zur Verfügung.

6 Veröffentlichung der Zertifizierung

6.1 Veröffentlichung durch das BSI

Informationen zu zertifizierten Produkten, Schutzprofilen und Standorten 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 / Standorten / Schutzprofilen gegliedert aufgelistet und der Zertifizierungsreport, etwaige Ergänzungen und die Sicherheitsvorgaben zum Download angeboten. Bestätigungen nach dem früheren dt. Signaturgesetz werden für die Dauer ihrer Gültigkeit noch aufgelistet. Produkte die gemäß europäischer Verordnungen zertifiziert werden, werden in der jeweiligen Rubrik des Produkttyps aufgelistet. Ebenso werden in Zertifizierung befindliche Produkte bei Zustimmung des Antragstellers in separaten Listen aufgeführt.
- Druckschrift „Deutsche IT-Sicherheitszertifikate“ (BSI 7148): Hier werden in Form von Übersichtslisten Zertifikate nach Produkttypen / Standorten / Schutzprofilen gegliedert aufgelistet. Noch gültige Bestätigungen nach dem früheren dt. Signaturgesetz werden ebenfalls noch aufgelistet.

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 SOG-IS MRA und CCRA.

Erteilte Bestätigungen nach dem früheren dt. Signaturgesetz müssen gemäß Vorgabe der Bundesnetzagentur veröffentlicht werden. Zertifikate die gemäß europäischer Verordnungen erteilt wurden, müssen ebenso veröffentlicht werden.

6.2 Veröffentlichung durch andere Stellen

6.2.1 Internetseiten der Anerkennungsabkommen

Im Rahmen des internationalen Anerkennungsabkommens CCRA wird auf der Internetseite http://www.commoncriteriaportal.org für Zertifikate, die unter das Abkommen fallen, eine Übersicht der nach CC zertifizierten Produkte und Schutzprofile geführt. Für die Form der Veröffentlichung gelten die für diese Webseite im CCRA abgestimmten Regeln.

Produktzertifikate, die unter das europäische Anerkennungsabkommen SOG-IS MRA fallen, werden auf den Internetseiten der zugehörigen nationalen Zertifizierungsstellen veröffentlicht. Seitens der SOG-IS MRA Mitglieder empfohlene Schutzprofile sind auf der Internetseite http://www.sogisportal.eu veröffentlicht.

6.2.2 Internetseite der Bundesnetzagentur

Die Bundesnetzagentur veröffentlicht auf ihrer Internetseite http://www.bundesnetzagentur.de in der Rubrik „Qualifizierte elektronische Signatur“ die noch gültigen erteilten Bestätigungen nach dem früheren Signaturgesetz aller durch die Bundesnetzagentur anerkannten ehem. Bestätigungsstellen. Für die Form der Veröffentlichung gelten die für diese Webseite durch die Bundesnetzagentur abgestimmten Regeln.

7 Referenzen und Glossar

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