Bundesamt
für Sicherheit in der
Informationstechnik

Hinweise für Antragsteller für die IT-Sicherheitszertifizierung von Produkten, Schutzprofilen und Standorten

(einschließlich Bestätigungen nach SigG)

BSI 7138

Version 2.2, Stand 28. Februar 2014

Common Criteria

Dokumentenhistorie

Version	**Datum**	**Änderungsgrund**	**Status**	**Verteiler**
1.0	Februar 2005		Abgenommen	Öffentlich
2.0	Oktober 2010	Grundlegende Aktualisierung und Ergänzung	Abgenommen	Öffentlich
e2.1	September 2011	Korrekturen nach VPA, Einbindung CertLab	Entwurf	BSI-intern, Prüfstellen
2.1	November 2012	Korrekturen nach int/ext. Kommentierung, Aktualisierung	Abgenommen	Öffentlich
2.2	Februar 2014	Korrekturen Aktualisierung zu internat. Anerkennung, spezifischen Prozessaspekten, Maintenance	Abgenommen	Öffentlich

Vorwort

Informationstechnische (IT) Systeme haben in unserer Informationsgesellschaft einen hohen Stellenwert. Mit der steigenden Abhängigkeit vom reibungslosen Funktionieren solcher Systeme und der Bedeutung der Sicherheit der Informationstechnik in technischen Infrastrukturen müssen deshalb zwangsläufig auch die Ansprüche an die Sicherheit steigen - dies vor allem vor dem Hintergrund der informationellen Selbstbestimmung des einzelnen Bürgers, der Schutzbedürftigkeit von Informationen des Staates und der Wirtschaft, der Tatsache, dass in manchen Bereichen die Gesundheit und das Leben von Menschen von informationstechnischen Systemen abhängen und zum Schutz kritischer Infrastrukturen.

Eingebunden in viele Aktivitäten zur Erhöhung der IT-Sicherheit bietet dazu das Bundesamt für Sicherheit in der Informationstechnik verschiedene Dienstleistungen zur Zertifizierung von IT auf Basis des BSI-Gesetzes [BSIG] an.

Dieses Dokument konkretisiert die Anforderungen aus der übergeordneten Verfahrensbeschreibung zur Zertifizierung von Produkten durch das BSI [VB-Produkte] und beinhaltet alle notwendigen Informationen zum Verfahren, Regelungen und Anforderungen, die ein Antragsteller berücksichtigen muss.

Somit richtet sich diese Druckschrift als technische Leitlinie zum Zertifizierungsverfahren insbesondere an Hersteller, Vertreiber und Entwickler von IT-Produkten, die ein Deutsches IT-Sicherheitszertifikat für ein IT-Produkt oder eine Bestätigung von technischen Komponenten nach dem deutschen Signaturgesetz [SigG] anstreben, um damit einen Nachweis zur Vertrauenswürdigkeit der Sicherheitseigenschaften der Produkte von einer unabhängigen Stelle zu erhalten.

Ebenso richtet sich diese Druckschrift an Autoren von Schutzprofilen, die diese auf Konformität mit den Common Criteria [CC] hin zertifizieren lassen sowie an Betreiber von Entwicklungs- und Produktionsstandorten, die diese nach CC zertifizieren lassen wollen.

Die Zertifizierung von Managementsystemen für Informationssicherheit (engl.: Information Security Management System, ISMS) nach ISO 27001 auf der Basis von IT-Grundschutz wird in anderen Druckschriften des BSI beschrieben.

Ebenso kann es erforderlich sein, die Erfüllung weiterer Anforderungen z. B. hinsichtlich Funktionalität und Interoperabilität im Betrieb eines IT-Produktes oder IT-Systems nachzuweisen. Hierfür stellt das BSI Technische Richtlinien (TR) zur Verfügung, die jeweils für eine bestimmte Klasse von Produkten diese Anforderungen und Prüfvorschriften beschreiben. Die Konformität eines IT-Produktes oder IT-Systems zu einer solchen Technischen Richtlinie des BSI kann vom BSI ebenfalls in einem Zertifikat bestätigt werden. Das diesbezügliche Verfahren ist ebenfalls in anderen Druckschriften des BSI beschrieben.

Weitergehende Informationen sind beim BSI, auf der Internetseite des BSI (https://www.bsi.bund.de/zertifizierung) und den vom BSI für diese Prüfungen anerkannten Prüfstellen erhältlich. Für eine erste Kontaktaufnahme mit dem BSI können sich Interessenten an die folgende Adresse wenden:

Bundesamt für Sicherheit in der Informationstechnik
Referat S22/S23
Postfach 20 03 63
53133 Bonn

Telefon (Infoline): +49 22899 9582-111
E-Mail: zertifizierung@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Übersicht der Zertifizierungs- und Bestätigungsverfahren

1.1 Grundsätzliches zum Verfahren der Zertifizierung

Die Vergabe von Sicherheitszertifikaten für IT-Produkte, Schutzprofile und Standorte ist im BSI-Gesetz [BSIG] geregelt. Ausführungsbestimmungen sind enthalten in der BSI-Zertifizierungsverordnung [BSIZertV], in der BSI-Kostenverordnung [BSIKostV] und in Erlassen des Bundesministeriums des Inneren zu Detailfragen.

Das Verfahren wird im BSI durchgeführt

- gemäß den Regeln und Prozessen des Qualitätsmanagementhandbuches, der übergeordneten Verfahrensbeschreibung des BSI für die Produktzertifizierung [VB-Produkte] und den Verfahrensanweisungen der Zertifizierungsstelle (zur Einhaltung insbesondere der Normen DIN EN ISO/IEC 17065 und DIN EN ISO 9001),
- nach den Anforderungen der internationalen Anerkennungsvereinbarungen [CCRA] und [SOGIS-MRA],
- als Prüfprozess unter Verwendung öffentlich bekannt gemachter und transparenter Prüfkriterien, d. h. der jeweils relevanten Version der Standards CC/CEM[1] sowie ergänzender Anwendungshinweise und Interpretationen zum Schema (AIS) und
- möglichst unter Verwendung eines zertifizierten CC-Schutzprofils (Protection Profiles (PP)).

Die Zertifizierung wird als Antragsverfahren durchgeführt. Nach Vorprüfung und Annahme des Antrages erfolgt die technische Prüfung (Evaluierung) unter Anwendung der jeweils relevanten Prüfkriterien. Die Evaluierung wird von einer vom BSI anerkannten Prüfstelle (siehe Kapitel 3.2) durchgeführt und von der Zertifizierungsstelle fachlich begleitet. Die Evaluierung schließt mit einer positiven (pass) oder negativen (fail) Prüfaussage ab. Auf Basis dieses Votums erhält der Antragsteller einen Bescheid. Anlage zum Bescheid ist bei positivem Prüfergebnis das Zertifikat und der Zertifizierungsreport. Der Antragsteller kann Rechtsmittel gegen einen Bescheid einlegen. Ebenso wird bei positivem Abschluss einer Zertifizierung der Zertifizierungsreport auf der Internetseite des BSI veröffentlicht, außer wenn der Veröffentlichung explizit widersprochen wurde.

Die Zertifizierung kann gemäß [BSIG] verweigert werden, wenn überwiegend öffentliche Interessen der Zertifizierung entgegenstehen.

Alle beteiligten Stellen (das BSI und die durch das BSI anerkannten Prüfstellen) sind zur Wahrung der Vertraulichkeit von Firmengeheimnissen verpflichtet und garantieren durch vielfältige Maßnahmen die Einhaltung dieser wichtigen Voraussetzung. In besonderen Einzelfällen kann zwischen den Parteien eine separate Vertraulichkeitsvereinbarung (NDA) abgeschlossen werden. Ein NDA darf jedoch nicht die Auskunftspflicht der Prüfstelle zu Prüfgegenstand, Prüfmethoden und -ergebnissen gegenüber der Zertifizierungsstelle beeinträchtigen. Zertifizierungsverfahren können jeweils in den Ausprägungen Erst-Zertifizierung, Re-Zertifizierung, Maintenance oder Neubewertung (Re-Assessment) erfolgen.

Bestätigungsverfahren nach dem Signaturgesetz (SigG) werden nach denselben Grundregeln in den Ausprägungen Erst-Bestätigung, Re-Bestätigung oder Nachtragsbestätigung durchgeführt.

Die Besonderheiten zu den genannten Ausprägungen sind in Kap. 5 erläutert.

Im Folgenden werden die Verfahrenstypen mit ihren jeweiligen Besonderheiten gegenüber den o. g. grundsätzlichen Aspekten vorgestellt.

1.2 Zertifizierung der Sicherheit von IT-Produkten

Um die mit dem Einsatz der Informationstechnik (IT) verbundenen Risiken hinreichend zu minimieren, müssen Sicherheitsfunktionen integraler Bestandteil moderner IT sein. Ziel muss es deshalb sein, informationsverarbeitende Systeme so zu entwerfen, herzustellen und einzusetzen, dass ein angemessener Schutz z. B. gegenüber Bedienungsfehlern und Manipulationsversuchen sowie gegenüber gezielten Angriffen auf zu schützende Werte gegeben ist. Hersteller und Entwickler von

1 In besonderen Ausnahmefällen können auch andere Kriterien relevant sein.

IT-Produkten[2] haben sich dieser Problematik in vielfältiger Weise angenommen und bieten heute Produkte an, mit denen man dem Ziel "IT-Sicherheit" ein gutes Stück näher kommt.

Ein Zertifikat kann vom Hersteller oder Vertreiber des zertifizierten Produktes im Rahmen seines Marketings, als Qualifizierungsnachweis bei Ausschreibungen oder zur Erfüllung von Anforderungen seitens seiner Kunden eingesetzt werden. Das BSI-Sicherheitszertifikat für IT-Produkte, genannt „Deutsches IT-Sicherheitszertifikat“, wird in bestimmten Prüfstufen im Rahmen internationaler Anerkennungsvereinbarungen von zahlreichen Nationen anerkannt (siehe Kap. 2.2).

Mit sogenannten Schutzprofilen / Protection Profiles (PP) nach Common Criteria ist die Möglichkeit gegeben, Sicherheitsanforderungen für Produktklassen und Sicherheitsdienstleistungen als Quasi-Standard festzulegen (siehe Kap. 5.4). Die Berücksichtigung von Schutzprofilen bei der Produktentwicklung erleichtert deren Evaluierung und führt zu Produkten, die in besonderem Maße den spezifischen Anforderungen der Anwender entsprechen. Ein Schutzprofil wird verwendet, um einheitliche und vergleichbare Sicherheitsvorgaben für IT-Produkte zu erstellen. Die unter dem Dach des europäischen SOGIS Anerkennungsabkommens organisierten Nationen erklären bestimmte Schutzprofile, die sie als Standard für den jeweiligen Technologiebereich ansehen, zu sogenannten SOGIS Recommended PPs. Zukünftig stellen aber auch die in internationalen Arbeitsgruppen unter dem Dach des internationalen 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 sollte auf ein jeweils im Technologiebereich relevantes Schutzprofil als Mindestanforderung an die erforderlichen Produkte Bezug genommen werden.

Zertifizierte Schutzprofile sind auf der BSI Internetseite https://www.bsi.bund.de/zertifizierung, der CC-Webseite http://www.commoncriteriaportal.org, der SOGIS-Webseite http://www.sogisportal.eu oder zusätzlich auf den Webseiten der anderen nationalen Zertifizierungsstellen verfügbar.

Die Anforderungen der Anwender stehen vor allem in Zusammenhang mit den klassischen Bedrohungen des Verlustes der

- Verfügbarkeit von Daten und Dienstleistungen,
- Vertraulichkeit von Informationen,
- Unversehrtheit / Integrität von Daten und
- Authentizität von Daten.

Zur Prüfung der Sicherheitsfunktionalitäten stehen als Hauptkriterienwerk die Common Criteria [CC], die auch ISO-Standard sind (ISO/IEC 15408) zur Verfügung. Ältere Sicherheitskriterien wie die europäischen ITSEC [ITSEC] sind nur noch in spezifischen Projekten im Einsatz. Neuanträge auf Zertifizierung nach ITSEC werden grundsätzlich nicht mehr angenommen. Der Zertifizierungsreport, der bei positivem Abschluss eines Zertifizierungsverfahrens zur Verfügung gestellt wird, enthält neben einer sicherheitstechnischen Beschreibung des Produktes die

- Bestätigung, dass die Evaluierung nach den anerkannten Verfahren und Kriterien durchgeführt wurde,
- Bestätigung, dass die in den Sicherheitsvorgaben spezifizierten Sicherheitsanforderungen hinsichtlich Funktionalität und Prüfumfang durch das Produkt erfüllt werden,
- Hinweise an den Anwender, wie das betreffende Produkt im Sinne der Ergebnisse der Zertifizierung in der Praxis einzusetzen, ist.

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.

1.3 Zertifizierung von Schutzprofilen

Mit Schutzprofilen / Protection Profiles (PP) nach Common Criteria [CC] ist die Möglichkeit gegeben, Sicherheitsanforderungen für Produktklassen oder Sicherheitsdienstleistungen als Quasi-Standard festzulegen. Die Berücksichtigung von Schutzprofilen bei der Produkt- und Systementwicklung erleichtert deren Evaluierung und führt zu Produkten und Systemen, die in besonderem Maße den spezifischen Anforderungen der Anwender entsprechen.

2 Hinsichtlich des Produktbegriffs s. Kapitel 2

Der Autor eines Schutzprofils ist i. d. R. eine Behörde oder eine Anwenderorganisation, da es sich bei einem Schutzprofil um einen Standard für Sicherheitsanforderungen im Hinblick auf spätere Produktzertifizierungen handelt. Eine Behörde oder eine Anwenderorganisation kann somit beim BSI einen Antrag auf Zertifizierung eines Schutzprofils stellen.

Das BSI entwickelt Schutzprofile, um nationale Sicherheitsanforderungen in Prüfvorschriften festzulegen. Schutzprofile werden evaluiert und zertifiziert, um deren Konformität mit den Konzepten der jeweiligen Prüfkriterien (z. B. der CC) zu bestätigen. Die Zertifizierung eines Schutzprofils, das dem öffentlichen Interesse an der Ausgestaltung eines Prüfstandards widerspricht, kann gemäß BSIG verweigert werden.

Derzeit werden Schutzprofile durch die an der Anerkennungsvereinbarung (siehe Kapitel 2.1) beteiligten Zertifizierungsstellen zertifiziert und national registriert. Die bisher zertifizierten oder registrierten Schutzprofile sind auf der BSI Internetseite https://www.bsi.bund.de/zertifizierung, der CC Webseite http://www.commoncriteriaportal.org, der SOGIS Webseite http://www.sogisportal.eu oder zusätzlich auf den Webseiten der anderen nationalen Zertifizierungsstellen verfügbar.

In internationalen Arbeitsgruppen unter dem Dach des CC Anerkennungsabkommens (CCRA) entwickelte Collaborative Protection Profiles (cPP) stehen den selben Zertifizierungsprozessen offen.

Auf der Webseite des BSI sowie den Seiten anderer nationaler Zertifizierungsstellen finden sich ebenfalls Informationen zu in Entwicklung befindlichen Schutzprofilen und ggf. die jeweiligen Entwurfsfassungen.

1.4 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 Prüfung der Standortssicherheit, Konfigurationsmanagement und Annahme- und Lieferprozesse. 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]).

Die Berücksichtigung eines Standortzertifikates in einem Produktzertifikat erfolgt im Rahmen der Produktevaluierung bei der Prüfklasse Life-Cycle – ALC der Common Criteria. Die besonderen Verfahrensregeln zur Einbindung eines Standortzertifikates in ein Produktzertifikat sind in spezifischen AIS-Dokumenten festgelegt.

Standortzertifikate fallen nicht automatisch 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 Zertifizierungsstelle.

1.5 Bestätigung von technischen Komponenten nach dem Signaturgesetz (SigG)

Das Bundesamt für Sicherheit in der Informationstechnik ist durch die Bundesnetzagentur, der gemäß §18 (1) SigG zuständigen Regulierungsbehörde für Telekommunikation und Post, als Bestätigungsstelle[3] anerkannt.

Am 22. Mai 2001 ist das an die EU – Richtlinie 1999/93/EG angepasste Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (vom 16. Mai 2001) (Signaturgesetz – SigG) in Kraft getreten. Die dazugehörige Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) ist am 22. November 2001 in Kraft getreten und legt die

3 Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für Produkte gemäß §15 Abs. 7 S. 1 (oder §17 Abs. 4) SigG

Rahmenbedingungen und Anforderungen für die Anwendung qualifizierter elektronischer Signaturen fest. Das Signaturgesetz wurde zuletzt am 17. Juli 2009 geändert, die Signaturverordnung am 15. November 2010.

Produkte für qualifizierte elektronische Signaturen sind nach §2 Nr. 13 SigG sichere Signaturerstellungseinheiten, Signaturanwendungskomponenten und technische Komponenten für Zertifizierungsdienste. Sie müssen die Anforderungen nach §17 (1) – (3) SigG und der Signaturverordnung §24 SigV erfüllen. Entsprechend den Angaben §17 (4) und §18 (1) SigG sind die Produkte nach dem Stand von Wissenschaft und Technik hinreichend zu prüfen und durch eine Bestätigungsstelle nach §18 SigG zu bestätigen. Eine Ausnahme gilt für die Signaturanwendungskomponenten und für einen Teil der technischen Komponenten für Zertifizierungsdienste gemäß §17 Abs. 2 und 3 Nr. 2 und 3 SigG. Für diese Fälle sind Herstellererklärungen gemäß §15 (5) SigV ausreichend.

Die Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen sind in der Anlage 1 der Signaturverordnung enthalten.

Anforderungen an Prüftiefen:

Die Prüfung der Produkte für qualifizierte elektronische Signaturen nach Maßgabe des §15 Abs. 7 und des §17 Abs. 4 des Signaturgesetzes hat nach den Common Criteria [CC][4] in der jeweils geltenden Fassung zu erfolgen.

Die Prüfung muss

a) bei technischen Komponenten nach §2 Nr. 12 Buchstabe a)[5] des SigG mindestens die Prüftiefe EAL 4 umfassen,

b) bei sicheren Signaturerstellungseinheiten nach §2 Nr. 10[6] des Signaturgesetzes mindestens die Prüftiefe EAL 4 umfassen,

c) i) bei technischen Komponenten für Zertifizierungsdienste für digitale Signaturen nach §2 Nr. 12 Buchstabe b) und c)[7] des Signaturgesetzes, die außerhalb eines besonders gesicherten Bereichs („Trustcenter“) eingesetzt werden, mindestens die Prüfstufe EAL 4 umfassen,
ii) bei technischen Komponenten für Zertifizierungsdienste für digitale Signaturen nach §2 Nr. 12 b) und c) des Signaturgesetzes, die innerhalb eines besonders gesicherten Bereichs eingesetzt werden, mindestens die Prüfstufe EAL 3 umfassen,

d) bei Signaturanwendungskomponenten nach § 2 Nr. 11[8] des Signaturgesetzes mindestens die Prüfstufe EAL 3 umfassen.

Bei den Prüfstufen EAL 3 und EAL 4 ist außer bei Prüfungen nach Punkt c) ii), ergänzend zu den bei dieser Prüfstufe vorgeschriebenen Maßnahmen gegen ein hohes Angriffspotenzial zu prüfen und eine vollständige Missbrauchsanalyse durchzuführen[9]. Die Mechanismen für Signatur- und

---

4 Die Prüfung unter Verwendung der ITSEC [ITSEC] ist grundsätzlich noch statthaft, jedoch unterstützt das BSI die Verwendung der ITSEC für diese Prüfungen nicht mehr, da die ITSEC und die zugehörige Evaluierungsmethodologie nicht mehr dem aktuellen Stand der Technik entspricht.

5 „Technische Komponenten für Zertifizierungsdienste“ sind Software- und Hardwareprodukte, die dazu besimmt sind, Signaturschlüssel zu erzeugen und in eine sichere Signaturerstellungseinheit zu übertragen.

6 „Sichere Signaturerstellungseinheiten“ sind Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels.

7 „Technische Komponenten für Zertifizierungsdienste“ sind Software- oder Hardwareprodukte, die dazu bestimmt sind, b) qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar zu halten oder c) qualifizierte Zeitstempel zu erzeugen.

8 „Signaturanwendungskomponenten“ sind Software- und Hardwareprodukte, die dazu bestimmt sind, a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.

9 Dies bedeutet bei der aktuellen Fassung der CC Version 3.1 ab Revison 4, dass bei geforderten Prüfungen nach EAL 4 die in dieser Kriterienversion definierte Stufe EAL 4 zuzüglich der Komponente AVA_VAN.5 verwendet werden muss, bei geforderten Prüfungen nach EAL 3 die in dieser Kriterienversion definierte Stufe EAL 3 zuzüglich der Komponente AVA_VAN.5 sowie ADV_FSP.4, ADV_TDS.3 und ADV_IMP.1.

Hashwertberechnungen müssen dem von der Bundesnetzagentur veröffentlichen Katalog [Sig-AlgoKat] entsprechen.

Die Bestätigung von technischen Komponenten nach dem Signaturgesetz ist eine besondere Ausprägung eines Evaluierungs- und Zertifizierungsverfahrens. Grundlage ist eine Evaluierung des jeweiligen IT-Produktes nach CC, jedoch unter Berücksichtigung der besonderen Anforderungen des Gesetzes und der zugehörigen Verordnung hinsichtlich Funktionalität, Prüfumfang und Prüftiefe (s. o.). Diese besonderen Anforderungen müssen im jeweiligen produktspezifischen Dokument „Sicherheitsvorgabe“ verankert werden und sind dann damit im Rahmen der Produktevaluierung durch die Prüfstelle zu berücksichtigen. Die Verwendung von geeigneten Schutzprofilen wird vom BSI dringend empfohlen. Grundsätzlich wird ein Evaluierungsprozess durchlaufen, auf dessen Basis ein Zertifikat erteilt wird und ergänzend eine Bestätigung der Gesetzeskonformität erfolgt.

Um Synergieeffekte in der Durchführung der Zertifizierung und der Bestätigung zu erzielen, sollten die Anträge auf Zertifizierung und Bestätigung zeitgleich gestellt werden. Andernfalls ist mit erhöhten Aufwänden und Kosten zu rechnen.

Im Rahmen der technischen Prüfung (Evaluierung) sind neben der Anwendung der jeweils relevanten Prüfkriterien der CC, Anforderungen und Vorgaben, ggf. auch besondere Anforderungen bzw. Gesetzesauslegungen der Bundesnetzagentur zu berücksichtigen. Bei positivem Ergebnis der Prüfung erhält der Antragsteller neben dem Bescheid die Bestätigungsurkunde mit dem Bestätigungsreport.

Da das Verfahren zur Bestätigung von Produkten im wesentlichen dem Ablauf eines Zertifizierungsverfahrens gleicht, wird in der weiteren Beschreibung des Verfahrens daher nur an den Stellen auf das Bestätigungsverfahren eingegangen, wo Unterschiede und Besonderheiten bestehen.

1.6 Informationsaustausch

Das Evaluierungs- und Zertifizierungskonzept basiert auf einer engen Kooperation zwischen den beteiligten Parteien Antragsteller (z. B. Produkthersteller), Prüfstelle (zugewiesene Evaluatoren und Leiter des Evaluationsprojektes) und der Zertifizierungsstelle (zugewiesener Zertifizierer und ggf. benannte Prüfbegleiter für spezielle Prüfaspekte). 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 Parteien sind aufgefordert, konstruktiv an den Fachaufgaben zu arbeiten. Sollte es auf der Arbeitsebene zu nicht lösbaren Problemen oder Konflikten kommen, so kann die Leitung der Zertifizierungsstelle zur Klärung kontaktiert werden (BSI, Leitung Referat S22 bzw. S23, Postfach 20 03 63, 53133 Bonn oder über E-Mail an zertifizierung@bsi.bund.de).

2 Nationale und internationale Aspekte der Zertifizierung

2.1 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))[10].

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 (siehe Kap. 5.4). 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 Produkt spezifischen Sicherheitsvorgabe über die grundsätzliche Zertifizierbarkeit.

---

10 Anzumerken ist hier, dass erst mit der Zertifizierung, d. h. zum Zeitpunkt der Unterzeichnung eines Zertifizierungsbescheids und des Zertifikates abschließend entschieden wird, das überwiegende öffentliche Interesse, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen. Durch die Prüfung bei Antragsannahme wird versucht sicherzustellen, dass am Ende keine negative Entscheidung bzgl. öffentlichem Interesse erfolgt.

Die Prüftiefe bzw. die Auswahl der Prüfkomponenten entsprechend der Prüfkriterien, die für ein Zertifizierungsverfahren zugelassen werden, richtet sich grundsätzlich nach den gültigen internationalen Vereinbarungen, d. h. derzeit Prüfkomponenten der Common Criteria bis einschließlich Prüfkomponenten der Stufe EAL 4 sowie der Prüfkategorie Fehlerbehebung (Familie ALC_FLR). Das BSI kann aber auch die akzeptierte Prüfstufe unterhalb der Regelungen der Abkommen begrenzen, z. B. auf EAL 2.

Die Verwendung höherwertiger 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. Höhere Prüfstufen können grundsätzlich akzeptiert werden, wenn Prüfvorschriften für nationale IT-Sicherheitsprojekte, nationale oder EU Gesetze oder Vorschriften oder vom BSI anerkannte Schutzprofile dies erfordern. Dies gilt ebenso in besonders definierten technischen Bereichen der europäischen Anerkennungsvereinbarung wie z. B. der Smartcard Technical Domain. Ob der Antragsteller ein besonderes Interesse an der Verwendung einer höheren Prüfstufe geltend machen kann, z. B. aufgrund eines besonderen Vertrauenswürdigkeitsbedarfs in der typischen Einsatzumgebung eines Produktes und gefordert in einer Ausschreibung, entscheidet die Zertifizierungsstelle im Einzelfall.

Die Bearbeitung von Zertifizierungsverfahren erfolgt nach Annahme des vollständigen Antrages auf Basis einer gemeinsam zwischen Antragsteller, Prüfstelle und Zertifizierungsstelle abgestimmten Zeitplanung, grundsätzlich aber nach Antragseingang. 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).

2.2 Internationale Anerkennungsvereinbarungen

2.2.1 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 Mehrfach-Zertifizierung des gleichen Produktes in verschiedenen Staaten vermieden, wenn die IT-Sicherheitszertifikate auf CC oder ggf. auf ITSEC beruhen. Diese Anerkennungsabkommen regeln grundsätzlich:

- wie das jeweilige Abkommen koordiniert und umgesetzt wird. Dafür ist jeweils ein Management Komitee (wie das SOGIS-MC oder das CCRA-MC) verantwortlich, dem verschiedene Arbeitsgruppen zuarbeiten,
- 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 nationale, internationale oder EU-Gesetze oder -Verordnungen entgegenstehen. Dies gilt insbesondere in Anwendungsbereichen 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, sofern der Prüfgegenstand (EVG) aus Nationen stammt, die dem CCRA oder dem SOGIS-MRA

angehören oder bei Produktherkunft aus EU oder EFTA[11] Staaten (sofern diese nicht schon Mitglied in CCRA oder SOGIS-MRA sind). Andernfalls ist die Anerkennung durch das BSI grundsätzlich begrenzt bis zur Prüfstufe EAL 2 (CC) bzw. E1 (ITSEC). Ausnahmen von der letztgenannten Begrenzung der Anerkennung bezüglich der Prüfstufe liegen vor, wenn das Zertifikat Bezug nimmt auf eine EU-Verordnung, die eine bestimmte Prüfstufe fordert oder wenn eine für den Produkteinsatz verantwortliche europäische (EU oder EFTA) Zulassungsstelle oder Behörde die Zertifizierung befürwortet und die kritischen Produktionsschritte in der EU oder einer EFTA Nation stattfinden.

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. Hier haben nationale Regelungen und Vorschriften Vorrang. Über Ausnahmen und den Umfang der erforderlichen Nachprüfung durch die beim BSI anerkannte Prüfstelle oder das BSI selbst wird im Einzelfall entschieden.

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, ausgestellt von anderen Zertifizierungsstellen, unterliegen grundsätzlich nicht der Anerkennung durch das BSI, jedoch können die jeweiligen Evaluierungsergebnisse im Einzelfall bei BSI Zertifizierungsverfahren wiederverwendet werden.

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

Die Anerkennung von Bestätigungen nach dem deutschen Signaturgesetz oder der entsprechenden EU Richtlinie sind von den internationalen Anerkennungsabkommen CCRA und SOGIS-MRA nicht erfasst.

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

Die Einbringung der Ergebnisse eines bestehenden Produktzertifikates, das von einer anderen nationalen Zertifizierungsstelle der CCRA oder SOGIS-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.

2.2.2 Das europäische Abkommen (SOGIS-MRA V3)

Das derzeit gültige europäische Abkommen wurde im April 2010 von den nationalen Stellen der folgenden Staaten unterzeichnet: Deutschland, Finnland, Frankreich, Großbritannien, Niederlande, Norwegen, Schweden und Spanien. In diesem Abkommen ist eine Anerkennung von Zertifikaten für IT-Produkte auf Basis der Common Criteria bzw. ITSEC bis zu bestimmten Vertrauenswürdigkeitsstufen (Evaluation Assurance Level (EAL)) festgelegt. Anerkannte Zertifizierungsstellen hierfür sind zum Zeitpunk des Inkrafttretens die nationalen Stellen aus Deutschland, Frankreich, Großbritannien, den Niederlanden und Spanien. Weitere Staaten sind mittlerweile hinzugekommen. Eine aktuelle Liste der Unterzeichnerstaaten und der anerkannten Zertifizierungsstellen kann auf der Internetseite http://www.sogisportal.eu eingesehen werden.

Darüber ist eine höherwertige Anerkennung für bestimmte technische Bereiche („Technical Domains“) unter besonderen Rahmenbedingungen vorgesehen.

Im Abkommen wurde dazu der technische Bereich "Smart cards 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 Konformität des Produktes zu einem dieser Kategorie zugeordneten empfohlenen Schutzprofile („SOGIS

11 EFTA: European Free Trade Association (Island, Liechtenstein, Norwegen, Schweiz)

Recommended PP“) und die Verwendung der jeweils zugehörigen Unterstützungsdokumente („JIWG Supporting Documents“) (siehe http://www.sogisportal.eu).

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

Eine aktuelle Liste der SOGIS Recommended PPs kann auf der Internetseite http://www.sogisportal.eu eingesehen werden.

Im Rahmen dieser europäischen Anerkennung erkennt das BSI unter Berücksichtigung der o.g. Randbedingungen, und wenn die o. g. übergeordneten Einschränkungen (siehe Kap. 2.2.1) nicht greifen die folgenden Zertifikate an:

- Zertifikate für IT-Produkte auf Basis der ITSEC, die vor April 2010 durch die nationalen Zertifizierungsstellen von Frankreich, Großbritannien und ab Januar 2009 der Niederlande ausgestellt worden sind oder Zertifikate mit hohen Prüfstufen, die unter dem Vorgängerabkommen ausgestellt worden sind und bis Ende April 2012 unter dem neuen Abkommen re-zertifiziert wurden.
- Zertifikate für IT-Produkte auf Basis der Common Criteria bis EAL 7, die vor April 2010 durch die nationalen Zertifizierungsstellen von Frankreich, Großbritannien und ab Januar 2009 der Niederlande ausgestellt worden sind oder Zertifikate mit hohen Prüfstufen, die unter dem Vorgängerabkommen ausgestellt worden sind und bis Ende April 2012 unter dem neuen Abkommen re-zertifiziert wurden.
- Zertifikate für IT-Produkte auf Basis der ITSEC bis E3, Mechanismenstärke niedrig (basic), der nationalen Zertifizierungsstellen von Frankreich, Großbritannien, Niederlanden und Spanien, die ab April 2010 ausgestellt wurden.
- Zertifikate für IT-Produkte auf Basis der Common Criteria bei Verwendung von Prüfkomponenten bis EAL 4 der nationalen Zertifizierungsstellen von Frankreich, Großbritannien, Niederlanden und Spanien, die ab April 2010 ausgestellt wurden und von Italien ab Dezember 2010 sowie von Schweden und Norwegen ab Mai 2013[12] .
- Zertifikate für IT-Produkte auf Basis der Common Criteria bei Verwendung von Prüfkomponenten bis EAL 7 im technischen Bereich „Smart cards and similar devices“ der nationalen Zertifizierungsstellen aus Frankreich, Großbritannien und den Niederlanden, die ab April 2010 ausgestellt wurden und von Spanien ab Mai 2013.
- Zertifikate für Schutzprofile auf Basis der Common Criteria der nationalen Zertifizierungsstellen von Frankreich, Großbritannien, Niederlanden und Spanien, die ab April 2010 ausgestellt wurden und von Italien ab Dezember 2010 sowie von Schweden und Norwegen ab Mai 2013[13].

Eine aktuelle Liste der jeweils anerkannten Zertifizierungsstellen kann auf der Internetseite http://www.sogisportal.eu eingesehen werden.

Durch die Zusammenarbeit in verschiedenen Arbeitsgruppen ist ein kontinuierlicher Austausch von Informationen zwischen den unterzeichnenden Staaten sichergestellt.

Das SOGIS-Logo mit entsprechendem Zusatztext kennzeichnet auf einem Zertifikat des BSI, ob und wie es unter diese Anerkennungsvereinbarung 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.

2.2.3 Das internationale CC-Abkommen (CCRA)

Im Mai 2000 wurde eine Vereinbarung (Common Criteria-Vereinbarung) über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten und Schutzprofilen auf Basis der CC bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 ergänzt um die Prüfkategorie Fehlerbehebung (Familie ALC_FLR) verabschiedet (CC-MRA). Der Vereinbarung sind bis Juli 2011 die nationalen Stellen folgender Nationen beigetreten: Australien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Indien, Israel, Italien, Japan, Kanada, Malaysia, Neuseeland, Niederlande, Norwegen, Österreich, Pakistan, Republik Korea, Republik Singapur, Schweden,

12 Einschränkung bzgl. Norwegen: Die Evaluierung muss durch eine europäische Prüfstelle erfolgt sein.

13 Einschränkung bzgl. Norwegen: Die Evaluierung muss durch eine europäische Prüfstelle erfolgt sein.

Spanien, Tschechische Republik, Türkei, Ungarn, USA. Weitere Staaten sind mittlerweile hinzugekommen. Eine aktuelle Liste der Unterzeichnerstaaten und der anerkannten Zertifizierungsstellen kann auf der Internetseite http://www.commoncriteriaportal.org eingesehen werden.

Im Rahmen dieses Abkommens erkennt das BSI unter Berücksichtigung der o. g. Randbedingungen, und wenn die o. g. übergeordneten Einschränkungen (siehe Kap. 2.2.1) nicht greifen, die folgenden Zertifikate an:

- Zertifikate für IT-Produkte auf Basis der Common Criteria unter Verwendung von Prüfkomponenten bis EAL 4 oder der Prüfkategorie Fehlerbehebung (Familie ALC_FLR) und Zertifikate für Schutzprofile auf Basis der Common Criteria der nationalen Zertifizierungsstellen von: Australien/Neuseeland, Frankreich, Großbritannien, Kanada, und USA sowie Japan (ab Oktober 2003), Niederlande (ab Januar 2006), Norwegen (ab Februar 2006), Republik Korea (ab Mai 2006), Spanien (ab August 2006), Schweden (ab Februar 2008), Italien (ab September 2009), Türkei (ab Nov 2010), Malaysia (ab Sept. 2011) und Indien (ab September 2013)

Eine aktuelle Liste der anerkannten Zertifizierungsstellen kann auf der Internetseite http://www.commoncriteriaportal.org eingesehen werden.

Die Common Criteria werden kontinuierlich durch eine Reihe von verschiedenen Gremien weiterentwickelt, wodurch ein ständiger Austausch zwischen den verschiedenen Nationen sichergestellt ist.

Durch das CCRA-Logo mit entsprechendem Zusatztext ist auf einem Zertifikat des BSI gekennzeichnet, ob und wie ein Zertifikat unter diese Anerkennungsvereinbarung fällt. Beinhaltet ein Zertifikat Vertrauenswürdigkeitskomponenten oberhalb der Stufe EAL 4, so werden nur die der Stufe EAL 4 zugeordneten Komponenten dieser Komponentenfamilien anerkannt.

Derzeit wird zwischen den Nationen des CCRA eine Umgestaltung des Abkommens diskutiert, die zukünftig eine stärkere Bindung der Anerkennung an die Verwendung gemeinsam abgestimmter Schutzprofile (sog. collaborative Protection Profiles, cPP) sowie zugehöriger technologiespezifischer Evaluierungsmethodik (Supporting Documents) bedeuteten kann. Weitere Details zu dieser Entwicklung finden sich unter http://www.commoncriteriaportal.org (Vision Statement).

3 Die beteiligten Partner im Zertifizierungsprozess

Am Gesamtprozess der Zertifizierung sind drei Partner beteiligt:

- der Antragsteller (Hersteller, Sponsor oder Vertreiber eines IT-Produkts / Behörde oder Anwenderorganisation als Verfasser eines Schutzprofils[14] / verantwortlicher Betreiber eines Entwicklungs- oder Produktionsstandortes),
- die vom Antragsteller ausgewählte anerkannte Prüfstelle und
- die Zertifizierungs- (und Bestätigungs-) stelle des BSI.

3.1 Der Antragsteller mit Aufgaben und Pflichten

Der Antragsteller stellt beim BSI einen Antrag auf

- Zertifizierung und/oder Bestätigung nach SigG seines Produktes,
- Zertifizierung eines Schutzprofils oder
- Zertifizierung eines Entwicklungs- oder Produktionsstandortes.

Er schließt mit einer vom BSI anerkannten Prüfstelle einen Evaluierungsvertrag (außer bei den Prozessen ohne Re-Evaluierung wie Maintenanceprozess (bei Minor Change) oder Nachtragsbestätigung).

Der Evaluierungsvertrag regelt die Beauftragung der Prüfstelle zur Durchführung der Evaluierung. Da die Prüfstelle durch die Anerkennungsvereinbarung mit dem BSI zur Einhaltung den Vorgaben des Zertifizierungsschemas verpflichtet ist, darf der Evaluierungsvertrag keine die Evaluierung be-

14 Der Antragsteller für eine Schutzprofilzertifizierung ist grundsätzlich eine Behörde, eine regulatorisch wirkende öffentliche Instanz oder eine Organisation, die mit Standardisierung befasst ist. Der Antrag auf Zertifizierung eines Schutzprofils erfolgt immer in Abstimmung mit der Zertifizierungsstelle des BSI.

hindernden Regelungen enthalten, insbesondere bezüglich der Informationsweitergabe zu Erkenntnissen aus der Evaluierung an die Zertifizierungsstelle. 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) ergeben können, welche die Evaluierungsaufwände beeinflussen.

Wird der Antrag durch einen Sponsor oder Vertreiber des Produktes gestellt, muss dem Antrag eine schriftliche Erklärung des Herstellers beigefügt werden, um die Mitwirkung im Verfahren und die Bereitstellung der erforderlichen Produktnachweise sicherzustellen.

Mit dem Antrag verpflichtet sich der Antragsteller zur Mitwirkung im Verfahren, d. h.

- alle zur Zertifizierung oder Bestätigung nach SigG nötigen Informationen (Nachweise) zum Prüfgegenstand der Prüfstelle und der Zertifizierungsstelle zur Verfügung zu stellen einschließlich notwendiger Nachbesserungen, falls bei der Evaluierung sicherheitsrelevante Mängel festgestellt werden und die Zertifizierungsstelle oder die Prüfstelle Ergänzungen zu gelieferten Nachweisen fordern,
- bei einer Produktzertifizierung oder Bestätigung nach SigG das Produkt selbst und ggf. erforderliche Testwerkzeuge und ggf. Produktschulungen für Evaluator und Zertifizierer zur Verfügung zu stellen,
- der Prüfstelle und der Zertifizierungsstelle zur Durchführung von Prüftätigkeiten Zugang zu allen Entwicklungs- und Produktionsstandorten, die in den Evaluierungsprozess einbezogen sind, zu gewähren. Ein NDA mit der Prüfstelle darf nicht die Auskunftspflicht der Prüfstelle zum Prüfgegenstand, Prüfmethoden und -ergebnissen gegenüber der Zertifizierungsstelle beeinträchtigen,
- die vom BSI auf Basis der BSI Kostenverordnung [BSIKostV] sowie Reisekosten der ggf. vom BSI beauftragten externen Prüfbegleiter gemäß der Regelungen wie bei Mitarbeitern des BSI abgerechneten Aufwände des Verfahrens (Gebühren und Auslagen) zu erstatten.

Der Antragsteller steht für die Richtigkeit seiner Angaben ein. Bei fehlenden oder unzureichenden Nachweisen kann ein Zertifizierungsverfahren durch die Zertifizierungsstelle abgebrochen oder mit negativem Ergebnis beendet werden.

Die Firmenpolitik des Antragstellers und die Praxis hinsichtlich der vertraulichen Handhabung oder Weitergabe der Unterlagen zum evaluierten Produkt an Dritte 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.

Da in der Zertifizierungsstelle eine Vielzahl von Zertifizierungsverfahren parallel bearbeitet werden und auch bei der Prüfstelle i. d. R. mehrere Evaluierungen gleichzeitig durchgeführt werden, ist der Antragsteller verpflichtet, den zu Beginn des Verfahrens vereinbarten Zeitplan möglichst einzuhalten. Bei sich abzeichnenden Verzögerungen sind die Prüfstelle und die Zertifizierungsstelle zu informieren, um eine aktualisierte Verfahrensplanung neu abzustimmen.

Mit dem Antrag auf Zertifizierung stimmt der Antragsteller zu:

- dass alle evaluierungsrelevanten Nachweise und (bei Produktprüfungen) das evaluierte Produkt für einen Zeitraum von mindestens 5 Jahren (in besonderen Fällen 10 Jahre) beim Antragsteller archiviert werden und dem BSI ggf. auf Anfrage kostenlos zur Verfügung gestellt werden, falls Nachprüfungen zum Zertifizierungsergebnis erforderlich werden,
- dass die dem BSI bereitgestellten Unterlagen und die BSI internen Verfahrensakten durch das BSI entsprechend den Registratur-Richtlinien des Zertifizierungsschemas im BSI archiviert werden,
- dass nach positivem Abschluss des Verfahrens das Ergebnis der Zertifizierung und ggf. der Bestätigung nach SigG sowie der Zertifizierungsreport und ggf. der Bestätigungsreport einschließlich der öffentlichen Fassung der Sicherheitsvorgaben - ganz oder auszugsweise, auch in digitaler Form - durch das BSI veröffentlicht werden,[15]
- dass Personenbezogene Daten, die aus dem Antrag resultieren, zum Zwecke der Durchführung des beantragten Verfahrens im BSI elektronisch gespeichert werden dürfen.

15 Der Antragsteller kann in besonderen Fällen während des laufenden Verfahrens diese Zustimmung zurückziehen. In diesem Fall wird das Zertifikat jedoch nicht im Rahmen der internationalen Anerkennungsvereinbarungen anerkannt.

Der Antragsteller hat bei Produktprüfungen die Möglichkeit bei positivem Abschluss des Verfahrens einen Zertifizierungsbutton zu erhalten (als elektronische Druckvorlage), der z. B. im Rahmen des Marketings verwendet werden kann.

Mit Zustimmung des Antragstellers kann die Tatsache des laufenden Verfahrens nach Beginn der Evaluierung in BSI-Publikationen unter der Rubrik "...in der Zertifizierung befindlich..." mit Angabe des Namens des Antragstellers (Name der Organisation) und des Namens des Prüfgegenstandes aufgeführt werden.

Bei der Erstellung und Dokumentation der für die Zertifizierung / Bestätigung erforderlichen Nachweise, kann sich der Antragsteller Beratungsleistungen z. B. bei anerkannten 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.

Der Antragsteller erhält das Ergebnis des Verfahrens (z. B. Zertifizierungsbescheid, Zertifikat, Zertifizierungsreport und Kostenbescheid) postalisch zugestellt.

Der Antragsteller kann innerhalb eines Monats nach Zugang des Bescheides Widerspruch gegen die Entscheidung des BSI einlegen, ein Zertifikat oder eine Bestätigung nach SigG zu erteilen oder zu versagen. Der Widerspruch ist bei der Zertifizierungsstelle schriftlich einzureichen. Zur Verkürzung der Frist und damit zur schnelleren Veröffentlichung des Zertifizierungsergebnisses kann der Antragsteller schriftlich auf Widerspruch verzichten.

3.2 Anerkannte Prüfstellen mit Aufgaben und Pflichten

Evaluierungen mit dem Ziel der Zertifizierung eines Produktes, eines Schutzprofils oder eines Entwicklungs- oder Produktionsstandortes oder mit dem Ziel der Bestätigung nach dem Signaturgesetz werden von den durch das BSI anerkannten Prüfstellen durchgeführt. Da die Anerkennung der Prüfstelle durch das BSI die Erfüllung der Anforderungen nach ISO 17025 einschließt, gilt sie als grundsätzlich hinreichend unabhängige und unparteiische Stelle, muss dies aber darüber hinaus gegenüber der Zertifizierungsstelle im Einzelfall zusätzlich erklären und bestätigen.

Die Anerkennung einer Prüfstelle bezieht sich immer auf einen Anerkennungsbereich, d. h. auf ein konkretes Kriterienwerk, d. h. auf CC oder ggf. ITSEC und ggf. spezifische technische Fachgebiete oder Prüfstufen. Beispielsweise sind für Evaluierungen im Produktspektrum Smartcards und ähnlicher Produkte wie Hardware Sicherheitsmodule oder Integrierte Schaltungen besondere Anforderungen zu erfüllen. Eine Voraussetzung für die Anerkennung einer Prüfstelle ist die Einhaltung der DIN EN ISO/IEC 17025 und die nachgewiesene Fachkompetenz für den entsprechenden Geltungsbereich. Das BSI überwacht die Anerkennung u. a. durch regelmäßige Begutachtungen.

Die durch das BSI anerkannten Prüfstellen und das BSI haben einen Vertrag geschlossen, der die gegenseitigen Rechte und Pflichten regelt. Das Verfahren zur Anerkennung von Prüfstellen ist in dem Dokument „Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern“ [VB-Stellen] beschrieben, die detaillierten Anforderungen zum jeweiligen Anerkennungsbereich im Programm [Prog-Stellen]. Prozessbezogene Anforderungen, die die Prüfstelle zur Durchführung der Evaluierungen beachten muss, sind in dem Dokument „Anforderungen an die Prüfstelle für die Evaluierung von Produkten, Schutzprofilen und Standorten nach CC“ [BSI 7125] dargelegt. Anwendungshinweise und Interpretationen zum Schema (AIS) ergänzen diese Vorgaben.

Die Prüfstelle ist auf Basis der Anerkennungsvereinbarung mit dem BSI in jedem Evaluierungsverfahren verpflichtet, die Vertraulichkeit der zur Verfügung gestellten Unterlagen und die Vertraulichkeit der Prüfergebnisse intern in der Prüfstelle sowie in der Kommunikation mit Antragsteller und Zertifizierungsstelle nach dem Need-to-know Prinzip sicherzustellen.

Die Prüfstelle ist vertraglich verpflichtet, alle Anforderungen des Zertifizierungsschemas, sowie Anforderungen der Prüfkriterien und der Evaluierungsmethodologie einzuhalten, und ist für die technische Korrektheit ihrer Prüfergebnisse verantwortlich. Die Prüfergebnisse werden in Prüfberichten dokumentiert und die Entscheidung des Evaluators wird in diesen Prüfberichten begründet. Nachforderungen der Zertifizierungsstelle zur Durchführung der Evaluierung und zu Prüfberichten müssen durch die Prüfstelle erfüllt werden.

Der Antragsteller erhält die Prüfberichte nach Abnahme oder Kommentierung durch die Zertifizierungsstelle von der Prüfstelle. Bei Nachforderungen an den Hersteller bzw. Antragssteller seitens

der Prüfstelle oder der Zertifizierungsstelle können auf dieser Basis Ergänzungen der erforderlichen Nachweise durch den Antragsteller bereitgestellt werden.

Da eine Vielzahl von Zertifizierungsverfahren parallel bearbeitet werden, ist die Prüfstelle verpflichtet, den zu Beginn des Verfahrens vereinbarten Zeitplan möglichst einzuhalten. Bei sich abzeichneten Verzögerungen sind die Zertifizierungsstelle und der Antragsteller zu informieren, um eine aktualisierte Verfahrensplanung abzustimmen.

Eine Übersicht der anerkannten Prüfstellen wird vom BSI in der Publikation [BSI 7148] und auf der Internetseite des BSI in der Rubrik „Zertifizierung und Anerkennung“ veröffentlicht.

3.3 Zertifizierungsstelle und Bestätigungsstelle des BSI mit Aufgaben und Pflichten

Die Aufgabe der Zertifizierungs- und Bestätigungsstelle ist es, die Gleichwertigkeit aller Evaluierungsergebnisse und den vollständigen und korrekten Ablauf des Verfahrens sicherzustellen. Um dies zu erreichen, führt die Zertifizierungsstelle in jedem Verfahren eine Prüfbegleitung im Hinblick auf eine einheitliche Vorgehensweise und Methodik und damit vergleichbarer Bewertungen durch. Diese Arbeiten können durch eine von BSI anerkannte externe Prüfbegleitungsstelle unterstützt werden (siehe Kap. 3.4)

Konkrete Aufgaben der Zertifizierungs- bzw. Bestätigungsstelle sind bei Produkt- oder Standortevaluierungen die Abnahme der Sicherheitsvorgaben, die Prüfung, Kommentierung und Abnahme der Prüfberichte, die Teilnahme an Evaluierungssitzungen, die Begleitung von Audits von Entwicklungs- und Produktionsstandorten und von Test- und Penetrationsaktivitäten der Prüfstelle (bei Produktevaluierungen) sowie die Erstellung und Abstimmung von ggf. notwendigen Interpretationen der Kriterienwerke.

Bei Bestätigungsverfahren nach SigG schließt die Abnahme des abschließenden Prüfberichtes (Evaluation Technical Report, ETR) in einem besonderen Schritt die abschließende Prüfung auf Konformität mit dem Signaturgesetz ein.

Zum Abschluss des Zertifizierungsverfahrens erstellt die Zertifizierungsstelle den Zertifizierungsbescheid, das Zertifikat und den Zertifizierungsreport sowie ggf. Bestätigungsbescheid und Bestätigung (hier Urkunde und Report in einer Datei). Zertifizierungsreporte und Bestätigungsreporte werden durch die Zertifizierungsstelle veröffentlicht.[16] Die Bestätigung sowie der zugehörige abschließende Evaluierungsbericht eines Bestätigungsverfahrens wird der Bundesnetzagentur zur Verfügung gestellt.

Die Zertifizierungsstelle des BSI ist auf Grund ihres Charakters als nationale IT-Sicherheitsbehörde, auf Grund der notwendigen Erfüllung der inhaltlichen Anforderungen aus der DIN EN ISO/IEC 17065 und aus den internationalen Anerkennungsabkommen heraus in jedem Zertifizierungsverfahren verpflichtet die Vertraulichkeit der zur Verfügung gestellten Unterlagen und die der Prüfergebnisse intern in der Zertifizierungsstelle sowie in der Kommunikation mit Antragsteller und Prüfstelle nach dem Need-to-know Prinzip sicherzustellen. In Ausnahmefällen kann, unter bestimmten Bedingungen, zwischen Antragsteller und BSI eine zusätzliche Vertraulichkeitsvereinbarung (Non-Disclosure Agreement (NDA)) abgeschlossen werden.

Bei Zertifizierung eines Schutzprofils sind die Aufgaben der Zertifizierungsstelle die Kommentierung des Schutzprofils selbst und die Prüfung, Kommentierung und Abnahme der Prüfberichte sowie die Erstellung und Abstimmung von ggf. notwendigen Interpretationen der Kriterienwerke.

Da in der Zertifizierungsstelle eine Vielzahl von Zertifizierungs- und Bestätigungsverfahren parallel bearbeitet werden und der Umfang notwendiger Kommentierungen zu Prüfberichten nicht im Detail vorhersehbar ist, kann es mitunter zu Verzögerungen in der Bearbeitung der Verfahren kommen. Ebenso kann eine notwendige priorisierte Bearbeitung nationaler Zertifizierungsprojekte zu Verzögerungen in anderen Verfahren führen (siehe Kap. 2.1). Die Zertifizierungsstelle kommuniziert sich abzeichnende Verzögerungen an den Antragsteller und an die Prüfstelle zeitnah, um ggf. eine aktualisierte Verfahrensplanung abzustimmen.

---

16 Der Antragsteller kann der Veröffentlichung des Zertifizierungsreportes vor Abschluss des Verfahrens widersprechen. In diesem Fall fällt das Zertifikat jedoch nicht unter die internationalen Abkommen zur Anerkennung CCRA / SOGIS-MRA.

Die Anforderungen der Kriterienwerke wurden generisch formuliert, um sie auf ein möglichst breites Produktspektrum anwenden zu können. Dies hat zur Folge, dass Kriterienanforderungen immer wieder für konkrete Einzelfälle zu interpretieren sind. Um die Vergleichbarkeit der Evaluierungsergebnisse unterschiedlicher Prüfstellen sicherzustellen, erstellt die Zertifizierungsstelle in solchen Fällen in Abstimmung mit der Prüfstelle verbindliche Interpretationen. Auf der Basis dieser Einzelfallentscheidungen aus bestimmten Zertifizierungsverfahren können dann von der Zertifizierungsstelle unter Beteiligung aller Prüfstellen verallgemeinerte Interpretationen erarbeitet werden. Diese Interpretationen werden als AIS-Dokumente veröffentlicht. Es gibt wenige Ausnahmen, in denen bestimmte AIS-Dokumente nicht veröffentlicht werden. Die Zertifizierungsstelle bringt nationale Interpretationen, wo erforderlich, in die internationale Abstimmung in Hinblick auf eine Anerkennung durch die Mitglieder der Anerkennungsabkommen ein.

3.4 Externe Unterstützung bei der Prüfbegleitung

Das BSI hat eine vertraglich vereinbarte Kooperation in der Prüfbegleitung bei Produktzertifizierungsverfahren mit dem Fraunhofer-Institut für offene Kommunikationssysteme, FOKUS, Berlin geschlossen. Das dort eingerichtete "CertLab" kann vom BSI beauftragt werden, eine bestimmte Prüfbegleitung im Rahmen eines Zertifizierungsverfahrens durchzuführen. Die Regelungen und Prozesse der Zertifizierungsstelle und die darauf abgestimmten Regelungen und Prozesse von CertLab stellen sicher, dass die Vertraulichkeit gewahrt ist und Prüfbegleitungen bei CertLab vergleichbar mit denen beim BSI durchgeführt werden. Der Prüfbegleiter bei CertLab hat dieselbe Rolle und damit dieselben Aufgaben und Pflichten wie ein Prüfbegleiter im BSI. 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.

4 Der Zertifizierungsprozess als Phasenmodell

Die Erst- und Re-Zertifizierung von Produkten und Standorten[17] bzw. Erst- und Re-Bestätigung[18] von Produkten ist in folgende Phasen unterteilt:

4.1 Phase 1 (Vorphase und Logistik):

Der Zertifizierung geht i. d. R. ein Informationsgespräch mit dem Antragstellers durch das BSI bzw. eine anerkannten Prüfstelle voraus (gelegentlich als Vor-Evaluierung bezeichnet). In dieser Phase wird der Entwurf der Sicherheitsvorgaben erstellt und analysiert, welche Nachweise beim Hersteller bereits vorliegen bzw. noch erstellt oder ergänzt werden müssen. Ebenso werden weitere Anlagen zum Zertifizierungsantrag erstellt: eine Übersicht der Entwicklungs- und Produktionsstandorte sowie eine Liste der im Produkt (in externen Schnittstellen und Protokollen) implementierten kryptografischen Mechanismen.

Für ein Folgeverfahren (z. B. eine Re-Zertifizierung, Maintenance, partielle ALC Re-Evaluierung) erstellt der Antragsteller eine Änderungsbeschreibung mit sog. Auswirkungsanalyse (Impact Analysis Report (IAR); Anm.: AIS 38 erläutert den geforderten Inhalt des IAR) um die Entscheidung der Wiederverwendbarkeit von Herstellernachweisen oder Evaluierungsergebnissen aus früheren Verfahren zu unterstützen.

Zwischen Antragsteller und Prüfstelle wird der Evaluierungsvertrag abgeschlossen.

Die Prüfstelle erstellt auf dieser Basis einen Evaluierungsplan. Der Evaluierungsplan enthält Angaben zur inhaltlichen Durchführung der Evaluierung, der anzuwendenden Kriterien und Interpretationen sowie zur zeitlichen Planung (Meilensteinplan) sowie eine Unabhängigkeits- und Unparteilichkeitserklärung. Er sollte auch Workshops zur Besprechung von Teilergebnissen, wie zu ADV, ATE, AVA beinhalten.

---

17 Das Phasenmodell ist identisch nur mit entsprechend angepassten Begrifflichkeiten bezogen auf die Zertifizierung von Standorten (bspw. „Standort-Sicherheitsvorgaben“ anstelle von „Sicherheitsvorgaben“ oder „Standort“ anstelle von „Produkt“)

18 Bei Bestätigungsverfahren sinngemäß: Bestätigungsantrag, Bestätigungs-ID, Bestätigungsreport, Bestätigungsbescheid,...

Danach wird beim BSI der Zertifizierungsantrag gestellt. Unter Mitwirkung von BSI und Prüfstelle werden dann die Sicherheitsvorgaben und die Evaluierungsplanung in einem gemeinsamen Kick-off Meeting abgestimmt. 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.

Nach Abschluss dieser Vorbereitungen wird das Verfahren in das Zertifizierungsschema aufgenommen und der Antragsteller erhält vom BSI eine formale Eingangsbestätigung, in der ihm die Zertifizierungskennung[19] und die Prüfbegleiter der Zertifizierungsstelle des BSI oder von CertLab mitgeteilt werden. Das Produkt wird, wenn der Antragsteller dies im Zertifizierungsantrag wünscht, in die Liste der im Zertifizierungsverfahren befindlichen Produkte, die auf der Webseite des BSI veröffentlicht wird, aufgenommen. Sofern erforderlich, schult der Antragsteller Evaluatoren und Prüfbegleiter.

Entsprechend der o. g. nationalen Zertifizierungspolitik kann die Bearbeitung priorisiert erfolgen.

4.1.1 Zertifizierungsantrag / Bestätigungsantrag

Der Antrag enthält Angaben, die für den Start des Verfahrens und seine Abwicklung benötigt werden. Es gibt gesonderte Antragsformulare für die Produktzertifizierung, die Zertifizierung von Schutzprofilen, für die Bestätigung nach SigG und für die Zertifizierung von Standorten nach CC.

Die Antragsformulare sind auf der Internetseite des BSI in der Rubrik Zertifizierung und Anerkennung verfügbar.

Folgende Antragsmöglichkeiten sind zu unterscheiden:

1. a) Der Zertifizierungsantrag bezieht sich auf die Zertifizierung eines Produktes.
   b) Der Zertifizierungsantrag bezieht sich auf die Re-Zertifizierung eines bereits zertifizierten Produktes, wenn sicherheitsrelevante Änderungen an diesem Produkt oder Änderungen an sicherheitsrelevanten Produktteilen vorgenommen wurden.
   c) Der Zertifizierungsantrag bezieht sich auf eine die Re-Zertifizierung oder den Maintenanceprozess, da möglicherweise nur nicht sicherheitsrelevante Änderungen am Produkt oder Produktteilen vorgenommen wurden. Hier prüft die Zertizierungsstelle, ob der vereinfachte Maintenanceprozess zur Anwendung kommen kann.
   Bei einer Re-Zertifizierung besteht die Möglichkeit, die Zertifizierungs-ID aus dem Vorgängerverfahren fortzusetzen.
   d) Der Zertifizierungsantrag bezieht sich nur auf Änderungen an den Nachweisen für die Prüfklasse ALC (Lebenszyklus, Entwicklungs- oder Produktionsstandorte) (partielle ALC Re-Evaluierung).
   e) Der Zertifizierungsantrag bezieht sich auf die Neubewertung eines bereits zertifizierten Produktes nach dem jeweils aktuellen Stand der Technik.
2. a) Der Antrag bezieht sich auf die Bestätigung eines Produktes nach SigG.
   b) Der Antrag bezieht sich auf die Re-Bestätigung oder Nachtragsbestätigung eines bereits bestätigten Produktes, da Änderungen an diesem Produkt vorgenommen wurden.

---

19 Die Zertifizierungskennung/Zertifizierungs-ID ist die Vorgangskennung beim BSI; sie wird bei jedem Schriftwechsel zur Kennzeichnung von Dokumenten und des Zertifizierungsreports verwendet;
Produktzertifikate: 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))
Standortzertifikate: 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 Schutzprofile: 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 ID um: -MA-kk-llll (MA=Maintenance, kk=lfd. Nummer, llll=Jahr der Maintenanceergänzung.
Bestätigung nach SigG: BSI.nnnnn.TE.mm.jjjj (nnnnn = laufende Antragsnummer, TE=technische Komponente nach SigG/SigV, mm=Monat, jjjj=Jahr der Erteilung der Bestätigung (wird erst bei Erteilung der Bestätigung angefügt))

3. a) Der Zertifizierungsantrag bezieht sich auf die Zertifizierung eines Schutzprofils.
   b) Der Antrag bezieht sich auf die Re-Zertifizierung oder Maintenance eines bereits zertifizierten Schutzprofils, da Änderungen vorgenommen wurden.
4. a) Der Zertifizierungsantrag bezieht sich auf die Zertifizierung eines Entwicklungs- oder Produktionsstandortes.
   b) Der Antrag bezieht sich auf die Re-Zertifizierung oder Maintenance eines bereits zertifizierten Standortes, da Änderungen vorgenommen wurden.

Im Rahmen des Antrags (Vordruck) werden u. a. folgende Daten erfasst:

- die genaue Bezeichnung des Prüfgegenstands,
- die Prüfgrundlagen auf Basis der CC Version 3.1:
  - die vom Antragsteller angestrebte Prüfstufe gemäß der CC Methodik, z. B. EAL3, + ALC_DVS.2 (bei einem Bestätigungsantrag sind entsprechend SigG nur bestimmte Stufen möglich),
  - das bei Produktprüfungen heranzuziehende Schutzprofil sowie ergänzende Angaben,
  - optional Angaben zu relevanten Technischen Richtlinien des BSI,
  - optional Angaben zu relevanten Bedarfsträgern für das Zertifizierungsverfahren,
- Art der Zertifizierung (Erst-Zertifizierung, Re-Zertifizierung, Re-Zertifizierung/Maintenance, Partielle ALC Re-Evaluierung, Neubewertung) bzw. Art der Bestätigung (Erst-Bestätigung, Re-Bestätigung/Nachtragsbestätigung),
- die vom Antragsteller beauftragte anerkannte Prüfstelle (bei Nachtragsbestätigung nicht erforderlich, bei Maintenance nur in bestimmten Fällen erforderlich),
- Verschiedene Erklärungen des Antragstellers:
  - eine Erklärung zu Beratung durch die für die Evaluierung beauftragte Prüfstelle bzw. zu möglichen Abhängigkeiten zwischen Hersteller und Prüfstelle,
  - eine Erklärung hinsichtlich der Archivierung,
  - eine Erklärungen zur Bekanntgabe des laufenden Verfahrens,
- Verschiedene Einverständniserklärungen des Antragsteller:
  - zur Veröffentlichung des Zertifizierungs- bzw. Bestätigungsergebnisses,
  - dass ggf. eine vom BSI zugelassene externe Stelle die Prüfbegleitung unterstützt,
  - Bei Bestätigungsantrag: Einverständniserklärung des Antragstellers, dass bei positivem Abschluss des Verfahrens der Evaluierungsbericht sowie eine Kopie der Bestätigung an die Bundesnetzagentur gegeben werden dürfen,
  - Einverständnis bzgl. Datenschutz bei der Speicherung relevanter Verfahrensdaten,
- ggf. Hinweis auf Bedarf nach einem Zertifizierungsbutton (bei Produkten).

Bei Produktzertifizierung oder Bestätigung nach SigG gehören zum Antrag verschiedene Anlagen, wie z. B.

- die Erklärung des Herstellers bezüglich seiner Mitwirkung: Die Erklärung des Herstellers bezüglich seiner Mitwirkung ist erforderlich, wenn der Antragsteller selbst nicht der Hersteller sämtlicher Bestandteile des Produktes ist oder nicht selbst die Rechte an den erforderlichen vollständigen Unterlagen zum Gegenstand der Zertifizierung hat. 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.
- das Dokument Sicherheitsvorgaben: Die Konzeption des Dokumentes Sicherheitsvorgaben ist in den Prüfkriterien (Common Criteria Teil 1) definiert. Bei Bestätigung nach SigG ist ein Anhang zu den Sicherheitsvorgaben erforderlich, aus dem hervorgeht, wie die relevanten Anforderungen aus SigG und SigV durch das Produkt umgesetzt werden.
- die zur Abstimmung vorgeschlagene Evaluierungsplanung der Prüfstelle: Die Evaluierungsplanung umfasst Angaben zu Art, Umfang und geplanter Durchführung der Evaluierung entsprechend der Vorgaben für die Prüfstellen.

- eine Auflistung, der für das Produkt relevanten Entwicklungs- und Produktionsstandorte (gemäß Beispiel im Anhang des Antragsformulars). Die Angaben sind zur Umsetzung der BSI Zertifizierungspolitik erforderlich und unterstützen eine frühzeitige Planung der ALC Prüfaspekte nach CC. Diese Auflistung soll umfassen:
  (i) Name der Organisation, die den Standort betreibt und, wenn abweichend, auch Name der Organisation, die für den Standort und die am Standort vorliegenden Prüfnachweise verantwortlich ist;
  (ii) Genaue Anschrift des Standortes;
  (iii) Art des Standortes (z. B. Produktentwicklung / Test / Auslieferung / Chipproduktion / Gerätemontage /...) ergänzt um eine Kurzbeschreibung der Rolle des Standortes im Lebenszyklus des Produktes[20].
- eine Auflistung der (in externen Schnittstellen und Protokollen) implementierten kryptografischen Mechanismen gemäß Beispiel im Anhang des Antragsformulars.
  Sind in dem in den Sicherheitsvorgaben beschriebenen Evaluierungsgegenstand auf externen Schnittstellen Sicherheitsfunktionalitäten mittels kryptografischer Mechanismen realisiert oder werden kryptografische Services angeboten (z.B. Verschlüsselungsfunktion, Hashwertbildung, Signaturerzeugung, Zufallszahlenerzeugung, Schlüsselerzeugung, Protokolle mit kryptografischen Anteilen), so erfordert deren Evaluierung und Zertifizierung aufgrund nationaler Erfordernisse besondere Aufmerksamkeit. Um den Ablauf des Verfahrens möglichst optimal gestalten zu können und mögliche Ausschlüsse frühzeitig erkennen zu können, ist der Antragsteller gebeten, eine Übersichtsliste mit den diesbezüglichen verwendeten Mechanismen bereitzustellen.

Bei Standortzertifizierungen gehören zum Antrag verschiedene Anlagen wie z. B.

- das Dokument Standort-Sicherheitsvorgaben: Die Konzeption des Dokumentes Standortsicherheitsvorgaben ist in den im Antrag genannten Prüfgrundlagen definiert (siehe Dokument Anwendungshinweise und Interpretationen AIS 47 [AIS 47]),
- die zur Abstimmung vorgeschlagene Evaluierungsplanung der Prüfstelle (Die Evaluierungsplanung umfasst Angaben zu Art, Umfang und geplanter Durchführung der Evaluierung entsprechend der Vorgaben für die Prüfstellen).

Bei Folgeverfahren wie Re-Zertifizierung / Maintenance bzw. Re-Bestätigung / Nachtragsbestätigung sind folgende Anlagen zusätzlich erforderlich:

- eine Beschreibung der Änderungen mit einer Auswirkungsanalyse (IAR). Die geforderten Inhalte sind im Dokument Anwendungshinweise und Interpretationen AIS 38 [AIS 38] dargelegt, das auf der Webseite des BSI verfügbar ist,
- eine aktualisierte Konfigurationsliste gemäß den Anforderungen der relevanten Prüfstufe. Der aktuelle Stand der Änderungen gegenüber der Konfigurationsliste der zertifizierten / bestätigten Version des Produktes muss erkennbar ausgewiesen sein,
- ggf. geänderte Anwendungshandbücher zum Prüfgegenstand. Der aktuelle Stand der Änderungen gegenüber den Handbüchern der zertifizierten / bestätigten Vorgängerversion des Produktes muss erkennbar ausgewiesen sein.

Mit dem Antrag erkennt der Antragsteller die Kostenverordnung des BSI an. Ebenso erkennt er die Vorgehensweise in den Prozessen der Zertifizierungsstelle und die mögliche Auslagerung der Prüfbegleitung an CertLab (s. o.) einschließlich der Abrechnung externer Reisekosten von CertLab entsprechend den Vorgaben für BSI Mitarbeiter an.

Der Antrag muss handschriftlich unterzeichnet werden und einen Firmenstempel enthalten.

Der Zertifizierungs- oder Bestätigungsantrag ist in schriftlicher Form zu leiten an:

Bundesamt für Sicherheit in der Informationstechnik
Referate S22/S23- Zertifizierungsstelle
Postfach 20 03 63
53133 Bonn

Vorab kann der Antrag per E-Mail gesendet werden an: zertdokus@bsi.bund.de

---

20 Anm.: Es werden an dieser Stelle noch nicht die vollständigen Unterlagen zur Beschreibungen der Prozesse, Verfahren und Regeln, die am jeweiligen Standort gelten, benötigt.

4.1.2 Dokumentenaustausch im laufenden Verfahren

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 das BSI gesendet.

Bei Verwendung anderer Verschlüsselungsprogramme seitens des Antragstellers gegenüber dem BSI kann auf Grund der BSI internen Sicherheitspolitik und der verwendeten IT nicht sichergestellt werden, dass die Unterlagen entschlüsselbar sind oder zeitgerecht in die elektronische Dokumentenablage des jeweiligen Zertifizierungsverfahrens eingestellt sind.

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

zertdokus@bsi.bund.de

erfolgen, da die Entschlüsselung und Registrierung eingehender Unterlagen i. d. R. nicht von den Zertifizierern selbst, sondern durch die Administration der Zertifizierungsstelle durchgeführt wird. Die Lieferung an persönliche BSI-E-Mail Adressen von Zertifizierern erfolgt in der Regel zusätzlich in Kopie zur Kenntnis.

Dokumente, die in Papierform an das BSI geschickt werden oder die per Kurierversand direkt an der Pforte des BSI, Godesberger Allee 185-189 abgegeben werden, müssen in einem geeignet versiegelten inneren Sicherheitsumschlag verpackt und mit dem Vermerk „ungeöffnet an die Zertifizierungsstelle“ versehen werden, damit die Vertraulichkeit der Unterlagen auf dem Postweg, auch auf dem BSI-internen Postweg, gegeben ist. Ein äußerer Umschlag trägt dann die Postanschrift des BSI:

Bundesamt für Sicherheit in der Informationstechnik
Referate S22/S23– Zertifizierungsstelle
Postfach 20 03 63
53133 Bonn

Dokumente, die per CD an das BSI geschickt werden, müssen auf der CD verschlüsselt gespeichert werden.
Prüfstelle und Zertifizierungsstelle kennzeichnen ihre jeweiligen Dokumente zum Verfahren (Prüfunterlagen, Kommentierungen) als „firmenvertraulich“ bzw. „company confidential“.

4.2 Phase 2 (Evaluierung):

Der Antragsteller stellt die jeweils erforderlichen Nachweise, und bei produktbezogenen Verfahren das betreffende Produkt, zur Verfügung.

Die Prüfstelle führt die als Evaluierung bezeichnete technische Prüfung durch. Die Evaluierung ist entsprechend der Prüfaspekte des angewendeten Kriterienwerks in verschiedene Teilschritte unterteilt. Die Prüfstelle dokumentiert und begründet die Prüfergebnisse in Teil-Prüfberichten entsprechend der diesbezüglichen Vorgaben des Zertifizierungsschemas des BSI. Diese Teil-Prüfberichte sind Bestandteil des abschließenden Evaluierungsberichtes (ETR).

Die Zertifizierungsstelle begleitet die Evaluierung (Prüfbegleitung), um eine einheitliche Vorgehensweise und Methodik und vergleichbare Bewertungen sicherzustellen. Dazu werden die Prüfberichte vom Prüfbegleiter geprüft und ggf. kommentiert. Kommentare und Nachforderungen sind durch die Prüfstelle und ggf. auch durch den Antragsteller zu bearbeiten. Der Prüfbegleiter kann bestimmte Aktivitäten der Prüfstelle wie z. B. die Durchführung von Test/Penetrationstests oder die Durchführung von Standort-Audits beim Hersteller jeweils vor Ort überwachen.

Nachbesserungen am Produkt und an der Herstellerdokumentation sind seitens des Antragstellers während des Verfahrens stets möglich.

Die Zertifizierungsstelle kann Evaluierungsbesprechungen mit der Prüfstelle und/oder Hersteller ansetzen, um sich Detailplanungen und Prüfergebnisse darlegen zu lassen oder strittige Fragen zu klären (z.B. ADV / ATE / AVA Workshop). Im Kick-off Meeting sollten diese Workshops bereits in die Planung einbezogen werden. Zur Abstimmung der Aktivitäten zur Schwachstellenanalyse und Penetrationstests wird mit der Prüfstelle i. d. R. ein sog. AVA-Kick-off Meeting abgehalten. Diesem

Meeting kann auch der Hersteller beiwohnen. In diesem Meeting oder separat werden auch die Fragen zur Analyse und zum Test kryptografischer Verfahren besprochen (AVA-Krypto-Kick-off-Meeting).

Alle Projektbeteiligten sind verpflichtet, Abweichungen von der vereinbarten Zeitplanung den anderen Beteiligten mitzuteilen und dann den Meilensteinplan erneut abzustimmen. Regelmäßige Telefonkonferenzen zum Abgleich des Verfahrensstatus werden empfohlen. Dies wird im Kick-off Meeting ebenfalls vereinbart.

Nachdem alle Teil-Prüfberichte akzeptiert sind, erstellt die Prüfstelle zum Abschluss der Evaluierung den zusammenfassenden Teil des Evaluierungsberichtes. Dieser wird in der Sprache (dt. oder engl.) erstellt, in dem die Sicherheitsvorgaben erstellt wurden. Die Zertifizierungsstelle führt dann eine formale Abnahme des ETR durch. Antragsteller und Prüfstelle werden über diese Abnahme informiert. Damit sind die inhaltlichen Voraussetzungen für die Erteilung des Zertifikates gegeben. Zur Veröffentlichung der Sicherheitsvorgaben im Zuge der Zertifizierung kann nach bestimmten Regeln (siehe AIS 35) eine reduzierte öffentliche Fassung der Sicherheitsvorgaben zwischen Antragsteller und BSI abgestimmt werden.

4.2.1 Prüfgegenstand, Evaluierungsgegenstand (EVG, TOE)

Die Prüfung und Bewertung nach Common Criteria oder ITSEC bezeichnet man als Evaluierung. Der Prüfgegenstand wird daher im Rahmen einer Zertifizierung nach CC oder ITSEC als Evaluierungsgegenstand (EVG, engl. Target of Evaluation, TOE) bezeichnet.

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) definiert.

Es können Produkte unterschiedlichster Art evaluiert werden:

- Software-Produkte (z. B. Betriebssysteme, Datenbanksysteme, Anwendungsprogramme, VPN-Software, Firewalls)
- Hardware-Produkte (z. B. Smart Card Integrated Circuits)
- Kombinationen aus Software und Hardware (z. B. Hardware einer Smart Card zusammen mit einem Betriebssystem und einer darauf befindlichen Anwendung, Hardware-Sicherheitsmodule, Kartenterminals)
- Kombinationen aus einzelnen SW-Produkten

Eine wesentliche Voraussetzung 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.

Bei einer Schutzprofilzertifizierung ist der EVG das jeweilige Dokument Schutzprofil und es wird dessen Konformität mit den Konzepten der CC abgeglichen und bestätigt.

Bei Standortzertifizierungen ist der EVG ein Entwicklungs- oder Produktionsstandort oder eine entsprechende Organisationseinheit, die bestimmte Services im Rahmen der Entwicklung oder Produktion eines 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. Die physische Abgrenzung ist durch die relevanten Räumlichkeiten und den Ort gegeben. Innerhalb dieser Abgrenzungen werden Verfahren, Prozesse und Regeln geprüft. Der zu prüfende Standort wird zu Beginn eines Standortzertifizierungsverfahrens vom Antragsteller im Dokument Standortsicherheitsvorgaben (Site Security Target, SST) definiert.

Bei einer Bestätigungen nach SigG handelt es sich bei dem EVG um ein IT-Produkt einschließlich der Anwendungshandbücher, so wie es auch für Produktzertifizierungen gilt. Das Produkt muss jedoch im Sinne des Signaturgesetzes und der Signaturverordnung eine sichere Signaturerstellungseinheit, eine Signaturanwendungskomponente oder eine technische Komponente für Zertifizierungsdienste sein.

4.2.2 Entwicklungsstadium eines Produktes

In Abhängigkeit vom Entwicklungsstadium des Produktes können verschiedene Arten der Evaluierung und Zertifizierung eines Produktes unterschieden werden. In der folgenden Übersicht werden beispielhaft die verschiedenen Entwicklungsstadien eines Produktes aufgezeigt.

Entwicklungsstadium	**Art der Evaluierung und Zertifizierung**
Planung / Konzeption	Entwicklungsbegleitende Evaluierung und Zertifizierung bzw. Bestätigung nach SigG
Entwurf	Entwicklungsbegleitende Evaluierung und Zertifizierung bzw. Bestätigung nach SigG
Implementierung	Entwicklungsbegleitende Evaluierung und Zertifizierung bzw. Bestätigung nach SigG
Prototyp	Entwicklungsbegleitende Evaluierung und Zertifizierung bzw. Bestätigung nach SigG
Existierendes Produkt	Evaluierung und Zertifizierung bzw. Bestätigung nach SigG eines fertigen Produktes Erneuerung eines bestehenden Zertifikates durch Neubewertung / Re-Assessment Prozess, d. h.: Re-Evaluierung der Angriffsresistenz der zertifizierten Version eines Produktes im Kontext der jeweiligen Sicherheitsvorgaben nach aktuellem Stand der Technik sowie Aktualisierung der Standortsicherheit relevanter Entwicklungs- und Produktionsstandorte, anlassbezogen
Weiterentwicklung/Update	Assurance Continuity Prozess, d. h.: Re-Evaluierung / Re-Zertifizierung bzw. Re-Bestätigung nach SigG oder Maintenance bzw. Nachtragsbestätigung nach SigG 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.

Die entwicklungsbegleitende Evaluierung und Zertifizierung findet parallel zur Produktentwicklung statt. Dabei werden Zug um Zug die notwendigen Prüfschritte durchgeführt, so dass das Zertifikat fast zeitgleich mit der Markteinführung vorliegen kann.

Verfahrensbezogene Besonderheiten dieser Arten der Evaluierung und Zertifizierung sind in Kap. 5 dargelegt.

4.2.3 Zustand eines Standortes bei Zertifizierung

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.

4.2.4 Herstellernachweise zur Erfüllung der Prüfanforderungen

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 Produkt (z. B. Designinformationen, Handbücher und Testnachweise) in dokumentierter Form benötigt. Umfang und Beschreibungstiefe dieser Informationen richten sich nach den jeweils verwendeten Prüfkomponenten aus den CC bzw. ITSEC, die im Dokument Sicherheitsvorgaben festgelegt sind. Die entsprechenden Informationen müssen vom Antragsteller bereitgestellt werden. Dies kann in unterschiedlicher Form geschehen:

1. Im Rahmen einer Vor-Evaluierung kann eine anerkannte Prüfstelle vorab prüfen, welchen Zustand die vorhandene Dokumentation zum Evaluierungsgegenstand hat. Anhand dessen kann die erreichbare Prüfstufe bzgl. der dokumentierten Nachweise festgestellt werden und

der Aufwand für notwendige Ergänzungen möglichst realistisch abgeschätzt und eine sinnvolle Projektplanung ermöglicht werden. Ebenso kann im Rahmen der Vor-Evaluierung eine erste Analyse der Sicherheitseigenschaften des Produktes erfolgen, um so grundsätzlichen Problemen bei der Evaluierung vorzubeugen.

2. Die Produktentwickler oder Prozessverantwortlichen selbst erstellen die erforderlichen Nachweise im Rahmen des normalen Entwicklungsprozesses als Design- oder Prozessdokumentation. Erkannte Fehler in der Dokumentation, z. B. Inkonsistenzen oder nicht dokumentierte Eigenschaften werden von den Entwicklern während der Evaluation korrigiert. Dies erfordert jedoch, dass der Hersteller bereits Erfahrungen mit Zertifizierungen nach CC besitzt.
3. Eine externe Stelle erstellt im Auftrag des Antragstellers in direkter Zusammenarbeit mit Entwicklern und Prozessverantwortlichen beim Hersteller noch fehlende Nachweise. Diese Aufgabe kann u. a. von einer der anerkannten Prüfstellen wahrgenommen werden. Sollte diese Prüfstelle zusätzlich auch mit der Evaluierung des Produktes beauftragt werden, so muss zur Wahrung der Objektivität bei der späteren Evaluierung gewährleistet sein, dass die Evaluatoren in keiner Weise an der Erstellung der Nachweise beteiligt waren oder eine Abhängigkeit zwischen Evaluator und Ersteller der Unterlagen besteht.
4. In bestimmten Fällen kann der Evaluator 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 [AIS 23]).
5. Quellcode von Produkten oder anderweitig hochsensible Designinformationen, die nach einer dokumentierten Sicherheitspolitik des Herstellers klassifiziert sind und die Entwicklungsumgebung nicht verlassen dürfen, können vom Evaluator in Abstimmung mit der Zertifizierungsstelle auch in der Entwicklungsumgebung selbst begutachtet werden.

Das BSI stellt für Antragsteller die Broschüren AIS 42 „Hinweise zur Erstellung von Herstellerdokumenten für eine CC-Evaluierung“ [AIS 42] und AIS 41 „Anleitungen zur Erstellung von Protection Profiles and Security Targets“ [AIS 41] auf der Internetseite des BSI zur Verfügung.

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, die im Dokument Standortsicherheitsvorgaben festgelegt sind. Für die Bereitstellung der Unterlagen gelten sinngemäß dieselben Regeln, die für die Evaluierung von IT-Produkten genannt wurden.

4.3 Phase 3 (Zertifizierung):

Die Zertifizierungsstelle erstellt die Zertifikatsurkunde, den Zertifizierungsreport und erteilt einen Zertifizierungsbescheid (bei Bestätigungsverfahren: Bestätigungsbescheid und Bestätigungsurkunde mit -report). Antragsteller und Prüfstelle haben die Möglichkeit den Entwurf des Zertifizierungsreportes bzw. der Bestätigung zu kommentieren. Der Zertifizierungsreport enthält u.a. ausgewählte Angaben zum Ergebnis der Evaluierung, Hinweise und Auflagen zur Benutzung des zertifizierten Gegenstandes (Produkt, PP, Standort) sowie bei Produktzertifikaten Angaben zur Eignung der implementierten kryptografischen Mechanismen aus Sicht des BSI. Der Zertifizierungsbescheid stellt das im rechtlichen Sinne offizielle Votum der Zertifizierungsstelle dar. Der Bescheid enthält Hinweise zur Verwendung des Zertifikates und Nebenbestimmungen (Auflagen), die vom Inhaber des Zertifikates zu beachten sind.

Sofern der Antragsteller der Zustimmung zur Veröffentlichung nicht widerrufen hat, werden die Ergebnisse des Verfahrens öffentlich bekannt gegeben. Die internationalen Anerkennungsvereinbarungen fordern die Veröffentlichung des Zertifizierungsreportes, so dass ein Zertifikat nur bei veröffentlichtem Zertifizierungsreport international anerkannt wird.

Ein Kostenbescheid ergeht gesondert an den Antragsteller.

4.3.1 Veröffentlichung von Zertifizierungs- und Bestätigungsergebnissen

Veröffentlichung durch das BSI

Informationen zu zertifizierten Produkten, Schutzprofilen und Standorten werden vom BSI in regelmäßig aktualisierten Publikationen veröffentlicht. Die Veröffentlichung erfolgt grundsätzlich nur für einen Zeitraum von 5 Jahren ab Zertifizierungsdatum. Bei in der Gültigkeit befristeten Zertifikaten (z.B. Standortzertifikaten, Bestätigungen nach SigG) erfolgt die Veröffentlichung für den Gültigkeitszeitraum. Ältere Zertifikate werden ggf. noch in einer öffentlichen Archivliste auf der BSI Webseite geführt.

- 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 oder einer Bestätigung zusammenfassend dargestellt.
- Rubrik Zertifizierung und Anerkennung auf den Internetseiten des BSI (https://www.bsi.bund.de/zertifizierung)
  Hier werden in Form von Übersichtslisten Zertifikate nach Produkttypen / Standorten / Schutzprofilen gegliedert sowie für Bestätigungen nach SigG das jeweilige Zertifikat bzw. die Bestätigung aufgelistet und der Zertifizierungsreport ggf. die Bestätigung und die Sicherheitsvorgaben zum Download angeboten.

  Ebenso werden in Zertifizierung / in Bestätigung 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 sowie für Bestätigungen nach SigG das jeweilige Zertifikat bzw. die Bestätigung 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 SOGIS-MRA und CCRA.

Erteilte Bestätigungen nach SigG müssen gemäß Vorgabe der Bundesnetzagentur veröffentlicht werden.

Veröffentlichung durch andere Stellen

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 SOGIS-MRA fallen, werden auf den Internetseiten der zugehörigen nationalen Zertifizierungsstellen veröffentlicht. Seitens der SOGIS-MRA Mitglieder empfohlene Schutzprofile sind auf der Internetseite http://www.sogisportal.eu veröffentlicht.

Internetseite der Bundesnetzagentur:

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

Veröffentlichung durch den Antragsteller

Bei einem Verweis auf die Tatsache der Zertifizierung oder Bestätigung nach SigG in Veröffentlichungen des Antragstellers muss der Antragsteller die Zertifizierungskennung z. B. BSI-DSZ-CC-nnnn-yyyy und einen Verweis auf die Fundstelle des Zertifizierungs-/Bestätigungsreportes auf der Internetseite des BSI angeben oder den sogenannten Zertifizierungsbutton (s. u.) verwenden.

4.3.2 Weitere Unterstützung des Antragstellers

Sprache für den Zertifizierungsreport / für eine Bestätigung nach SigG:
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. Eine Bestätigung nach SigG wird in deutscher Sprache erstellt.

Öffentliche Fassung der Sicherheitsvorgaben:
Das Dokument Sicherheitsvorgaben ist als Anlage zum Zertifizierungsreport Teil der Veröffentlichung des Zertifizierungsergebnisses. Der Antragsteller kann eine reduzierte öffentliche Fassung der vollständigen Sicherheitsvorgaben 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.

Zertifikatsübergabe / Presseerklärung:
Veröffentlicht der Antragsteller nach Abschluss des Verfahrens eine Presseerklärung, so bittet das BSI, den Wortlaut zuvor mit der Zertifizierungsstelle des BSI abzustimmen.

Das BSI bietet die Möglichkeit, auf bestimmten öffentlichen Veranstaltungen wie z. B. Kongressen und Messen, auf denen das BSI vertreten ist, das Zertifikat / die Bestätigung an einen Vertreter des Unternehmens auszuhändigen. Insbesondere fallen hierunter die Veranstaltungen: CeBIT, ITSA, Common Criteria Konferenz, Moderner Staat, RSA-Konferenz.

Nach Absprache kann ebenso eine Übergabe an einen Vertreter des Unternehmens in den Räumen des BSI organisiert werden.

Zeichensatzung
a) Zertifizierungsbutton:
Auf Wunsch des Antragstellers (siehe Zertifizierungsantrag) stellt das BSI für erteilte Produktzertifikate eine Druckvorlage für einen Zertifizierungsbutton in bestimmten Grafikformaten (rgb, cmyk) zur Verfügung. Dieser wird nach Abschluss des Verfahrens erstellt und dem Antragsteller zugesandt. Es gelten besondere Verwendungsbedingungen, so darf der Button z. B. nur verwendet werden, so lange die Zertifizierung gültig ist und solange die Archivierungszusage (meist 5 Jahre) gemacht ist.

b) BSI Logo, Common Criteria Logo und Logos der Anerkennungsabkommen CCRA und SOGIS-MRA:

Das BSI Logo und die Logos der Anerkennungsabkommen CCRA (siehe Kap. 2.2.3) und SOGIS-MRA (siehe Kap. 2.2.2) dürfen nur als Teil der Zertifikatsurkunde verwendet und reproduziert werden.

Das Common Criteria Logo ("rotes CC-Rechteck", siehe Deckblatt) darf für Werbezwecke für zertifizierte Produkte und Services in der Anwendung der Common Criteria verwendet werden.

4.3.3 Kosten der Zertifizierung und Bestätigung

Das BSI berechnet gegenüber dem Antragsteller Gebühren und Auslagen für ein Zertifizierungs- oder Bestätigungsverfahren per Kostenbescheid auf Basis der Kostenverordnung [BSIKostV]. Dabei handelt es sich bei Erstverfahren um Pauschalen in Abhängigkeit von der Komplexität des Verfahrens zuzüglich weiterer Zusatzaufwände sowie Auslagen bei Dienstreisen. Bei Folgeverfahren (z. B. Re-Zertifizierung, Maintenance, Neubewertung) wird neben einer Grundpauschale nach Aufwand abgerechnet. Die beratenden Vorgespräche mit dem BSI vor Antragstellung sind kostenfrei.

Mit dem Antrag erkennt der Antragsteller die Kostenverordnung des BSI an. Ebenso erklärt er sich einverstanden, dass bei Auslagerung der Prüfbegleitung an CertLab (s.o.) das BSI externe Reisekosten von CertLab mit dem Antragsteller abrechnen darf.

Die Prüfstelle und der Antragsteller vereinbaren i. d. R. für eine Vor-Evaluierung eine Kostenregelung. 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.

Zusätzliche optionale Leistungen des BSI wie z. B. die Prüfung von nachträglichen Übersetzungen des Zertifizierungsreportes werden nach Aufwand abgerechnet.

4.3.4 Abbruch / Einstellung von Zertifizierungs- oder Bestätigungsverfahren

Zu jedem Zeitpunkt im Verfahren kann der Antragsteller den Antrag auf Zertifizierung oder Bestätigung zurückziehen. Dies muss dem BSI schriftlich mitgeteilt werden. In diesem Fall wird das Verfahren seitens des BSI kostenpflichtig beendet.

Ebenfalls kann zu jedem Zeitpunkt im Verfahren auf Grund besonderer Umstände das Verfahren seitens des BSI eingestellt werden. Hierzu zählen die Fälle, dass

- der Antragsteller oder die Prüfstelle über einen Zeitraum von mehr als 3 Monaten entgegen der vereinbarten Planung keine Unterlagen liefern. Die Einstellung wird mit einer Frist von 4 Wochen schriftlich angekündigt und dann umgesetzt, wenn das Verfahren nicht erneut durch Bereitstellung der geforderten Unterlagen und Abstimmung einer neuen Zeitplanung aktiviert wird;
- es sich abzeichnet, dass das Verfahren z. B. wegen technischer Mängel am Produkt nicht erfolgreich abgeschlossen werden kann. In diesem Fall kann auch ein formaler Versagungsbescheid erteilt werden;
- die Prüfstelle die erforderliche Anerkennung des BSI verloren hat,
- ein unvollständig eingereichter Antrag nicht innerhalb von 4 Wochen vervollständigt wird.

Antragsteller und Prüfstelle werden über die Einstellung eines Verfahrens informiert und die Kosten werden abgerechnet.

5 Arten der Zertifizierung und Bestätigung

Dieses Kapitel konzentriert sich auf die möglichen Arten der Evaluierung, Zertifizierung und Bestätigung und daraus resultierende Besonderheiten im Ablauf des Prozesses. Die Informationen zu technischen, rechtlichen und organisatorischen Rahmenbedingungen gelten, wie in den obigen Kapiteln beschrieben.

5.1 Erstmalige Zertifizierung eines Produktes

Bei der erstmaligen Zertifizierung eines Produktes stellt der Antragsteller möglichst technische Information zum Produkt vor Antragstellung bzw. mit dem Antrag zur Verfügung. Umfang und Tiefe der geplanten Zertifizierung wird vom Antragsteller im Dokument Sicherheitsvorgaben nach den Anforderungen der Prüfkriterien dargelegt.

Das BSI entscheidet über die grundsätzliche Zertifizierbarkeit des Produktes aus technischer Sicht vorbehaltlich des positiven Abschlusses der Evaluierung unter Berücksichtigung der Sicherheitsvorgaben und der rechtlichen Rahmenbedingungen.

Der Antragsteller entscheidet über Auswahl der Prüfstelle. Die Prüfstelle muss die für die Evaluierung notwendige Anerkennung durch das BSI haben und über Kenntnisse der Produkttechnologie verfügen und diese gegenüber der Zertifizierungsstelle nachweisen können.

Der positive Abschluss einer Zertifizierung erfordert, dass der Antragsteller alle nach den Prüfkriterien und ggf. nach besonderen Anforderungen des BSI erforderlichen Nachweise der Prüfstelle und dem BSI zur Verfügung stellt. Es empfiehlt sich, vor Beginn des Verfahrens die bereits beim Antragsteller zur Verfügung stehenden Nachweise durch eine anerkannte Prüfstelle im Hinblick auf Verwendbarkeit für das Verfahren sichten zu lassen, um den Ergänzungsbedarf frühzeitig festzustellen und damit eine genauere Planung zu ermöglichen.

Die Einbeziehung kryptografischer Verfahren in die Zertifizierung kann zusätzliche Begutachtungen durch das BSI einschließen. Ebenso kann das BSI die Einbeziehung kryptografischer Verfahren in die Zertifizierung verweigern, insbesondere wenn ein öffentliches Interesse vorliegt oder Fragen der nationalen Sicherheit betroffen sind.

Nach Antragseingang erhält der Antragsteller eine Eingangsbestätigung. Der Antrag und die zugehörigen Anlagen werden inhaltlich geprüft. Dann entscheidet das BSI, ob der Antrag angenommen wird, ob die Prüfbegleitung an CertLab ausgelagert wird und ob der Evaluierungsprozess bei der Prüfstelle begonnen werden kann. Ein gemeinsames Kick-off Meeting dient der Abstimmung inhaltlicher und verfahrenstechnischer Fragen wie z. B. der Abstimmung einer gemeinsamen Zeitplanung für die Bearbeitung der jeweils verschiedenen Prüfaspekte. Mit Annahme des Antrags wird eine eindeutige Zertifizierungskennung vergeben.

Die Prüfstelle stellt der Zertifizierungsstelle die Ergebnisse zu den einzelnen Prüfaspekten entsprechend der abgestimmten Planung in Prüfberichten zur Verfügung. Die Zertifizierungsstelle begutachtet die Prüfberichte und macht inhaltliche Stichproben unter Einbeziehung der Herstellernachweise. Ggf. werden Nachforderungen oder offene Fragen an die Prüfstelle kommuniziert. Bei größeren Problemen erfolgen in der Regel Evaluierungsbesprechungen.

Vor Beginn der Testdurchführung und Schwachstellenanalyse (Prüfklasse AVA nach CC) werden die detaillierten Evaluierungsanforderungen und Konzepte zu diesem Prüfkomplex in einer Besprechung abgestimmt (AVA-Kick-off Meeting).

Im Verfahren erforderliche Audits der Entwicklungs- und Produktionsumgebung beim Hersteller werden in der Regel von der Zertifizierungsstelle vor Ort begleitet. Diese Audits sind z. B. in der Prüfklasse ALC nach CC Version 3.1 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.

Eine Reise zum Hersteller kann jedoch auch im Rahmen der Tests, falls einige der Testaktivitäten direkt beim Hersteller durchgeführt werden müssen, notwendig sein.

Nach Bearbeitung der verschiedenen Prüfaspekte durch die Prüfstelle und Begutachtung durch die Zertifizierungsstelle oder ggf. durch CertLab erfolgt die Bereitstellung und Abnahme des Abschlussberichtes der Prüfstelle (Evaluation Technical Report (ETR)). Die Abnahme erfolgt schriftlich durch das BSI.

Nun erfolgt die Erstellung des Zertifizierungsreportes und der Abschluss des Verfahrens mit Erteilung des Zertifikates durch das BSI.

Nach Ablauf der Widerspruchsfrist gemäß Verwaltungsverfahrensgesetz ist der Zertifizierungsbescheid bestandskräftig und es erfolgt die Veröffentlichung, Abrechnung und Archivierung.

5.2 Erstmalige Bestätigung eines Produktes nach SigG

Der Prozess erfolgt so wie bei der Produktzertifizierung. Zusätzlich wird vor Annahme des Bestätigungsantrages geprüft, ob das Produkt die Anforderungen des Signaturgesetzes grundsätzlich erfüllt und in den Sicherheitsvorgaben bzw. in der geforderten Anlage die relevanten Anforderungen in Bezug auf das Signaturgesetz enthalten sind. Die Prüfstelle muss diese Anforderungen in die Evaluierung einbeziehen und die Ergebnisse in den Prüfberichten dokumentieren.

Mit der Abnahme des ETR erfolgt zusätzlich die abschließende Prüfung, ob die Evaluierung bestätigen konnte, dass die in den Sicherheitsvorgaben dargelegten Gesetzesanforderungen erfüllt sind. Anstelle des Zertifizierungsreportes wird ein Bestätigungsreport entsprechend der Anforderungen der Bundesnetzagentur erstellt. Die Bestätigung wird erteilt und das Verfahren wie bei einer Zertifizierung abgeschlossen. Die Bundesnetzagentur wird durch das BSI über die erteilte Bestätigung unterrichtet.

5.3 Aufrechterhaltung der Vertrauenswürdigkeit eines Produktes

Da ein Zertifikat und eine Bestätigung nach SigG für eine bestimmte evaluierte Version eines Produktes gilt, ist bei Änderung am Produkt oder den Entwicklungs-/ggf. Produktionsprozessen eine Erneuerung des Zertifikates bzw. der Bestätigung unter Berücksichtigung der jeweiligen Änderungen und unter Berücksichtigung der aktuellen Angriffstechniken erforderlich.

- Bei sicherheitsrelevanten Änderungen am Produkt oder den Entwicklung-/ggf. Produktionsprozessen oder bei umfangreichen Änderungen, ist eine Re-Zertifizierung bzw. Re-Bestätigung erforderlich (sogenannter „major change“).
- Bei sicherheitsirrelevanten Änderungen und überschaubarem Umfang der Änderungen am Produkt oder den Entwicklungs-/ggf. Produktionsprozessen kann ein bestehendes Zertifikat bzw. eine Bestätigung auf die neue Produktversion oder die geänderten Prozessbedingungen erweitert werden (Maintenance / Nachtragsbestätigung mit sogenanntem „minor change“).

Der Antragsteller beschreibt die Änderungen in einem Impact Analyse Report (IAR), der dem Zertifizierungs-/Bestätigungsantrag beizufügen ist. Die Entscheidung über die erforderliche Wahl des Prozesses liegt bei der Zertifizierungsstelle nach Prüfung des IAR. 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.

Ein in der Gültigkeit zeitlich befristetes Zertifikat kann in Rahmen einer Re-Zertifizierung / Re-Bestätigung erneuert werden.

5.3.1 Re-Zertifizierung / Re-Bestätigung

Die o. g. Aspekte für eine Erstzertifizierung in Bezug auf den grundsätzlichen Ablauf des Verfahrens, die Evaluierung durch die Prüfstelle und die Begleitung durch die Zertifizierungsstelle gelten auch für eine Re-Zertifizierung/Re-Bestätigung. Allerdings kann die Betrachtung auf die am Produkt vorgenommenen Änderungen konzentriert werden. Bei einer Re-Zertifizierung/Re-Bestätigung wird auf Basis der Änderungen am Produkt und den Herstellernachweisen (IAR) zwischen Zertifizierungsstelle und Prüfstelle im Rahmen der Verfahrensplanung festgelegt, welchen Umfang die Re-Evaluierung hat, welche Prüfschritte erneut durchgeführt werden müssen bzw. welche früheren Prüfergebnisse wiederverwendbar sind und damit zu welchen Prüfschritten aktualisierte Prüfberichte vorzulegen sind.

Die Angriffsresistenz 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.

Auch Audits der Entwicklungs- und Produktionsumgebung werden, falls sie älter als als zwei Jahre sind, erneut durchgeführt.

Nach positivem Abschluss der Re-Evaluierung werden die technischen Ergebnisse durch die Zertifizierungsstelle in einem aktualisierten Zertifizierungsreport bzw. Bestätigungsreport dokumentiert und ein neues Zertifikat bzw. eine neue Bestätigung erteilt.

5.3.2 Maintenance / Nachtragsbestätigung

Bei einem Maintenanceprozess bzw. einer Nachtragsbestätigung wird auf Basis der Beschreibung der Änderungen am Produkt (IAR) und den aktualisierten Herstellernachweisen die Aufrechterhaltung der Vertrauenswürdigkeit des Produktes direkt durch die Zertifizierungsstelle begutachtet, sofern die vorangegangene Zertifizierung nicht länger als zwei Jahre zurückliegt.

Dieser Prozess gilt nur für sogenannte "Minor Changes" am Produkt, die keine Sicherheitsrelevanz haben oder wo die Auswirkung auf die Sicherheit minimal und überschaubar ist und für Änderungen in der Entwicklungs- oder Produktionsumgebung zum Produkt (Prüfaspekt ALC Assurance Life-Cycle), bei denen die zu beauftragende Prüfstelle eine in diesem Bereich partielle Re-Evaluierung vornimmt.

Die Angriffsresistenz des Produktes (Prüfaspekt AVA) wird jedoch nicht nach dem jeweils aktuellen Stand der Technik neu bewertet, sondern es gilt die Angriffsresistenz zum Zeitpunkt der erfolgten letzten Erst- oder Re-Zertifizierung oder der letzten Neubewertung. Das jeweilige Ergebnis zu einem Maintenanceverfahren bzw. zu einer Nachtragsbestätigung 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 Kataloge der Bundesnetzagentur) sich geändert haben.

Bei einer Nachtragsbestätigung wird die Erfüllung der Anforderungen aus dem Signaturgesetz SigG bezogen auf die Änderungen am Produkt geprüft.

Bei positiver Entscheidung wird das Ergebnis durch die Zertifizierungsstelle in einem Maintenancereport als Ergänzung zum bestehenden Zertifizierungsreport dokumentiert, bei einer Nachtragsbestätigung entsprechend in einem Nachtrag zum Bestätigungsreport.

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

5.3.3 Partielle ALC Re-Evaluierung

Beziehen sich die Änderungen lediglich auf die zum Prüfaspekt ALC (Lifecycle Support) relevanten Aspekte, so kann eine partielle ALC Re-Evaluierung wie im CC Supporting Document [CC-AC] unter dem Begriff Subset-Evaluation beschrieben, durchgeführt werden. Dabei wird die Klasse ALC durch die Prüfstelle re-evaluiert. In diesem Fall konzentriert sich die Re-Evaluierung auf die ALC Klasse. 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 Re-Zertifizierung 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 Maintenancereport abgeschlossen und nicht mit einem neuen Zertifikat.

5.3.4 Neubewertung (Re-Assessment)

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, die die letzte Evaluierung durchgeführt hat, unterzogen. Ausgangspunkt ist die letzte durchgeführte Zertifizierung, Re-Zertifizierung oder das letzte Re-Assessment einschließlich aller erfolgten Maintenanceverfahren.

Der Umfang der Arbeiten wird zwischen Prüfstelle und Zertifizierungsstelle abgestimmt. Die Arbeiten sind konzentriert auf den Prüfaspekt Schwachstellenanalyse (AVA). Eine Aktualisierung des Dokumentes zur Unterstützung von Kompositionsverfahren (ETR for Composite Evaluation) ist ggf. ebenfalls zu erstellen (siehe auch Kap. 5.5). 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. Die Dokumente ETR for Composition der Plattform dürfen zum Zeitpunkt der Abnahme der Prüfergebnisse durch die Zertifizierungsstelle 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. Liegen die relevanten Audits länger als zwei Jahre zurück oder haben sich Änderungen ergeben, so werden diese Prüfaspekte ebenfalls aktualisiert (ALC).

Zur Abstimmung der notwendigen Arbeiten wird zu Beginn ggf. ein AVA-Kickoff Meeting durchgeführt. Der Antragsteller muss alle Herstellernachweise aus der vorangegangenen Zertifizierung und aus ggf. nachträglich durchgeführten Maintenanceverfahren sowie das Produkt in allen zurvor 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. ALC (Aktualisierung der Audits), ggf. ETR for Composition, ETR) der Zertifizierungsstelle zur Verfügung. Nach Abnahme der Berichte und positivem Ergebnis wird das bestehende Zertifikat durch die Zertifizierungsstelle mit aktuellem Datum bestätigt, andernfalls wird dem Antragsteller die aktuelle (ggf. niedrigere) Angriffsresistenz mitgeteilt. In letzterem Fall behält sich die Zertifizierungsstelle vor, ein Zertifikat zurückzuziehen.

5.4 Verwendung eines Schutzprofiles bei der Produktzertifizierung

Bei Erstellung des Dokumentes Sicherheitsvorgaben (Security Target, ST) muss grundsätzlich ein vom BSI zertifiziertes oder als geeignet anerkanntes Schutzprofil angewendet werden (siehe Kap. 1.3). Damit wird die Vergleichbarkeit von verschiedenen Produktzertifikaten für einen Produkttyp, z. B. im Rahmen von Ausschreibungen, 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

produktspezifischen 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 CC-Anerkennungsabkommens CCRA zur Verfügung. Die Konformität eines zertifizierten Schutzprofils mit den CC wird im Rahmen des CCRA anerkannt. Die inhaltliche Eignung eines Schutzprofils, das nicht vom BSI zertifiziert wurde, und das zur Durchführung einer Produktzertifizierung beim BSI verwendet werden soll, wird im Einzelfall geprüft.

Entsprechend der Konzepte der CC wird in einem Schutzprofil unterschieden, ob eine Sicherheitsvorgabe „strict" konform oder „demonstrable" konform zum Schutzprofil sein muss. „Strict" konform erfordert die Übernahme aller Sicherheitsanforderungen des Schutzprofils in die Sicherheitsvorgaben, ggf. ergänzt um zusätzliche Anforderungen. „Demonstrable" konform lässt dem Autor der Sicherheitsvorgaben mehr Freiheiten, wie die Anforderungen aus dem Schutzprofil zu übernehmen sind.

Details zur Erstellung von Sicherheitsvorgaben sind in dem Dokument AIS 41 „Guidelines for PPs and STs" [AIS 41] erläutert, das auf der Internetseite des BSI zur Verfügung steht.

5.5 Unterstützung von aufbauenden Folgeverfahren (Komposition)

Bei Produkten aus der Klasse „Smartcard 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 Evaluierung erstellt und von der Zertifizierungsstelle in die Abnahme der Evaluierung einbezogen.

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

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

5.6 Wiederverwendung von Prüfergebnissen bei Produktevaluierungen (Re-use)

a) 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. I. d. R. findet dieses Verfahren bei Wechsel der Prüfstelle zum Schutz des Know-hows der Prüfstelle des Basisverfahrens keine Anwendung, sondern nur wenn Basisverfahren und Folgeverfahren von derselben Prüfstelle durchgeführt werden. Typische Anwendung ist die Re-Evaluierung/Zertifizierung einer aktualisierten Version eines Produktes oder die Evaluierung/Zertifizierung ähnlicher Produkte eines Herstellers.

b) 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. Die Wiederverwendung von Ergebnissen eines Standortaudits, das in einem anderen Zertifizierungsschema unter SOGIS-MRA oder CCRA von einer dort lizenzierten fachlich geeigneten Prüfstelle durchgeführt wurde, ist grundsätzlich möglich, wenn das Protokoll des Audits vorliegt und die Prüfstelle mit diesen Informationen eine vollständige Evaluierung nachweisen kann.

Bei Standorten, die Hersteller übergreifend verwendet werden, ist der Prozess der Standortzertifizierung maßgeblich.

Weitere Erläuterungen finden sich in [AIS 38].

c) bei einer Neubewertung (Re-Assessment) der Angriffsresistenz eines zertifizierten Produktes wird im Einzelfall geprüft, welche Evaluierungsschritte zur Schwachstellenanalyse und Penetrationstests wiederverwendet werden können. Dies hängt von der Fortentwicklung der spezifischen Angriffsmöglichkeiten seit der vorhergehenden Bewertung des Produktes im Rahmen einer Erst- oder Rezertifizierung oder einer früheren Neubewertung ab.

d) 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.

5.7 Standortzertifizierung nach Common Criteria

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 Standort-Sicherheitsvorgaben (Site-Security-Target) erforderlich. Darin werden Umfang und Tiefe der geplanten Zertifizierung nach den Anforderungen der Prüfkriterien [CC] und [SupDoc-SC] sowie der zugehörigen AIS 47 dargelegt.

Das BSI entscheidet aus technischer Sicht über die grundsätzliche Zertifizierbarkeit des Standortes vorbehaltlich des positiven Abschlusses der Evaluierung und unter Berücksichtigung der Sicherheitsvorgaben und der rechtlichen Rahmenbedingungen.

Der Antragsteller entscheidet über Auswahl der Prüfstelle. Die Prüfstelle muss die für die Evaluierung notwendige Anerkennung durch das BSI haben.

Der positive Abschluss einer Zertifizierung erfordert, dass der Antragsteller alle nach den Prüfkriterien und ggf. nach besonderen Anforderungen des BSI erforderlichen Nachweise der Prüfstelle und dem BSI zur Verfügung stellt.

Wenn technische Gründe gegen eine Zertifizierung sprechen, kann das BSI den Zertifizierungsprozess stoppen oder ablehnen.

Nach positivem Abschluss der Evaluierung werden die technischen Ergebnisse durch die Zertifizierungsstelle in einem Zertifizierungsreport dokumentiert.

Bei Änderungen am Standort kann eine Re-Zertifizierung oder ein Maintenanceprozess analog wie bei Produktverfahren (siehe Kap. 5.3) durchgeführt werden.

6 Sicherheitskriterien und Interpretationen

Als Prüf- und Bewertungsgrundlage wurden im Laufe der Jahre mehrere Kriterienwerke entwickelt. Das aktuelle und zur Anwendung kommende Kriterienwerk sind die „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ / „Common Criteria for Information Technology Security Evaluation (CC)“ [CC]. Historisch sind die CC durch Weiterentwicklung und Harmonisierung aus früheren nationalen oder europäischen Kriterien hervorgegangen (ITSEC [ITSEC], Orange Book, Federal Criteria der USA, damalige kanadische Kriterien). Für die konsistente Anwendung der CC wurde das Evaluationshandbuch „Common Evaluation Methodology (CEM)“ [CEM] erstellt und international abgestimmt. Als einführende Übersicht zu den Common Criteria empfiehlt sich der Teil 1 der CC [CC], der das Konzept der Sicherheitskriterien erläutert. Ergänzende Informationen finden sich auf der Internetseite des BSI.

Auf der Internetseite des CC-Anerkennungsabkommens CCRA (http://www.commoncriteriaportal.org) sind aktuelle Informationen zu den CC zu finden. Die aktuell gültige, sowie auch frühere Versionen der Kriterien, stehen dort zum Download bereit.

Die europäischen Kriterien ITSEC [ITSEC] können im BSI Zertifizierungsschema nur noch in besonderen Ausnahmefällen angewendet werden, z. B. wenn Altverträge zwischen einem Bedarfsträger und einem Hersteller bestehen oder Gesetze und Verordnungen dies ausschließlich erfordern.

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 sowie verschiedene verfahrensbezogene Regelungen.

Die AIS-Dokumente schließen die international abgestimmten Dokumente zur Anwendung der Kriterienwerke wie z. B. die Dokumente der Joint Interpretation Working Group (JIWG Supporting Documents aus dem SOGIS-Anerkennungsabkommen)[21] und die sogenannten CC Supporting Documents aus dem internationalen Anerkennungsabkommen CCRA[22] ein.

Im BSI Zertifizierungsschema ist im Dokument [AIS 32] geregelt, welche Versionen der Prüfkriterien zur Anwendung kommen können sowie etwaige Übergangsregeln und -fristen. Zusätzlich listet AIS 32 abgestimmte und gültige Änderungen an den Kriterien auf, die noch nicht in ein neues Release oder eine neue Version der Kriterien eingeflossen sind.

Die genannten Dokumente können von der Webseite des BSI unter https://www.bsi.bund.de/zertifizierung in der Rubrik „Zertifizierung und Anerkennung“ abgerufen werden. Sie sind in den jeweiligen Evaluierungs- und Zertifizierungsverfahren entsprechend ihrer Einstufung (z. B. als Leitfaden oder verbindlich) anzuwenden.

Resultierend aus dem Zertifizierungsvorbehalt bei öffentlichem Interesse nach BSIG § 9, Abs. 4 (2) werden besondere Anforderungen an die Auswahl kryptografischer Algorithmen und Funktionen und an die diesbezügliche Evaluierungsmethodik gestellt. Die geltenden Rahmenbedingungen sind in spezifischen Verfahrensvorgaben, in AIS 46 oder in Technischen Richtlinien des BSI verankert und werden zu Beginn eines Zertifizierungs/Bestätigungsverfahrens besprochen.

Für die Auswahl von kryptografischen Algorithmen gilt für bestimmte Anwendungen der Katalog der Bundesnetzagentur, die Technische Richtlinie BSI TR-03116 [TR-03116] oder die Technische Richtlinie BSI TR-02102 [TR-02102]. Bei Verwendung schwächerer oder proprietärer Algorithmen erfolgt eine Entscheidung durch das BSI im Einzelfall, ggf. unter Auflagen, ob der jeweilige Algorithmus im Rahmen der Zertifizierung akzeptiert werden kann. Bei Verwendung proprietärer Algorithmen ist mit erhöhtem Zeitaufwand für die Evaluierung und Abnahme durch das BSI zu rechnen.

Für Bestätigungsverfahren nach SigG sind die o. g. Anforderungen des Signaturgesetzes und der Signaturverordnung sowie ggf. ergänzende Umsetzungsrichtlinien der Bundesnetzagentur zu berücksichtigen (siehe http://www.bundesnetzagentur.de, Rubrik „Qualifizierte elektronische Signatur“).

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. Diese sind dann für das laufende Verfahren maßgeblich und werden bei Abschluss des Verfahrens im Zertifizierungsreport referenziert. Ein Übergang auf neuere Versionen ist in gegenseitiger Abstimmung während des laufenden Verfahrens möglich. Dies kann ggf. mit Mehraufwänden bei Antragsteller oder Evaluator verbunden sein. Dieses Verfahren gilt nicht für AIS, die sich auf Angriffstechniken beziehen. Für diesen Bereich der Evaluierung sind jeweils die aktuellsten Prüfvorgaben zu berücksichtigen und die Zertifizierungsstelle entscheidet hierzu im Einzelfall über die Anwendung der relevanten Interpretationen.

---

21 Die JIWG Supporting Documents bzw. Dokumente der Joint Interpretation Library (JIL) werden von den im europäischen Anerkennungsabkommen (SOGIS-MRA) anerkannten Zertifizierungsstellen erarbeitet und über die nationalen Zertifizierungsstellen sowie die Internetseite http://www.sogisportal.eu veröffentlicht.

22 Die CC Supporting Documents des CCRA werden von den Arbeitsgremien des Abkommens erstellt und über die nationalen Zertifizierungsstellen sowie die Internetseite http://www.commoncriteriaportal.org veröffentlicht.

7 Gültigkeit des Zertifikates und der Bestätigung

7.1 Gültigkeit und ihre Randbedingungen

Ein Produktzertifikat und eine Bestätigung nach SigG beziehen 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 Umgebung betrieben wird, die im Zertifizierungsreport bzw. Bestätigungsreport und in den Sicherheitsvorgaben beschrieben ist.

Ein Zertifikat bzw. eine Bestätigung nach SigG bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da Angriffe mit neuen oder weiterentwickelten 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 Re-Zertifizierung oder Neubewertung). 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 bzw. einer Bestätigung nach SigG auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller die Aufrechterhaltung der Vertrauenswürdigkeit (d. h. eine Re-Zertifizierung / Maintenance Verfahren bzw. eine Re-Bestätigung / Nachtragsbestätigung) in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen aufdeckt.

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

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

Auflagen für den Zertifikatsinhaber ergeben sich aus dem Zertifizierungsbescheid / Bestätigungsbescheid.

Der Anwender eines zertifizierten oder bestätigten Produktes muss die mit dem Zertifikat / der Bestätigung 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 / der Bestätigung über das Assurance Continuity-Programm des BSI verlangen.

Die Verpflichtung zur Archivierung der Herstellernachweise, des zertifizierten / bestätigten Produkts und der Evaluierungsnachweise ist i. d. R. auf fünf Jahre nach Ausstellung eines Zertifikates / einer Bestätigung begrenzt. Nach Ablauf dieser Zeit ist eine Überprüfung eines Zertifikates dann nicht mehr möglich.

7.2 Befristung

Die Zertifizierungsstelle kann die formale Gültigkeit eines Zertifikates zeitlich befristen. Produktzertifikate sind i. d. R. aber nicht mit einer Gültigkeitsfrist ausgestellt, da die Zertifikatsaussage zur Vertrauenswürdigkeit des Produktes sich auf den Zeitpunkt der Ausstellung bezieht und eine Abschätzung der Angriffsresistenz in die Zukunft schwierig zu bewerten ist und individuell sehr unterschiedlich sein kann.

Die Gültigkeit eines Zertifikates kann jedoch begrenzt sein durch die Gültigkeit der Laufzeit verwendeter kryptografischer Algorithmen oder Parameter abhängig vom Einsatzbereich des Produktes. Dies ist im Zertifizierungsreport vermerkt.

Die Gültigkeit eines Standortzertifikates ist zeitlich auf zwei Jahre begrenzt.

Die Gültigkeit einer Bestätigung nach SigG ist aufgrund der Festlegung durch die Bundesnetzagentur zeitlich begrenzt. Zusätzliche oder spezifische Randbedingungen der Bundesnetzagentur wie z. B. besondere Laufzeiten kryptografischer Algorithmen oder Parameter im Kontext von SigG sind zu berücksichtigen.

7.3 Widerruf

Zertifikate oder Bestätigungen nach SigG können unter Berücksichtigung der Regelungen des Verwaltungsverfahrensgesetzes in bestimmten Fällen zurückgezogen werden, in dem der Bescheid widerrufen wird, z. B. wenn sich herausstellt, dass die Grundlage für die Erteilung nicht gegeben war oder Nebenbestimmungen (Auflagen) aus dem Bescheid nachweislich nicht erfüllt werden, z. B. Verstoß gegen die Archivierungspflicht, unsachgemäße Werbung mit dem Zertifikat oder Verweigerung der Bereitstellung der gemäß Zertifizierungsreport für die Benutzung des Produktes erforderlichen Unterlagen, Verlust der Vertraulichkeit von Design- oder Evaluierungsunterlagen; Missachtung der Informationspflicht hinsichtlich bekannt gewordener Schwachstellen.

8 Glossar

Im folgenden sind wichtige in dieser Druckschrift verwendete Begriffe aufgelistet und erläutert. Die Erläuterungen gelten im Kontext der BSI-Zertifizierung und Bestätigung nach SigG und erheben keinen Anspruch auf Allgemeingültigkeit und Vollständigkeit. Quellenangaben ([...]) sind im Kapitel 'Quellen' aufgeführt.

AIS	Anwendungshinweise und Interpretationen zum Schema
Anerkennung von Prüfstellen	Allgemein: Bestätigung, dass eine Prüfstelle die an sie gestellten Anforderungen zur Durchführung von Zertifizierungen im Rahmen von Qualitätsmanagementverfahren, Konformitätsbewertungen etc. erfüllt. Speziell: Eine Anerkennung beim BSI als Prüfstelle kann dann erfolgen, wenn nachweislich die Anforderungen der DIN EN ISO/IEC 17025 und ein Qualifikationsnachweis Durchführung von Evaluierungen für ein bestimmtes Fachgebiet (z. B. Common Criteria) erfüllt werden. Eine Anerkennung kann auch bestimmte Spezialgebiete wie z. B. den Bereich „Smart Card and Similar Devices“ betreffen.
Antragsteller (engl. Applicant)	die (natürliche oder juristische) Person, die eine Zertifizierung beim BSI beantragt
Auswirkungsanalyse (Impact Analysis Report, IAR)	Bei beabsichtigter Wiederverwendung von Evaluierungsergebnissen aus früheren Verfahren wird in der Auswirkungsanalyse erläutert, welche Änderungen am Produkt durchgeführt wurden, welche Sicherheitsrelevanz diese Änderungen haben und welche Evaluierungsergebnisse wiederverwendet werden sollen.
BSIG	Gesetz, das die Aufgaben des BSI regelt [BSIG]
CC	Kurzbezeichnung für die Common Criteria for Information Technology Security Evaluation [CC]: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik; ISO/IEC15408
CEM	Kurzbezeichnung der Common Methodology for Information Technology Security Evaluation [CEM]
DIN EN ISO/IEC 17065	Norm, die die Standards für Zertifizierungsstellen enthält
EAL	Kurzbezeichnung für Evaluation Assurance Level (siehe Vertrauenswürdigkeitsstufe)
Einzelprüfberichte	Bericht einer Prüfstelle zu Teilen von in den Kriterienwerken festgelegten Prüfaspekten eines Evaluierungsgegenstandes (EVG) entsprechend der Regelungen im Zertifizierungsschema
entwicklungsbegleitende Evaluierung	Evaluierung, die parallel zur Entwicklung eines EVG (und mit der Entwicklung verzahnt) durchgeführt wird
entwicklungsbegleitende Zertifizierung	Zertifizierungsverfahren mit entwicklungsbegleitender Evaluierung
Erst-Zertifizierung	Erstmalige Durchführung einer Zertifizierung z. B. für ein IT-Produkt (siehe Re-Zertifizierung)
Evaluierung	Prüfung und Bewertung eines EVG gemäß den Anforderungen eines

	Kriterienwerkes
Evaluierungsbericht Evaluation Technical Report	Von einer Prüfstelle vorgelegter abschließender Bericht über den Verlauf und die Ergebnisse der Evaluierung eines EVG. Der Evaluierungsbericht (ETR) enthält die Einzelprüfberichte zu allen Prüfaspekten, die in einem Verfahren relevant sind.
Evaluierungsplan	Projekt- und Terminplan für die Durchführung der Evaluierung. Der Plan enthält u. a. Angaben zur inhaltlichen Planung, zu beteiligten Personen sowie zur Zeitplanung.
Evaluierungsvertrag	Vertrag zwischen Antragsteller einer Zertifizierung und einer anerkannten Prüfstelle über die durchzuführende Evaluierung
EVG (engl. TOE)	Evaluationsgegenstand (engl. Target of Evaluation)
Firmenvertraulich (engl.: company confidential)	Als firmenvertraulich werden vertrauliche Verfahrensdokumente gekennzeichnet, wie z. B. Herstellerdokumente, Prüfberichte und Review-Protokolle. Die am Zertifizierungsverfahren beteiligten Stellen haben durch geeignete Maßnahmen sicherzustellen, dass firmenvertrauliche Dokumente vor unbefugter Kenntnisnahme geschützt sind.
ISO/IEC 17025	Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien.
IT-Komponente	Begriff aus dem BSIG: Die Begriffe IT-Komponente und IT-Produkt werden synonym gebraucht.
IT-Produkt	Zusammenfassender Begriff für Objekte, für die gemäß BSIG eine Zertifizierung durchgeführt werden kann (Ausprägung kann durch die technischen Regelwerke eingeschränkt sein, i. d. R. jede Kombination von Hardware und / oder Software).
IT-Sicherheitszertifikat (engl.: IT-Security Certificate)	siehe Zertifikat
IT-System	Eine spezifische IT-Installation mit einem bestimmten Zweck und einer spezifischen Einsatzumgebung.
ITSEC	Kurzbezeichnung für die europäischen 'Information Technology Security Evaluation Criteria' [ITSEC]: Kriterienwerk zur Bewertung der Sicherheitseigenschaften von IT-Produkten und IT-Systemen.
ITSEM	Kurzbezeichnung für das europäische 'Information Technology Security Evaluation Manual' [ITSEM]: Evaluationshandbuch zu ITSEC.
Kostenbescheid	Gemäß [BSIKostV] werden dem Antragsteller die dem BSI entstandenen Aufwände mit einem Kostenbescheid in Rechnung gestellt.
Kriterienwerk	Sammelbezeichnung für Sicherheitskriterien, Evaluationskriterien, Sicherheitsstandards und -normen, o. ä.: Regelwerke mit (technischen) Anforderungen an einen EVG und / oder Vorgaben für die Durchführung der Evaluierung des EVG und Bewertung der Ergebnisse, (hier: vom BSI öffentlich bekannt gemacht oder allgemein anerkannt)
Maintenance	Vereinfachtes Verfahren zur Erweiterung der Gültigkeit eines Zertifikats auf neue Produktversionen bei Änderungen ohne Sicherheitsrelevanz (wird auch „assurance continuity with minor change“ genannt).
Need-To-Know	("Kenntnis nur wenn nötig") Prinzip zur Wahrung der Vertraulichkeit von Informationen: Nur solche Personen erhalten Kenntnis, für die eine Berechtigung und eine dringende Notwendigkeit bestehen.
Neubewertung (engl.: Re-Assessment	Aktualisierung der Bewertung der Angriffsresistenz der zertifizierten Version eines Produktes im Kontext der jeweiligen Sicherheitsvorgaben nach aktuellem Stand der Technik sowie Aktualisierung der Standortsicherheit relevanter Entwicklungs- und Produktionsstandorte.

Ortsbesichtigung	Auditierung der Entwicklungsumgebung des Herstellers. Im Rahmen der Ortsbesichtigung wird überprüft, ob die dokumentierten Verfahren zur Konfigurationskontrolle und zur Sicherheit in der Entwicklungsumgebung angewendet werden.
Protection Profile (PP)	Eine implementierungsunabhängige Menge von Sicherheitsanforderungen, die eine identifizierbare Teilmenge von Sicherheitszielen abdeckt.
Prüfbegleiter	Mitarbeiter der Zertifizierungsstelle des BSI oder CertLab, die die Prüfbegleitung in einem Zertifizierungsverfahren durchführen und i. d. R. auch den Zertifizierungsreport verfassen.
Prüfbegleitung	Die Zertifizierungsstelle oder CertLab begleiten jede Evaluierung, die mit dem Ziel einer BSI-Zertifizierung durchgeführt wird, um einheitliche Vorgehensweise und Methodik und vergleichbare Bewertungen sicherzustellen.
Prüfstelle	(staatliche oder privatwirtschaftliche) Institution, die Evaluierungen durchführt und deren Ergebnisse für die Erteilung von Zertifizierungsbescheiden anerkannt werden (hier: eine vom BSI anerkannte Prüfstelle oder eine solche, die aufgrund einer gesetzlichen Ermächtigung arbeitet).
Prüfstufe (engl. Assurance level)	Paket mit Anforderungen an das Dokumentieren und Prüfen (bei CC: Vertrauenswürdigkeitsstufe bzw./-paket).
Re-Zertifizierung	Erneute Zertifizierung auf der Basis einer schon erfolgten Zertifizierung z. B. nach Änderungen am Produkt, Änderung des Auslieferungsverfahrens etc.
Schutzprofil	dt. Übersetzung des Begriffs Protection Profile
Security Target	Engl. Bezeichnung für Sicherheitsvorgaben
Sicherheitskriterien	siehe Kriterienwerk
Sicherheitsvorgaben (engl.: security target, ST)	Teil der Dokumentation eines EVG. Sicherheitsvorgaben nach CC oder ITSEC beinhalten eine Spezifikation der von einem EVG geforderten Sicherheitsleistungen, die während einer Evaluierung verifiziert werden sollen. Sie spezifizieren u. a. die sicherheitsspezifischen Funktionen bzw. funktionalen Anforderungen, die Sicherheitsziele, die Bedrohungen dieser Ziele sowie die vorgesehene Einsatzumgebung.
Vertrauenswürdigkeitsstufe (engl.: assurance level)	Eine vordefinierte Menge von Vertrauenswürdigkeitskomponenten aus Teil 3 der CC, die einen bestimmten Punkt auf der in den CC definierten Skala zur Messung der Vertrauenswürdigkeit darstellt.
Vor-Evaluierung (engl.: pre-evaluation)	Optionales, nach Absprache zwischen dem Antragsteller, der Zertifizierungsstelle und der Prüfstelle vor der Evaluierung ablaufendes Verfahren zur Feststellung, ob und wie das Zertifizierungsziel erreicht werden kann bzw. welche Vorarbeiten noch zu leisten sind.
Zertifikat (engl.: certificate)	Im Zertifikat wird das Zertifizierungsergebnis in kurzer Zusammenfassung bestätigt. Das Zertifikat ist eine der Anlagen des Zertifizierungsbescheids.
Zertifizierung (engl.: certification)	Bezeichnung des Gesamtverfahrens, bestehend aus den folgenden Phasen: Antragstellung beim BSI, Evaluierung des EVG durch eine Prüfstelle mit Prüfbegleitung durch das BSI, abschließende Zertifizierung, Erteilung und Veröffentlichung des Zertifikates.
Zertifizierungs-ID (engl.: Certification ID)	Synonym des Begriffs Zertifizierungskennung.
Zertifizierungsantrag (engl.: application for a certificate)	Formeller Antrag, der die Grundlage zur Aufnahme eines Zertifizierungsverfahrens bildet.

Zertifizierungsbescheid (engl.: certification ordinance)	Verwaltungsbescheid, in dem dem Antragsteller das Zertifizierungsergebnis mitgeteilt wird. Anlagen des Zertifizierungsbescheids sind das Zertifikat, der Zertifizierungsreport und der gesondert zugestellte Kostenbescheid.
Zertifizierungskennung (engl.: Certification ID)	Ordnungsmerkmal der Zertifizierungsverfahren, das aus der Angabe des technischen Regelwerkes und einer laufenden Nummer besteht. Nach Erteilung des Zertifikats wird das Jahr der Erteilung des Zertifikats ergänzt. Synonym des Begriffs Zertifizierungs-ID.
Zertifizierungsreport (engl.: Certification Report)	Von der Zertifizierungsstelle erstellter Bericht über Gegenstand, Verlauf und Ergebnisse des Zertifizierungsverfahrens. Der Zertifizierungsreport wird (i. d. R. durch den Antragsteller) veröffentlicht.

9 Quellen

AIS	Anwendungshinweise und Informationen zum Schema; Web-Site des BSI https://www.bsi.bund.de/zertifizierung
AIS 1	Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
AIS 14	Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
AIS 19	Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
AIS 23	Zusammentragen von Nachweisen der Entwickler
AIS 27	Transition from ITSEC to CC
AIS 32	CC-Interpretationen im deutschen Zertifizierungsschema
AIS 35	Öffentliche Fassung eines Security Target (ST-lite)
AIS 36	ETR-lite für zusammengesetzte EVGs (ETR-lite)
AIS 38	Wiederverwendung von Evaluationsergebnissen
AIS 41	Guidelines for PPs and STs
AIS 42	Hinweise zur Erstellung von Herstellerdokumenten für eine CC-Evaluierung mit Anlage: Guidelines for Developer Documentation according to Common Criteria Version 3.1
AIS 45	Erstellung und Pflege von Meilensteinplänen
AIS 46	Info zur Evaluierung von Krypto und RNG
AIS 47	Regelungen zu Site Certification
BSI 7148	Druckschrift "Deutsche IT-Sicherheitszertifikate" in der jeweils aktuellen Fassung
BSI 7125	Anforderungen an die Prüfstelle für die Evaluierung von Produkten, Schutzprofilen und Standorten nach CC
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, (BSI-Gesetz – BSIG), Bezugsquelle: Bundesgesetzblatt Jahrgang 2009 Teil I Nr. 54, 19. August 2009, https://www.bsi.bund.de/zertifizierung
BSIKostV	BSI-Kostenverordnung - Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik, aktuelle Fassung siehe Web-Site des BSI https://www.bsi.bund.de/zertifizierung
BSIZertV	Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung-BSIZertV) vom 7. Juli 1992, Bundesgesetzblatt I S. 1230
CC	Common Criteria for Information Technology Security Evaluation - Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von

	Informationstechnik, Aktuelle Fassung siehe http://www.commoncriteriaportal.org (September 2012: Version 3.1 Release 4)
CC-AC	Assurance Continuity, CCRA Requirements, Aktuelle Fassung siehe http://www.commoncriteriaportal.org
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, Mai 2000, siehe http://www.commoncriteriaportal.org
CEM	Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, – Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (CEM), Aktuelle Fassung siehe http://www.commoncriteriaportal.org (September 2012: Version 3.1 Release 4)
ITSEC	Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), vorläufige Form der harmonisierten Kriterien, Version 1.2, Juni 1991, hrsg. v. d. Europäischen Union, Bundesanzeiger-Verlag Köln (1991), ISBN 92-826-3003-X (englische Fassung:) Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonised Criteria, Version 1.2, June 1991, ISBN 92-826-3004-8
ITSEM	Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik, Vorläufige Form der harmonisierten Methodik, Version 1.0, September 1993, hrsg. v. d. Europäischen Union, Bundesanzeiger Verlag Köln, ISBN 92-826-7078-2 (englische Fassung:) Information Technology Security Evaluation Manual (ITSEM), Version 1.0, 1993
JIL	Joint Interpretation Library, Teil der AIS-Dokumente
Sig-AlgoKat	Übersicht über geeignete Algorithmen, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, aktuelle Fassung siehe http://www.bundesnetzagentur.de
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG): Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091), aktuelle Fassung siehe http://www.bundesnetzagentur.de
SigV	Verordnung zur elektronischen Signatur: "Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 17. Dezember 2009 (BGBl. I S. 3932), aktuelle Fassung siehe http://www.bundesnetzagentur.de
SOGIS-MRA	Mutual Recognition Agreement of Information Technology Security EvaluationCertificates, Version 3.0, Januar 2010, SOG-IS, siehe http://www.sogisportal.eu
SupDoc-SC	Supporting Document Site-Certifikation, CCDB-2007-11-001, siehe http://www.commoncriteriaportal.org
TR-03116	BSI TR-03116 „TR-03116 Kryptografische Vorgaben für Projekte der Bundesregierung“, aktuelle Fassung siehe https://www.bsi.bund.de/TR
TR-02102	BSI TR-02102 „Kryptografische Verfahren: Empfehlungen und Schlüssellängen“, aktuelle Fassung siehe https://www.bsi.bund.de/TR
VB-Produkte	Verfahrensbeschreibung zur Zertifizierung von Produkten, aktuelle Fassung siehe https://www.bsi.bund.de/zertifizierung

VB-Stellen	Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern, aktuelle Fassung siehe https://www.bsi.bund.de/zertifizierung