Bundesamt
für Sicherheit in der
Informationstechnik

Verfahrensbeschreibung zur Zertifizierung von Produkten

VB-Produkte

Version 2.2 vom 07.06.2018

Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	28.02.2014	QMB	Erstausgabe
2.0	20.07.2015	QMB	Neuausgabe aufgrund Dokumentenumstrukturierung und neuer [BSI-ZertV]
2.1	02.08.2016	QMB	Revision: • Austausch der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramme) • kleinere sprachliche Korrekturen.
2.1.1	10.01.2017	QMB	Revision: • Austausch der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramme)
2.2	07.05.2018	QMB	Revision: • Kapitel 2.1: Wegfall SigG.

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

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nach dem BSI-Gesetz [BSIG] die Aufgabe, Zertifizierungen informationstechnischer Produkte oder Komponenten sowie informationstechnischer Systeme durchzuführen.

Um diese Aufgaben zu erfüllen, betreibt das BSI Zertifizierungsprogramme, in denen jeweils die Regeln (Geltungsbereiche, bedarfsgerechte Prüfkriterien, Anforderungen und Nachweise), das Verfahren sowie das Management zur Durchführung der Zertifizierung festgelegt und beschrieben sind.

Die Zertifizierung eines Produktes wird auf Antrag durchgeführt. Voraussetzung für eine Zertifizierung ist eine technische Evaluierung bzw. Prüfung gemäß den im Zertifizierungsprogramm veröffentlichten Sicherheitskriterien bzw. Technischen Richtlinien.

Zur Unterstützung der Produktzertifizierung im Bereich der Common Criteria (CC) kann im Vorfeld eine Schutzprofil- oder Standortzertifizierung durchgeführt werden.

1.1 Zielsetzung und Eingliederung der VB-Produkte

Einen Überblick über die Zertifizierungsprogramme sowie der zugehörigen Dokumente gibt die folgende Abbildung. Diese Dokumente stellen Informationen zielgruppenorientiert zur Verfügung.

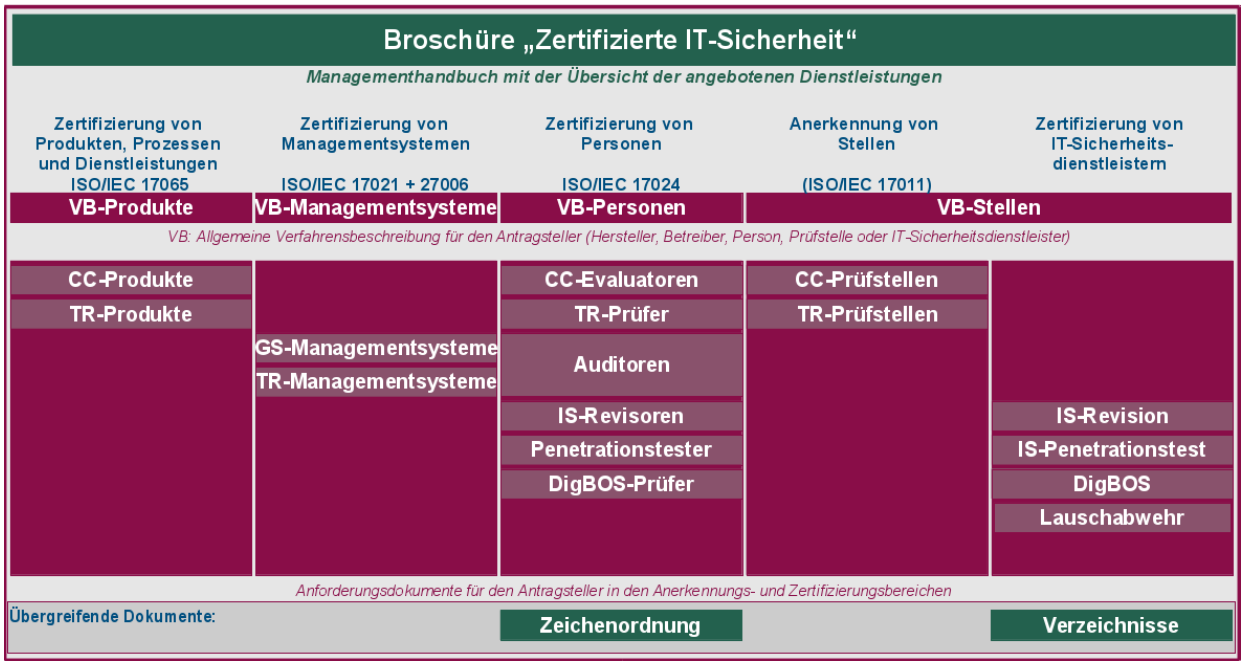

Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramme)

Die übergeordnete Broschüre „Zertifizierte IT-Sicherheit“ [Broschüre] richtet sich an Personen, die sich über den Auftrag des BSI im Bereich der Konformitätsbewertung im Allgemeinen informieren möchten.

In den „Verfahrensbeschreibungen“ (VB) des Zertifizierungs- und Anerkennungsprogramms werden der Nutzen für den Antragsteller, das Verfahren und die damit verbundenen Rechte und Pflichten sowie Obliegenheiten dargestellt. Sie sind Entscheidungshilfe, wenn die Absicht besteht einen Antrag zu stellen und richtet sich somit an:

- Hersteller, die ihre Produkte zertifizieren (vorliegende VB-Produkte),
- Betreiber, die ihre Systeme zertifizieren [VB-Managementsysteme],
- Personen, die sich zertifizieren [VB-Personen],
- Prüfstellen, die sich anerkennen [VB-Stellen] und
- IT-Sicherheitsdienstleister, die sich zertifizieren [VB-Stellen]

lassen wollen.

Spezielle Anforderungen für den jeweiligen Geltungsbereich mit detaillierten Hinweisen zu Verfahrensabläufen befinden sich in den jeweiligen „Anforderungsdokumenten“ und richten sich an den konkreten Antragsteller.

Die vorliegende VB-Produkte wird durch die Anforderungsdokumente

- Anforderungen für Antragsteller zur IT-Sicherheitszertifizierung von Produkten, Schutzprofilen und Standorten [CC-Produkte] und
- Anforderungen für Antragsteller zur Zertifizierung von Produkten nach Technischen Richtlinien [TR-Produkte]

ergänzt.

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

Das Dokument „Zeichenordnung“ [Zeichenordnung] enthält alle Zeichen der Konformitätsbewertung mit den jeweiligen Rechten und Bedingungen.

1.2 Nutzen der Zertifizierung für den Antragsteller

Ein Zertifikat als unabhängiger Konformitätsnachweis kann von einem Antragsteller im Rahmen seines Marketings als Qualifizierungsnachweis zur Erfüllung von Anforderungen seitens seiner Kunden oder bei Ausschreibungen eingesetzt werden. Es schafft Vertrauen für Verbraucher, Behörden, Industrie und andere interessierte Parteien, dass festgelegte Anforderungen an das Produkt erfüllt wurden. Darunter z. B. Produktleistung, Sicherheit, Interoperabilität und Nachhaltigkeit. Ziel der Produktzertifizierung ist ein erhöhter Marktwert durch die objektive Überprüfung des Produkts. In einigen Bereichen ist eine Produktzertifizierung durch Gesetz, Verordnung, Richtlinie oder Standard verbindlich vorgeschrieben.

Informationen zu zertifizierten Produkten werden vom BSI in regelmäßig aktualisierten Publikationen und elektronischen Medien veröffentlicht.

Eine IT-Sicherheitszertifizierung von Produkten wird in bestimmten Prüfgebieten und Prüfstufen im Rahmen internationaler Abkommen von zahlreichen Nationen anerkannt, so dass weitestgehend eine Mehrfachzertifizierung eines Produktes in verschiedenen Staaten vermieden werden kann. Das BSI hat dazu ein Abkommen zur Anerkennung von IT-Sicherheitszertifizierungen in Europa für CC- und ITSEC-Zertifizierungen [SOG-IS-MRA] und ein weltweites Abkommen [CCRA] zur Anerkennung von CC-Zertifizierungen unterzeichnet. Weitere Details zu diesen Abkommen finden sich im nachgelagerten Anforderungsdokument [CC-Produkte].

2 Zertifizierungsprogramm für Produkte

Die Zertifizierungsstelle des BSI betreibt ein Zertifizierungsprogramm, in dem die Regeln (Geltungsbereiche, bedarfsgerechte Prüfkriterien, Anforderungen und Nachweise), das Verfahren sowie das Management zur Durchführung der Zertifizierung festgelegt und beschrieben ist.

Das BSI ist für diese genannten Geltungsbereiche der Produktzertifizierung bei der DAkkS nach DIN EN ISO/IEC 17065:2013 akkreditierte Produktzertifizierungsstelle [D-ZE-19615-01-00].

Im Folgenden sind die Geltungsbereiche mit den zugehörigen Dokumenten aufgeführt.

2.1 Geltungsbereiche für die IT-Sicherheitszertifizierung

Folgende IT-Sicherheitszertifizierungen können beim BSI beantragt werden:

1. Zertifizierung eines Produktes, Standortes oder Schutzprofils nach den Common Criteria [CC], [1]
2. Zertifizierung eines Produktes nach den Information Technology Security Evaluation Criteria [ITSEC].

Die Verfahrensbeschreibung für diesen Geltungsbereich besteht aus der vorliegenden VB-Produkte und dem präzisierenden Anforderungsdokument [CC-Produkte].

Zur Unterstützung der Produktzertifizierung werden folgendes Verfahren angeboten:

- Standortzertifizierung nach Common Criteria (CC).
  Die Regelungen aus dieser Verfahrensbeschreibung gelten analog.

2.2 Geltungsbereiche für die Zertifizierung von Produkten nach Technischen Richtlinien

Beim BSI kann eine Zertifizierung eines Produktes nach einer im Anforderungsdokument [TR-Produkte] aufgeführten Technischen Richtlinie des BSI (BSI-TR) beantragt werden.

Die Verfahrensbeschreibung für diese Geltungsbereiche besteht aus der vorliegenden VB-Produkte und dem präzisierenden Anforderungsdokument [TR-Produkte].

1 Dies schließt die Zertifizierung von Produkten nach den Anforderungen bestimmter EU-Verordnungen (bspw. eIDAS und Digitaler Fahrtenschreiber) ein, wenn die in der Verordnung oder nachgelagerten Regularien genannten Schutzprofile verwendet werden.

3 Verfahren zur Zertifizierung

Ein Zertifikat wird erteilt, wenn die jeweiligen Prüfkriterien bzw. Technischen Richtlinien erfüllt sind und das Bundesministerium des Innern festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen (§ 9 Abs.4 BSIG) [BSIG].

3.1 Beteiligte Stellen an einer Produktzertifizierung

An einer Produktzertifizierung sind folgende Stellen beteiligt:

- der Antragsteller,
- die für den gewünschten Geltungsbereich anerkannte Prüfstelle,
- die Zertifizierungsstelle und ggf. eine externe vom BSI beauftragte Stelle für die Prüfbegleitung.

3.1.1 Der Antragsteller

Der Hersteller oder Vertreiber beauftragt eine vom BSI für den entsprechenden Geltungsbereich anerkannte Prüfstelle mit der Evaluierung und beantragt er beim BSI die Zertifizierung. Gemäß [BSI-ZertV] hat der Antragsteller Mitwirkungsobliegenheiten, z.B. die notwendige Mitwirkung Dritter sicherzustellen und bei Produktprüfungen das zu prüfende Produkt und die erforderlichen dokumentarischen Nachweise, die für den Geltungsbereich, das Prüfgebiet, Prüftiefe und Umfang durch das BSI festgesetzt sind, der Prüfstelle und der Zertifizierungsstelle bereitzustellen.

Bei der Erstellung und Dokumentation der für die Zertifizierung erforderlichen Nachweise kann der Antragsteller Beratungsleistungen, z. B. bei einer anerkannten Prüfstelle, beauftragen. Hierbei muss der Grundsatz der Unparteilichkeit und die Regelungen des Zertifizierungsschemata in dem jeweiligen Geltungsbereich, d. h. insbesondere die wirksame Trennung von Beratung und Evaluierung, berücksichtigt werden.

3.1.2 Die vom BSI anerkannte Prüfstelle

Die vom BSI anerkannte Prüfstelle nimmt als sachverständige Stelle die Prüfung und Bewertung (im Folgenden Evaluierung) des Produktes vor. Sie stellt die technische Korrektheit und die inhaltliche Vollständigkeit der Prüfergebnisse sicher und stellt der Zertifizierungsstelle die vollständigen Prüfergebnisse zur Verfügung.

Die Anerkennung von Prüfstellen ist in der Verfahrensbeschreibung zur Anerkennung von Stellen und Zertifizierung von IT-Sicherheitsdienstleistern [VB-Stellen] beschrieben. Die Anerkennungsstelle des BSI überwacht die Prüfstellen und veröffentlicht diese auf der Internetseite des BSI. Die Anerkennung einer Prüfstelle bezieht sich immer auf einen konkreten Anerkennungsbereich, z. B. ein Kriterienwerk (ITSEC oder CC oder ggf. Teile davon), ein spezifisches technisches Gebiet oder eine Technische Richtlinie.

3.1.3 Die Zertifizierungsstelle

Aufgabe der Zertifizierungsstelle 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 durch, um damit vergleichbare Bewertungen zu erhalten.

Das BSI kann eine externe Stelle zur Unterstützung bei der Prüfbegleitung beauftragen, die dann unter Kontrolle des BSI arbeitet. Die Abnahme des abschließenden Prüfberichtes und die Zertifizierung des Produktes erfolgt ausschließlich und in Verantwortung durch das BSI.

Die Zertifizierungsstelle erstellt die Zertifizierungsunterlagen bestehend aus Zertifizierungsbescheid und Zertifikat mit dem Zertifizierungsreport.

3.2 Vorbereitungsphase

Zur Vorbereitung auf die Beantragung einer Zertifizierung kann ein Informationsgespräch durchgeführt werden. Dies ist insbesondere für Antragsteller hilfreich, die zum ersten Mal ein Produkt beim BSI zertifizieren lassen.

Zwischen Antragsteller und Prüfstelle wird grundsätzlich ein Evaluierungsvertrag bzw. Vertrag zur Konformitätsprüfung abgeschlossen. Im Falle der Beantragung einer Zertifizierung nach Common Criteria erfolgt dies bereits vor Antragstellung in der Vorbereitungsphase.

Das BSI hat auf seiner Internetseite Antragsformulare bereitgestellt. Je nach Geltungsbereich sind mit dem Antrag bereits technische Anlagen einzureichen.

Der Antrag wird in der zeitlichen Reihenfolge des Eingangs bearbeitet. Hiervon kann abgewichen werden, wenn das BSI wegen der Zahl und des Umfangs anhängiger Prüfungsverfahren eine Prüfung in angemessener Zeit nicht durchführen kann und an der Erteilung eines Zertifikats ein öffentliches Interesse besteht.

Der Antragsteller erhält vom BSI eine Eingangsbestätigung, in der ihm die Zertifizierungskennung und die Prüfbegleiter seitens des BSI mitgeteilt werden.

3.3 Evaluierungs- bzw. Prüfphase

Der Antragsteller stellt den Evaluierungsgegenstand/Prüfgegenstand (z. B. das zu zertifizierende Produkt) und die jeweils erforderlichen Herstellernachweise zur Verfügung. Sofern weitere initiale Produktkenntnisse für die Evaluierung/Konformitätsprüfung notwendig sind, schult der Antragsteller zu Beginn Evaluatoren und Prüfbegleiter.

Die Prüfstelle führt die Evaluierung/Konformitätsprüfung durch, dokumentiert die Ergebnisse gemäß den Vorgaben für den Geltungsbereich und stellt der Zertifizierungsstelle die vollständigen Prüfergebnisse zur Verfügung. Im Rahmen der Prüfbegleitung durch die Zertifizierungsstelle werden die Prüfergebnisse begutachtet, offene Punkte adressiert und ggf. Ergänzungen nachgefordert.

Nachbesserungen am Produkt und an der Herstellerdokumentation sind während des Zertifizierungsverfahrens bis zum Ende dieser Evaluierungs- bzw. Prüfphase seitens des Antragstellers möglich.

Alle Beteiligten am Zertifizierungsverfahren teilen Abweichungen von der Verfahrensplanung den anderen Beteiligten mit und stimmen diese erneut ab.

3.4 Zertifizierungsphase

Auf Grundlage von Prüfberichten entscheidet das BSI gemäß den Regelungen § 9 Abs. 4 [BSIG] über die Zertifizierung.

Die Zertifizierungsstelle erstellt nach positiver Zertifizierungsentscheidung das Zertifikat, den Zertifizierungsreport, das Zertifizierungszeichen und den Zertifizierungsbescheid. Die Zertifizierung kann Nebenstimmungen (siehe Kapitel 5.4.1 „Bestimmungen zur Aufrechterhaltung“) enthalten und wird befristet.

Vor Erteilung der Zertifizierung hat der Antragsteller Gelegenheit, sich zu den Nebenbestimmungen und den weiteren Inhalten der Zertifizierungsdokumente im Rahmen einer Anhörung zu äußern.

Eine negative Zertifizierungsentscheidung erfolgt, wenn die Prüfung und Bewertung ergeben hat, dass das Produkt die entsprechenden Prüfkriterien nicht erfüllt oder das Bundesministerium des Innern festgestellt

hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen. In diesem Fall werden dem Antragsteller vor Ablehnung des Antrags die Gründe der voraussichtlichen Ablehnung mitgeteilt. Er hat innerhalb einer Frist Gelegenheit zur Äußerung und zur Nachbesserung.

Innerhalb eines Monats nach Bekanntgabe des Bescheides kann beim BSI, Godesberger Allee 185-189, 53175 Bonn, schriftlich oder zur Niederschrift Widerspruch erhoben werden. Der Antragsteller kann auf den Widerspruch verzichten, um eine schnellere Veröffentlichung der Anerkennung bzw. Zertifizierung zu ermöglichen.

Die Erteilung eines Kostenbescheids ergeht separat.

4 Aufrechterhaltung der Zertifizierung

Eine Produktzertifizierung bezieht sich nur auf die angegebene Version des Produktes und unter Berücksichtigung aller Nebenbestimmungen, Auflagen und Inhalte des Zertifizierungsreports.

Bedingungen für den Anwender eines zertifizierten Produktes (u. a. Angaben zur Einsatzumgebung) ergeben sich aus dem Zertifizierungsreport, etwaigen Anlagen sowie den evaluierten Handbüchern. Die Zertifizierungsstelle fordert dabei auch vom Anwender, die mit dem Zertifikat zum Ausdruck gebrachten Ergebnisse und Randbedingungen in seinem Risikomanagementprozess zu berücksichtigen und empfiehlt seinerseits, vom Hersteller eine regelmäßige Aktualisierung des Zertifikates nach dem jeweils aktuellen Stand der Technik bereitzustellen.

Die Bestätigung der Erfüllung der Prüfkriterien bezieht sich auf den Zeitpunkt der Zertifizierung. Die Zertifizierungsstelle befristet zusätzlich die formale Gültigkeit einer Zertifizierung Dabei kann das BSI jederzeit anlassbezogen überprüfen, ob die Voraussetzungen für die Zertifizierung weiterhin vorliegen.

Bei Änderungen am Produkt oder den Entwicklungs- und Produktionsprozessen kann eine Aufrechterhaltung der Zertifizierung durch folgende Maßnahmen erfolgen:

4.1 Maintenance

Bei geringem Umfang der Änderungen am Produkt oder den Entwicklungs- bzw. Produktionsprozessen und bei sicherheits- bzw. TR-irrelevanten Änderungen kann auf Antrag eine bestehende Zertifizierung auf die neue Produktversion oder die geänderten Prozessbedingungen erweitert werden.

Die Befristung des zugrunde liegenden Zertifikates bleibt unberührt.

4.2 Rezertifizierung

Bei größeren oder sicherheits- bzw. TR-relevanten Änderungen am Produkt oder den Entwicklungs-/ Produktionsprozessen ist eine erneute Zertifizierung erforderlich.

Je nach den Regelungen im Geltungsbereich können Anteile der früheren Evaluierung bzw. Prüfung wiederverwendet werden und der Fokus auf die Änderungen konzentriert werden.

4.3 Aufrechterhaltung der Zertifizierung durch Reassessment im Bereich der Common Criteria

Zur Verifikation der Angriffsresistenz eines zertifizierten Produktes kann eine Neubewertung nach dem aktuellen Stand der Technik beantragt und durchgeführt werden (Reassessment).

Die Zertifizierungsstelle empfiehlt, regelmäßig (z. B. jährlich) eine Einschätzung der Widerstandsfähigkeit gegen Angriffe gemäß den jeweils geltenden Sicherheitsvorgaben vornehmen zu lassen. Es gibt Zertifikate, bei denen eine Auflage zur Neubewertung nach einem bestimmten Zeitraum enthalten ist.

5 Rahmenbedingungen

5.1 Grundlage für die Zertifizierung

Das Verfahren wird nach der „Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik“ [BSI-ZertV], dem Verwaltungsverfahrensgesetz [VwVfG] sowie dieser Verfahrensbeschreibung mit den zugehörigen Anforderungsdokumenten durchgeführt.

5.2 Vertraulichkeit und Dokumentenaustausch mit der Zertifizierungsstelle

Die Zertifizierungsstelle im BSI erfüllt zur Festigung der Qualität die Erfüllung der Anforderungen aus DIN EN ISO/IEC 17065 [ISO/IEC 17065]. Auch aus den internationalen Anerkennungsabkommen SOG-IS-MRA und CCRA heraus ist sie in jedem Zertifizierungsverfahren im Geltungsbereich Common Criteria 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.

Die Beteiligten eines Verwaltungsverfahrens haben nach § 30 des Verwaltungsverfahrensgesetzes [VwVfG] Anspruch darauf, dass ihre Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden. Die Mitarbeiter im BSI werden schriftlich auf die gewissenhafte Erfüllung ihrer Obliegenheiten sowie der Wahrung des Datengeheimnisses nach § 5 des Bundesdatenschutzgesetzes [BDSG] verpflichtet und gemäß Sicherheitsüberprüfungsgesetz überprüft.

Der Dokumentenaustausch zwischen Antragsteller, Prüfstelle und Zertifizierungsstelle erfolgt auf elektronischem Wege per E-Mail grundsätzlich verschlüsselt.

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 versiegeltem inneren Umschlag verpackt und mit dem Vermerk „ungeöffnet an die Zertifizierungsstelle“ versehen werden, damit die Vertraulichkeit der Unterlagen und das Need-to-know-Prinzip auch auf dem BSI-internen Postweg gegeben ist.

Dokumente, die auf elektronischen Medien, z.B. CDs oder USB-Sticks, an das BSI geschickt werden, müssen auf dem Medium verschlüsselt gespeichert werden.

Prüfstelle und Zertifizierungsstelle kennzeichnen ihre jeweiligen Dokumente zum Verfahren (Prüfunterlagen, Kommentierungen) als „firmenvertraulich“ bzw. „company confidential“.

5.3 Rahmenbedingungen zum Verfahren

5.3.1 Unparteilichkeit

Die Zertifizierungs- bzw. Evaluierungs- und Prüftätigkeiten müssen unparteiisch durchgeführt werden. In diesem Rahmen richtet sich die Produktzertifizierung nach den Anforderungen der DIN EN ISO/IEC 17065. Daher wird kommerzieller, finanzieller oder sonstiger Druck, der die Unparteilichkeit gefährden könnte, nicht zugelassen.

Die an der Durchführung der Zertifizierung bzw. Evaluierung und Prüfung Beteiligten dürfen nicht

1. Entwickler, Hersteller, Installateur, Verteiler oder Instandhalter des zu zertifizierenden bzw. zertifizierten Produkts sein oder

2. Beratungen für den Antragsteller bzw. Kunden anbieten, bereitstellen oder durchführen.

Für das BSI gelten insbesondere die Regelungen der §§ 20f. VwVfG [VwVfG].

5.3.2 Obliegenheiten des Antragstellers

Dem Antragsteller obliegt es:

- dem BSI und der Prüfstelle kostenfrei das zu zertifizierende Produkt, die für dessen oder deren Betrieb notwendigen Einrichtungen und Rechte sowie die erforderlichen Unterlagen zur Verfügung zu stellen. Unterlagen können beim Antragsteller in Augenschein genommen werden, wenn der Antragsteller glaubhaft macht, dass einer Weitergabe der Unterlagen wesentliche Interessen des Antragstellers entgegenstehen.

  Zur Zertifizierung von Schutzprofilen obliegt es dem Antragsteller, dem BSI und der Prüfstelle kostenfrei das zu zertifizierende Schutzprofil zur Verfügung zu stellen.
- zur Durchführung des Zertifizierungsverfahrens, das BSI und die beauftragte Prüfstelle kostenfrei durch fachkompetente Vertreter zu unterstützen.

  Soweit notwendig, obliegt es dem Antragsteller, kostenfrei das mit der Prüfung, Bewertung und Zertifizierung befasste Personal produkt-, komponenten- oder systembezogen einzuweisen oder Schulungen durchzuführen.
- die Einhaltung des zu Beginn des Verfahrens vereinbarten Zeit- bzw. Evaluierungsplans seinerseits zu ermöglichen: Im Rahmen des Verfahrens muss bei der Gestaltung des Zeit- oder Evaluierungsplans aktiv mit dem BSI zusammengearbeitet werden. Bei sich abzeichnenden Verzögerungen ist die Prüfstelle und die Zertifizierungsstelle umgehend zu informieren, um eine aktualisierte Verfahrensplanung abzustimmen.

5.3.3 Rücknahme eines Antrages

Zu jedem Zeitpunkt im Verfahren kann der Antragsteller den Antrag auf Zertifizierung zurückziehen. In diesem Fall wird das Verfahren beendet.

Seitens des BSI werden die angefallenen Kosten und Auslagen erhoben.

5.3.4 Ablehnung eines Antrags

Das BSI kann einen Antrag bei nicht vorliegen der im BSIG § 9 genannten Voraussetzungen ablehnen sowie wenn

- ein unvollständig eingereichter Antrag nicht innerhalb von 6 Monaten vervollständigt wird oder
- der Antragsteller über einen Zeitraum von mehr als 3 Monaten entgegen der vereinbarten Planung keine Unterlagen liefert.

5.4 Rahmenbedingungen zur Aufrechterhaltung der Zertifizierung

5.4.1 Bestimmungen zur Aufrechterhaltung

Zur Aufrechterhaltung der Zertifizierung muss der Antragsteller die Festlegungen der [VB-Produkte] sowie im Bescheid enthaltene Nebenbestimmungen einhalten.

Im Rahmen der Festlegungen der [VB-Produkte] wird insbesondere bestimmt, dass:

- der Inhaber des Zertifikats bei der Nutzung der Zertifizierung, insbesondere bei der Verwendung zu Werbezwecken, Vorlage und Nachweisführung (z.B. gegenüber Kunden), auf den Zertifizierungsreport und das Zertifikat hinweisen und diese Dokumente samt der für den Anwender bestimmten Anlagen zur Verfügung stellen muss.
- der Inhaber des Zertifikats unaufgefordert das BSI informieren muss, wenn sich die Sicherheitseigenschaften des Zertifizierungsgegenstandes ändern oder die Erfüllung der Zertifizierungsanforderungen beeinträchtigt sind. Dies gilt insbesondere bei Bekanntwerden von Schwachstellen an der zertifizierten Version des Produktes, bei sicherheits- oder TR-relevanten Änderungen an der Herstellungsmethode, bei Einbußen an der Vertraulichkeit von als vertraulich angenommenen Unterlagen sowie der Kontaktadressen und der Entwicklungs- bzw. Produktionsstätten.
- der Inhaber des Zertifikats regelmäßig oder anlassbezogen auf seine Kosten durch das BSI oder durch von diesem beauftragte Personen oder Stellen überprüfen lassen muss, ob die Voraussetzungen zur Zertifizierung des Produkts weiterhin vorliegen.
- eine Zertifizierung von der Gültigkeit eines Schutzprofils oder einer technischen Richtlinie abhängig ist.
- Nutzungsbedingungen zur Verwendung von Zertifizierungszeichen (siehe Kapitel 6.2 „Zertifizierungszeichen“ anzuwenden sind.

5.5 Regelungen zur Archivierung von Dokumenten und Aufzeichnungen

Der Antrag, die mit dem Antrag eingereichten Unterlagen und die im Zertifizierungsverfahren anfallenden Unterlagen werden beim BSI elektronisch oder in Papierform gemäß den geltenden Bestimmungen aufbewahrt.

Soweit der Antragsteller nach BSIZertV § 3 Abs. 2 dazu berechtigt ist, dem BSI Unterlagen oder sonstige Beweismittel nur zeitweise zur Verfügung zu stellen, hat er diese Unterlagen oder sonstigen Beweismittel nach der Inaugenscheinnahme durch das BSI beim Antragsteller während des Antragsverfahrens und des Gültigkeitszeitraums der Zertifizierung aufzubewahren. Nach Ablauf der Geltungsdauer der Zertifizierung sind diese Unterlagen oder sonstigen Beweismittel für mindestens drei weitere Jahre aufzubewahren und dem BSI jederzeit auf Anfrage kostenfrei zur Verfügung zu stellen.

5.6 Aufhebung einer Zertifizierung

Zur Aufhebung einer Zertifizierung werden die Regelungen des Verwaltungsverfahrensgesetzes berücksichtigt.

Ist eine Zertifizierung unanfechtbar aufgehoben (d.h. widerrufen oder zurückgenommen) oder ist die Gültigkeit der Zertifizierung aus einem anderen Grund nicht oder nicht mehr gegeben, so kann das BSI die auf Grund des Zertifizierungsverfahrens erteilten Zertifikate, die zum Nachweis der Zertifizierung im betreffenden Geltungsbereich bestimmt sind, zurückfordern. Der Antragsteller ist zu ihrer Herausgabe verpflichtet. Er kann jedoch verlangen, dass ihm die Zertifikate wieder ausgehändigt werden, nachdem sie durch das BSI als ungültig gekennzeichnet wurden.

Das Produkt wird nicht mehr auf der öffentlichen Liste der zertifizierten Produkte gelistet.

5.6.1 Widerruf einer rechtmäßigen Zertifizierung

Ein Widerruf einer rechtmäßigen Zertifizierung kann aufgrund nachträglich eingetretener Tatsachen bzgl. der zugrundeliegenden Sach- und Rechtslage erfolgen (siehe hierzu §§ 48 und 49 [VwVfG]).

Gründe, die zu einem Widerruf einer Zertifizierung führen können, sind beispielsweise, wenn der Antragsteller:

- im Bescheid enthaltene Nebenbestimmungen selbst nicht beachtet (siehe Kapitel 5.4.1 „Bestimmungen zur Aufrechterhaltung“).
- der Antragsteller Zertifikate oder Zertifizierungszeichen missbräuchlich verwendet.

5.6.2 Rücknahme einer rechtswidrigen Zertifizierung

Eine rechtswidrige Zertifizierung kann ganz oder teilweise zurückgenommen werden, beispielsweise, wenn

- bewusst falsche Angaben zu den Zertifizierungsvoraussetzungen gemacht wurden.
- für die Zertifizierungsentscheidung bewusst wesentliche Informationen verschwiegen wurden.

5.7 Beschwerde- und Verbesserungsmanagement

Die Zertifizierungsstelle verfügt über ein Verfahren, um Beschwerden und Verbesserungsvorschläge entgegenzunehmen, zu evaluieren sowie Entscheidungen über diese zu treffen. Das Verfahren ist auf der Internetseite des BSI veröffentlicht. Der Erhalt der Beschwerde wird bestätigt. Der Beschwerdeführer wird, sofern möglich, über das Ergebnis und den Abschluss des Verfahrens informiert.

Es wird in der Konformitätsbewertung ein Beschwerde- und Verbesserungsmanagement gelebt. Dabei fließt jegliche Anregung ein.

Auslöser für den Verbesserungsprozess sind unter anderem:

- Beschwerden und fehlerhafte Arbeitsergebnisse sowie
- Verbesserungsvorschläge und festgestellte Abweichungen.

5.8 Haftung

Für die wirtschaftliche Verwertbarkeit der Produktzertifizierung im Sinne dieser Verfahrensbeschreibung wird keine Gewähr übernommen.

Das BSI haftet ausschließlich nach den gesetzlichen Vorschriften.

5.9 Kosten

Mit Antragstellung erkennt der Antragsteller die Kostenverordnung des BSI an und stimmt zu, die vom BSI auf Basis der BSI Kostenverordnung [BSIKostV] mit ihm abzurechnenden Aufwände des Verfahrens (Gebühren und Auslagen) zu erstatten. Ebenso erklärt er sich einverstanden, dass bei Auslagerung der Prüfbegleitung an eine externe Stelle das BSI Reisekosten dieser Stelle mit dem Antragsteller abrechnen darf.

Ein Informationsgespräch mit dem BSI vor Antragstellung ist kostenfrei.

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

Die Abrechnung der bei der Prüfstelle anfallenden Kosten für die Evaluierung wird zwischen Antragsteller und Prüfstelle vertraglich vereinbart. Es wird empfohlen, einen Kostenvoranschlag bei einer Prüfstelle vor Antragstellung einzuholen.

6 Veröffentlichung der Zertifizierung

6.1 Veröffentlichung „Zertifizierte Produkte“

Das BSI veröffentlicht mindestens vierteljährlich im Internet oder in anderen Medien Gesamtlisten oder seit der letzten Veröffentlichung geänderte oder hinzugefügte Listeneinträge der zertifizierten informationstechnischen Schutzprofile, Produkte, Komponenten und Standorte sowie die zugehörigen Sicherheitszertifikate und Zertifizierungsreporte.

Der Inhaber eines Zertifikats kann der Veröffentlichung widersprechen. Das BSI sieht von der Veröffentlichung ab, soweit durch die Veröffentlichung die öffentliche Sicherheit beeinträchtigt werden könnte. Das BSI kann von der Veröffentlichung ganz oder teilweise absehen, wenn durch die Veröffentlichung öffentliche oder private Interessen beeinträchtigt würden.

Im Bereich der Common Criteria kann auf Wunsch des Antragstellers bereits die Tatsache des laufenden Zertifizierungsverfahrens nach Beginn der Evaluierung veröffentlicht werden.

Internationalen Anerkennungsvereinbarungen fordern die Veröffentlichung des Zertifizierungsreports, so dass ein Zertifikat nur bei veröffentlichtem Zertifizierungsreport international anerkannt wird.

6.2 Zertifizierungszeichen

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

Im Bereich der Technischen Richtlinien gibt es bei Hardware-Produkten auf Wunsch ein zusätzliches Prüfsiegel. Die Verwendung dieses Prüfsiegels kann bei Einsatz des Produktes in hoheitlichen Bereichen verpflichtend sein.

Die Zeichenordnung des BSI [Zeichenordnung] enthält die Nutzungsbedingungen aller Zertifizierungszeichen. Die Nutzungsbedingungen sowie die Benennung der Zertifizierungskennung bei Veröffentlichungen in Bezug auf die Zertifizierung eines Produktes kann Gegenstand von Nebenbestimmungen (siehe Kapitel 5.4.1 „Bestimmungen zur Aufrechterhaltung“) sein.

6.3 Verwendung von Zertifikaten

Die Verwendung des Zertifikats ist im Zertifizierungsbescheid geregelt. Als vorbeugende Maßnahmen gegen Missbrauch wird der Antragsteller auf seine Pflichten hingewiesen. Bei inkorrekten Bezugnahmen auf das Zertifizierungssystem oder irreführender Verwendung von Zertifikaten oder Zertifizierungszeichen durch den Antragsteller kann die Aufhebung der Zertifizierung gemäß Kapitel 5.6.1 „Widerruf einer rechtmäßigen Zertifizierung“ erfolgen.

6.4 Zertifikatsübergabe und 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 an einen Vertreter des Unternehmens auszuhändigen. Insbesondere fallen hierunter die Veranstaltungen: CeBIT, ITSA, ICCC und RSA-Konferenz.

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

7 Referenzen und Glossar

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