Bundesamt
für Sicherheit in der
Informationstechnik

BSI TR

Zertifizierte IT-Sicherheit

Prüfstandards für IT-Sicherheit
Technische Richtlinien und Schutzprofile

Konformitätsbewertung
Zertifizierung und Anerkennung

Inhaltsverzeichnis

1 Unsere Gesellschaft auf dem Daten-Highway

1 Unsere Gesellschaft auf dem Daten-Highway

Wir befinden uns heute in einer globalen Informationsgesellschaft. Immer komplexere, schnellere und weltweit vernetzte informationstechnische Systeme übernehmen zunehmend weitreichendere Aufgaben.

Die Informationstechnik (IT) hat inzwischen alle gesellschaftlichen Bereiche erfasst und ist ein selbstverständlicher und teilweise unsichtbarer Bestandteil des Alltags geworden.

Die Funktionsweise von informationstechnischen Produkten und Systemen ist für weite Kreise der Anwender nicht sofort und ohne fundiertes Fachwissen durchschaubar. Vertrauen in die Informationstechnik kann aber nur dann entstehen, wenn sich die Nutzer auf ihre Anwendung verlassen können. Das gilt insbesondere für die Sicherheit von Daten im Hinblick auf Vertraulichkeit, Verfügbarkeit und Integrität.

Um einen sicheren Umgang mit Daten und informationsverarbeitenden Systemen zu gewährleisten, ist es erforderlich, entsprechend der jeweiligen Gefährdung, Sicherheitsstandards zu entwickeln und einzuhalten.

2 Das BSI im Dienst der Öffentlichkeit

2 Das BSI im Dienst der Öffentlichkeit

Das Bundesamt für Sicherheit in der Informationstechnik wurde am 1. Januar 1991 mit Sitz in Bonn gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern.

Mit seinen derzeit rund 600 Mitarbeiterinnen und Mitarbeitern und ca. 80 Mio. Euro Haushaltsvolumen ist das BSI eine unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Als zentraler IT-Sicherheitsdienstleister des Bundes ist das BSI operativ für den Bund, kooperativ mit der Wirtschaft und informativ für den Bürger tätig.

Durch die Grundlagenarbeit im Bereich der IT-Sicherheit übernimmt das BSI als nationale IT-Sicherheitsbehörde Verantwortung für unsere Gesellschaft und ist dadurch eine tragende Säule der Inneren Sicherheit in Deutschland.

Ziel des BSI ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. IT-Sicherheit soll als wichtiges Thema wahrgenommen und eigenverantwortlich umgesetzt werden. Sicherheitsaspekte sollen schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden.

Das BSI wendet sich mit seinem Angebot an die Anwender und Hersteller von Informationstechnik. Zielgruppen sind die öffentlichen Verwaltungen in Bund, Ländern und Kommunen sowie Privatanwender und Unternehmen.

Die Sicherheit der zum Einsatz kommenden Produkte ist die Basis für vertrauenswürdige Geschäftsprozesse. Das BSI hat hier insbesondere die Aufgabe, IT-Sicherheitszertifizierungen von IT-Produkten und -Systemen durchzuführen und die dafür benötigten Prüfkriterien bzw. Grundlagen zu entwickeln. Grundlage für die Erteilung eines Zertifikates sind geeignete Prüfkriterien, ein notwendiges Verfahren zur Durchführung von Zertifizierungen sowie Prüfstellen oder Auditoren, die über eine nachgewiesene Kompetenz verfügen und ein Zertifikat bzw. eine Anerkennung für ihr Prüfgebiet besitzen.

Folgende Arten der Zertifizierung bietet das BSI an:

» Zertifizierung von Produkten nach Common Criteria

» Bestätigung von Produkten nach dem deutschen Signaturgesetz

» Konformitätsprüfung

» Zertifizierung von IT-Sicherheitsdienstleistungen

» Anerkennung von Prüfstellen sowie Zertifizierung von IT-Sicherheitsdienstleistern

» Zertifizierung und Anerkennung von Personen

Das BSI betreibt ein Qualitätsmanagementsystem, das den Anforderungen der DIN EN ISO/IEC 9001 sowie einschlägigen Anforderungen an Zertifizierungsstellen entspricht.

Das Verfahren zur Zertifizierung von Produkten wurde in bestimmten Bereichen von der nationalen Akkreditierungsstelle der Bundesrepublik Deutschland (DAkkS) akkreditiert. Das BSI weist damit seine Kompetenz und gleichbleibende Qualität in der Zertifizierung nach.

Diese Broschüre gibt einen Überblick über die vom BSI angebotenen Zertifizierungsverfahren.

3 Profilierte Sicherheit – Prüfstandards des BSI

3 Profilierte Sicherheit – Prüfstandards des BSI

Das BSI entwickelt Prüfstandards unter Beteiligung betroffener Behörden und in Kooperation mit Anwenderorganisationen und Herstellern. Mithilfe dieser Standards können informationstechnische Produkte und Systeme geprüft und zertifiziert werden. Diese Prüfvorgaben sind auf den Webseiten des BSI veröffentlicht und können dort heruntergeladen werden.

Vorgaben in Form von Schutzprofilen, Technischen Richtlinien und BSI-Standards haben zunächst Empfehlungscharakter. Verbindlichkeit kann jedoch durch Gesetze und Verordnungen entstehen oder wenn die Vorgaben eines Schutzprofils oder einer Technischen Richtlinie in Ausschreibungsverfahren Verwendung finden oder von einem Bedarfsträger explizit gefordert werden.

3.1 Schutzprofile nach Common Criteria (CC) für IT-Produkte

In Schutzprofilen sind generische Anforderungen an eine Produktkategorie festgeschrieben. Sie sind zunächst implementierungsunabhängig, können aber durch die daraus ableitbaren Sicherheitsvorgaben auf einen konkreten Evaluationsgegenstand (EVG) zugeschnitten werden. Anforderungen an die Funktionalität sowie an die Vertrauenswürdigkeit werden in Schutzprofilen zusammengefasst und decken eine bestimmte Menge von Sicherheitszielen vollständig ab. Durch das Verfassen von Schutzprofilen kann das BSI somit Mindeststandards für bestimmte Produktgruppen setzen. Anwendungen, für die Schutzprofile entwickelt wurden, sind z. B. der elektronische Reisepass (ePass), neuer Personalausweis, mobile Synchronisationsdienste und Produkte für die Digitale Signatur. Schutzprofile existieren aber u.a. auch für Betriebssysteme und Firewalls.

Bedingt durch das allgemeine Sicherheitskonzept eines Schutzprofils ist für den IT-Anwender somit eine gute Vergleichbarkeit verschiedener Produkte gewährleistet, die auf Basis ein und desselben Schutzprofils zertifiziert worden sind. Der IT-Hersteller erhält durch die Verwendung eines zertifizierten Schutzprofils die Sicherheit, dass das Schutzprofil ein sinnvolles, im Markt gewünschtes Konzept für ein IT-Sicherheitsprodukt darstellt und sich als Vorgabe zur Entwicklung eines entsprechenden Produktes anbietet.

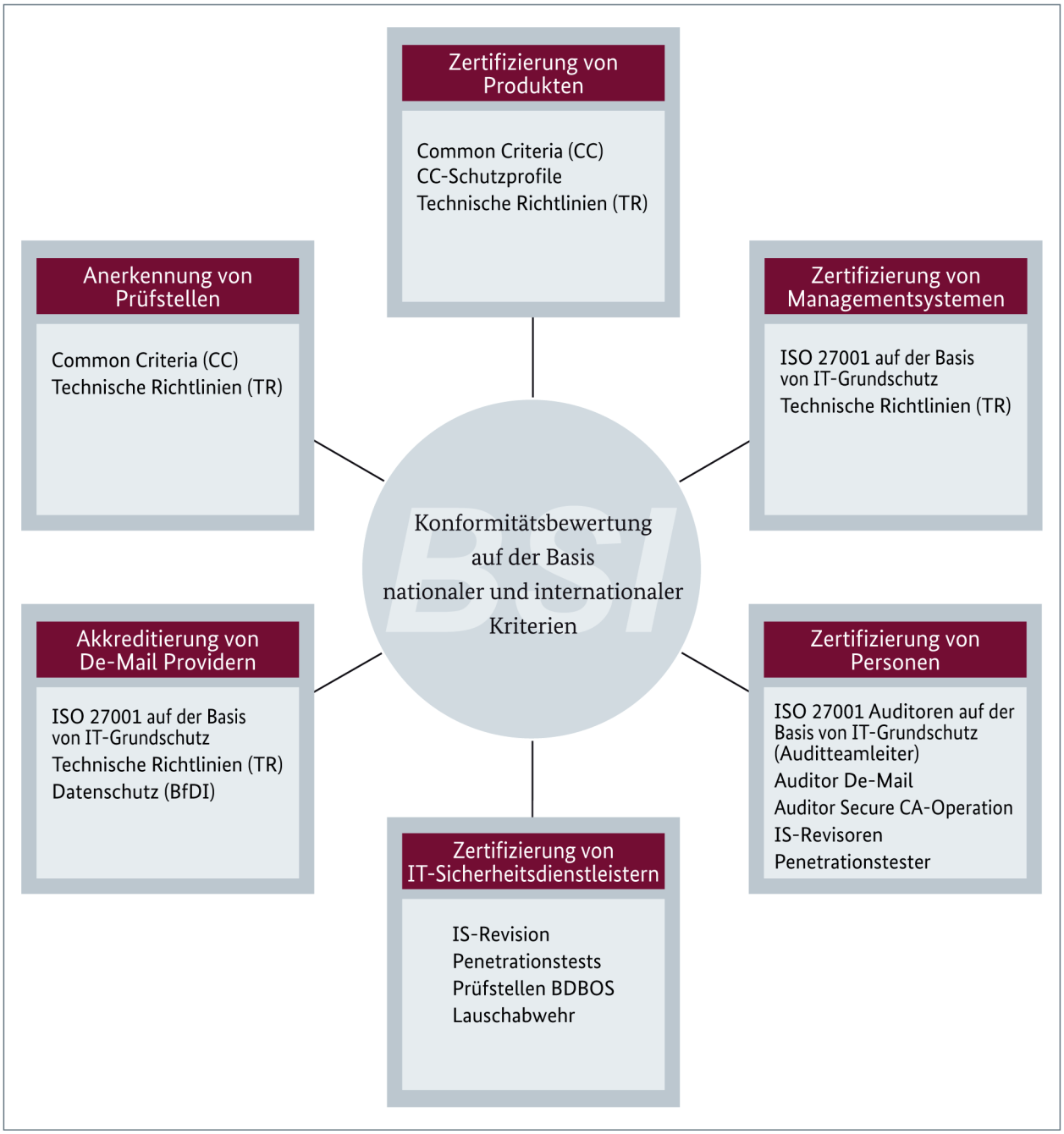
In einem Schutzprofil sind die allgemeinen IT-Sicherheitseigenschaften sowie die Bedingungen für den sicheren Einsatz des Produktes festgelegt. Dieses IT-Sicherheitskonzept beschreibt nicht nur den Wert der Daten und deren Verarbeitung, sondern erfasst auch die Annahmen an eine typische Einsatzumgebung. Einzuhaltende gesetzliche Auflagen oder vorgeschriebene Sicherheitsstandards finden in dem Sicherheitskonzept des Schutzprofils ebenso ihren Niederschlag wie alle durch die IT abzuwehrenden Bedrohungen auf die zu schützenden Werte.

Mit der Zertifizierung eines Schutzprofils wird der Nachweis erbracht, dass das Schutzprofil vollständig, konsistent und technisch stimmig ist.

3.2 Technische Richtlinien des BSI für IT-Produkte und Managementsysteme

Technische Richtlinien (TR) beschreiben funktionale und qualitative Anforderungen an IT-Produkte und -Systeme und definieren Merkmale und Schnittstellen, die für deren Interoperabilität, Funktionalität und Integration entscheidend sind. Sie werden vom BSI entwickelt und publiziert. Dies erfolgt ausschließlich nach Feststellung eines Bedarfs der nationalen Sicherheit oder des öffentlichen Interesses.

Technische Richtlinien werden auf der BSI-Webseite veröffentlicht und können dort heruntergeladen werden. Mit der Veröffentlichung Technischer Richtlinien stellt das BSI der Wirtschaft und Verwaltung konkrete Handlungsempfehlungen für die Planung, Beschaffung, Konfiguration und den Betrieb von IT-Produkten und Systemen zur Verfügung.



Interoperabilität und Funktionalität

Das Ziel der Technischen Richtlinien des BSI ist die Verbreitung von angemessenen IT-Sicherheitsstandards. Technische Richtlinien richten sich daher in der Regel an alle, die mit dem Aufbau, der Absicherung oder dem Betrieb von IT-Systemen zu tun haben. Sie ergänzen die technischen Prüfvorschriften des BSI und liefern Kriterien und Methoden für Konformitätsprüfungen sowohl der Interoperabilität von IT-Sicherheitskomponenten als auch der umgesetzten IT-Sicherheitsanforderungen und deren Funktionalität.

Verbindlichkeit

Technische Richtlinien des BSI haben zunächst den formalen Status einer technischen Empfehlung. Verbindlichkeit entsteht erst, wenn sie in Ausschreibungsverfahren Verwendung finden, von Bedarfsträgern für ihren Zuständigkeitsbereich explizit gefordert werden oder in einem Gesetz oder einer Rechtsverordnung referenziert werden.

TR Secure Certification Authority Operation

Public Key Infrastructures (PKI) sichern die Vertraulichkeit, Authentizität und Integrität von Informationen. Dies setzt voraus, dass PKI-Betreiber, die Certification Authorities (CA), einerseits vertrauenswürdig sind und ihnen andererseits auch von Dritten vertraut wird. Zwei Bedingungen müssen erfüllt werden, um dieses Vertrauen herzustellen. Erstens muss es eine Basis für Vertrauenswürdigkeit geben, d.h. die CA muss auf einem angemessenen Sicherheitsniveau organisatorische und technische Maßnahmen implementieren und Regeln für alle PKI-Teilnehmer aufstellen. Zweitens müssen diese Sicherheitsmaßnahmen transparent dokumentiert werden.

Die BSI TR-03145 unterstützt CAs bei beiden Schritten. Sie formuliert Anforderungen an die zu implementierenden Sicherheitsmaßnahmen und dient als Grundlage für einen Audit- und Zertifizierungsprozess.

TR Smart Energy

Die Technische Richtlinie BSI TR-03109 ergänzt die Sicherheitsanforderungen des Smart Meter Schutzprofils für die Kommunikationseinheit eines intelligenten Messsystems um funktionale Anforderungen zur Gewährleistung der Interoperabilität der in Smart Metering Systemen vorhandenen Komponenten. Zusätzlich werden die Anforderungen an die Kommunikationseinheit und ihre Einsatzumgebung um Vorgaben zu Kommunikationsprotokollen, Tarif- und Berechtigungsprofilen sowie kryptographischen Verfahren erweitert.

TR-ESOR

Nicht nur die Verwaltung, auch Unternehmen stehen vor der Herausforderung, für immer mehr elektronisch erzeugte, verarbeitete und gespeicherte Dokumente und Daten auch in Zukunft die Lesbarkeit, Verfügbarkeit sowie Integrität und Authentizität gewährleisten zu müssen.

Produktmarken des BSI

Mit der Technischen Richtlinie ‚Beweiswerterhaltung kryptographisch signierter Dokumente' (BSI TR-03125 / TR-ESOR) stellt das BSI einen Leitfaden zur Verfügung, der beschreibt, wie elektronisch signierte Daten und Dokumente über lange Zeiträume – bis zum Ende der Aufbewahrungsfristen – im Sinne eines rechtswirksamen Beweiswerterhalts vertrauenswürdig gespeichert werden können.

3.3 BSI-Standards zu IT-Grundschutz und IT-Grundschutz-Kataloge für IT-Systeme

Im Bereich IT-Grundschutz existieren nachfolgende BSI-Standards:

» 100-1: Managementsysteme für Informationssicherheit (ISMS)

» 100-2: IT-Grundschutz-Vorgehensweise

» 100-3: Ergänzende Risikoanalyse auf der Basis von IT-Grundschutz und

» 100-4: Notfallmanagement

Managementsysteme für Informationssicherheit

Der BSI-Standard 100-1 definiert allgemeine Anforderungen an ein ISMS. Er ist vollständig kompatibel zum ISO-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der anderen ISO-Standards der ISO 2700x-Familie wie beispielsweise ISO 27002 (früher ISO 17799). Er bietet Lesern eine leicht verständliche und systematische Einführung und Anleitung, unabhängig davon, mit welcher Methode sie die Anforderungen umsetzen möchten.

Das BSI stellt den Inhalt dieser ISO-Standards in einem eigenen BSI-Standard dar, um einige Themen ausführlicher beschreiben zu können und so eine didaktischere Darstellung der Inhalte zu ermöglichen. Zudem wurde die Gliederung so gestaltet, dass sie zur IT-Grundschutz-Vorgehensweise kompatibel ist. Durch die einheitlichen Überschriften in beiden Dokumenten ist eine Orientierung für die Leser sehr einfach.

IT-Grundschutz-Vorgehensweise

Der BSI-Standard 100-2 beschreibt den schrittweisen Aufbau und den Betrieb eines Managementsystems für Informationssicherheit. Die Aufgaben des Sicherheitsmanagements und der Aufbau von Organisationsstrukturen für Informationssicherheit sind dabei wichtige Themen. Die IT-Grundschutz-Vorgehensweise geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept erstellt werden kann, wie angemessene Sicherheitsmaßnahmen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzeptes zu beachten ist. Auch die Frage, wie die Informationssicherheit im laufenden Betrieb aufrecht erhalten und verbessert werden kann, wird beantwortet.

IT-Grundschutz interpretiert damit die sehr allgemein gehaltenen Anforderungen der ISO-Standards der 2700x-Reihe und hilft den Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrundinformationen und Beispielen. Im Zusammenspiel mit den IT-Grundschutz-Katalogen wird in der IT-Grundschutz-Vorgehensweise nicht nur erklärt, was gemacht werden sollte, sondern es werden auch konkrete Hinweise gegeben, wie eine Umsetzung (auch auf technischer Ebene) aussehen kann. Ein Vorgehen nach IT-Grundschutz ist eine erprobte und effiziente Möglichkeit, allen Anforderungen der oben genannten ISO-Standards nachzukommen.

Risikoanalyse auf der Basis von IT-Grundschutz

Der BSI-Standard 100-3 bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit den IT-Grundschutz-Maßnahmen arbeiten und möglichst nahtlos eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten. Hierfür kann es verschiedene Gründe geben:

» Die Sicherheitsanforderungen des Unternehmens bzw. der Behörde gehen teilweise deutlich über das normale Maß hinaus (hoher oder sehr hoher Schutzbedarf).

» Die Institution betreibt wichtige Anwendungen oder Komponenten, die (noch) nicht in den IT-Grundschutz-Katalogen des BSI behandelt werden.

» Die Zielobjekte werden in Einsatzszenarien (Umgebung, Anwendung) betrieben, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Die Vorgehensweise richtet sich sowohl an Anwender der Informationstechnik (Sicherheitsverantwortliche und -beauftragte) als auch an Berater und Experten. Häufig ist es allerdings empfehlenswert, bei der Durchführung von Risikoanalysen auf Expertensachverstand zurückzugreifen.

Notfallmanagement

Mit dem BSI-Standard 100-4 wird ein systematischer Weg aufgezeigt, ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen, um die Kontinuität des Geschäftsbetriebs sicherzustellen. Aufgaben eines Notfallmanagements sind daher, die Ausfallsicherheit zu erhöhen und somit die Institution auf Notfälle und Krisen adäquat vorzubereiten, damit die wichtigsten Geschäftsprozesse bei Ausfall schnell wieder aufgenommen werden können. Es gilt, Schäden durch Notfälle oder Krisen zu minimieren und die Existenz der Behörde oder des Unternehmens auch bei einem größeren Schadensereignis zu sichern.

4 Zertifizierung von Produkten nach Common Criteria

4 Zertifizierung von Produkten nach Common Criteria

4.1 Gemeinsame Sicherheitskriterien – Common Criteria

Die „Common Criteria for Information Technology Security Evaluation (CC)“ stellen die international anerkannten Kriterien zur Prüfung und Bewertung der Sicherheit von Produkten dar. Sie sind für die Bewertung der Sicherheitseigenschaften praktisch aller informationstechnischen Produkte geeignet. Typische Produktklassen sind im Softwarebereich z. B. Betriebssysteme, Datenbanken, Firewalls, PC-Sicherheitsprodukte, VPN-Produkte, E-Mail-Server und Signaturanwendungskomponenten, im Hardwarebereich z. B. Produkte zum digitalen Tachographen, Sicherheitsmodule, Smartcard-Controller, Signaturkarten, Gesundheitskarten und Chipkartenleser.

Die Common Criteria bestehen aus 3 Teilen. Im Teil 1 (Einführung und allgemeines Modell) werden die Grundlagen der IT-Sicherheitsevaluation und der allgemeine Geltungsbereich der CC erläutert sowie Schutzprofile (Protection Profiles) und Sicherheitsvorgaben (Security Targets) für den zu prüfenden Evaluationsgegenstand (EVG) beschrieben. Der Teil 2 (Funktionale Sicherheitsanforderungen) enthält einen umfangreichen Katalog von Funktionalitätsanforderungen. Er stellt ein empfohlenes Angebot für die Beschreibung der Funktionalität eines Produktes bzw. Systems dar, von dem jedoch in begründeten Fällen abgewichen werden kann. Im Teil 3 (Anforderungen an die Vertrauenswürdigkeit) sind die Anforderungen an die Vertrauenswürdigkeit und damit Prüfaufwand, -tiefe und -genauigkeit aufgelistet. Wichtig ist, dass ein Evaluationsergebnis immer auf einem Vertrauenswürdigkeitspaket (z. B. einer Vertrauenswürdigkeitsstufe (EAL)) basieren sollte, eventuell ergänzt durch weitere Anforderungen.

Die Common Criteria bieten 7 Prüfstufen (Evaluation Assurance Level (EAL)) an. Mit zunehmender Prüfstufe nehmen sowohl Umfang als auch Tiefe der Prüfung zu. Im kommerziellen Umfeld werden in der Regel die Stufen EAL1 bis EAL4 verwendet. Neben den Sicherheitskriterien selbst sorgt eine ebenfalls international abgestimmte Methodologie („Common Methodology for Information Security Evaluation“ (CEM)) dafür, dass Prüfungen in vergleichbarer Weise durchgeführt werden.

Die Common Criteria liegt aktuell in der Version 3.1 vor und und ist als ISO 15408 international akzeptiert. Die CC sind eine Weiterentwicklung und Harmonisierung der europäischen „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)“, des „Orange-Book (TCSEC)“ der USA und der kanadischen Kriterien (CTCPEC). Die Kompatibilität zu den Vorgängerkriterien ist dabei weitgehend erhalten geblieben, der Informationsgehalt und die Flexibilität sind in den CC jedoch deutlich höher. Das BSI nimmt im internationalen Umfeld die Rolle des deutschen Partners bei der Erarbeitung und Fortentwicklung der Kriterien ein.

Die Kriterien und weitere Informationen dazu finden sich auf www.commoncriteriaportal.org bzw. www.bsi.bund.de.

4.2 Nutzen eines zertifizierten Produktes für den Anwender

Bereits eine Zertifizierung auf der untersten Stufe EAL1 nach den Common Criteria ist eine wertvolle Aussage hinsichtlich der Sicherheit des eingesetzten Produktes, die weit über die gängigen

Produkttests hinausgeht. Bei einem zertifizierten Produkt ist gewährleistet, dass eine vom Hersteller unabhängige Stelle das Produkt begutachtet hat. Mit Hilfe des Zertifizierungsreports und der zugehörigen Sicherheitsvorgabe kann ein Anwender oder Betreiber über die Einbindung eines zertifizierten Produktes in sein System- und Sicherheitskonzept entscheiden.

Das BSI-Sicherheitszertifikat macht Informationstechnik in ihrer Sicherheitsleistung:

» **transparent** durch die exakte Beschreibung der Sicherheitsleistung des IT-Produktes in Verbindung mit den abzuwehrenden Bedrohungen und einer Bewertung, die angibt, wie stark die Sicherheitsfunktionen sich diesen Bedrohungen widersetzen.

» **vertrauenswürdig** durch die Prüfung der Aspekte wie Vertraulichkeit, Integrität und Verfügbarkeit vom Entwurf über die Produktion und die Auslieferung bis zum Einsatz des IT-Produktes.

» **sachgemäß** nutzbar durch eine die Handbücher ergänzende Beschreibung der Administration und der Einsatzumgebung, um das Produkt in einer sicheren Konfiguration zu betreiben.

4.3 Hinweise für den Hersteller für die Zertifizierung eines Produktes

Ein Sicherheitszertifikat hat für den Hersteller oder Vertreiber des zertifizierten Produktes viele Vorteile:

» Internationale Marktchancen angesichts des steigenden Sicherheitsbewusstseins der Anwender kann der Nachweis von unabhängiger Stelle erbracht werden, dass das Produkt die im Zertifikat definierte Sicherheitsleistung erfüllt. Vereinbarungen mit anderen Staaten zur gegenseitigen Anerkennung von Zertifikaten eröffnen einen Zugang zu internationalen Märkten.

» Steigerung der Produktqualität Die Common Criteria (CC) schreiben die Prüfung aller Aspekte vom Entwurf über die Produktion bis zur Auslieferung und zum Einsatz des Produktes vor.

4.4 Das Verfahren

Die Zertifizierung eines Produktes wird auf Veranlassung des Herstellers oder eines Vertreibers durchgeführt. Bestandteil des Zertifizierungsverfahrens ist die technische Prüfung (Evaluierung) des Produktes gemäß den Common Criteria. Diese Prüfung wird von einer vom BSI anerkannten Prüfstelle durchgeführt, die der Antragsteller aus der Liste der vom BSI anerkannten Prüfstellen wählen kann.

Die Sicherheitskriterien stellen detaillierte Prüfanforderungen unter anderem an das IT-Produkt, die Entwicklung, die Entwicklungsumgebung, die Anwenderdokumentation, die Auslieferung und den Betrieb. Ziel der Evaluierung ist es, die Fähigkeit der Sicherheitsfunktionen eines IT-Produktes, den betrachteten Bedrohungen zu widerstehen, zu bestätigen.

Jede Evaluierung wird mit dem Ziel, eine einheitliche Vorgehensweise und Methodik sicherzustellen, von Mitarbeitern der Zertifizierungsstelle begleitet. Die Dauer eines Zertifizierungsverfahrens ist abhängig von der Komplexität des Produktes und von der gewählten Prüftiefe (EAL-Stufe).

Das Ergebnis des Zertifizierungsverfahrens wird in einem Zertifizierungsreport festgehalten. Dieser enthält unter anderem das Sicherheitszertifikat und den detaillierten Zertifizierungsbericht mit Einzelheiten zur Bewertung sowie Hinweisen und ggf. Auflagen für den Anwender.

Am Zertifizierungsprozess sind drei Parteien beteiligt

Der Antragsteller/Hersteller

» wählt eine Prüfstelle aus und

» beantragt die Zertifizierung bei der Zertifizierungsstelle des BSI,

» stellt das zu zertifizierende Produkt mit den erforderlichen Nachweisen bereit,

» erhält nach erfolgreichem Abschluss des Verfahrens den Zertifizierungsreport mit dem BSI-Sicherheitszertifikat.

Die Prüfstelle

» prüft das Produkt nach Maßgabe der technischen Regelwerke und

» übergibt die Prüfresultate an die BSI-Zertifizierungsstelle und den Hersteller.

Die BSI-Zertifizierungsstelle

» berät den Hersteller zu allen Fragen der Zertifizierung,

» unterstützt ihn bei der Erarbeitung der Sicherheitsvorgaben,

» begleitet jede bei einer Prüfstelle stattfindende Prüfung,

» erteilt nach Abnahme der Evaluierung das Zertifikat, erstellt den Zertifizierungsreport und

» veröffentlicht, sofern der Hersteller damit einverstanden ist, den Zertifizierungsreport mit Zertifikat auf den Internetseiten des BSI.

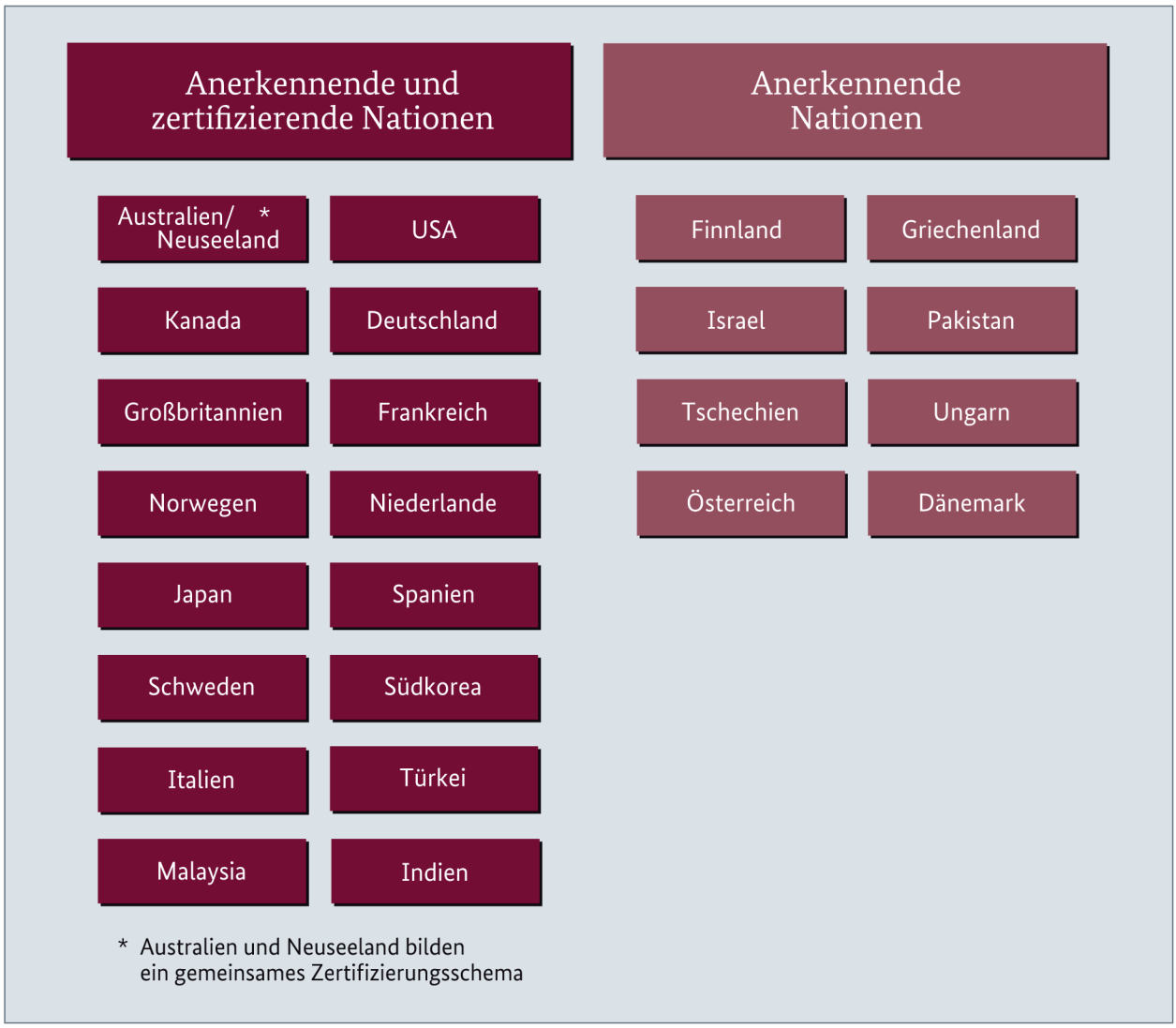
4.5 Internationale Anerkennung

Um die Mehrfachzertifizierung des gleichen Produktes in verschiedenen Staaten zu vermeiden, wurde eine gegenseitige Anerkennung von Informationssicherheitszertifikaten – sofern sie auf den Common Criteria (CC) beruhen – unter bestimmten Voraussetzungen vereinbart (CCRA) und September 2014 erneuert. Zertifikate, die unter diese Vereinbarung fallen, sind entsprechend mit einem spezifischen Logo gekennzeichnet. Diese Anerkennungsvereinbarung gilt bis einschließlich der Evaluierungsstufe EAL2 bzw. bei Verwendung von speziellen Schutzprofilen bis einschließlich EAL4. Die aktuelle Liste der Unterzeichnerstaaten kann unter www.commoncriteriaportal.org eingesehen werden. Anfang 2016 waren nationale Zertifizierungsstellen von 15 Nationen und darüber hinaus 10 anerkennende Nationen dem Abkommen beigetreten.

Im April 2010 ist das neue SOGIS-Abkommen (Senior Officials Group Information System Security) zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten in Europa in Kraft getreten.

Mit diesem Abkommen ist eine Anerkennung von Zertifikaten für IT-Produkte auf Basis der Common Criteria bzw. ITSEC (Europäische Vorgängerkritieren) bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 bzw. E3 (niedrig) verbunden. Anerkannte Zertifizierungsstellen hierfür sind seit Anfang 2016 die nationalen Stellen aus Deutschland, Frankreich, Großbritannien, den Niederlanden, Spanien, Italien, Norwegen und Schweden.

Darüber hinaus ist eine höherwertige Anerkennung (höher als EAL4 bzw. E3 (niedrig)) für bestimmte technische Bereiche (sog. „Technical Domains“) unter besonderen Rahmenbedingungen vorgesehen. Im Abkommen wurde dazu der technische Bereich „Smart cards and similar devices“ definiert. Anerkannte Zertifizierungsstellen hierfür sind Anfang 2016 die nationalen Stellen aus Deutschland, Frankreich, Großbritannien, den Niederlanden und Spanien. Darüber hinaus existiert der technische Bereich „Hardware Devices with Security Boxes“, für den Deutschland, Frank-



reich, Großbritannien und Spanien anerkannte Zertifizierungsstellen sind.

Mit diesem Abkommen wurde die Basis geschaffen, um das bis dahin lediglich auf Frankreich, Deutschland, Großbritannien und die Niederlande beschränkte Abkommen von 1999 für alle Mitgliedsstaaten der EU zu öffnen.

Im Management-Komitee ist geplant, weitere EU-Staaten in das Abkommen aufzunehmen. Die aktuellen Unterzeichner sind unter www.sogis.eu zu finden.

4.6 Gültigkeit eines Zertifikats nach CC

Das Zertifikat bezieht sich jeweils nur auf die zertifizierte Version des Produktes. Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung und ist mit einer – der Technologie entsprechenden – Gültigkeitsdauer befristet. Da Angriffe mit neuen oder weiterentwickelten Methoden in Zukunft denkbar sind, besteht die Möglichkeit, die Widerstandsfähigkeit des Produktes im Rahmen des Assurance Continuity-Programms des BSI regelmäßig überprüfen zu lassen. Die Zertifizierungsstelle empfiehlt, regelmäßig eine Einschätzung der Widerstandsfähigkeit vornehmen zu lassen.

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller die Aufrechterhaltung der Vertrauenswürdigkeit (d. h. eine Re-Zertifizierung oder ein Maintenanceverfahren) in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Schwächen aufdeckt.

5 Zertifizierungsbeispiele

5 Zertifizierungsbeispiele

Hoheitliche Dokumente & elektronische Ausweise

Das BSI ist an der Pilotierung und Umsetzung neuer Technologien und der Erstellung von Spezifikationen für elektronische Ausweisdokumente wie den neuen elektronischen Personalausweis (nPA), den elektronischen Reisepass (ePass) und den elektronischen Aufenthaltstitel (eAT) maßgeblich beteiligt.

Elektronische Ausweisdokumente unterscheiden sich dadurch von den bisher gängigen Ausweisdokumenten, dass im Dokument ein elektronischer Chip integriert ist, auf welchem die persönlichen Daten des Ausweisinhabers zusätzlich in sicherer elektronischer Form gespeichert sind.

Antragsdatenerfassung für hoheitliche Dokumente

Um die internationale Lesbarkeit elektronischer Ausweisdokumente zu gewährleisten, müssen die Daten des Ausweisinhabers dort in einheitlicher Form gespeichert werden. Insbesondere die biometrischen Sicherheitsmerkmale – Gesichtsbild und Fingerabdrücke – müssen in hinreichender Qualität vorliegen, um einen zuverlässigen Abgleich z.B. im Rahmen von Grenzkontrollen zu ermöglichen.

Um dies sicherzustellen, schreiben Passgesetz (PassG), Personalausweisgesetz (PAuswG) und deren Verordnungen vor, dass sämtliche zur Antragsdatenerfassung für hoheitliche Dokumente eingesetzte Komponenten über eine BSI-Zertifizierung nach Technischen Richtlinien verfügen müssen. Die Technischen Richtlinien des BSI definieren hierzu u.a. ein einheitliches xml-basiertes Datenformat (xhD) sowie Qualitätsanforderungen für die in den Ausweisdokumenten gespeicherten biometrischen Merkmale.

Chipkartenleser mit nPA Unterstützung

Die wichtigste Anforderung an einen Chipkartenleser ist der fehlerfreie, störungsfreie und zuverlässige Betrieb sowie die Unversehrtheit der Chipkarten. Ebenso muss auch die Informationssicherheit berücksichtigt werden, um die Vertraulichkeit und die Integrität der Abläufe und der Kommunikation gewährleisten zu können.

Eine Zertifizierung nach der Technischen Richtlinie BSI TR-03119 dient vorrangig als Nachweis der Eignung eines Chipkartenlesers zur Verwendung mit dem neuen Personalausweis (nPA), aber auch für die Nutzung im Rahmen weiterer Kartenprojekte des Bundes (z.B. eGK) oder anderen nicht-hoheitliche Anwendungen.

Mainframe-Betriebssysteme

Das BSI zertifiziert im Umfeld der Mainframe-Systeme seit mehreren Jahren sowohl Software,

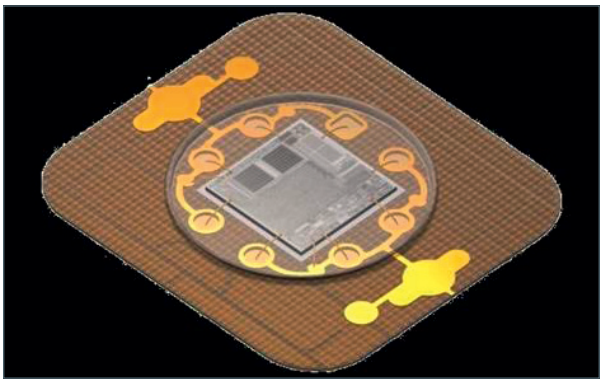
die zur physikalischen Partitionierung dieser Systeme verwendet wird als auch das zum Einsatz kommende Betriebssysteme. Die Prüfstufe nach Common Criteria liegt hier typischerweise bei EAL4 oder höher.

Virtuelle Poststelle

Die Produkte einer Virtuellen Poststelle (VPS) ermöglichen an zentraler Stelle in einer Organisation kryptografische Dienste, wie die Ver- und Entschlüsselung von Daten, die Erzeugung und Prüfung von elektronischen Signaturen, die Einholung und Prüfung von kryptografischen Zeitstempeln, sowie die Abwicklung eines Arbeitsablauf über entsprechende Schnittstellen zur Verfügung zu stellen. Die Produkte werden in wesentlichen Teilen nach der Common Criteria Prüfstufe EAL3+ zertifiziert und entsprechend nach dem Signaturgesetz bestätigt.

Smartcard Controller und Smartcard Anwendungen

Produkte der Familie der Smartcard Controller werden seit vielen Jahren nach Common Criteria bis zur Stufe EAL5+ zertifiziert. Die Produkte finden Verwendung in zertifizierten Bankkarten, hoheitlichen Dokumenten, Gesundheitskarten, etc. – Der sogenannten Kompositionszertifizierung kommt dabei eine besondere Bedeutung zu. Bei dieser wird eine Zertifizierung eines Kartenbetriebssystems inklusive einer oder mehrerer Applikationen (z. B. Gesundheitskarte) auf einem bereits zertifizierten Smartcard Controller durchgeführt.



Weitere Produkttypen im Rahmen der Zertifizierung sind z. B.:

» Firewall-Produkte

» Mailserver

» Datenbankserver

» Biometrische Verifikationssysteme

» Datenübertragungsprodukte

» Signaturanwendungskomponenten

» Produkte des Digitalen Tachographen

» Betriebssysteme für Server mittlerer Systeme

» PC-Sicherheitsoberflächen

» Signaturkarten für die qualifizierte elektronischeSignatur

» Gesundheitskarten

» Chipkarten-Lesegeräte z. B. für Gesundheitskarten

» Hardware-Sicherheitsmodule (HSM)

6 Konformitätsprüfung

6 Konformitätsprüfung

Konformitätsprüfungen werden im Bereich von IT-Produkten und Europäischen Bürgerinitiativen (EBI) auf Antrag durchgeführt. Hierbei werden IT-Produkte und Online-Sammelsystem (OCS) auf die Erfüllung von festgelegten Standards oder anderer definierter Kriterien untersucht. Darüber hinaus werden auch Managementsysteme nach Technischen Richtlinien zertifiziert.

6.1 Zertifizierung von Produkten und Managementsystemen nach Technischen Richtlinien

Die Konformität eines IT-Produkts zu einer Technischen Richtlinie kann vom BSI mit einem Zertifikat bestätigt werden.

Um ein Zertifikat zu erhalten, stellt der Hersteller oder ein Vertreiber beim BSI einen Zertifizierungsantrag und beauftragt anschließend eine vom BSI anerkannte Prüfstelle mit der Konformitätsprüfung des Produkts.

Im Rahmen der Konformitätsprüfung wird sichergestellt, dass das Produkt die in der jeweiligen Technischen Richtlinie festgelegten Vorgaben und Anforderungen erfüllt.

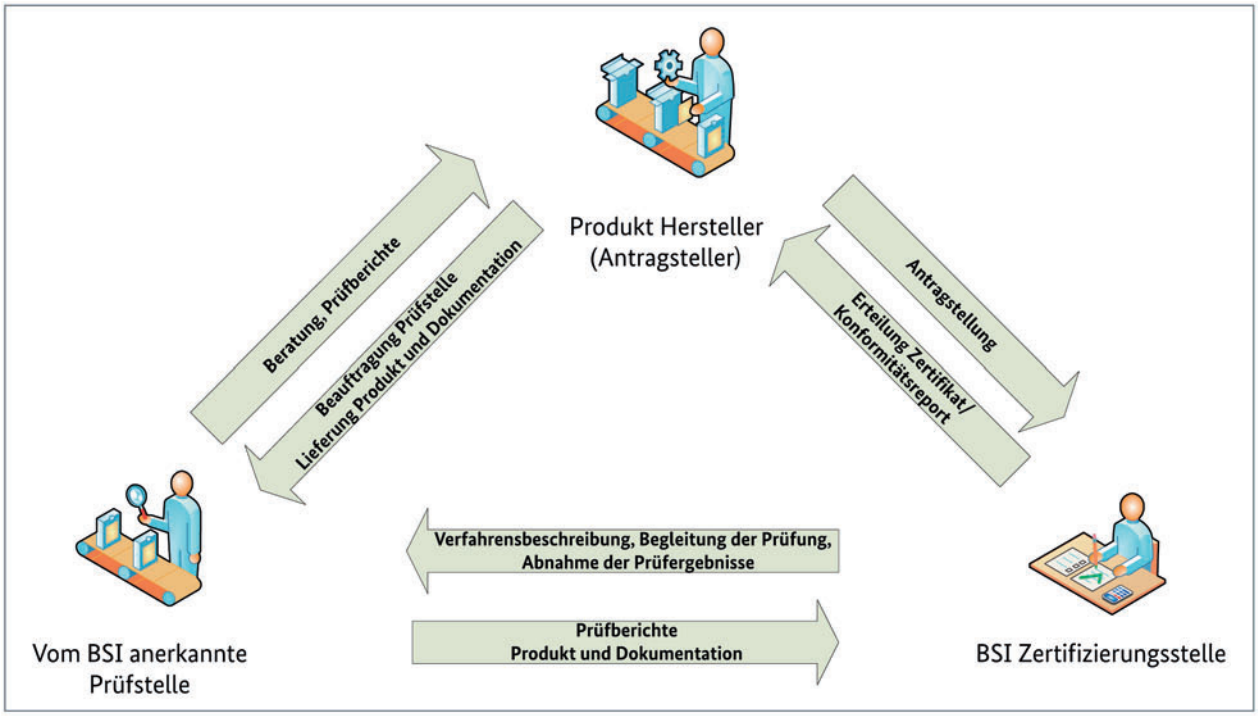
Die Ergebnisse der Konformitätsprüfung werden von der Prüfstelle in einem Prüfbericht zusammengefasst, auf dessen Grundlage das BSI eine Zertifizierungsentscheidung trifft.

Neben der Zertifizierung von Produkten kann in bestimmten Prüfbereichen auch die Konformität von Managementsystemen zu Technischen Richtlinien vom BSI mit einem Zertifikat bestätigt werden. Das Verfahren entspricht weitestgehend dem der Produktzertifizierung nach Technischen Richtlinien und ist im Detail auf der Internetseite des BSI unter www.bsi.bund.de/zertifizierungtr dokumentiert.

Nutzen

Hersteller, die für ihre Produkte beim BSI ein Zertifikat beantragen, profitieren von der hohen Qualität der Prüfung und erhalten einen Konformitätsnachweis durch eine neutrale, behördliche Stelle.

Eine Zertifizierung nach Technischen Richtlinien steigert den Marktwert eines Produktes und kann



einem Hersteller entscheidende Vorteile gegenüber konkurrierenden Anbietern sichern, die nicht über ein derartiges Gütesiegel verfügen.

In verschiedenen hoheitlichen Anwendungsbereichen der Bundesrepublik Deutschland ist ein Zertifikat nach Technischen Richtlinien Grundvoraussetzung für den Markteintritt.

Prüfbereiche

Konformitätsprüfungen von Produkten mit dem Ziel der Zertifizierung durch das BSI können in verschiedenen Prüfbereichen durchgeführt werden. Hierzu zählen u.a.:

» BSI TR-03105 – Prüfung elektronischer Ausweisdokumente (ePass/nPA/eAT) sowie Lesegeräte und Inspektionssysteme für elektronsiche Ausweisdokumente (z.B. nPA-Änderungsterminal)

» BSI TR-03119 – Prüfung von nPA-Chipkartenlesern

» BSI TR-03121 – Prüfung von Hardware- und Softwarekomponenten zur Erfassung und Qualitätssicherung der biometrischen Merkmale für elektronsiche Ausweisdokumente (Fingerabdruckscanner, Enrollment-Terminals, QS-Software)

Konformitätsprüfungen von Managementsystemen mit dem Ziel der Zertifizierung durch das BSI können derzeit im folgenden Bereich durchgeführt werden:

» BSI TR-03145 – Secure CA Operation

Weitere Informationen zum Zertifizierungsverfahren nach Technischen Richtlinien sind auf der Internetseite des BSI unter www.bsi.bund.de/zertifizierungtr veröffentlicht.

6.2 Zertifizierung von Managementsystemen: ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz

Informationssicherheit ist ein Prozess, der durch die Leitungsebene einer Behörde oder eines Unternehmens gesteuert werden muss. Mit dem Zertifikat „ISO 27001 auf der Basis von IT-Grundschutz“ können Institutionen nachweisen, dass sie ein effizientes und effektives Informationssicherheitsmanagementsystem betreiben. Dies zeigt nicht nur in der Institution den Stellenwert der Informationssicherheit, sondern erhöht auch gegenüber anderen Institutionen das Vertrauen in die eigene Zuverlässigkeit. Ein solches Zertifikat wird zunehmend auch in Ausschreibungen gefordert. Daneben ist das Zertifikat ISO 27001 auf der Basis von IT-Grundschutz Voraussetzung für die Akkreditierung von DE-Mail Anbietern.

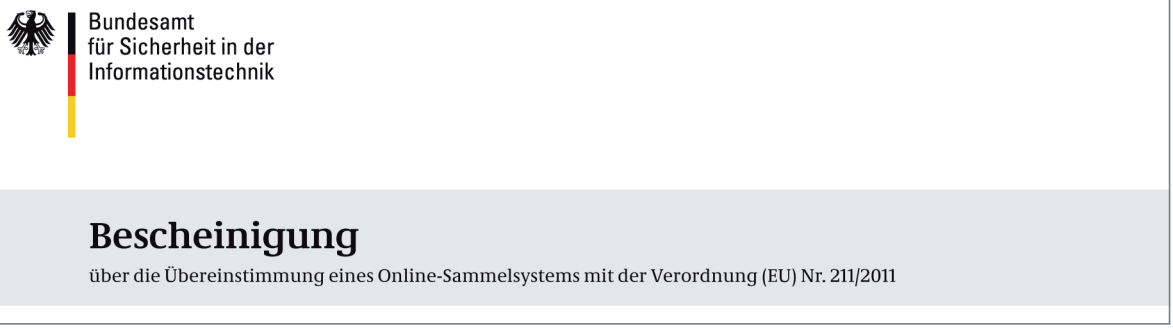
Die IT-Grundschutz-Vorgehensweise stellt zusammen mit den IT-Grundschutz-Katalogen und dessen Empfehlungen von Standard-Sicherheitsmaßnahmen inzwischen einen De-Facto-Standard für Informationssicherheit dar. Der Wunsch vieler Institutionen nach einer Bestätigung, dass IT-Grundschutz umgesetzt wurde, führte zur Einführung der Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz. Die Zertifizierung umfasst dabei sowohl eine Prüfung des Managementsystems für Informationssicherheit als auch der konkreten Umsetzung von Sicherheitsmaßnahmen auf der Basis von IT-Grundschutz.

6.2.1 Überblick über den Zertifizierungsprozess

Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung des Untersuchungsgegenstandes durch einen vom BSI zertifizierten Auditor. Von diesem werden im Rahmen eines Audits von der Institution erstellte Referenzdokumente gesichtet, eine Vor-Ort-Prüfung durchgeführt und ein Auditbericht erstellt. Für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz wird dieser Auditbericht von der Zertifizierungsstelle im BSI geprüft. Das erlangte Zertifikat ist drei Jahre gültig. Mit jährlichen Überwachungsaudits wird geprüft, dass das Sicherheitsniveau aufrechterhalten bleibt.

6.2.2 Was sagt ein Zertifikat „ISO 27001 auf der Basis von IT-Grundschutz“ aus?

Durch ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz wird nachgewiesen, dass der betrachtete Informationsverbund bzw. das Sicherheitsmanagementsystem die Anforderungen nach



ISO/IEC 27001 erfüllt und Anforderungen der IT-Grundschutz-Methodik erfolgreich umgesetzt worden sind. Darüber hinaus zeigt ein Zertifikat auch, dass in der jeweiligen Institution

» Informationssicherheit ein anerkannter Wert ist,

» ein Sicherheitsmanagement vorhanden ist und außerdem

» zu einem bestimmten Zeitpunkt ein definiertes Sicherheitsniveau erreicht wurde.

Das BSI bietet an, die Tatsache der Zertifizierung auf dem BSI-Webserver zu veröffentlichen. Eine aktuelle Liste aller erteilten Zertifikate, bei denen einer Veröffentlichung zugestimmt wurde, finden Sie unter:

https://www.bsi.bund.de/iso27001-zertifikate.html

6.3 Europäische Bürgerinitiative

Mit der Europäischen Bürgerinitiative (EBI) wurde zum 01. April 2012 ein neues Instrument der partizipativen Demokratie eingeführt, welches EU-Bürgerinnen und -Bürgern eine Mitsprache bei Gesetzgebungsvorhaben der Europäischen Union ermöglicht. Mit einer erfolgreichen Bürgerinitiative können sie die Europäische Kommission auffordern, Rechtsakte in Bereichen vorzuschlagen, die in die Zuständigkeit der EU fallen. Hierzu muss eine EBI jedoch zunächst von mindestens einer Million wahlberechtigter EU-Bürgerinnen und -Bürger unterstützt werden.

Für die Sammlung von Unterstützungsbekundungen sind die Organisatoren einer EBI verantwortlich. Die Sammlung kann dabei nicht nur klassisch in Papierform, sondern auch mit Hilfe eines Online-Sammelsystems (engl.: online collection system, OCS) über das Internet erfolgen.

Da Online-Sammelsysteme über die Laufzeit einer EBI personenbezogene Daten von über einer Million EU-Bürgerinnen und -Bürgern enthalten können, muss ein besonderes Augenmerk auf den Datenschutz und die Datensicherheit gelegt werden. Entscheiden sich Organisatoren für die Nutzung eines OCS, müssen sie sicherstellen, dass die von ihnen betriebenen Systeme über angemessene Sicherheitsmerkmale verfügen. Diese sind in der Verordnung (EU) Nr. 211/2011 (EBI-VO) und den Technischen Spezifikationen für Online-Sammelsysteme (Durchführungsverordnung (EU) Nr. 1179/2011) festgelegt.

Gemäß EBI-VO müssen EBI-Organisatoren, bevor sie mit der Online-Sammlung beginnen, von den jeweils zuständigen Behörden der EU-Mitgliedstaaten eine „Bescheinigung über die Übereinstimmung eines Online-Sammelsystems mit der Verordnung (EU) Nr. 211/2011“ als Konformitätsnachweis erhalten.

Entsprechende Bescheinigungen können in Deutschland beim BSI beantragt werden.

Eine detaillierte Beschreibung des Bescheinigungsverfahrens sowie weiterführende Informationen zur Europäischen Bürgerinitiative, Online-Sammelsystemen, usw. sind auf der Internetseite des BSI unter www.bsi.bund.de/ebi veröffentlicht.

7 Akkreditierung von De-Mail-Diensteanbietern

7 Akkreditierung von De-Mail-Diensteanbietern

Auf der Grundlage des „Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften“ (De-Mail-Gesetz) können künftig De-Mail-Dienste angeboten werden.

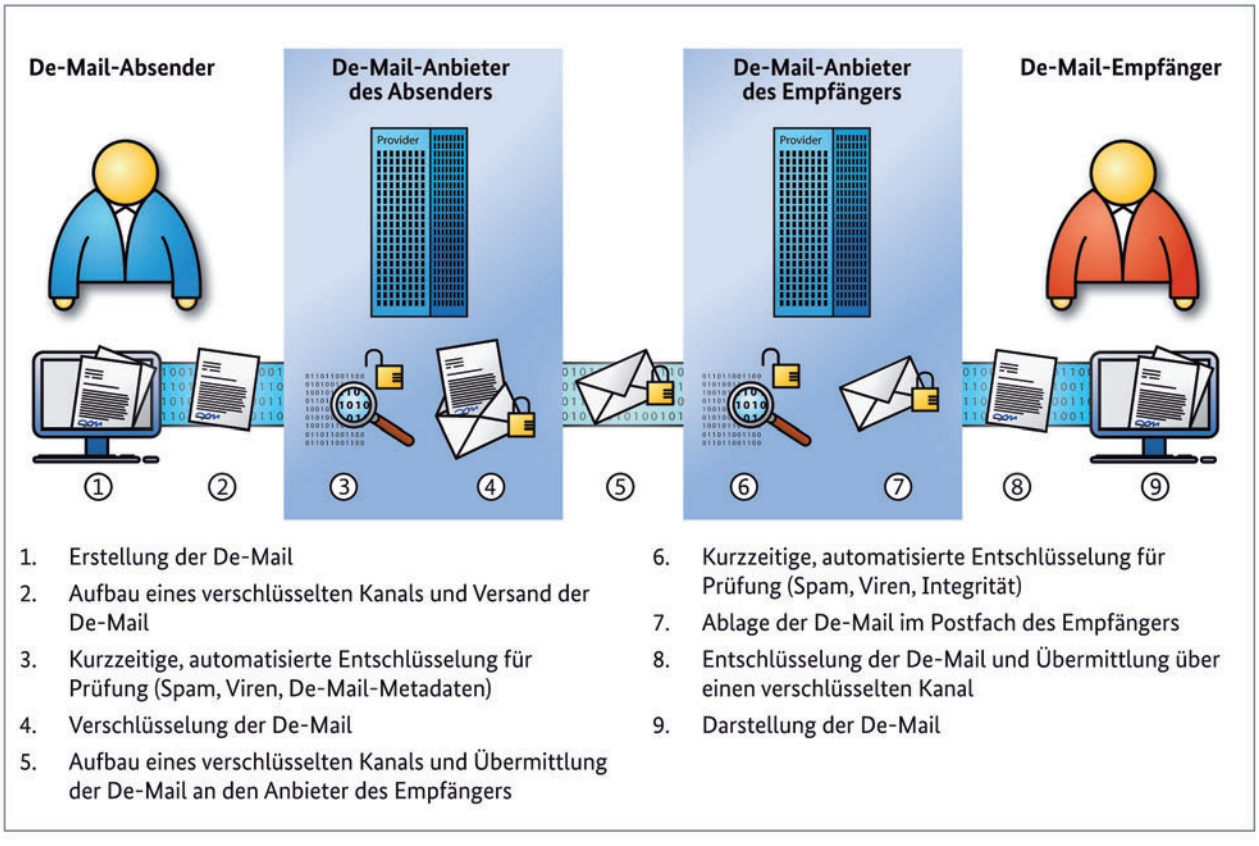
Mit De-Mail-Diensten wird der verbindliche und vertrauliche Versand elektronischer Dokumente und Nachrichten deutlich einfacher sein als bisher. In der Handhabung gleichen De-Mails den herkömmlichen E-Mails, verfügen jedoch über wichtige Eigenschaften, die der E-Mail fehlen:

» Die Identitäten von Absender und Adressat können eindeutig nachgewiesen und nicht gefälscht werden.

» Die Nachrichten werden ausschließlich über verschlüsselte Kanäle übertragen und verschlüsselt abgelegt. Sie sind für Unbefugte zu keiner Zeit zugänglich und können weder mitgelesen, noch verändert werden.

Mit De-Mail sparen Sie Zeit und Geld für den Versand oder gar die persönliche Überbringung von gedruckten Unterlagen. Sie nutzen die Schnelligkeit der E-Mail in Verbindung mit der Sicherheit eines Briefes und der Nachweisbarkeit eines Einschreibens.

Diese Vorzüge werden möglich, weil De-Mail eine gesetzliche Grundlage hat und die Anbieter von De-Mail-Diensten strenge Auflagen erfüllen müssen, um die erforderliche Akkreditierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu erhalten. Zudem müssen sie eine gültige Datenschutzprüfung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) vorweisen. Auch



De-Mails sind auf ihrem Weg durch das Internet geschützt.

nach der Akkreditierung müssen Anbieter von De-Mail-Diensten ihre Prozesse und Systeme regelmäßig von unabhängigen Prüfstellen kontrollieren lassen. Auf diese Weise wird sichergestellt, dass alle technischen und organisatorischen Vorgaben, u. a. zum Schutz der Daten vor dem Zugriff Unbefugter, jederzeit erfüllt werden.

Eine aktuelle Liste der akkreditierten De-Mail-Diensteanbieter ist unter www.bsi.bund.de veröffentlicht.

7.1 Testat Funktionalität / Interoperabilität als Voraussetzung einer De-Mail-Akkreditierung

Im Rahmen der Akkreditierung müssen zukünftige De-Mail Diensteanbieter durch die Vorlage von Testaten nachweisen, dass ihre Systeme die Anforderungen der BSI TR-01201 (TR De-Mail) hinsichtlich Funktionalität und Interoperabilität für die angebotenen Dienste erfüllen.

Grundlage für den Erhalt dieser Testate ist eine erfolgreich absolvierte Konformitätsprüfung gemäß TR De-Mail. Konformitätsprüfungen zur Bestätigung der Interoperabilität und Funktionalität nach TR De-Mail werden von anerkannten De-Mail-Prüfstellen durchgeführt.

Der Ablauf eines Testierungsverfahren beim BSI ist identisch zum Zertifizierungsverfahren nach Technischen Richtlinien. Ein vom BSI erteiltes Zertifikat nach TR De-Mail wird somit auch als „Testat Funktionalität / Interoperabilität“ anerkannt.

Weitere Informationen zum Zertifizierungsverfahren nach Technischen Richtlinien sind auf der Internetseite des BSI unter www.bsi.bund.de/zertifizierungtr veröffentlicht.

7.2 Testat Informationssicherheit als Voraussetzung einer De-Mail-Akkreditierung

De-Mail-Dienstanbieter müssen gemäß De-Mail-Gesetz ein „Testat Informationssicherheit“ nachweisen.

Ein für den Informationsverbund des DMDA erteiltes ISO 27001-Zertifikat auf der Basis von IT-Grundschutz wird als „Testat Informationssicherheit“ anerkannt.

Weitere Informationen zur ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz sind auf der Internetseite des BSI unter www.bsi.bund.de veröffentlicht.

8 Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern

8 Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern

Das Bundesamt für Sicherheit in der Informationstechnik führt im Bereich der **Konformitätsbewertung** Anerkennungen von Prüfstellen und Zertifizierungen von IT-Sicherheitsdienstleistern auf Grundlage des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG) vom 19. August 2009 durch.

Ziel der Anerkennung bzw. Zertifizierung durch das BSI ist die Sicherstellung der Qualität und Vergleichbarkeit der Konzepte, Vorgehensweisen und Arbeitsergebnisse der Stellen.

Die Anerkennung bzw. Zertifizierung beim BSI erfolgt für den jeweils beantragten Geltungsbereich. Neben der nachgewiesenen Fachkompetenz für den beantragten Geltungsbereich ist die Grundvoraussetzung für die Anerkennung bzw. Zertifizierung die Umsetzung und Aufrechterhaltung der Norm DIN EN ISO/IEC 17025 „Allgemeine Anforderungen an die Kompetenz von Prüf- oder Kalibrierlaboratorien“ bezogen auf den jeweiligen Geltungsbereich.

Die Anerkennung bzw. Zertifizierung für den beantragten Bereich erfolgt nach positiver Anerkennungs- bzw. Zertifizierungsentscheidung, wenn in den Begutachtungen der Anforderungen an das Management sowie der technischen und fachlichen Anforderungen festgestellt wurde, dass alle Voraussetzungen erfüllt sind.

Eine Anerkennung gem. § 9 Abs. 6 und 3 BSIG kann für die im Programm aufgeführten Bereiche erfolgen, z.B. als Prüfstelle für IT-Sicherheit nach allgemein anerkannten Sicherheitskriterien (Common Criteria (CC)):

Eine Prüfstelle für IT-Sicherheit prüft und bewertet Produkte, die ein IT-Sicherheitszertifikat erhalten sollen. Die Zertifizierungsstelle des BSI erteilt nach positiver Prüfung durch die Prüfstelle ein Produktzertifikat.

8.1 Prüfstelle für IT-Konformität nach Technischen Richtlinien (TR)

Eine Prüfstelle für IT-Konformität prüft und bewertet Produkte, die ein Zertifikat nach TR erhalten sollen. Die Zertifizierungsstelle des BSI bestätigt auf Basis der Prüfberichte der Prüfstelle die Konformität und erteilt ein Produktzertifikat.

8.2 IT-Sicherheitsdienstleister für den Digitalfunk BOS

Eine Zertifizierung gem. § 9 Abs. 5 und 2 BSIG als zertifizierter IT-Sicherheitsdienstleister kann für die im Programm aufgeführten Bereiche erfolgen, z. B. als IT-Sicherheitsdienstleister im Digitalfunk BOS:

Ein IT-Sicherheitsdienstleister im Digitalfunk BOS (Behörden und Organisationen mit Sicherheitsaufgaben) prüft und bewertet Produkte (Funkgeräte und Leitstellen), die ein Zertifikat nach den BOS-Interoperabiliätsrichtlinien erhalten sollen. Die Zertifizierungsstelle des BDBOS (Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben) erteilt nach positiver Prüfung ein Produktzertifikat.

8.3 IT-Sicherheitsdienstleister im Bereich IS-Revision und IS-Beratung sowie Penetrationstests

Benötigt eine Behörde externen Sachverstand, um ein IT-Sicherheitskonzept zu erstellen, umzusetzen und zu überprüfen, kann sie auf einen IT-Sicherheitsdienstleister zurückgreifen. Das BSI zertifiziert vertrauenswürdige und kompetente IT-Sicherheitsdienstleister – insbesondere zur Durchführung von qualifizierten Informationssicherheitsrevisionen (IS-Revisionen) und Penetrationstests.

8.4 IT-Sicherheitsdienstleister im Bereich Lauschabwehr (im Bereich der Wirtschaft)

Zertifiziert werden können private Anbieter von Lauschabwehr-Dienstleistungen, die nach Einschätzung des BSI die Gewähr dafür bieten, Lauschabwehrprüfungen sowohl fachlich mit der erforderlichen Qualität als auch mit der nötigen Unabhängigkeit und Zuverlässigkeit durchzuführen.

8.5 Verfahrensablauf zur Anerkennung einer Prüfstelle bzw. Zertifizierung eines IT-Sicherheitsdienstleisters

Das Verfahren beginnt in der Antragsphase mit einem Informationsgespräch sowie der Antragsstellung und -prüfung für den betreffenden Geltungsbereich.

Die Begutachtungsphase dient der Vorbereitung der Anerkennungs- bzw. Zertifizierungsentscheidung, die auf Grundlage der Begutachtungsergebnisse in den Berichten zu System- und Fachbegutachtungen getroffen wird.

Innerhalb der Anerkennungs- bzw. Zertifizierungsdauer (3 Jahre) werden zwei Begutachtungen zur Systemförderung durchgeführt.

Stellt das BSI einen Verstoß gegen Verfahrensbeschreibungen oder Richtlinien fest oder weist die Stelle insbesondere erhebliche Kompetenzmängel auf, kann das BSI in einer Mahnphase die Aussetzung der Anerkennung bzw. Zertifizierung aussprechen und danach aufheben. Weitergehende Informationen zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern sind im Dokument „Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern“ zu finden.

Eine Liste der beim BSI anerkannten Prüfstellen und zertifizierten IT-Sicherheitsdienstleistern ist unter www.bsi.bund.de veröffentlicht.

9 Zertifizierung von Personen

9 Zertifizierung von Personen

Das Bundesamt für Sicherheit in der Informationstechnik führt im Bereich der Konformitätsbewertung Zertifizierungen von Personen auf Grundlage des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG § 9) durch.

Zur Durchführung von Evaluierungen und Prüfungen zum Zwecke der Zertifizierung von Produkten und Managementsystemen sowie zur Unterstützung des BSI und anderer Behörden wie bspw. der BDBOS im Bereich IT-Sicherheitsdienstleistungen werden qualifizierte Personen benötigt, deren Kompetenz durch die Personenzertifizierungsstelle des BSI für den entsprechenden Geltungsbereich festgestellt wurde. Für einige Geltungsbereiche wird der Person dann auf Antrag eine Personenzertifizierung ausgesprochen. Das Verfahren ist ausschließlich natürlichen Personen vorbehalten.

Ziel der Zertifizierung von Personen durch das BSI ist die Sicherstellung der Qualität und Vergleichbarkeit der Arbeitsergebnisse dieser Personen.

Für die Zertifizierung müssen diese Personen ihre Fachkompetenz nachweisen. Nach erfolgreichem Abschluss sind sie zur Durchführung von Evaluierungen und Prüfungen bzw. von Dienstleistungen im entsprechenden Bereich autorisiert.

Eine Zertifizierung kann für die im Zertifizierungsprogramm aufgeführten Bereiche erfolgen, z. B. als

» Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz
Befähigung zur Durchführung von Audits für Organisationen, die ein Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz erhalten und aufrecht erhalten wollen.

» Auditor De-Mail
Befähigung zur Durchführung von Audits bei Organisationen, die als De-Mail-Diensteanbietern (DMDA) akkreditiert werden wollen bzw., diese Akkreditierung aufrecht erhalten wollen.

» IS-Revisions- und IS-Beratungs-Experte
Befähigung zur Unterstützung von Behörden bei der Erstellung und Umsetzung von Sicherheitskonzepten sowie die regelmäßige Durchführung von IS-Revisionen gemäß dem „Leitfaden für die Informationssicherheitsrevision auf der Basis von IT-Grundschutz“.

» Penetrationstester
Befähigung zur Unterstützung von Bundesbehörden bei der Durchführung von Penetrationstests.

9.1 Verfahrensablauf zur Zertifizierung einer Person

Das Zertifizierungsverfahren beginnt mit der Antragsstellung und -prüfung für den betreffenden Zertifizierungsbereich.

Sind in der Vorbereitungsphase alle Voraussetzungen erfüllt, wird die Person zu einer Schulung eingeladen oder es wird ein Termin für eine Fachbegutachtung abgestimmt, um die Kompetenzanforderungen zu evaluieren (Evaluierungsphase).

Weist die Person erfolgreich die Fachkompetenz im betreffenden Bereich nach, wird ihr abschließend ein Personenzertifikat für 3 Jahre ausgesprochen.

Um während der Gültigkeitsdauer der Zertifizierung die Fachkunde der Person sicherzustellen, wird zum einen über die Tätigkeiten der Person (z. B. durch die Bewertung der Prüf- oder Auditberichte) möglicher Qualifikationsbedarf ermittelt, zum anderen finden jährliche Treffen statt, an denen die Personen verpflichtend teilnehmen müssen. Diese Treffen dienen dem Erfahrungsaustausch, können aber auch zur Behandlung aktueller Entwicklungen und häufiger Fragen bzw. Probleme genutzt werden

Stellt das BSI einen Verstoß der Person gegen Verfahrensbeschreibungen oder Richtlinien fest oder weist diese insbesondere erhebliche Kompetenzmängel auf, kann das BSI in einer Mahnphase die Ausset-

zung der Zertifizierung aussprechen und diese – falls notwendig – danach aufheben.

Weitergehende Informationen zur Zertifizierung von Personen sind im Dokument „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“ zu finden. Eine Liste der beim BSI zertifizierten Personen ist unter www.bsi.bund.de veröffentlicht.

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53175 Bonn
E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de

www.bsi-fuer-buerger.de · www.facebook.com/bsi.fuer.buerger

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53175 Bonn
Telefon: +49 (0) 22899 9582 – 0
Telefax: +49 (0) 22899 9582 – 5400

Stand
Februar 2016

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
60386 Frankfurt am Main

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Artikelnummer
BSI-MIBro16/331