Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierte IT-Sicherheit

Bewährte Säule der Digitalisierung

Vorwort

Liebe Leserin, lieber Leser,

Ihre täglichen Begleiter – Ihr Personalausweis, Reisepass oder Ihre Gesundheitskarte sind zertifiziert nach Sicherheitsvorgaben des BSI.

Seit vielen Jahren gestaltet das BSI den digitalen Wandel, um sichere Informationstechnik in die Geschäftsprozesse von Staat und Wirtschaft zu integrieren.

Das starke Vertrauen nationaler und internationaler Partner in die Transparenz und hohe Fachlichkeit des BSI fußt in seinen langjährigen Aktivitäten bei der Formulierung und Harmonisierung von Sicherheitsvorgaben. Mehr als tausend Zertifizierungsverfahren sowie zahlreiche Standards und Richtlinien des BSI bezeugen dieses Vertrauen.

In diesem Verantwortungsbewusstsein gestaltet das BSI die Herausforderung der Datensouveränität im Cyberraum mittels Sicherheitsvorgaben zur fundierten Planung, Entwicklung und Prüfung sicherer Informationstechnik.

Akteure aus Staat, Wirtschaft und Gesellschaft meistern diese Herausforderung gemeinsam mit dem BSI – heute wie gestern, national und international.

Sie halten mit dieser Broschüre das Lösungsangebot des BSI zur Digitalisierung, Zertifizierung und Standardisierung von Produkten und Dienstleistungen in Ihren Händen – für Ihr Vertrauen in sichere Informationstechnik von morgen.

Arne Schönbohm
Präsident

Bernd Kowalski
Abteilungspräsident
Digitalisierung, Zertifizierung und Standardisierung

Inhaltsverzeichnis


Smart Grid
Industrie 4.0
E-Identity
Automotive
Digitalisierung
Payment
E-Health
Prüfung
IT-Grundschutz
Stellen
Technische Richtlinie
Zertifizierung
Common Criteria
Personen
CCRA
DIN
ISO
Norm
SOGIS
Bundesregierung
Europäische Kommission
Standardisierung

Das BSI im Dienst der Öffentlichkeit im digitalen Raum

Mit seinen 700 Mitarbeiterinnen und Mitarbeitern ist das BSI eine unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Durch die Grundlagenarbeit im Bereich der IT-Sicherheit übernimmt das BSI als nationale IT-Sicherheitsbehörde Verantwortung für unsere Gesellschaft und leistet dadurch einen wichtigen Beitrag zur Inneren Sicherheit in Deutschland.

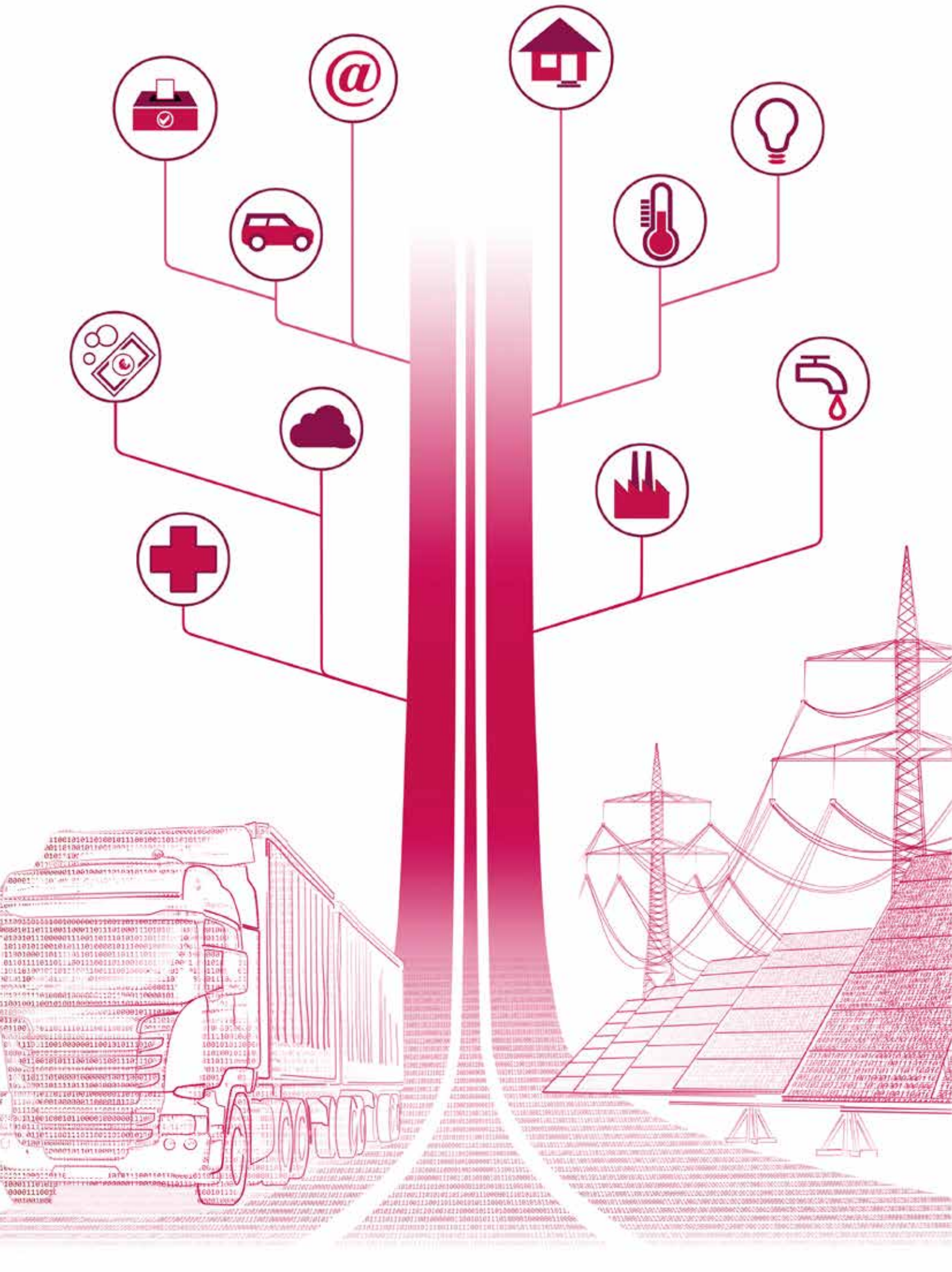
Ziel des BSI ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. Informationssicherheit ist eine wichtige Voraussetzung zur Bewahrung gesellschaftlicher Werte, z.B. der Datensouveränität. Sicherheitsaspekte sollen schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden: „Security by Design".

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

Das BSI hat die Aufgabe, IT-Sicherheitszertifizierungen von IT-Produkten und -Systemen durchzuführen und die dafür benötigten Prüfkriterien bzw. Grundlagen zu entwickeln.

Zu diesem Zweck betreibt das BSI ein Qualitätsmanagementsystem, das den jeweiligen Anforderungen an die Zertifizierungsstellen entspricht. Es ist z. B. für die Produktzertifizierung für verschiedene Zertifizierungsbereiche von der DAkkS gemäß DIN EN ISO/IEC 17065 akkreditiert.

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.



Das BSI gestaltet die Digitalisierung – sicher und zuverlässig

Das BSI entwickelt seit seiner Gründung mit Politik, Industrie und Interessenverbänden Sicherheitsanforderungen für IT-Produkte und -Systeme und gestaltet damit aktiv Informationssicherheit für die digitale Gesellschaft.

Mit dem Digitalen Tachographen bewies das BSI bereits vor vielen Jahren seine Fachkompetenz bei der Konzeption und Prüfung sicherer Fahrtenschreiber und Umsetzung europäischer Vorgaben.

Im Jahr 2006 folgte in Zusammenarbeit mit der gematik die elektronische Gesundheitskarte, für die das BSI die Sicherheitsfunktionalität und Prüfanforderungen an die Konnektoren in der Arztpraxis sowie die Chipkarten von Patient und Leistungserbringer entwickelte.

Mit der Entwicklung der technischen Standards für die Identitätsdaten des neuen Personalausweis bereitete das BSI schon 2008 den Weg zur Nutzung elektronischer Identifizierungsfunktionen für die Digitalisierung von Geschäfts- und Verwaltungsprozessen.

Die Digitalisierung der Energiewende unterstützt das BSI seit 2010 im Auftrag des Bundesministeriums für Wirtschaft und Energie mit Anforderungskatalogen, Prüfvorschriften und Interoperabilitätsstandards an Smart Meter Gateways.

Das BSI ist mit seiner langjährigen Erfahrung bei der Konzeption und Prüfung elektronischer Geschäftsprozesse der Ansprechpartner für die Digitalisierungsagenda der Bundesregierung in Fragen der Informationssicherheit.

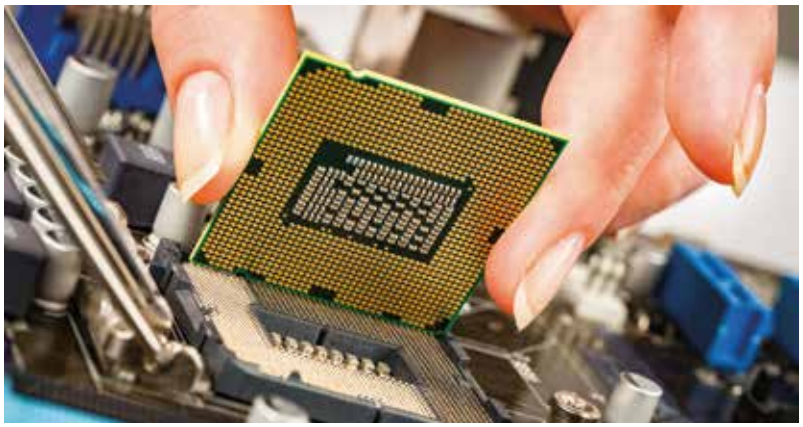
Die Vorteile eines BSI-Zertifikats

1 Das BSI ist Motor der Standardisierung: Gründungsmitglied der Common Criteria und Editor einiger ISO/IEC Standards.

2 Jede 2. weltweit zertifizierte Smartcard wurde in Deutschland begutachtet und vom BSI zertifiziert.

3 Jedes 3. gültige Produktzertifikat weltweit trägt das Siegel des BSI.

Für die digitale Wirtschaft



Die Zertifizierung und Anerkennung des BSI gewährleistet, dass eine unabhängige Partei die Begutachtung durchgeführt hat.

Für Ersteller oder Vertreiber von Systemen und Dienstleistungen bedeutet ein Zertifikat:

» erhöhte **nationale und internationale Chancen in Märkten** mit hohen Sicherheitsanforderungen mit einem **unabhängigen und international anerkannten Nachweises der Konformität**

» **objektive Bewertung und Vergleichbarkeit der Sicherheitsleistungen,** bescheinigt durch das unabhängige und international respektierte Mandat des BSI.

» **Produktqualität** wird in allen Prozessen des Lebenszyklus eines Systems oder einer Dienstleistung gelebt, aufrechterhalten und verbessert.

» **Innovationsfähigkeit** wird in der Entwicklungsumgebung des Systems, bei der Bereitstellung von Systemen und Dienstleistungen durch eine strukturierte Organisation etabliert.

» Optimierung der **Wirtschaftlichkeit** weiterer Zertifizierungen und Reevaluierungen.

Für die digitale Gesellschaft

5 gute Gründe für ein Zertifikat des BSI: Vertrauenswürdigkeit, Unabhängigkeit, Verlässlichkeit, langjährige Expertise und Sachlichkeit.

7 von 10 der weltweit herausgegebenen Produktzertifikate mit Stufe EAL 5 bis EAL 7 stammen vom BSI.

Mit Hilfe des Zertifizierungsreports und der zugehörigen Sicherheitsvorgabe können Beschaffer und Betreiber über die Einbindung des zertifizierten Produktes oder Dienstleistung in ihr Sicherheitskonzept entscheiden.

Anwender gewinnen aus dem Zertifizierungsreport einen Einblick, wie effektiv das zertifizierte Produkt ihren Sicherheitsbedarf erfüllt und geprüft wurde.

Beschaffer entnehmen einem Zertifikat des BSI:

» **Transparenz** über die Wirksamkeit einer Sicherheitsleistung eines Produkts oder einer Dienstleistung.

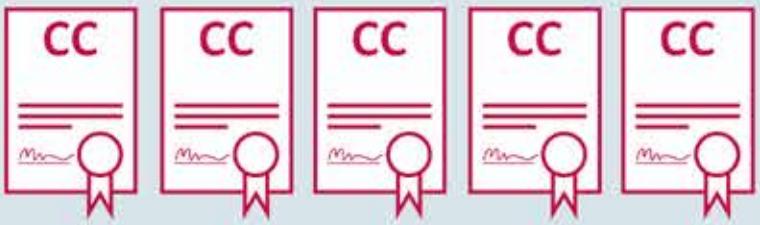
» **Vertrauenswürdigkeit** in die Vertraulichkeit, Integrität und Verfügbarkeit eines Produktes oder einer Dienstleistung durch die unabhängige Prüfung des BSI.

» **Nutzbarkeit** der Produkte oder Dienstleistungen anhand der Beschreibung ihres Anwendungsbereiches.

» **Vergleichbarkeit der Sicherheitsleistung** und ihrer Konformität zu internationalen oder nationalen Standards.

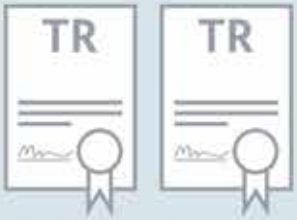
» auf **Korrektheit und Wirksamkeit** getestete Produkte sind die **Basis für vertrauenswürdige Geschäftsprozesse.**

Von 10 Produkt- und Systemzertifikaten des BSI sind



5 Common Criteria

3 IT-Grundschutz



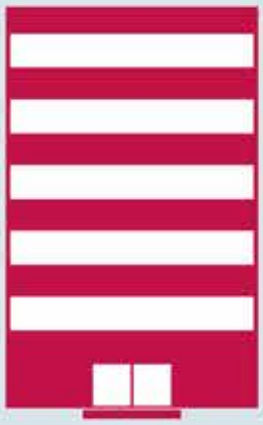
2 Technische Richtlinie

Das BSI zertifiziert von 10 Personen

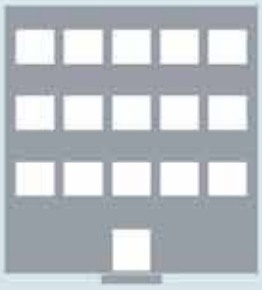
* TR oder Pen-Test

Bundesamt für Sicherheit in der Informationstechnik

IT-Sicherheits-dienstleister



CC-Prüfstellen



TR-Prüfstellen

sind vom BSI anerkannt

Die Konformitätsbewertung – Das BSI als Partner der Digitalisierung

An der Bewertung sind drei Parteien beteiligt:

Antrag

Der Antragsteller
» wählt eine Prüfstelle aus und
» beantragt die Prüfung bei der Zertifizierungsstelle des BSI;
» stellt die erforderlichen Nachweise zum Prüfgegenstand bereit und
» erhält nach erfolgreichem Abschluss des Verfahrens die Konformitätsurkunde, z.B. das Deutsche IT-Sicherheitszertifikat des BSI.

Prüfung

Die Prüfstelle
» untersucht den Prüfgegenstand nach Maßgabe des beantragten Kriterienwerks,
» übergibt die Prüfresultate der BSI- Zertifizierungsstelle sowie dem Antragsteller und
» kommuniziert die Prüfergebnisse zwischen dem Antragsteller und der BSI-Zertifizierungsstelle.

Zertifizierung

Die BSI-Zertifizierungsstelle
» berät den Antragsteller in Verfahrensfragen,
» unterstützt bei der Erarbeitung der Sicherheitsvorgaben,
» begleitet die Evaluierungsaktivitäten,
» erstellt den Prüfreport,
» erteilt mit Prüfabnahme die Konformitätsurkunde und
» veröffentlicht nach Einvernehmen mit dem Antragsteller den Prüfreport samt Konformitätsurkunde auf den Internetseiten des BSI.

Das BSI ist Motor der Standardisierung:
Gründungsmitglied der Common Criteria und Editor einiger ISO/IEC Standards.

1996
Die Common Criteria werden in Version 1.0 herausgegeben.

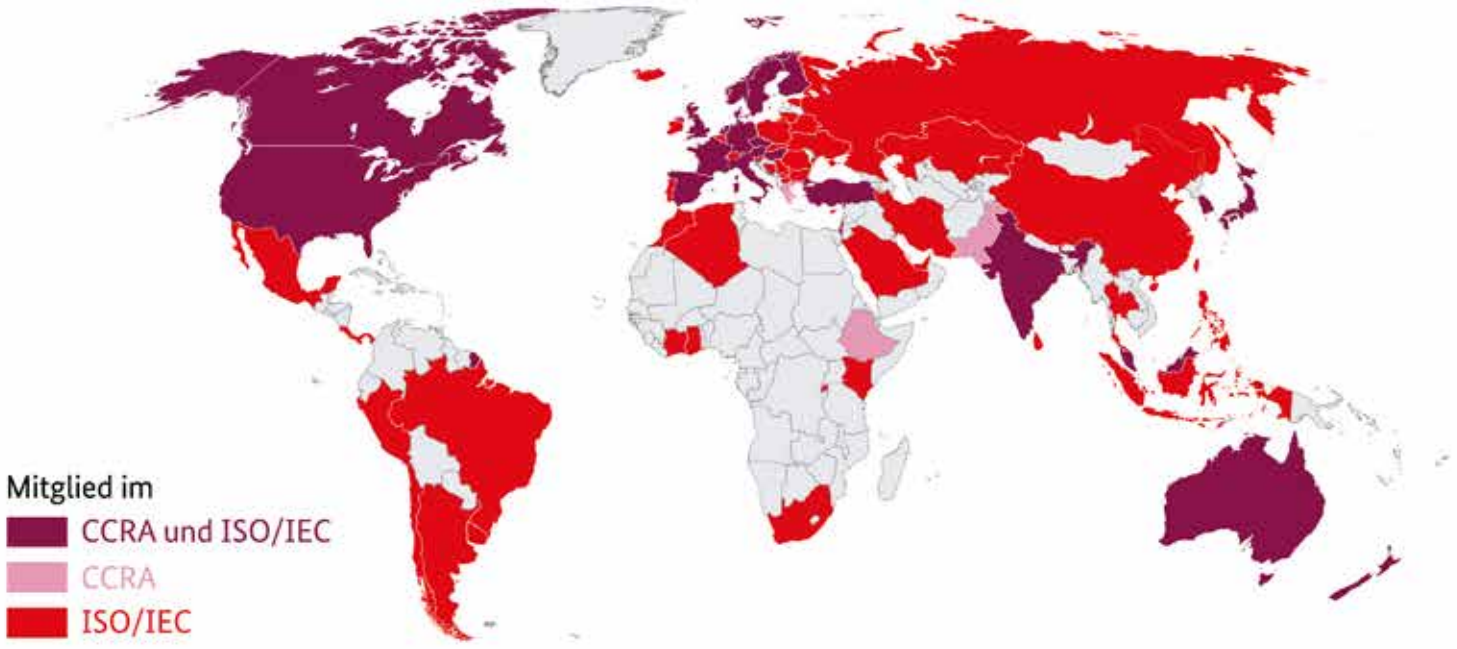
1998
Sechs Nationen, darunter Deutschland, vereinbaren die gegenseitige Anerkennung von CC-Zertifikaten.

1999
Die Common Criteria wird internationaler Standard: ISO/IEC 15408.
SOG-IS nimmt die Common Criteria als europäischen Prüfstandard an.

2006
Version 3.1 der Common Criteria erscheint mit überarbeiteten Anforderungen an die Vertrauenswürdigkeit.

2010
Zur Harmonisierung der Anerkennung führt SOG-IS technische Domänen ein, z.B. für Smart Cards.

2014
Das CCRA eröffnet Herstellern die kollaborative Entwicklung von Sicherheitsanforderungen für Produkttypen.



Das BSI – Schaltstelle für Standards einer digitalen Welt

Das BSI ist international und national die Stimme der deutschen Sicherheitswirtschaft und öffentlichen Beschaffer in der Welt.

Das BSI entwickelt Prüfstandards unter Beteiligung interessierter Behörden und in Kooperation mit Anwenderorganisationen und Herstellern.

Die Interessen der nationalen Sicherheitswirtschaft und der Bedarf der digitalen Gesellschaft Deutschlands werden vom BSI international und national bei der Formulierung von angemessenen Sicherheitsanforderungen mit hoher Qualität vertreten.

Die gegenseitige Anerkennung von Common Criteria Zertifikaten im CC Recognition Agreement (CCRA) eröffnet die Herstellung und Beschaffung von Sicherheitsprodukten in vielen Nationen, ohne diese mehrfach zertifizieren zu müssen. Seitdem sind viele Nationen dem Abkommen beigetreten.

Zertifikate, die unter diese Vereinbarung fallen, sind entsprechend mit einem spezifischen Logo gekennzeichnet. Im europäischen Raum erkennen zahlreiche Nationen IT-Sicherheitszertifikate, ausgestellt von europäischen Zertifizierungstellen, im SOGIS bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 an. Smart Cards und ähnliche Geräte sind bis zur Prüftiefe EAL7 gegenseitig anerkannt.

International sind die Common Criteria als ISO/IEC 15408 und 18045 veröffentlicht. Die ISO/IEC JTC 1/SC 27/WG 3 ist federführend in der Standardisierung.

» Aktuelle Liste der Unterzeichnerstaaten des CCRA
www.commoncriteriaportal.org

» Aktuelle Liste der Unterzeichnerstaaten der SOGIS
www.sogis.org

» VB-Produkte:
„Verfahrensbeschreibung zur Zertifizierung von Produkten“
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/VB-Produkte.pdf

» VB-Managementsysteme:
„Verfahrensbeschreibung zur Zertifizierung Managementsystemen“
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema.pdf

» VB-Personen:
„Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/VB-Personen.pdf

» VB-Stellen:
„Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern“
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/VB-Stellen.pdf

» De-Mail – Sicherer und einfacher elektronischer Nachrichtenverkehr
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/De-Mail-Broschuere.pdf

» Das Smart-Meter-Gateway – Sicherheit für intelligente Netze
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Smart-Meter-Gateway.pdf

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185–189
53175 Bonn
E-Mail: zertifizierung@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 9582-111
Telefax: +49 (0) 22899 9582-5400

Stand
September 2017

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
63086 Frankfurt am Main
Internet: www.zarbock.de

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis
Fotolia, BSI

Grafiken
BSI

Artikelnummer
BSI-MIBro17/331

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierte IT-Sicherheit

Common Criteria Produktzertifizierung

Internationale Anerkennung

Anwendervertrauen in das Gütesiegel des BSI

Nachvollziehbare und sorgfältige Prüfungen

Zertifizierungsstelle mit breiter Industrieexpertise

Förderung sicherer Entwicklungsprozesse

Bundesamt für Sicherheit in der Informationstechnik
Abteilung D – Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung
Godesberger Allee 185–189
53175 Bonn
E-Mail: zertifizierung@bsi.bund.de

Seit 1994 lassen Hersteller die technischen Sicherheitsfunktionen ihres IT-Produktes im gesamten Lebenszyklus vom BSI bestätigen.

Die Common Criteria sind ein etablierter und international anerkannter Kriterienkatalog für das Design, die Implementierung, Auslieferung und Wartung der Sicherheitsfunktionen ihrer Produkte.

Der Hersteller wählt aus diesem Katalog geeignete Sicherheitsanforderungen für sein Produkt aus und lässt diese von einer Prüfstelle und dem BSI evaluieren.

Das Produkt sollte als Kombination mehrerer Sicherheitsfunktionen eine eigenständige Sicherheitsleistung erbringen.

Alternativ kann ein Produkt nach einem Schutzprofil zertifiziert werden. Ein Schutzprofil (Protection Profile) formuliert generische und von der Implementierung unabhängige Sicherheitsanforderungen, ein allgemeines Sicherheitskonzept sowie Betriebsanforderungen an eine Produktkategorie.

Mit einem Common Criteria Zertifikat bestätigt das BSI als unabhängige und vertrauenswürdige Stelle die Korrektheit und Effektivität der vom Produkt angebotenen Sicherheitsfunktionen.

Die Widerstandsfähigkeit eines Produktes gegen neue und weiterentwickelte Angriffsmethoden kann im Rahmen des Assurance Continuity-Programms des BSI regelmäßig geprüft werden.

Die Gültigkeit des Zertifikats kann auf neue Produktversionen im Rahmen einer Re-Zertifzierung oder eines Maintenanceverfahrens ausgedehnt werden.

Die Kosten der Zertifizierung richten sich nach BSI-Kostenverordnung (BSIKostVO).

Eine Zertifizierung weist nach, dass ein Produkt die von Rechts- oder Prüfvorschriften geforderten Eigenschaften und Anforderungen in einem bestimmten Geltungsbereich erfüllt.
Ein **Produktzertifikat** kann Grundlage einer Zulassung sein.

Sicherheitsniveau:
niedrig (EAL 1) bis hoch (EAL 7)

Grundlage:
Common Criteria sowie

zertifizierte Sicherheitsvorgaben (Protection Profile) oder individuelle Sicherheitsvorgaben (Security Target)

Beteiligte:
Hersteller, Prüfstelle, BSI

Gültigkeit:
grundsätzlich 5 Jahre

Geltung:
Für eine Produktversion

Verfahrensdauer:
je nach Sicherheitsniveau und Produktkomplexität

Dokumente:
CC-Produkte: „Anforderungen an Antragssteller zur IT-Sicherheitszertifizierung von Produkten, Schutzprofilen und Standorten“

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierte IT-Sicherheit

Technische Richtlinie Konformitätsbewertung

Mindestsicherheits-anforderungen des BSI

Vergleichbarkeit des Prüfungsbereiches

Nachvollziehbare und sorgfältige Prüfungen

Förderung von Sicherheits-prozessen in kritischen und sensitiven Bereichen

Bundesamt für Sicherheit in der Informationstechnik
Abteilung D – Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung
Godesberger Allee 185–189
53175 Bonn
E-Mail: zertifizierung@bsi.bund.de

Hersteller und Beschaffer von elektronischen Identitätsnachweisen, elektronischen Messdaten oder sicheren Datenverarbeitungssystemen zertifizieren ihre interoperablen Produkte nach Technischen Richtlinien.

Nationale Prüfstandards für spezialgesetzliche Produkte wie Smart Meter, die elektronische Gesundheitskarte und der neue Personalausweis sind Technische Richtlinien.

Technische Richtlinien (TR) beschreiben funktionale und qualitative Anforderungen bestimmter 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.

Ziele einer Technischen Richtlinie sind vor allem die Interoperabilität von IT-Sicherheitskomponenten als auch ihrer IT-Sicherheitsanforderungen und Funktionalität.

Das Zertifikat kann nach Änderungen am Produkt auf seine neue Version im Rahmen einer Rezertifizierung oder Maintenance ausgedehnt werden.

Die Kosten der Konformitätsbewertung richten sich nach BSI-Kostenverordnung (BSIKostVO).

Technische Richtlinien

sind nationale Empfehlungen für bestimmte Produktkategorien. Bei besonderem öffentlichen Interesse können Standards für bestimmte Produkte und Systeme im Rahmen der Regulierung zur Norm erklärt werden.

Sicherheitsniveau:
Gemäß Technischer Richtlinie

Grundlage:
Technische Richtlinie für den Prüfungsbereich

Beteiligte:
Hersteller, Prüfstelle, BSI

Gültigkeit:
grundsätzlich 5 Jahre

Geltung:
für ein System

Verfahrensdauer:
Je nach Sicherheitsniveau und Komplexität der Systeme

Dokumente:
TR-Produkte: „Anforderungen an Antragsteller zur Zertifizierung von Produkten nach Technischen Richtlinien“

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierte IT-Sicherheit

IT-Grundschutz Managementsysteme

PLAN

DO

CHECK

ACT

Volle Kompatibilität zur ISO 27001 Norm

Detaillierte und nachvollziehbare Sicherheitsmaßnahmen

Transparenz der Prüfanforderungen

Förderung des Sicherheits-managements

Bundesamt für Sicherheit in der Informationstechnik
Abteilung D – Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung
Godesberger Allee 185–189
53175 Bonn
E-Mail: gs-zert@bsi.bund.de

Organisationen weisen ihren Kunden und Lieferanten ihre Managementfähigkeiten der Informationssicherheit mit einem Qualitätszertifikat nach.

Managementsysteme können gegen die BSI-Standards des IT-Grundschutz und gegen Technische Richtlinien auf Konformität geprüft werden.

Das Vorgehen nach IT-Grundschutz ist eine erprobte und effiziente Möglichkeit, die allgemeinen Anforderungen der ISO-Standards der 2700x-Reihe in der eigenen Organisation umzusetzen. Die IT-Grundschutz-Kataloge helfen Anwendern mit konkreten Hinweisen, Hintergrundinformationen und Beispielen bei der Umsetzung von Sicherheitsmaßnahmen.

Organisationen weisen die Konformität ihres Informationssicherheitsmanagements mit einem Zertifikat „ISO 27001 auf Basis IT-Grundschutz“ nach. Das Zertifikat bestätigt dann die Erfüllung der Anforderungen des internationalen Standard ISO 27001 und des nationalen Standards IT-Grundschutz.

Die Kosten der Zertifizierung richten sich nach BSI-Kostenverordnung (BSIKostVO).

Eine Zertifizierung weist nach, dass ein System die von Rechts- oder Prüfvorschriften geforderten Eigenschaften und Anforderungen in einem bestimmten Geltungsbereich erfüllt und kontinuierlich fortentwickelt.

Sicherheitsniveau:
Je nach Geltungsbereich

Grundlage:
IT-Grundschutz

Beteiligte:
Organisation, Prüfstelle, BSI

Gültigkeit:
3 Jahre

Geltung:
Je nach Geltungsbereich

Verfahrensdauer
Maximal 7 Monate

Dokumente:
„Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Zertifizierungsschema“

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierte IT-Sicherheit

Personen
Personenzertifizierung

Unabhängiger Nachweis der Sachkunde und Kompetenz

Förderung des Wissensausbaus

Vertrauen in das BSI-Prüfsiegel

Zugang zu sicherheitskritischen Bereichen

Bundesamt für Sicherheit in der Informationstechnik
Abteilung D – Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung
Godesberger Allee 185–189
53175 Bonn
E-Mail: auditor@bsi.bund.de

Zertifizierte Personen weisen ihre Fachkompetenz und Fachwissen für Evaluierungen, Audits und Dienstleistungen mit einem Personenzertifikat nach.

Die Evaluierung und Prüfung von Produkten und Managementsystemen und die Unterstützung des BSI im Bereich IT-Sicherheitsdienstleistungen erfordern qualifizierte Personen. Das BSI stellt daher die Fachkunde und Kompetenz von Personen in verschiedenen Bereichen fest:

» Auditteamleiter für ISO 27001-Audits auf der Basis IT-Grundschutz

» Auditoren für De-Mail, PKI-Zertifikatsausgabe, Smart-Meter-Gateway-Administration, Sicheren E-Mail-Betrieb und Resiscan

» IS-Revisoren

» Penetrationstester

Ziel der Zertifizierung durch das BSI ist die Sicherstellung der Fachkompetenz und Vergleichbarkeit der Arbeitsergebnisse zertifizierter Personen.

Das Zertifikat basiert auf der Überprüfung der Fachkompetenz und persönlichen Eignung und gilt bis zur Rezertifizierung. Verstöße gegen Verfahrensbeschreibungen und Kompetenzmängel können zur Aufhebung des Zertifikats führen.

Für die Personenzertifizierung wird vom BSI eine Grundpauschale erhoben. In bestimmten Geltungsbereichen müssen weitere Aufwände für Qualifizierungsmaßnahmen oder Vor-Ort-Begutachtungen hinzugerechnet werden.

Die Kosten der Zertifizierung richten sich nach BSI-Kostenverordnung (BSIKostVO).

Eine Zertifizierung weist nach, dass eine Person die von Rechts- oder Prüfvorschriften geforderten Eigenschaften und Anforderungen in einem bestimmten Geltungsbereich erfüllt.

Grundlage:
Je nach Geltungsbereich

Beteiligte:
Antragsteller, BSI

Gültigkeit:
3 Jahre

Geltung:
Je nach Geltungsbereich

Verfahrensdauer:
Je nach Geltungsbereich

Dokumente:
VB-Personen:
„Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierte IT-Sicherheit

Prüfstellen und Dienstleister Anerkennung

Unabhängiger Nachweis der Sachkunde und Kompetenz

Förderung des Wissensausbaus

Vertrauen in das BSI-Prüfsiegel

Zugang zu sicherheitskritischen Bereichen

Bundesamt für Sicherheit in der Informationstechnik
Abteilung D – Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung
Godesberger Allee 185–189
53175 Bonn
E-Mail: postfach-anerkennung@bsi.bund.de

Prüfstellen und Dienstleister weisen durch ihre Anerkennung nach, dass ihre Leistungen mit Fachkompetenz und kontinuierlicher Qualität erbracht werden.

Das BSI verantwortet nach § 9 (3) BSIG die Anerkennung von Prüfstellen und die Zertifizierung als IT-Sicherheitsdienstleister.

Zielgruppen dieses Anerkennungsangebots sind:

» Prüfstellen zur Feststellung der Konformität von Produkten im Bereich Common Criteria oder Technische Richtlinien

» IT-Sicherheitsdienstleister für IS-Revision, IS-Beratung sowie Penetrationstests

» IT-Sicherheitsdienstleister im Bereich Digitalfunk BOS und Lauschabwehr

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

Voraussetzung ist die Umsetzung und Aufrechterhaltung der Norm DIN EN ISO/IEC 17025 „Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien".

Das BSI prüft regelmäßig nach Erteilung der Anerkennung, dass Stellen und Dienstleister die Vorraussetzungen weiterhin erfüllen.

Die Kosten der Anerkennung richten sich nach BSI-Kostenverordnung (BSIKostVO).

Eine Anerkennung bestätigt die Fachkunde und Eignung einer Organisation in dem von ihnen beantragten Geltungsbereich. Vom BSI anerkannte Organisationen können der Bundesverwaltung spezialisierte Dienste im Bereich der Revision der Informationssicherheit oder Penetrationstests anbieten.

Grundlage:
Je nach Geltungsbereich

Beteiligte:
Antragsteller, BSI, weitere Behörden

Gültigkeit:
3 Jahre

Verfahrensdauer:
Je nach Geltungsbereich

Dokumente:
VB-Stellen: „Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern"