Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie BSI TR-03163: Sicherheit in TK-Infrastrukturen

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	25.05.2022	BSI	erste öffentliche Version
1.1	14.12.2022	BSI	editorielle Verbesserungen, Kapitel 3.1.2 Internationale Anerkennung für BSZ aktualisiert

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: tr-5g@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

1.1 Motivation

Die vorliegende Technische Richtlinie (TR) benennt die zulässigen Zertifizierungsschemata für kritische Komponenten in Telekommunikationsnetzen mit erhöhtem Gefährdungspotenzial im Sinne des „Kataloges von Sicherheitsanforderungen“ (kurz SiKa). Der [SiKa] wurde von der Bundesnetzagentur (BNetzA) im Einvernehmen mit dem BSI und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit veröffentlicht.

Parallel dazu unterstützt diese TR auch die Umsetzung der im Fokus liegenden Teile der „Cybersecurity of 5G networks EU Toolbox of risk mitigating Measures“ (kurz [EU 5G Toolbox]) der EU NIS Cooperation Group. Beide Aspekte werden nachfolgend kurz erläutert.

1.1.1 Telekommunikationsgesetz und Sicherheitskatalog

Nach § 165 Absatz 4 Telekommunikationsgesetz [TKG] dürfen Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial kritische Komponenten im Sinne von § 2 Absatz 13 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik [BSIG] nur dann einsetzen, wenn diese vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden. Eine anerkannte Zertifizierungsstelle stellt Zertifikate im Sinne der Nachweiserbringung der folgenden Absätze aus. Entsprechend § 167 Absatz 1 TKG werden hierzu weitere Regelungen im [SiKa] vorgenommen, der unter anderem in Form der "Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial" (LdkF) festlegt, welche Funktionen als kritische Funktionen im Sinne von § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b [BSIG] anzusehen sind. Die Realisierung einer kritischen Funktion bestimmt eine kritische Komponente.

Die vorliegende TR regelt die Nachweiserbringung für kritische Komponenten öffentlicher Kommunikationsnetze nach § 165 Absatz 4 TKG. Diese TR wird regelmäßig an den aktuellen Stand der Technik und Gesetzgebung angepasst.

1.1.2 EU-Instrumentarium für die 5G-Cybersicherheit (EU Toolbox for 5G Security)

Die „EU 5G Toolbox“ wurde von der NIS Cooperation Group veröffentlicht. Sie enthält strategische und technische sowie unterstützende Maßnahmen als Empfehlungen zur Mitigation der Risiken aus der EU-weit koordinierten Risikobewertung in Bezug auf die Cybersicherheit in den Mobilfunknetzen der fünften Generation (5G) [EU Risk Assessment].

In den folgenden Absätzen werden die technischen Maßnahmen der EU 5G Toolbox aufgegriffen, welche einen direkten Bezug zum Regelungsgegenstand dieser TR haben.

- *TM02 Ensuring and evaluating the implementation of security measures in existing 5G standards:*
  Im Rahmen der Zertifizierung von kritischen Komponenten bezüglich der IT-Sicherheit soll u. a. nachgewiesen werden, dass mit vertretbarem Aufwand auffindbare Sicherheitsschwachstellen gefunden und behoben werden, bevor die betroffenen Komponenten in Telekommunikationsnetzen eingebaut werden. Die Sicherstellung der Implementierung und Evaluierung von existierenden Sicherheitsmaßnahmen im Sinne von Basissicherheitsanforderungen ist eine explizit genannte Maßnahme und spiegelt sich im Zusammenspiel des SiKas mit dieser TR wieder.
  Der Zertifizierungspflicht für kritische Komponenten nach § 165 Absatz 4 TKG wird durch

Zertifizierungsmaßnahmen nachgekommen, die durch diese TR spezifiziert werden.

- *TM07 Reinforcing software integrity, update and patch management:*
  Die Vorgabe von zulässigen Zertifizierungsschemata in Kapitel 3, welche neben der eigentlichen 5G-Netzkomponenten auch Teile der Hersteller-Prozesse überprüfen, setzt eine Maßnahme zur Einführung von Softwareintegritäts-, Update- und Patch-Management-Mechanismen um.

- *TM09 Using EU certification for 5G network components, customer equipment and/or suppliers' processes:*
  Mit der Benennung der zulässigen Zertifizierungsschemata in Kapitel 3 und dem jeweiligen Bezug zu zukünftigen EU-weiten Cybersecurity Act (CSA) Schemata wird eine Maßnahme zur Zertifizierung von 5G-Netzkomponenten und Zulieferer-Prozessen umgesetzt.

1.2 Adressat

Diese TR richtet sich an Hersteller von kritischen Komponenten in Telekommunikationsnetzen. Die Kritikalität einer Komponente wird vom Netzbetreiber mit Hilfe der -[LdkF] bestimmt.

Die [LdkF] enthält neben der eigentlichen Liste der kritischen Funktionen auch einen Identifikationsprozess zur Bestimmung von kritischen Komponenten.

1.3 Struktur der Technischen Richtlinie

In Kapitel 2 werden die grundlegenden Überlegungen zur Auswahl der Zertifizierungsschemata dargestellt.

In Kapitel 3 werden die zulässigen Zertifizierungsschemata benannt und u.a. Aussagen zur Zertifikatsgültigkeit und dem Umgang mit Updates gemacht. Des Weiteren werden Vorgaben für die Sicherheitsaussagen von Zertifikaten aufgeführt sowie die verpflichtend anzuwendenden Anforderungsdokumente referenziert.

1.4 Begriffe

Diese TR nutzt Begriffe generell analog zu [BSIG], [TKG] und [SiKa]. Ergänzend dazu werden Erläuterungen der nachfolgenden Begriffe vorgenommen.

Tabelle 2 Begriffe und Erläuterungen

Begriff	***Erläuterung***
Evaluierungsgegenstand	Abgegrenzter Teil eines IT-Produktes, welcher in der Zertifizierung betrachtet wird. Dieser besteht aus Hardware, Firmware und/oder Software sowie der zugehörigen Dokumentation.
Kritische Komponente	Kritische Komponenten im Sinne des § 2 Absatz 13 BSIG sind IT-Produkte die in Kritischen Infrastrukturen eingesetzt werden, bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können und die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift eine auf Grund eines Gesetzes (hier konkret §§ 165 (4), 167 (1) Nr. 2 TKG) als kritisch bestimmte Funktion realisieren.
IT-Produkt	IT-Produkte im Sinne des [BSIG] sind Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten.
Security Target	Dokument zur Definition von Sicherheitsvorgaben in Common Criteria (CC) und Beschleunigte Sicherheitszertifizierung (BSZ)
Zertifizierungsschema	Der Umfang aller Prüfvorgaben und weiterer Regelungen für die Ausstellung von Zertifikaten durch Zertifizierungsstellen.
Zertifiziertes IT-Produkt	IT-Produkt eines Herstellers, welches nach einem zulässigen Zertifizierungsschema zertifiziert wurde. Zusätzlich zum IT-Produkt können auch Prozesse des Herstellers in den Umfang der Zertifizierung einfließen.

2 Grundlagen zur Zertifizierung von kritischen Komponenten

2.1 Durchführung der IT-Produktzertifizierung

Kritische Komponenten im Kontext dieser TR sind IT-Produkte, die aufgrund der gesetzlichen Regelungen des [BSIG] und [TKG] mit Hilfe der [LdkF] bestimmt werden. Eine IT-Produktzertifizierung wird durch den Antragssteller initiiert. Die Zertifizierung ist ein Zusammenspiel zwischen Zertifizierungsstelle, Prüfstelle, Hersteller und ggf. Auditoren. In der Zertifizierung tritt der Hersteller in der Regel (aber nicht ausschließlich) als Antragssteller auf, zudem hat der Hersteller bei der Zertifizierung aktiv mitzuwirken. Wie ist jeweils im Zertifizierungsschema geregelt.

Die Zertifizierungsstelle definiert das Zertifizierungsschema und hat damit die administrative Hoheit über den Ablauf der Zertifizierung. Sie dient als unparteiische Instanz, um sicherzustellen und aufzuzeigen, dass Evaluationsergebnisse festgelegten normativen Anforderungen entsprechen. Die Prüfstelle übernimmt die technische Prüfung des IT-Produktes auf Basis der im Zertifizierungsverfahren vorgegebenen Kriterien. Des Weiteren können Auditoren herangezogen werden, die im Rahmen der Zertifizierung des betrachteten IT-Produktes zusätzliche prozessorientierte Prüfungen beim Hersteller durchführen.

Beim Umfang der Zertifizierung und den beschriebenen Einsatzbedingungen ist durch den Hersteller zu beachten, dass das IT-Produkt so zertifiziert wird, dass der Anwender (d.h. der Netzbetreiber) dieses dann auch wie beschrieben einsetzen kann.

2.2 Sicherheit im Produktlebenszyklus

Der Produktlebenszyklus beinhaltet die Anforderungs- und Designphase, die Entwicklungsphase, die Validierungsphase, den Produktionsprozess, die weitere Unterstützung des Produktes in der Betriebsphase (z. B. Bereitstellung von Softwareupdates) sowie die Außerbetriebnahme. Dies schließt Sicherheitsaspekte bei der Integration von Komponenten Dritter in Produkte ein. Relevante Aspekte sind hierbei u. a. die Integrität oder die sicherheitstechnische Wartung solcher Komponenten. In allen Phasen sind Aspekte bezüglich der IT-Sicherheit zu beachten.

Die Prüfung des Evaluierungsgegenstandes im Rahmen einer Zertifizierung erbringt einen Nachweis über die aktuell vorliegende Implementierung und die umgesetzte IT-Sicherheit. Darüber hinaus werden Prozesse des Produktlebenszyklus bewertet.

Die zulässigen Zertifizierungsschemata, siehe Kapitel 3, beinhalten mit unterschiedlicher Schwerpunktsetzung die Überprüfung von Aspekten des Produktlebenszyklus und der Lieferkette. Das BSZ Schema ist hier eine Ausnahme und betrachtet ausschließlich das Produkt und keine Prozesse. Weitere Details finden sich in den Verfahrensbeschreibungen der Zertifizierungsschemata sowie den zugrundeliegenden Sicherheitsanforderungen.

2.3 Einsatzbedingungen und Gültigkeit von Zertifikaten

Um die IT-Produkte gültig nach den Angaben im Zertifikat zu betreiben, d.h. entsprechend des Zertifizierungsreports und vorhandener Sicherheitsvorgaben, muss der beschriebene Verwendungszweck, deren Betriebszustand (z. B. Konfiguration) und die Vorgaben an die Einsatzbedingung (z. B. Betriebsumgebung) eingehalten werden. Um Anwender zertifizierter IT-Produkte bei der Einhaltung dieser Rahmenbedingungen zu unterstützen, müssen die Hersteller Beschreibungen der einzuhaltenden Auflagen zur Verfügung stellen.

Durch das Auftreten von neuen Schwachstellen wird es zukünftig notwendig werden, dass Hersteller auch für zertifizierte IT-Produkte zeitnah Sicherheitsupdates zur Verfügung stellen müssen. Der Hersteller hat für die Lebenszeit der kritischen Komponente für die Aufrechterhaltung des Zertifikats zu sorgen und daher eine regelmäßige Re-Zertifizierung durchzuführen.

Weiter sind Hersteller zertifizierter IT-Produkte dazu verpflichtet Schwachstellen unverzüglich nach Kenntniserlangung dem BSI zu melden.

Basierend auf den Vorgaben des Sicherheitskatalogs, führen die Netzbetreiber im Rahmen des Sicherheitskonzeptes eine Risikoanalyse durch, in der das Auftreten von Schwachstellen in kritischen Komponenten sowie entsprechende mitigierende Maßnahmen behandelt werden.

Im Zuge der Auditierung nach § 165 Abs. 9 TKG ist das BSI dazu angehalten, die eingesetzten kritischen Komponenten hinsichtlich der Gültigkeit der Zertifikate zu überprüfen.

Für die Aufrechterhaltung der Zertifikate bieten die verschiedenen Zertifizierungsschemata unterschiedliche Möglichkeiten an, die in Kapitel 3 beschrieben werden. Alle Details finden sich in den jeweiligen Verfahrensbeschreibungen der Zertifizierungsschemata.

3 Zertifizierungsschemata

3.1 Zulässige Zertifizierungsschemata

Das vorherige Kapitel führte Grundlagen zur Zertifizierung ein, hierauf aufbauend werden die konkret zulässigen Zertifizierungsschemata benannt.

Nachfolgend werden die Zertifizierungsschemata kurz vorgestellt. Die detaillierte und bindende Beschreibung jedes einzelnen Schemas findet sich in den Verfahrensbeschreibungen des BSI.

Für die Zertifizierung der kritischen Komponenten im Bereich Telekommunikation werden grundsätzlich anforderungsbasierte Zertifizierungen genutzt. Die entsprechenden Anforderungsdokumente werden im Kontext des jeweiligen Schemas benannt. Durch die Nutzung von anforderungsbasierten Zertifizierungen kann sichergestellt werden, dass die Einhaltung komponentenspezifischer Sicherheitsanforderungen nachgewiesen wird.

Das BSI strebt eine Harmonisierung der nachfolgend beschriebenen Schemata innerhalb der Europäischen Union an und bringt sich in die Erarbeitung dieser neuen Schemata unter dem CSA ein.

3.1.1 NESAS CCS-GI Schema

Für die Zertifizierung von 5G-Mobilfunkkomponenten hat das BSI das Schema NESAS CCS-GI (NESAS Cybersecurity Certification Scheme - German Implementation) eingeführt. Dem Schema wird das Network Equipment Security Assurance Scheme [NESAS] der Global System for Mobile Communications Association (GSMA) zugrunde gelegt.

NESAS ist ein von der GSMA und dem 3rd Generation Partnership Project (3GPP) entwickeltes Rahmenwerk zur Überprüfung, Gewährleistung und Verbesserung der Sicherheit in der Mobilfunkbranche. NESAS definiert eine gemeinsame globale Basis für die Erstellung von nationalen und internationalen Anforderungen zur Bewertung definierter Sicherheitseigenschaften von Netzwerkkomponenten für Mobilfunknetze.

In der 3GPP werden die Technical Specifications mit Bezug auf Sicherheitsaspekte entwickelt. Die sogenannten Security Assurance Specification (SCAS) Dokumente sind ein Typ von 3GPP Technical Specifications. Die SCAS Dokumente spezifizieren Sicherheitsprüfungen von 5G-Mobilfunkkomponenten in Form von Testfällen. Die Dokumente sind in Produktklassen gemäß der standardisierten 3GPP-Netzwerkfunktionen aufgeteilt.

GSMA NESAS und NESAS CCS-GI im Vergleich

Die SCAS-Dokumente stellen die Anforderungen innerhalb einer GSMA NESAS-Produktevaluierung dar. Bevor eine solche Evaluierung durchgeführt werden kann, muss der Hersteller als Vorbedingung seine Entwicklungs- und Produktlebenszyklusprozesse (development and product lifecycle processes) auditieren lassen. Ein Hersteller, welcher die GSMA NESAS-Produktevaluierung durchlaufen möchte, muss hierzu entsprechende Auditoren und eine Prüfstelle für die Produktevaluierung beauftragen.

Durch das GSMA NESAS-Schema existieren schon Grundlagen und Strukturen für die Bewertung von 5G-Mobilfunkkomponenten. Dieses durch die Industrie entwickelte Schema stellt allerdings kein Zertifizierungsschema dar.

Um die Zertifizierungspflicht nach § 165 Absatz 4 TKG zu erfüllen, bietet das BSI mit NESAS CCS-GI ein NESAS-basiertes Zertifizierungsschema an. Im NESAS CCS-GI Schema dienen die SCAS-Dokumente als Anforderungsdokumente.

Die Nutzung von NESAS in einem Zertifizierungsschema wurde von der GSMA bei der Entwicklung bereits beabsichtigt. Es ist daher anzunehmen, dass dauerhaft das GSMA NESAS sowie darauf basierende Zertifizierungsschemata nebeneinander existieren und weiterentwickelt werden.

Internationale Anerkennung

Um in der Industrie eine hohe Akzeptanz zu erreichen, soll eine weitgehende betriebliche Kompatibilität zum GSMA NESAS-Schema sichergestellt werden. Insbesondere sollen die beteiligten Auditoren und Prüfstellen die Möglichkeit erhalten, Prüfergebnisse aus einer NESAS CCS-GI Zertifizierung auch für das GSMA NESAS Schema nutzen zu können.

Die EU Kommission strebt zudem an, ein NESAS-basiertes Zertifizierungsschema für 5G-Mobilfunkkomponenten unter dem CSA einzuführen.

Auditierung des Produktlebenszyklus

NESAS CCS-GI definiert als ersten Prüfungsschritt ein Audit der Herstellerprozesse, nach denen ein Produkt entwickelt wird. Die zu überprüfenden Sicherheitsanforderungen an die Herstellerprozesse werden durch das Vorgabendokument der GSMA (Dokument FS.16 „NESAS Development and Lifecycle Security Requirements“) definiert.

Gültigkeit

NESAS CCS-GI Zertifikate haben grundsätzlich eine Laufzeit von zwei Jahren nach der Ausstellung. Zertifikate im NESAS CCS-GI decken im Rahmen ihrer Zertifikatslaufzeit geringfügige Aktualisierungen ab (siehe Abschnitt „Updates“).

Einsatzbedingungen

Die zertifizierungsrelevanten Einsatzbedingungen des Evaluierungsgegenstandes werden im Verlauf des konkreten Verfahrens spezifiziert und zum Abschluss im Zertifizierungsbericht dokumentiert.

Updates

Falls Produktaktualisierungen während der Zertifikatsgültigkeitslaufzeit veröffentlicht werden, die im Sinne des folgenden Absatzes als geringfügig eingestuft werden können, so sind diese Aktualisierungen ebenfalls von dem bestehenden Sicherheitszertifikat erfasst. Dies bedeutet das Produkt ist weiterhin zertifiziert. Die Zertifikatslaufzeit ändert sich dadurch nicht.

Geringfügige Aktualisierungen sind Anpassungen von Sicherheitsfunktionen oder der Beschaffenheit des Produktes, die der Aufrechterhaltung oder Wiederherstellung der zertifizierten Sicherheitsleistung dienen oder die für die Sicherheitsleistung nicht relevant sind. Das Hinzufügen neuer Funktionalität hingegen stellt keine geringfügige Aktualisierung des Produktes dar. Die abschließende Entscheidung, ob es sich um eine geringfügige Aktualisierung handelt, erfolgt durch die Zertifizierungsstelle. Details hierzu sind den Verfahrensdokumenten zu entnehmen.

Für den Fall zeitnah notwendiger Sicherheitsupdates besteht somit für die Hersteller die Möglichkeit, diese als geringfügige Änderungen bereitzustellen. Durch diese Möglichkeit kann somit die Zertifizierung des Produktes konstant gewährleistet werden.

Weitere Informationen:

> Produktzertifizierung: Network Equipment Security Assurance Scheme (NESAS), jeweils aktuelle Version
>
> https://www.bsi.bund.de/nesas

3.1.2 BSZ Schema

Eine weitere Alternative zum Erreichen von Vertrauenswürdigkeit für Sicherheitsfunktionalitäten ist der Ansatz eines detaillierten Produktpenetrationstests, also die gezielte Suche nach Schwachstellen im zu prüfenden Produkt. Diese Art von Zertifizierung wird als Fixed-Time Evaluierung (d.h. mit vordefiniertem Zeitrahmen) bezeichnet.

Das BSI bietet in diesem Bereich die Beschleunigte Sicherheitszertifizierung (BSZ) an. In der Evaluierung findet u. a. eine Konformitätsprüfung statt, um die Sicherheitsaussagen des Herstellers zu prüfen. Diese wird kombiniert mit einem Produktpenetrationstest, um zu prüfen, ob die Sicherheitsfunktionen umgangen werden können. Die BSZ-Evaluierung wird mit einem zuvor festgelegten festen Zeitbudget durchgeführt. Die Festlegung des Zeitbudgets erfolgt auf Basis der Produktkomplexität.

Zusätzlich werden in der Evaluierung das Installationshandbuch und die eingesetzte Kryptographie auf mögliche sicherheitstechnische Probleme hin untersucht. Grundlage für eine BSZ sind ebenfalls Sicherheitsvorgaben (Security Targets), wobei diese weniger formal gehalten werden als beim Common Criteria Schema (vgl. Kapitel 3.1.3). Im Security Target einer BSZ wird das Produkt, dessen Einsatzszenario und Betriebsumgebung beschrieben, die relevanten Sicherheitsperimeter spezifiziert sowie die Grenzen der Evaluierung festgelegt.

Die BSZ bietet verschiedene Geltungsbereiche an. In jedem Geltungsbereich der BSZ können Sicherheitsanforderungen für den Evaluierungsgegenstand definiert werden, diese werden als Anforderungsdokumente im Sinne dieser TR verstanden. Um der Zertifizierungspflicht mit Hilfe der BSZ nachzukommen, muss die Zertifizierung in einem für das zu zertifizierende Produkt zulässigen Geltungsbereich erfolgen (vgl. Kapitel 3.2).

Internationale Anerkennung

Zwischen dem BSI und der französischen ANSSI besteht ein Abkommen zur gegenseitigen Anerkennung von Zertifikaten der Certification de Sécurité de Premier Niveau (CSPN) und der BSZ, zunächst befristet auf zwei Jahre. Damit werden grundsätzlich alle CSPN-Zertifikate in Deutschland vom BSI und alle BSZ-Zertifikate in Frankreich von der ANSSI anerkannt. Es können allerdings Zertifikate von der Anerkennung ausgenommen werden, wenn sie zum Beispiel besonderer nationaler Regulierung unterliegen oder andere Gründe vorliegen. Das BSI erkennt in diesem Sinne CSPN-Zertifikate an, die in den Geltungsbereich dieser Technischen Richtlinie fallen.

Das BSI unterstützt zudem Bestrebungen, die BSZ in einem CSA-Schema zu vereinheitlichen.

Auditierung des Produktlebenszyklus

Die BSZ enthält grundsätzlich keine Auditanteile zum Produktlebenszyklus.

Gültigkeit

Durch die BSZ erlangte Zertifikate haben grundsätzlich eine Gültigkeit von maximal zwei Jahren, Ausnahmen hiervon sind aufgrund von besonderen Bedingungen möglich. Das Zertifikat bezieht sich nur auf die angegebene Version des Produktes und gilt nur unter Einhaltung aller Auflagen.

Einsatzbedingungen

Die Einsatzbedingungen des Evaluierungsgegenstandes werden im Security Target definiert. In einer Secure User Guidance wird beschrieben, wie das Produkt in eine sichere – und damit die zertifizierte – Konfiguration gebracht werden kann.

Updates

Falls Produktaktualisierungen während der Zertifikatsgültigkeitslaufzeit veröffentlicht werden, muss eine Re-Zertifizierung erfolgen, da sich das Zertifikat nur auf die angegebene Version des Produktes bezieht. Für

die Re-Zertifizierung muss eine Änderungsbeschreibung bereitgestellt werden, abhängig von dieser Beschreibung kann ein verringerter Zeitaufwand des BSZ-Verfahrens möglich werden.

Für den Fall zeitnah notwendiger Sicherheitsupdates besteht somit für die Hersteller die Möglichkeit einer kurzen Re-Zertifizierung. Hierdurch soll eine möglichst konstante Zertifizierung des Produktes gewährleistet werden.

Weitere Informationen:

> Produktzertifizierung: Beschleunigte Sicherheitszertifizierung (BSZ), jeweils aktuelle Version
>
> https://www.bsi.bund.de/bsz

3.1.3 Common Criteria Schema

Der internationale Common Criteria (CC) Standard bildet die Basis für das klassische Produktzertifizierungsschema des BSI. Insbesondere im Bereich von Smartcard-Zertifizierungen und Netzwerkprodukten ist CC etabliert. Über die Evaluation Assurance Levels (EAL-Stufen) ist es möglich, unterschiedliche Tiefen in der Zertifizierung und Evaluierung festzulegen.

Common Criteria erlaubt es mit der Nutzung von Protection Profiles (PP) sehr präzise Sicherheitsanforderungen zu spezifizieren. Über ein PP können der Verwendungszweck und die Einsatzbedingungen des Evaluierungsgegenstandes vorgegeben werden. Zudem werden explizit die Sicherheitsziele an die Einsatzumgebung bzw. die formulierten Annahmen angegeben.

Im Umfeld von mobilen Netzwerken und mobilen Endgeräten wurden bereits verschiedene PP von der GSMA entwickelt.

Um der Zertifizierungspflicht mit Hilfe von Common Criteria nachzukommen, muss ein zulässiges PP als Anforderungsdokument die Grundlage für die Zertifizierung bilden.

Internationale Anerkennung

Das BSI ist die deutsche Zertifizierungsstelle für Common Criteria (CC). Zudem wirkt das BSI im europäischen SOG-IS mit. Die CC-Zertifikate des BSI werden bei Einhaltung der Bedingungen des Abkommens, im Rahmen des SOG-IS-Abkommens ausgestellt.

Durch die Etablierung von Zertifizierungsschemata im Rahmen des CSA wird eine Überführung hin zu einem neuen Schema notwendig. Dieses neue EUCC-Schema wird die Funktion des SOG-IS-Abkommens übernehmen. Aktuell befindet sich das EUCC-Schema in Vorbereitung. Solange dieses Schema noch nicht in Kraft getreten und etabliert ist, wird das BSI Zertifikate im Rahmen des SOG-IS Abkommens ausstellen und anerkennen.

Auditierung des Produktlebenszyklus

Für bestimmte Common Criteria-Zertifizierungen werden bei der Prüfung der Lifecycle-Anforderungen (Vertrauenswürdigkeitsklasse ALC) sogenannte Site-Visits (oder Audits) durch die Evaluatoren durchgeführt. Die konkreten Anforderungen hängen von der gewählten EAL-Stufe ab. Unabhängig von einer konkreten Produktzertifizierung bietet das BSI auch Standortzertifizierungen an, in deren Rahmen die Erfüllung bestimmter Lifecycle-Anforderungen nachgewiesen werden kann.

Gültigkeit

Common Criteria-Zertifikate haben grundsätzlich einen Gültigkeitszeitraum von fünf Jahren, sofern diese vom BSI ausgestellt wurden. Das CC-Zertifikat bezieht sich nur auf die angegebene Version des Produktes und gilt nur unter Einhaltung aller Auflagen und Hinweise.

Einsatzbedingungen

Die Einsatzbedingungen des Evaluierungsgegenstandes werden im Security Target und den zugehörigen, referenzierten Handbüchern dargestellt.

Updates

Eine Erneuerung des Zertifikats erfolgt in der Regel durch eine Re-Zertifizierung. Weiterhin gibt es mit dem Maintenance Prozess die Möglichkeit zur Aufrechterhaltung der Vertrauenswürdigkeit nach einer sicherheitsirrelevanten Änderung (minor change).

Weitere Informationen:

> Produktzertifizierung: IT-Sicherheitszertifizierung Common Criteria (CC), jeweils aktuelle Version
>
> https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/zertifizierung-nach-cc_node.html

3.2 Auswahl des Schemas

Für kritische Komponenten liegt grundsätzlich eine Zertifizierungspflicht nach § 165 Absatz 4 TKG vor. Mithilfe der vorliegenden TR können betroffene Hersteller ein in diesem Dokument dargestelltes Zertifizierungsschema auswählen, um dieser Pflicht nachzukommen.

Grundsätzlich bietet sich NESAS CCS-GI als Zertifizierungsschema für 5G-Komponenten an, welche über SCAS-Tests geprüft werden können. Alternativ kann ein Zertifikat aus einem anderen zulässigen Zertifizierungsschema auf Basis von Anforderungsdokumenten genutzt werden.

Das BSI pflegt in der Anlage A dieser TR eine Liste von zulässigen Anforderungsdokumenten und Geltungsbereichen, welche zur Erfüllung der Zertifizierungspflicht genutzt werden können.

Zertifikate, die in einem zulässigen Schema von einer anerkannten Zertifizierungsstelle nach § 9 Absatz 7 BSIG ausgestellt wurden, können ebenfalls den Nachweis der Zertifizierung erfüllen. Die zulässigen Anforderungsdokumente sind Grundlage der ausgestellten Zertifikate.

Abkürzungsverzeichnis

3GPP	3rd Generation Partnership Project
5G	Fünfte Generation von Mobilfunk Standards
ANSSI	Agence nationale de la sécurité des systèmes d'information
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSZ	Beschleunigte Sicherheitszertifizierung
CC	Common Criteria
CSA	Cybersecurity Act, Rechtsakt zur Cybersicherheit (VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. April 2019)
CSPN	Certification de Sécurité de Premier Niveau (Zertifizierungsschema der ANSSI)
EU	Europäische Union
EU 5G Toolbox	Cybersecurity of 5G networks EU Toolbox of risk mitigating Measures
GSMA	Groupe Speciale Mobile Association
NESAS	Network Equipment Security Assurance Scheme
NESAS CCS	NESAS Cybersecurity Certification Scheme
NESAS CCS-GI	NESAS CCS-German Implementation
NIS CG	Network and Information Systems Cooperation Group
PP	Protection Profile
SCAS	SeCurity Assurance Specifications
SOG-IS	Senior Officials Group Information Systems Security
TR	Technische Richtlinie
TM	Technical Measures (Begriff aus der EU 5G Toolbox)

Literaturverzeichnis

[BSIG] Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik, https://www.gesetze-im-internet.de/bsig_2009/

[CSA] Verordnung (EU) 2019/881 Rechtsakt zur Cybersicherheit (Cybersecurity Act), http://data.europa.eu/eli/reg/2019/881/oj

[EU 5G Toolbox] NIS Cooperation Group, Cybersecurity of 5G networks EU Toolbox of risk mitigating Measures, 01/2020, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

[EU Risk Assessment] NIS Cooperation Group, EU coordinated risk assessment of the cybersecurity of 5G networks Report, 09.10.2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

[LdkF] Bundesnetzagentur, Liste der kritischen Funktionen nach § 109 Abs. 6 Satz 1 Nr. 2 TKG für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial, 18.08.2021, http://www.bundesnetzagentur.de/sicherheitsanforderungen

[NESAS] GSMA, Network Equipment Security Assurance Scheme, https://www.gsma.com/security/network-equipment-security-assurance-scheme/

[SiKa] Bundesnetzagentur, Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG) Version 2.0, 23.12.2020, http://www.bundesnetzagentur.de/sicherheitsanforderungen

[TKG] Telekommunikationsgesetz, https://www.gesetze-im-internet.de/tkg_2021/