Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Befugnis: Programm zur Befugniserteilung und Notifizierung nach EUCC für ITSEF high

Befugnis-EUCC_ITSEF-high

Version 1.0 vom 31.07.2024

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0)800 247 1000
E-Mail: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Änderungshistorie

Version	*Datum*	*Name/Org-Einheit*	*Beschreibung*
1.0	31.07.2024	NCCA/S 14	Erstausgabe

Tabelle: Änderungshistorie

Inhalt

1 Einleitung

Auf Grundlage der europäischen Durchführungsverordnung (EU) 2024/482EUCC-DV), welche am 27.02.2024 in Kraft getreten ist, können Konformitätsbewertungsstellen (KBS) beim Bundesamt für Sicherheit in der Informationstechnik (BSI) beantragen, im Rahmen der Verordnung (EU) 2019/881 Cybersecurity Act (CSA) tätig zu werden.

1.1 Zielsetzung des Programms

Dieses Dokument beinhaltet Anforderungen und weitere wichtige Informationen und Regelungen als Ergänzung zur übergeordneten „Verfahrensbeschreibung zur Befugniserteilung von Konformitätsbewertungsstellen gem. § 9a BSIG und Notifizierung gem. Verordnung (EU) 2019/881“ (VB-Befugnis). Es richtet sich an die antragstellende Organisation, welche sich dafür entschieden hat, eine Befugniserteilung und Notifizierung als ITSEF für die Vertrauenswürdigkeitsstufe „hoch/high“ gem. Art. 22, 23, 24 EUCC-DV im Bereich des Programms EUCC durchführen zu lassen. Als ITSEF (Information Technology Security Evaluation Facility) werden im vorliegenden Programmdokument jene KBS benannt, die gem. Art. 2 Nr. 7 EUCC-DV i.V.m. Art. 2 Nr. 13 der Verordnung (EG) Nr. 765/2008 als KBS definiert werden, die Evaluierungen durchführen. KBS, die vom BSI als ITSEF für die Vertrauenswürdigkeitsstufe „high“ gegenüber der Europäischen Kommission notifiziert wurden, erfüllen auch die Voraussetzung, um im Rahmen der Vertrauenswürdigkeitsstufe substantial der EUCC-DV tätig werden zu können.

Es werden die speziellen Anforderungen mit detaillierten Hinweisen zu Verfahrensabläufen benannt, welche die antragstellenden Organisationen berücksichtigen müssen.

2 Programm zur Erteilung der Befugnis und Notifizierung für ITSEFs im Rahmen der EUCC-DV

Das EUCC-Schema (European Common Criteria-based cybersecurity certification scheme) beinhaltet die Zertifizierung der Cybersicherheit von Produkten der Informations- und Kommunikationstechnik (IKT) und Schutzprofilen auf der Grundlage der Common Criteria (ISO/IEC 15408) und der Common Methodology for Information Technology Security Evaluation (ISO/IEC 18045).

Das bis dahin bestehende System im Rahmen des Senior Officials Group Information Systems Security Mutual Recognition Agreement (SOG-IS MRA) wurde in dieses europäische Schema für die Cybersicherheitszertifizierung auf Ersuchen der Europäischen Kommission gem. Art. 48 Abs. 2 CSA überführt.

Das vorliegende Programmdokument beschreibt die gesetzlichen Voraussetzungen zur Erteilung der Befugnis mit anschließender Notifizierung als ITSEF im Rahmen des Art. 22 der EUCC-DV und des § 9a BSIG:

- Die ITSEF muss die Anforderungen an die Kompetenz erfüllen, um die erforderlichen Sachkenntnisse für die Durchführung der Evaluationstätigkeiten zur Ermittlung der Widerstandsfähigkeit gegen Cyberangriffe, die dem neuesten Stand der Technik entsprechen und von Akteuren mit umfangreichen Fähigkeiten und Ressourcen durchgeführt werden, auch für die Bereiche Technical Domains und Schutzprofile, nachzuweisen.
- Die ITSEF gewährleisten, die Sicherheit und den Schutz von Unternehmensgeheimnissen und anderen vertraulichen Informationen, einschließlich Geschäftsgeheimnissen, sowie die Wahrung der Rechte des geistigen Eigentums durchzusetzen und alle hierzu erforderlichen und geeigneten technischen und organisatorischen Maßnahmen zu ergreifen.

2.1 Anforderungen an die Kompetenz

Die ITSEF muss die technischen Fachkompetenzen in den technischen Fachbereichen gem. EUCC-DV, für welche Evaluierungstätigkeiten gemäß Beantragung angeboten werden, nach dem Stand der Technik vorhalten und nachweisen.

Aus diesen Rahmenbedingungen heraus ergibt sich die Notwendigkeit, weitergehende fachliche Mindestanforderungen an die Mitarbeitenden der ITSEF zu formulieren.

Darüber hinaus gelten insbesondere die Anforderungen des Annex II des Dokuments (guidance authorisation).

Sobald die Beantragung Technical Domains umfasst, müssen zudem folgende Kompetenzen nachgewiesen werden:

2.1.1 Kompetenzanforderungen für die Technical Domain Smartcards and Similiar Devices

ITSEF, die in der Technical Domain „Smartcards and Similar Devices“ evaluieren möchten, müssen gewährleisten und nachweisen, dass eingesetztes Personal über die Kompetenzen gem. EUCC-DV verfügt.

2.1.2 Kompetenzanforderungen für Technical Domain Hardware Devices with Security Boxes

ITSEF, die in der Technical Domain „Hardware Devices with Security Boxes“ evaluieren möchten, müssen gewährleisten und nachweisen, dass eingesetztes Personal über die Kompetenzen gem. EUCC-DV verfügt.

2.2 Anforderungen an das Equipment

ITSEF müssen gewährleisten und nachweisen, dass das für die angebotenen Prüfverfahren das jeweils notwendige Equipment gem. EUCC-DV und Anlage 4 vorhanden ist und durch das eingesetzte Personal bedient werden kann.

2.3 Anforderungen an die Unterbeauftragung externer Stellen

Im Falle einer Unterbeauftragung muss die ITSEF gewährleisten, dass die Anlage 2 vorhanden ist und Verträge nachgewiesen werden.

2.4 Anforderungen an das Informationssicherheitsmanagementsystem (ISMS)

Das Informationssicherheitsmanagementsystem (ISMS) der Prüfstellen muss dem Dokument „Anforderungen an die Sicherheit von Stellen“ (AS-Stellen) entsprechen, wobei die Sicherheitsanforderungen als mindestens „hoch“ anzusetzen sind.

2.5 Nachweis der Akkreditierung

Für die Befugniserteilung und Notifizierung ist eine Akkreditierung nach Art. 24, 23 Abs. 1 EUCC-DV, Art. 60 Abs. 1 CSA notwendig.

Hinweis: Der Antrag auf Befugniserteilung sollte zeitgleich mit dem Antrag auf Akkreditierung erfolgen.

3 Verfahren zur Befugniserteilung und Notifizierung im Programm EUCC

Das Verfahren der Befugniserteilung und Notifizierung setzt nach EUCC-DV eine Akkreditierung nach Akkreditierungsstellengesetz (AkkStelleG) und Verordnung (EG) Nr. 765/2008 voraus.

Bei der Akkreditierung erfolgt zur Erfüllung der DIN EN ISO/IEC 17025 eine Fachbegutachtung, um nachzuweisen, dass ausreichend Fachkompetenz, das notwendige Equipment sowie bei einer Begutachtung des Informationssicherheitsmanagementsystems auf Grundlage des Dokuments „Anforderungen an die Sicherheit von Stellen“ (AS-Stellen) werden konkretisierte Anforderungen der DIN EN ISO/IEC 17025 bezüglich der Sicherstellung der Vertraulichkeit, Verfügbarkeit und der Integrität überprüft.

Für die Erteilung der Befugnis wird gemäß Beantragung eine Überprüfung der Anforderungen aus diesem Programm vorgenommen.

3.1 Durchführung Informationsgespräch

Nach vorab durchgeführtem Informationsgespräch (Kap. 3.2.1 (VB-Befugnis)), kann die ITSEF ihre Antragsunterlagen beim BSI einreichen. Anfragen sind an ncca@bsi.bund.de zu richten.

3.2 Antrags- und Dokumentenprüfung

3.2.1 Aufgaben der ITSEF

Jegliche Dokumentation an die DAkkS in Kopie an ncca@bsi.bund.de senden. Einen Antrag einreichen mit folgenden Nachweisen:

- Ausgefüllte Anlage 1 „Mitarbeitenden und deren Rollenzuordnung“ (Kompetenzanforderungen für Rollen vgl. Kap. 2.1 „Anforderungen an die Kompetenz“)
- Ausgefüllte Anlage 2 „Nachweis einer externen Laborleistung“
- Ausgefüllte Anlage 3 „Technology Types-Evaluation Technique Types“ gemäß Kap. 2.3 „Anforderungen an die Unterbeauftragung externer Stellen“
- Ausgefüllte Anlage 4 „Prüfverfahren und Kompetenzen“
- Dokumentation des Informationssicherheitsmanagementsystems (inkl. Netztopologie) und materieller Sicherheit (inkl. Lageplan der Räumlichkeiten) gem. Kap. 2.4 „Anforderungen an das Informationssicherheitsmanagementsystem (ISMS)“
- Ausgefüllter Fragenkatalog AS-Stellen (auf Anfrage über ncca@bsi.bund.de)
- Nachweis über die Zusammenarbeit zwischen ITSEF und der Zertifizierungsstelle High in Form individualvertraglicher Vereinbarungen.

3.2.2 Aufgaben der Aufsichtsführenden NCCA des BSI

Die Stelle für Befugniserteilung und Notifizierung bewertet die eingereichten Angaben und Nachweise im Antrag.

3.3 Erfordernis Pilotevaluierung

Bei einer erstmaligen Zusammenarbeit von CB und ITSEF, muss die ITSEF ihre Kompetenz durch eine erfolgreiche Pilotevaluierung gem. EUCC-DV nachweisen.

3.4 Durchführung der Begutachtung

Schwerpunkt der Begutachtung (Kap. 3.2.2 (VB-Befugnis)) sind die in Kapitel 2 „Programm zur Erteilung der Befugnis und Notifizierung für ITSEFs im Rahmen der " beschriebenen Anforderungen gemäß Antrag, die mittels Interview, Beobachtung und Einsichtnahme geprüft werden.

Eine Begutachtung wird gemäß der Verordnung EUCC-DV wie folgt durchgeführt:

- Interviews mit Mitarbeitenden sowie Sichtung notwendiger Dokumente
- Begutachtung der technischen Ausstattung, um das Vorhandensein und die Nutzung von notwendigem Equipment nachzuweisen

Aufgaben der ITSEF	**Aufgaben BSI (Begutachtende)**
Fachbegutachtung gemäß beantragter Technologietypen sicherstellen: • Die ITSEF muss sicherstellen, dass die benannten Mitarbeitenden am Begutachtungstermin vor Ort sind und interviewt werden können, um die Kompetenzanforderungen gemäß Kap. 2.1 „Anforderungen an die Kompetenz“ begutachten zu können. • Zusätzlich muss die ITSEF sicherstellen, dass das Equipment und das Bedienen dieses Equipments vor Ort überprüft und begutachtet werden kann gemäß Kap. 2.2. „Anforderungen an das Equipmen“. • Sofern die ITSEF im Rahmen einer Unterbeauftragung mit externen Stellen zusammenarbeitet, muss sie insbesondere die oben genannten Anforderungen gemäß Kap. 2.3 “Anforderungen an die Unterbeauftragung externer Stellen“ (insbesondere an Kompetenz und Equipment) nachweisen. Hierzu sind entsprechende Vertragsunterlagen bereitzuhalten.	Begutachtung durchführen: • Der Begutachter begutachtet die Anforderungen gemäß Kap. 2.1, 2.2, 2.3. • Das Begutachtungsergebnis sowie ggf. festgestellte Abweichungen werden im Abschlussgespräch erläutert und ggf. in Abweichungsberichten dokumentiert.
Begutachtung des Informationsmanagementsystems gewährleisten: • Die ITSEF muss die Angaben des vorab ausgefüllten Fragenkatalogs gemäß der Anforderungen aus Kap. 2.4 „Anforderungen an das Informationssicherheitsmanagementsystem (ISMS)“ belegen.	Begutachtung des Informationsmanagementsystems durchführen: • Der Begutachter begutachtet die Anforderungen gemäß Kap. 2.4. • Das Begutachtungsergebnis sowie ggf. festgestellte Abweichungen werden im Abschlussgespräch erläutert und ggf. in Abweichungsberichten dokumentiert.
Durchführung einer Ursachen- und Ausmaßanalyse und Vorschlag einer Korrekturmaßnahme: • Unterlagen an ncca@bsi.bund.de versenden Umsetzung geeigneter Korrekturmaßnahmen: • Unterlagen an ncca@bsi.bund.de versenden	Prüfung der Eignung von Korrekturvorschlägen auf Basis der Ursachen- und Ausmaßanalyse und der anschließenden Korrekturmaßnahmen
-	Nach Behebung der Abweichungen erstellt das BSI einen Begutachtungsbericht mit einer Begutachtungsempfehlung

Tabelle 1: Aufgaben bei der Fachbegutachtung

3.5 Erteilung einer Befugnis und Notifizierung

Das Vorliegen der Akkreditierungsurkunde ist für die Erteilung der Befugnis und Notifizierung im Bereich der EUCC-DV zwingend erforderlich. Sodann wird auf Grundlage des Begutachtungsberichts bewertet und über die Erteilung der Befugnis entschieden. Näheres regelt die VB-Befugnis. Im Nachgang erstellt die Aufsichtsführende NCCA des BSI erstellt entsprechend den Vorgaben des Programms den authorisation report gem. Art. 59 Abs. 3 d) CSA und den Bescheid.

Mit positiver Entscheidung notifiziert die Aufsichtsführende NCCA des BSI die ITSEF nach Ablauf der Widerspruchsfrist oder Verzicht gem. Art. 61 CSA an die Europäische Kommission.

4 Aufrechterhaltung der Befugniserteilung und Notifizierung

4.1 Begutachtungen im Rahmen der Überwachung

Im Rahmen der Befugniserteilung und Notifizierung als ITSEF werden regelmäßig Begutachtungen durch das BSI durchgeführt, um die Eignung der ITSEF im Bereich der erteilten Befugnis sicherzustellen, zu überprüfen und eventuelle Abweichungen von den Anforderungen und notwendigen Qualifizierungsbedarf zu erkennen. Diese können im Rahmen der Überwachungsbegutachtungen der DAkkS durch Begutachter des BSI durchgeführt werden. Außerordentliche Begutachtungen werden stichprobenartig oder anlassbezogen durchgeführt, sollte im Rahmen eines Beschwerdevorgangs die Notwendigkeit eintreten.

4.2 Erneuerung der erteilten Befugnis und Notifizierung

Sechs Monate vor Ablauf der Befugniserteilung und Notifizierung muss ein erneuter Antrag auf Befugniserteilung und Notifizierung gestellt werden, damit gewährleistet werden kann, dass die Befugniserteilung und Notifizierung lückenlos fortgeführt wird. Die Begutachtungen finden i.d.R. im Rahmen der Wiederholungsbegutachtungen der DAkkS statt.

4.3 Anlassbezogene Begutachtungen

Anlassbezogene Begutachtungen können stattfinden, insbesondere wenn

- sich in der ITSEF Änderungen (z.B. Umzug, neue Mitarbeitende oder Änderung der Unternehmenszugehörigkeit) ergeben, die Auswirkung auf die Erfüllung der Anforderungen dieses Programms haben,
- begründete Zweifel an der Einhaltung der Anforderungen oder an der Kompetenz der ITSEF besteht,
- Verfahrensänderungen, u.a. aufgrund von Durchführungsverordnungen oder Sachstandsdokumenten zu EUCC oder
- von Dritten Informationen über Unregelmäßigkeiten an das BSI herangetragen werden.

4.4 Meldung weitere Mitarbeitende

Die ITSEF hat jederzeit die Möglichkeit, weitere erfahrene, eingearbeitete Mitarbeitende dem BSI durch Aktualisierung der Anlage 4 nachzumelden.

Referenzen und Glossar

AkkStelleG	Akkreditierungsstellengesetz
AS-Stellen	Anforderungen an die Sicherheit von Stellen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
CSA	Cybersecurity Act
DAkkS	Deutsche Akkreditierungsstelle
DIN EN ISO/IEC 17025	Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien
EUCC-DV	Europäische Durchführungsverordnung (EU) 2024/482 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC)
EUCC-Schema	European Common Criteria-based cybersecurity certification scheme
ISMS	Informationssicherheitsmanagementsystem
ISO/IEC 15408	International Standard: ISO/IEC 15408: Information security, cybersecurity and privacy protection — Evaluation criteria for IT security
ISO/IEC 18045	International Standard: ISO/IEC 18045: Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation
IKT	Informations- und Kommunikationstechnik
ITSEF	Information Technology Security Evaluation Facility
KBS	Konformitätsbewertungsstelle
NCCA	National Cybersecurity Certification Authority
SOG-IS MRA	Senior Officials Group Information Systems Security Mutual Recognition Agreement
VB-Befugnis	Verfahrensbeschreibung zur Befugniserteilung von Konformitätsbewertungsstellen gem. § 9a BSIG und Notifizierung gem. Verordnung (EU) 2019/881
Verordnung (EG) Nr. 765/2008	Verordnung (EG) Nr. 765/2008 des Europäischen Parlamentes und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates