



**▼B****DURCHFÜHRUNGSVERORDNUNG (EU) 2024/482 DER KOMMISSION**

vom 31. Januar 2024

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)

(Text von Bedeutung für den EWR)

## KAPITEL I

## ALLGEMEINE BESTIMMUNGEN

*Artikel 1***Gegenstand und Anwendungsbereich**

In dieser Verordnung wird das auf den Gemeinsamen Kriterien beruhende europäische System für die Cybersicherheitszertifizierung (EUCC) festgelegt.

Diese Verordnung gilt für alle Produkte der Informations- und Kommunikationstechnik (IKT) und deren Dokumentation, die zur Zertifizierung im Rahmen des EUCC vorgelegt werden, sowie für alle Schutzprofile, die im Rahmen des IKT-Prozesses zur Zertifizierung von IKT-Produkten zur Zertifizierung vorgelegt werden.

*Artikel 2***Begriffsbestimmungen**

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

**▼M1**

1. „Gemeinsame Kriterien“ (*Common Criteria*) die Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit gemäß den Normen ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 oder ISO/IEC 15408-5:2022 oder gemäß den Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit, Version CC:2022, Teile 1 bis 5, veröffentlicht von den Beteiligten der Anerkennungsvereinbarung für die nach den Gemeinsamen Kriterien ausgestellten Zertifikate auf dem Gebiet der IT-Sicherheit (CCRA);
2. „Gemeinsame Evaluierungsmethodik“ die Gemeinsame Methodik für die Evaluierung der IT-Sicherheit gemäß der Norm ISO/IEC 18045:2022 oder die Gemeinsame Methodik für die Evaluierung der IT-Sicherheit, Version CEM:2022, veröffentlicht von den Beteiligten der Anerkennungsvereinbarung für die nach den Gemeinsamen Kriterien ausgestellten Zertifikate auf dem Gebiet der IT-Sicherheit (CCRA);

**▼B**

3. „Evaluierungsgegenstand“ ein IKT-Produkt oder ein Teil davon oder ein Schutzprofil als Teil eines IKT-Prozesses, das einer Cybersicherheitsbewertung zur Erteilung einer EUCC-Zertifizierung unterzogen wird;
4. „Sicherheitsziel“ eine Beanspruchung der Einhaltung umsetzungsabhängiger Sicherheitsanforderungen für ein bestimmtes IKT-Produkt;

**▼B**

5. „Schutzprofil“ einen IKT-Prozess, der die Sicherheitsanforderungen für eine bestimmte Kategorie von IKT-Produkten festlegt, umsetzungsunabhängige Sicherheitsbedarfe beschreibt und zur Bewertung der unter diese spezifische Kategorie fallenden IKT-Produkte im Hinblick auf deren Zertifizierung verwendet werden kann;
6. „technischer Evaluierungsbericht“ ein von einer ITSEF erstelltes Dokument mit den Ergebnissen, Beurteilungen und Begründungen aus der Evaluierung eines IKT-Produkts oder eines Schutzprofils gemäß den in dieser Verordnung festgelegten Vorschriften und Verpflichtungen;
7. „ITSEF“ (*Information Technology Security Evaluation Facility*) eine Einrichtung zur Evaluierung der IT-Sicherheit, die eine Konformitätsbewertungsstelle im Sinne des Artikels 2 Nummer 13 der Verordnung (EG) Nr. 765/2008 ist und Evaluierungstätigkeiten durchführt;
8. „AVA\_VAN-Stufe“ ein Niveau der Schwachstellenanalyse zur Zusage der Vertrauenswürdigkeit, die den Umfang der Tätigkeiten der Cybersicherheitsevaluierung angibt, die durchgeführt wurden, um den Grad Widerstandsfähigkeit gegen eine potenzielle Ausnutzung von Mängeln oder Schwachstellen des Evaluierungsgegenstands in seiner Betriebsumgebung gemäß den Gemeinsamen Kriterien zu ermitteln;
9. „EUCC-Zertifikat“ ein im Rahmen des EUCC ausgestelltes Cybersicherheitszertifikat für IKT-Produkte oder für Schutzprofile, die ausschließlich im IKT-Prozess der Zertifizierung von IKT-Produkten verwendet werden können;
10. „zusammengesetztes Produkt“ ein IKT-Produkt, das zusammen mit einem anderen zugrunde liegenden IKT-Produkt evaluiert wird, für das bereits ein EUCC-Zertifikat erteilt wurde und von dessen Sicherheitsfunktionen das zusammengesetzte IKT-Produkt abhängt;
11. „nationale Behörde für die Cybersicherheitszertifizierung“ eine von einem Mitgliedstaat gemäß Artikel 58 Absatz 1 der Verordnung (EU) 2019/881 benannte Behörde;
12. „Zertifizierungsstelle“ eine Konformitätsbewertungsstelle im Sinne des Artikels 2 Nummer 13 der Verordnung (EG) Nr. 765/2008, die Zertifizierungstätigkeiten durchführt;
13. „technischer Bereich“ einen gemeinsamen technischen Rahmen bezüglich einer bestimmten Technologie für die harmonisierte Zertifizierung mit einer Reihe charakteristischer Sicherheitsanforderungen;
14. „Sachstandsdokument“ ein Dokument, in dem Evaluierungsmethoden, -techniken und -instrumente für die Zertifizierung von IKT-Produkten oder von Sicherheitsanforderungen einer allgemeinen IKT-Produktkategorie oder andere für die Zertifizierung erforderliche Anforderungen festgelegt werden, um die Evaluierung, insbesondere von technischen Bereichen oder von Schutzprofilen, zu harmonisieren;
15. „Marktüberwachungsbehörde“ eine Marktüberwachungsbehörde im Sinne des Artikels 3 Nummer 4 der Verordnung (EU) 2019/1020.

**▼ M1***Artikel 3***Evaluierungsnormen**

(1) Für die im Rahmen des EUCC-Systems durchgeführten Evaluierungen gelten folgende Normen:

- a) die Gemeinsamen Kriterien (*Common Criteria*),
- b) die Gemeinsame Evaluierungsmethodik.

(2) Bis zum 31. Dezember 2027 kann ein Zertifikat im Rahmen des EUCC-Systems gemäß einer der folgenden Normen ausgestellt werden:

- a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 oder ISO/IEC 15408-3:2008,
- b) Gemeinsame Kriterien für die Evaluierung der IT-Sicherheit, Version 3.1, Revision 5, veröffentlicht von den Beteiligten der Anerkennungsvereinbarung für die nach den Gemeinsamen Kriterien ausgestellten Zertifikate auf dem Gebiet der IT-Sicherheit (CCRA),
- c) ISO/IEC 18045:2008,
- d) Gemeinsame Methodik für die Evaluierung der IT-Sicherheit, Version 3.1, Revision 5, veröffentlicht von den Beteiligten der Anerkennungsvereinbarung für die nach den Gemeinsamen Kriterien ausgestellten Zertifikate auf dem Gebiet der IT-Sicherheit (CCRA).

(3) Bis zum 31. Dezember 2027 kann ein Zertifikat, das Konformität mit einem Schutzprofil geltend macht, das den in Absatz 2 genannten Normen entspricht, im Rahmen des EUCC-Systems gemäß den in Absatz 1 genannten Normen ausgestellt werden.

(4) Ein Zertifikat gemäß den in Absatz 1 genannten Normen kann auch im Rahmen des EUCC-Systems ausgestellt werden, um Konformität mit einem Schutzprofil geltend zu machen, das einer der folgenden Normen entspricht, sofern nach der Durchführungsverordnung (EU) 2016/799 der Kommission <sup>(1)</sup>, der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates <sup>(2)</sup> oder dem Durchführungsbeschluss (EU) 2016/650 der Kommission <sup>(3)</sup> die Verwendung eines solchen Schutzprofils erforderlich ist:

<sup>(1)</sup> Durchführungsverordnung (EU) 2016/799 der Kommission vom 18. März 2016 zur Durchführung der Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates zur Festlegung der Vorschriften über Bauart, Prüfung, Einbau, Betrieb und Reparatur von Fahrtenschreibern und ihren Komponenten (ABl. L 139 vom 26.5.2016, S. 1. ELI: [http://data.europa.eu/eli/reg\\_impl/2016/799/oj](http://data.europa.eu/eli/reg_impl/2016/799/oj)).

<sup>(2)</sup> Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73. ELI: <http://data.europa.eu/eli/reg/2014/910/oj>).

<sup>(3)</sup> Durchführungsbeschluss (EU) 2016/650 der Kommission vom 25. April 2016 zur Festlegung von Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten gemäß Artikel 30 Absatz 3 und Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (ABl. L 109 vom 26.4.2016, S. 40. ELI: [http://data.europa.eu/eli/dec\\_impl/2016/650/oj](http://data.europa.eu/eli/dec_impl/2016/650/oj)).

**▼ M1**

- a) Gemeinsame Kriterien für die Evaluierung der IT-Sicherheit, Version 3.1, Revision 1-4, veröffentlicht von den Beteiligten der Anerkennungsvereinbarung für die nach den Gemeinsamen Kriterien ausgestellten Zertifikate auf dem Gebiet der IT-Sicherheit (CCRA),
- b) Gemeinsame Methodik für die Evaluierung der IT-Sicherheit, Version 3.1, Revision 1-4, veröffentlicht von den Beteiligten der Anerkennungsvereinbarung für die nach den Gemeinsamen Kriterien ausgestellten Zertifikate auf dem Gebiet der IT-Sicherheit (CCRA).

**▼ B***Artikel 4***Vertrauenswürdigkeitsstufen**

- (1) Die Zertifizierungsstellen erteilen EUCC-Zertifikate der Vertrauenswürdigkeitsstufen „mittel“ oder „hoch“.
- (2) EUCC-Zertifikate der Vertrauenswürdigkeitsstufe „mittel“ entsprechen Zertifikaten der AVA\_VAN-Stufe 1 oder 2.
- (3) EUCC-Zertifikate der Vertrauenswürdigkeitsstufe „hoch“ entsprechen Zertifikaten der AVA\_VAN-Stufe 3, 4 oder 5.
- (4) In der mit einem EUCC-Zertifikat bestätigten Vertrauenswürdigkeitsstufe wird nach Maßgabe der Gemeinsamen Kriterien gemäß Anhang VIII zwischen konformer und erweiterter Verwendung der Vertrauenswürdigkeitskomponenten unterschieden.
- (5) Die Konformitätsbewertungsstellen verwenden die Vertrauenswürdigkeitskomponenten, von denen die gewählte AVA\_VAN-Stufe nach den in Artikel 3 genannten Normen abhängt.

*Artikel 5***Methoden zur Zertifizierung von IKT-Produkten**

- (1) Die Zertifizierung eines IKT-Produkts erfolgt anhand seines Sicherheitsziels:
  - a) wie vom Antragsteller festgelegt oder

**▼ M1**

- b) unter Geltendmachung der Konformität mit einem zertifizierten Schutzprofil als Teil des IKT-Prozesses, wenn das IKT-Produkt in die von diesem Schutzprofil erfasste IKT-Produktkategorie fällt.

**▼ B**

- (2) Schutzprofile werden ausschließlich zur Zertifizierung von IKT-Produkten zertifiziert, die in die von diesem Schutzprofil erfasste besondere IKT-Produktkategorie fallen.



## Artikel 6

### Selbstbewertung der Konformität

Eine Selbstbewertung der Konformität im Sinne des Artikels 53 der Verordnung (EU) 2019/881 ist nicht zulässig.

## KAPITEL II

### ZERTIFIZIERUNG VON IKT-PRODUKTEN

#### ABSCHNITT 1

#### *Besondere Normen und Anforderungen für die Evaluierung*

## Artikel 7

### Evaluierungskriterien und -methoden für IKT-Produkte

(1) Ein zur Zertifizierung vorgelegtes IKT-Produkt wird zumindest anhand folgender Elemente evaluiert:

- a) zutreffende Elemente der in Artikel 3 genannten Normen;
- b) Klassen von Anforderungen an die sicherheitsbezogene Vertrauenswürdigkeit für die Schwachstellenbewertung und die unabhängige Funktionsprüfung gemäß den in Artikel 3 genannten Evaluierungsnormen;
- c) Risiken im Zusammenhang mit der beabsichtigten Verwendung der betreffenden IKT-Produkte gemäß Artikel 52 der Verordnung (EU) 2019/881 und deren Sicherheitsfunktionen hinsichtlich der in Artikel 51 der Verordnung (EU) 2019/881 festgelegten Sicherheitsziele;
- d) anwendbare Sachstandsdokumente, die in Anhang I aufgeführt sind;
- e) anwendbare zertifizierte Schutzprofile, die in Anhang II aufgeführt sind.

(2) In hinreichend begründeten Ausnahmefällen kann eine Konformitätsbewertungsstelle beantragen, von der Anwendung des einschlägigen Sachstandsdokuments abzusehen. In solchen Fällen unterrichtet die Konformitätsbewertungsstelle die nationale Behörde für die Cybersicherheitszertifizierung und legt ihr eine hinreichende Begründung für ihren Antrag vor. Die nationale Behörde für die Cybersicherheitszertifizierung prüft die Begründung der beantragten Ausnahme und genehmigt diese, falls sie diese für gerechtfertigt hält. Bis zur Entscheidung der nationalen Behörde für die Cybersicherheitszertifizierung darf die Konformitätsbewertungsstelle kein Zertifikat ausstellen. Die nationale Behörde für die Cybersicherheitszertifizierung teilt die genehmigte Ausnahme unverzüglich der Europäischen Gruppe für die Cybersicherheitszertifizierung mit, die eine Stellungnahme dazu abgeben kann. Die nationale Behörde für die Cybersicherheitszertifizierung muss der Stellungnahme der Europäischen Gruppe für die Cybersicherheitszertifizierung weitestgehend Rechnung tragen.

**▼B**

(3) Die Zertifizierung von IKT-Produkten auf AVA\_VAN-Stufe 4 oder 5 ist nur in folgenden Szenarios möglich:

- a) Wenn das IKT-Produkt zu einem der in Anhang I aufgeführten technischen Bereiche gehört, wird es nach dem betreffenden Sachstandsdocument dieses technischen Bereiches evaluiert,
- b) wenn das IKT-Produkt zu einer Kategorie von IKT-Produkten gehört, die von einem zertifizierten Schutzprofil erfasst wird, das auch für die AVA\_VAN-Stufe 4 oder 5 gilt, und das als Sachstandsdocument in Anhang II aufgeführt ist, wird es nach der für dieses Schutzprofil angegebenen Evaluierungsmethodik evaluiert,
- c) wenn die Buchstaben a und b dieses Absatzes nicht zutreffen und die Aufnahme eines technischen Bereichs in Anhang I bzw. eines zertifizierten Schutzprofils in Anhang II in absehbarer Zukunft unwahrscheinlich ist, und nur in hinreichend begründeten Ausnahmefällen unter den in Absatz 4 genannten Bedingungen.

(4) Wenn eine Konformitätsbewertungsstelle der Auffassung ist, dass ein hinreichend begründeter Ausnahmefall gemäß Absatz 3 Buchstabe c vorliegt, unterrichtet sie die nationale Behörde für die Cybersicherheitszertifizierung von der beabsichtigten Zertifizierung und legt ihr eine Begründung und eine vorgeschlagene Bewertungsmethode vor. Die nationale Behörde für die Cybersicherheitszertifizierung prüft die Begründung der Ausnahme und genehmigt oder ändert die von der Konformitätsbewertungsstelle anzuwendende Bewertungsmethode, wenn sie dies für gerechtfertigt hält. Bis zur Entscheidung der nationalen Behörde für die Cybersicherheitszertifizierung darf die Konformitätsbewertungsstelle kein Zertifikat ausstellen. Die nationale Behörde für die Cybersicherheitszertifizierung teilt die beabsichtigte Zertifizierung unverzüglich der Europäischen Gruppe für die Cybersicherheitszertifizierung mit, die eine Stellungnahme dazu abgeben kann. Die nationale Behörde für die Cybersicherheitszertifizierung muss der Stellungnahme der Europäischen Gruppe für die Cybersicherheitszertifizierung weitestgehend Rechnung tragen.

(5) Falls ein IKT-Produkt als zusammengesetztes Produkt nach den betreffenden Sachstandsdocumenten evaluiert wird, übermittelt die ITSEF, die die Evaluierung des zugrunde liegenden IKT-Produkts durchgeführt hat, die betreffenden Informationen an die ITSEF, die die Evaluierung des zusammengesetzten IKT-Produkts durchführt.

*ABSCHNITT II**Ausstellung, Erneuerung und Widerruf von EUCC-Zertifikaten**Artikel 8***▼M1****Für die Zertifizierung und Evaluierung erforderliche Informationen**

(1) Wer eine Zertifizierung im Rahmen des EUCC-Systems beantragt, muss der Zertifizierungsstelle und der ITSEF alle für die Zertifizierungs- und Evaluierungstätigkeiten erforderlichen Informationen vorlegen oder anderweitig zur Verfügung stellen.

**▼B**

(2) Zu den Absatz 1 genannten Informationen gehören alle einschlägigen Nachweise gemäß den Abschnitten über Aktionselemente für Entwickler (*Developer action elements*) im geeigneten Format nach Maßgabe der Abschnitte über Inhalt und Darstellung von Nachweiselementen (*Content and presentation of evidence element*) der Gemeinsamen Kriterien und der Gemeinsamen Evaluierungsmethodik für die gewählte Vertrauenswürdigkeitsstufe und die zugehörigen Anforderungen an die sicherheitsbezogene Vertrauenswürdigkeit. Die Nachweise umfassen erforderlichenfalls Einzelheiten zu dem IKT-Produkt und seinem Quellcode gemäß dieser Verordnung, vorbehaltlich bestehender Vorkehrungen gegen eine unbefugte Offenlegung.

(3) Zertifizierungsantragsteller können der Zertifizierungsstelle geeignete Evaluierungsergebnisse aus einer vorherigen Zertifizierung vorlegen, die erfolgt ist gemäß

- a) der vorliegenden Verordnung,
- b) einem anderen europäischen System für die Cybersicherheitszertifizierung, das gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurde,
- c) einem in Artikel 49 der vorliegenden Verordnung genannten System.

(4) Wenn die Evaluierungsergebnisse für ihre Aufgaben relevant sind, kann die ITSEF die vorgelegten Evaluierungsergebnisse weiterverwenden, sofern diese den geltenden Anforderungen entsprechen und ihre Echtheit bestätigt worden ist.

(5) Wenn die Zertifizierungsstelle erlaubt, dass das Produkt einer Zertifizierung als zusammengesetztes Produkt unterzogen wird, stellt der Zertifizierungsantragsteller der Zertifizierungsstelle und der ITSEF alle jeweils erforderlichen Elemente gemäß dem Sachstandsdocument zur Verfügung.

(6) Außerdem übermittelt der Zertifizierungsantragsteller der Zertifizierungsstelle und der ITSEF folgende Informationen:

- a) den Link zu seiner Website, die die in Artikel 55 der Verordnung (EU) 2019/881 genannten zusätzlichen Informationen über die Cybersicherheit enthält;
- b) eine Beschreibung der Verfahren des Antragstellers für das Schwachstellenmanagement und die Offenlegung von Schwachstellen.

(7) Alle in diesem Artikel genannten einschlägigen Unterlagen müssen von der Zertifizierungsstelle, der ITSEF und dem Antragsteller für einen Zeitraum von fünf Jahren nach Ablauf des Zertifikats aufbewahrt werden.

**▼ B***Artikel 9***Bedingungen für die Ausstellung eines EUCC-Zertifikats**

- (1) Die Zertifizierungsstellen stellen ein EUCC-Zertifikat aus, wenn alle folgenden Bedingungen erfüllt sind:
- a) Die Kategorie des IKT-Produkts fällt in den Anwendungsbereich der Akkreditierung und gegebenenfalls der Zulassung der Zertifizierungsstelle und der ITSEF, die an der Zertifizierung beteiligt sind.
  - b) Der Zertifizierungsantragsteller hat eine Erklärung unterzeichnet, mit der er alle in Absatz 2 aufgeführten Verpflichtungen eingetht.
  - c) Die ITSEF hat die Evaluierung gemäß den in den Artikeln 3 und 7 genannten Evaluierungsnormen, -kriterien und -methoden ohne Einwände abgeschlossen.
  - d) Die Zertifizierungsstelle hat die Überprüfung der Evaluierungsergebnisse ohne Einwände abgeschlossen.
  - e) Die Zertifizierungsstelle hat sich davon überzeugt, dass die ihr von der ITSEF vorgelegten technischen Evaluierungsberichte mit den vorgelegten Nachweisen übereinstimmen und dass die in den Artikeln 3 und 7 genannten Evaluierungsnormen, -kriterien und -methoden ordnungsgemäß angewandt wurden.
- (2) Der Zertifizierungsantragsteller muss sich dazu verpflichten,
- a) der Zertifizierungsstelle und der ITSEF alle erforderlichen vollständigen und korrekten Informationen zu übermitteln und auf Anfrage zusätzliche erforderliche Informationen bereitzustellen;
  - b) das IKT-Produkt nicht als im Rahmen des EUCC zertifiziert zu bewerben, bevor das EUCC-Zertifikat ausgestellt wurde;
  - c) das IKT-Produkt nur in Bezug auf den im EUCC-Zertifikat festgelegten Anwendungsbereich als zertifiziert zu bewerben;
  - d) im Fall der Aussetzung, des Widerrufs oder des Ablaufs des EUCC-Zertifikats die Bewerbung des IKT-Produkts als zertifiziert unverzüglich zu beenden;
  - e) sicherzustellen, dass die IKT-Produkte, die unter Bezugnahme auf das EUCC-Zertifikat verkauft werden, mit dem zertifizierten IKT-Produkt identisch sind;
  - f) die Vorschriften für die Verwendung des gemäß Artikel 11 für das EUCC-Zertifikat festgelegten Siegels und Kennzeichens einzuhalten.
- (3) Falls ein IKT-Produkt als zusammengesetztes Produkt nach den betreffenden Sachstandsdokumenten zertifiziert wird, übermittelt die Zertifizierungsstelle, die die Zertifizierung des zugrunde liegenden IKT-Produkts durchgeführt hat, die betreffenden Informationen an die Zertifizierungsstelle, die die Zertifizierung des zusammengesetzten IKT-Produkts durchführt.

**▼B***Artikel 10***Inhalt und Format eines EUCC-Zertifikats**

- (1) Ein EUCC-Zertifikat muss zumindest die in Anhang VII aufgeführten Angaben enthalten.
- (2) Der Anwendungsbereich und die Eingrenzung des zertifizierten IKT-Produkts sind eindeutig im EUCC-Zertifikat oder im Zertifizierungsbericht zu nennen und es ist anzugeben, ob das gesamte IKT-Produkt zertifiziert wurde oder nur Teile davon.
- (3) Die Zertifizierungsstelle stellt dem Antragsteller das EUCC-Zertifikat zumindest in elektronischer Form zur Verfügung.
- (4) Die Zertifizierungsstelle erstellt für jedes von ihr ausgestellte EUCC-Zertifikat einen Zertifizierungsbericht gemäß Anhang V. Der Zertifizierungsbericht beruht auf dem von der ITSEF erstellten technischen Evaluierungsbericht. In dem technischen Evaluierungsbericht und dem Zertifizierungsbericht werden die besonderen Evaluierungskriterien und -methoden gemäß Artikel 7 angegeben, die für die Evaluierung verwendet wurden.
- (5) Die Zertifizierungsstelle übermittelt der nationalen Behörde für die Cybersicherheitszertifizierung und der ENISA alle EUCC-Zertifikate und alle Zertifizierungsberichte in elektronischer Form.

*Artikel 11***Siegel und Kennzeichen**

- (1) Der Inhaber eines Zertifikats kann auf einem zertifizierten IKT-Produkt ein Siegel und ein Kennzeichen anbringen. Mit dem Siegel und Kennzeichen wird angezeigt, dass das IKT-Produkt gemäß dieser Verordnung zertifiziert wurde. Das Siegel und Kennzeichen wird gemäß diesem Artikel und gemäß Anhang IX angebracht.
- (2) Das Siegel und Kennzeichen wird gut sichtbar, leserlich und dauerhaft auf dem IKT-Produkt oder seinem Typenschild angebracht. Falls die Art des Produkts dies nicht zulässt oder nicht rechtfertigt, wird es auf der Verpackung und den Begleitunterlagen angebracht. Falls das zertifizierte IKT-Produkt in Form von Software geliefert wird, muss das Siegel und Kennzeichen gut sichtbar, leserlich und dauerhaft in der begleitenden Dokumentation erscheinen, oder diese Dokumentation muss den Nutzern über eine Website leicht und direkt zugänglich gemacht werden.
- (3) Das Siegel und Kennzeichen wird gemäß Anhang IX festgelegt und enthält
  - a) die Vertrauenswürdigkeitsstufe und die AVA\_VAN-Stufe des zertifizierten IKT-Produkts,
  - b) die eindeutige Kennung des Zertifikats, bestehend aus
    - 1) dem Namen des Systems,
    - 2) dem Namen und der eindeutigen Akkreditierungsnummer der Zertifizierungsstelle, die das Zertifikat ausgestellt hat,
    - 3) dem Jahr und Monat der Ausstellung,
    - 4) der Kennnummer, die von der Zertifizierungsstelle, die das Zertifikat ausgestellt hat, vergeben wurde.

**▼B**

- (4) Dem Siegel und Kennzeichen wird ein QR-Code mit einem Link zu einer Website beigefügt, die zumindest Folgendes enthält:
- a) die Angaben zur Geltung des Zertifikats,
  - b) die erforderlichen Zertifizierungsinformationen gemäß den Anhängen V und VII,
  - c) die Informationen, die der Zertifikatsinhaber gemäß Artikel 55 der Verordnung (EU) 2019/881 öffentlich zugänglich machen muss,
  - d) falls zutreffend, die historischen Informationen über die betreffende (n) Zertifizierung(en) des IKT-Produkts, um eine Rückverfolgbarkeit zu ermöglichen.

*Artikel 12***Geltungsdauer eines EUCC-Zertifikats**

- (1) Die Zertifizierungsstelle setzt für jedes EUCC-Zertifikat unter Berücksichtigung der Merkmale des zertifizierten IKT-Produkts eine Geltungsdauer fest.
- (2) Die Geltungsdauer eines EUCC-Zertifikats darf fünf Jahre nicht überschreiten.
- (3) Abweichend von Absatz 2 kann diese Geltungsdauer mit vorheriger Zustimmung der nationalen Behörde für die Cybersicherheitszertifizierung länger als fünf Jahre betragen. Die nationale Behörde für die Cybersicherheitszertifizierung unterrichtet die Europäische Gruppe für die Cybersicherheitszertifizierung unverzüglich über die erteilte Zustimmung.

*Artikel 13***Überprüfung eines EUCC-Zertifikats**

- (1) Auf Antrag des Zertifikatsinhabers oder aus anderen triftigen Gründen kann die Zertifizierungsstelle das EUCC-Zertifikat für ein IKT-Produkt überprüfen. Die Überprüfung erfolgt gemäß Anhang IV. Die Zertifizierungsstelle legt den Umfang der Überprüfung fest. Wenn dies für die Überprüfung erforderlich ist, fordert die Zertifizierungsstelle die ITSEF auf, eine erneute Evaluierung des zertifizierten IKT-Produkts durchzuführen.
- (2) Je nach den Ergebnissen der Überprüfung und gegebenenfalls der erneuten Evaluierung kann die Zertifizierungsstelle
  - a) das EUCC-Zertifikat bestätigen,
  - b) das EUCC-Zertifikat gemäß Artikel 14 widerrufen,
  - c) das EUCC-Zertifikat gemäß Artikel 14 widerrufen und ein neues EUCC-Zertifikat mit gleichem Anwendungsbereich und verlängerter Geltungsdauer ausstellen oder
  - d) das EUCC-Zertifikat gemäß Artikel 14 widerrufen und ein neues EUCC-Zertifikat mit einem veränderten Anwendungsbereich ausstellen.
- (3) Die Zertifizierungsstelle kann das EUCC-Zertifikat gemäß Artikel 30 unverzüglich aussetzen, bis der Inhaber des EUCC-Zertifikats Abhilfemaßnahmen getroffen hat.

**▼B***Artikel 14***Widerruf eines EUCC-Zertifikats**

- (1) Unbeschadet des Artikels 58 Absatz 8 Buchstabe e der Verordnung (EU) 2019/881 wird ein EUCC-Zertifikat von der Zertifizierungsstelle widerrufen, die dieses Zertifikat ausgestellt hatte.
- (2) Die in Absatz 1 genannte Zertifizierungsstelle unterrichtet die nationale Behörde für die Cybersicherheitszertifizierung über den Widerruf des Zertifikats. Sie unterrichtet auch die ENISA über einen solchen Widerruf, um ihr die Wahrnehmung ihrer Aufgabe gemäß Artikel 50 der Verordnung (EU) 2019/881 zu erleichtern. Die nationale Behörde für die Cybersicherheitszertifizierung unterrichtet andere einschlägige Marktüberwachungsbehörden.
- (3) Der Inhaber eines EUCC-Zertifikats kann den Widerruf des Zertifikats beantragen.

## KAPITEL III

## ZERTIFIZIERUNG VON SCHUTZPROFILEN

*ABSCHNITT I**Besondere Normen und Anforderungen für die Evaluierung**Artikel 15***Evaluierungskriterien und -methoden**

- (1) Ein Schutzprofil wird zumindest anhand folgender Elemente evaluiert:
- a) zutreffende Elemente der in Artikel 3 genannten Normen;
  - b) Risiken im Zusammenhang mit der beabsichtigten Verwendung der betreffenden IKT-Produkte gemäß Artikel 52 der Verordnung (EU) 2019/881 und deren Sicherheitsfunktionen hinsichtlich der in Artikel 51 der Verordnung festgelegten Sicherheitsziele;
  - c) anwendbare Sachstandsdokumente, die in Anhang I aufgeführt sind. Ein Schutzprofil, das sich auf einen technischen Bereich bezieht, wird anhand der in diesem technischen Bereich geltenden Anforderungen zertifiziert.
- (2) In hinreichend begründeten Ausnahmefällen kann eine Konformitätsbewertungsstelle ein Schutzprofil zertifizieren, ohne dabei die einschlägigen Sachstandsdokumente anzuwenden. In solchen Fällen unterrichtet sie die zuständige nationale Behörde für die Cybersicherheitszertifizierung und legt ihr eine Begründung der beabsichtigten Zertifizierung ohne Anwendung der einschlägigen Sachstandsdokumente sowie die vorgeschlagene Bewertungsmethode vor. Die nationale Behörde für die Cybersicherheitszertifizierung prüft die Begründung; falls sie dies für gerechtfertigt hält, genehmigt sie die Nichtanwendung der einschlägigen Sachstandsdokumente und genehmigt oder ändert gegebenenfalls die von der Konformitätsbewertungsstelle anzuwendende Bewertungsmethode. Bis zur Entscheidung der nationalen Behörde für die

**▼B**

Cybersicherheitszertifizierung darf die Konformitätsbewertungsstelle kein Zertifikat für das Schutzprofil ausstellen. Die nationale Behörde für die Cybersicherheitszertifizierung teilt die genehmigte Nichtanwendung der einschlägigen Sachstandsdokumente unverzüglich der Europäischen Gruppe für die Cybersicherheitszertifizierung mit, die eine Stellungnahme dazu abgeben kann. Die nationale Behörde für die Cybersicherheitszertifizierung muss der Stellungnahme der Europäischen Gruppe für die Cybersicherheitszertifizierung weitestgehend Rechnung tragen.

*ABSCHNITT II**Ausstellung, Erneuerung und Widerruf von EUCC-Zertifikaten für Schutzprofile***▼M1***Artikel 16***Für die Zertifizierung und Evaluierung von Schutzprofilen erforderliche Informationen**

Wer die Zertifizierung eines Schutzprofils beantragt, muss der Zertifizierungsstelle und der ITSEF alle für die Zertifizierungs- und Evaluierungstätigkeiten erforderlichen Informationen in vollständiger und korrekter Form vorlegen oder anderweitig zur Verfügung stellen. Artikel 8 Absätze 2, 3, 4 und 7 gilt entsprechend.

**▼B***Artikel 17***Ausstellung von EUCC-Zertifikaten für Schutzprofile****▼M1**


---

**▼B**

- (2) Die Artikel 9 und 10 gelten entsprechend.
- (3) Die ITSEF evaluiert, ob ein Schutzprofil vollständig, kohärent, technisch solide und wirksam für die beabsichtigte Verwendung und die Sicherheitsziele der von diesem Schutzprofil erfassten IKT-Produktkategorie ist.
- (4) Ein Schutzprofil darf nur zertifiziert werden von
  - a) einer nationalen Behörde für die Cybersicherheitszertifizierung oder einer anderen als Zertifizierungsstelle akkreditierten öffentlichen Stelle oder
  - b) einer Zertifizierungsstelle nach der vorherigen Genehmigung durch die nationale Behörde für die Cybersicherheitszertifizierung für jedes einzelne Schutzprofil.

*Artikel 18***Geltungsdauer von EUCC-Zertifikaten für Schutzprofile**

- (1) Die Zertifizierungsstelle setzt für jedes EUCC-Zertifikat eine Geltungsdauer fest.
- (2) Die Geltungsdauer kann sich bis zum Ende der Lebensdauer des betreffenden Schutzprofils erstrecken.

**▼ B***Artikel 19***Überprüfung von EUCC-Zertifikaten für Schutzprofile**

(1) Auf Antrag des Zertifikatsinhabers oder aus anderen triftigen Gründen kann die Zertifizierungsstelle ein EUCC-Zertifikat für ein Schutzprofil überprüfen. Die Überprüfung erfolgt unter Anwendung der in Artikel 15 festgelegten Bedingungen. Die Zertifizierungsstelle legt den Umfang der Überprüfung fest. Soweit dies für die Überprüfung erforderlich ist, fordert die Zertifizierungsstelle die ITSEF auf, eine erneute Evaluierung des zertifizierten Schutzprofils durchzuführen.

(2) Je nach den Ergebnissen der Überprüfung und gegebenenfalls der erneuten Evaluierung kann die Zertifizierungsstelle

- a) das EUCC-Zertifikat bestätigen,
- b) das EUCC-Zertifikat gemäß Artikel 20 widerrufen,
- c) das EUCC-Zertifikat gemäß Artikel 20 widerrufen und ein neues EUCC-Zertifikat mit gleichem Anwendungsbereich und verlängerter Geltungsdauer ausstellen oder
- d) das EUCC-Zertifikat gemäß Artikel 20 widerrufen und ein neues EUCC-Zertifikat mit einem veränderten Anwendungsbereich ausstellen.

*Artikel 20***Widerruf von EUCC-Zertifikaten für Schutzprofile**

(1) Unbeschadet des Artikels 58 Absatz 8 Buchstabe e der Verordnung (EU) 2019/881 wird ein EUCC-Zertifikat für ein Schutzprofil von der Zertifizierungsstelle widerrufen, die dieses Zertifikat ausgestellt hatte. Artikel 14 gilt entsprechend.

(2) Ein gemäß Artikel 17 Absatz 4 Buchstabe b ausgestelltes Zertifikat für ein Schutzprofil wird von der nationalen Behörde für die Cybersicherheitszertifizierung widerrufen, die dieses Zertifikat genehmigt hatte.

## KAPITEL IV

**KONFORMITÄTSBEWERTUNGSSTELLEN****▼ M1***Artikel 20a***Spezifikation der Anforderungen an die Akkreditierung von Konformitätsbewertungsstellen**

Bei der Akkreditierung von Konformitätsbewertungsstellen werden die Spezifikationen der Anforderungen an die Akkreditierung von Zertifizierungsstellen und ITSEFs berücksichtigt, die in den geltenden Sachstandsdocumenten festgelegt sind, die in Anhang I Nummer 2 aufgeführt sind.

*Artikel 21***Zusätzliche oder besondere Anforderungen für eine Zertifizierungsstelle**

(1) Eine Zertifizierungsstelle wird von der nationalen Behörde für die Cybersicherheitszertifizierung dazu ermächtigt, EUCC-Zertifikate der Vertrauenswürdigkeitsstufe „hoch“ auszustellen, wenn diese Stelle zusätzlich zur Erfüllung der Anforderungen des Artikels 60 Absatz 1 und des Anhangs der Verordnung (EU) 2019/881 in Bezug auf die Akkreditierung von Konformitätsbewertungsstellen Folgendes nachweist:

- a) Sie verfügt über die für die Zertifizierungsentscheidung auf der Vertrauenswürdigkeitsstufe „hoch“ erforderlichen Fachkenntnisse und Kompetenzen;
- b) sie führt ihre Zertifizierungstätigkeiten in Zusammenarbeit mit einer gemäß Artikel 22 zugelassenen ITSEF durch;
- c) sie verfügt zusätzlich zu den Anforderungen des Artikels 43 über die erforderlichen Kompetenzen und trifft geeignete technische und betriebliche Maßnahmen zum wirksamen Schutz vertraulicher und sensibler Informationen auf der Vertrauenswürdigkeitsstufe „hoch“.

(2) Die nationale Behörde für die Cybersicherheitszertifizierung bewertet, ob eine Zertifizierungsstelle alle in Absatz 1 genannten Anforderungen erfüllt. Diese Bewertung umfasst zumindest strukturierte Befragungen und die Überprüfung von mindestens einer Pilotzertifizierung, die von der Zertifizierungsstelle gemäß dieser Verordnung durchgeführt wurde.

Bei ihrer Bewertung kann die nationale Behörde für die Cybersicherheitszertifizierung alle geeigneten Nachweise aus einer vorherigen Zulassung oder ähnlichen Tätigkeiten weiterverwenden, die beruhen auf

- a) der vorliegenden Verordnung,
- b) einem anderen europäischen System für die Cybersicherheitszertifizierung, das gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurde,
- c) einem in Artikel 49 der vorliegenden Verordnung genannten System.

(3) Die nationale Behörde für die Cybersicherheitszertifizierung erstellt einen Zulassungsbericht, der einer gegenseitigen Begutachtung gemäß Artikel 59 Absatz 3 Buchstabe d der Verordnung (EU) 2019/881 unterzogen wird.

(4) Die nationale Behörde für die Cybersicherheitszertifizierung gibt die IKT-Produktkategorien und Schutzprofile an, auf die sich die Zulassung erstreckt. Die Zulassung gilt für einen Zeitraum, der nicht länger als die Geltungsdauer der Akkreditierung ist. Sie kann auf Antrag verlängert werden, sofern die Zertifizierungsstelle die Anforderungen dieses Artikels noch immer erfüllt. Für eine Erneuerung der Zulassung sind keine Pilotevaluierungen erforderlich.

(5) Die nationale Behörde für die Cybersicherheitszertifizierung widerruft die Zulassung der Zertifizierungsstelle, wenn diese nicht mehr alle in diesem Artikel festgelegten Bedingungen erfüllt. Ab dem Widerruf der Zulassung darf die Zertifizierungsstelle sich selbst nicht mehr als zugelassene Zertifizierungsstelle bezeichnen.

*Artikel 22***Zusätzliche oder besondere Anforderungen an eine ITSEF**

(1) Eine ITSEF wird von der nationalen Behörde für die Cybersicherheitszertifizierung dazu ermächtigt, Evaluierungen für IKT-Produkte durchzuführen, die auf der Vertrauenswürdigkeitsstufe „hoch“ zertifiziert werden sollen, wenn die ITSEF zusätzlich zur Erfüllung der Anforderungen des Artikels 60 Absatz 1 und des Anhangs der Verordnung (EU) 2019/881 in Bezug auf die Akkreditierung von Konformitätsbewertungsstellen die Erfüllung aller folgenden Bedingungen nachweist:

a) sie hat die erforderliche Sachkenntnis für die Durchführung der Evaluierungstätigkeiten zur Ermittlung der Widerstandsfähigkeit gegen Cyberangriffe, die dem neuesten Stand der Technik entsprechen und von Akteuren mit umfangreichen Fähigkeiten und Ressourcen durchgeführt werden;

b) sie verfügt für die technischen Bereiche und Schutzprofile, die Teil des IKT-Prozesses für die betreffenden IKT-Produkte sind, über

1) die Sachkenntnis zur Durchführung der besonderen Evaluierungstätigkeiten, die erforderlich sind, um die Widerstandsfähigkeit des Evaluierungsgegenstands in seiner Betriebsumgebung gegen kompetente Angreifer unter der Annahme eines „mäßigen“ oder „hohen“ Angriffspotenzials gemäß den in Artikel 3 genannten Normen zu bestimmen;

2) die technischen Kompetenzen gemäß den in Anhang I aufgeführten Sachstandsdokumenten;

c) sie verfügt zusätzlich zu den Anforderungen des Artikels 43 über die erforderlichen Kompetenzen und trifft geeignete technische und betriebliche Maßnahmen zum wirksamen Schutz vertraulicher und sensibler Informationen auf der Vertrauenswürdigkeitsstufe „hoch“.

(2) Die nationale Behörde für die Cybersicherheitszertifizierung bewertet, ob eine ITSEF alle in Absatz 1 genannten Anforderungen erfüllt. Diese Bewertung umfasst zumindest strukturierte Befragungen und die Überprüfung von mindestens einer Pilotevaluierung, die von der ITSEF gemäß dieser Verordnung durchgeführt wurde.

(3) Bei ihrer Bewertung kann die nationale Behörde für die Cybersicherheitszertifizierung alle geeigneten Nachweise aus einer vorherigen Zulassung oder ähnlichen Tätigkeiten weiterverwenden, die beruhen auf

a) der vorliegenden Verordnung,

b) einem anderen europäischen System für die Cybersicherheitszertifizierung, das gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurde,

c) einem in Artikel 49 der vorliegenden Verordnung genannten System.

(4) Die nationale Behörde für die Cybersicherheitszertifizierung erstellt einen Zulassungsbericht, der einer gegenseitigen Begutachtung gemäß Artikel 59 Absatz 3 Buchstabe d der Verordnung (EU) 2019/881 unterzogen wird.

**▼B**

(5) Die nationale Behörde für die Cybersicherheitszertifizierung gibt die IKT-Produktkategorien und Schutzprofile an, auf die sich die Zulassung erstreckt. Die Zulassung gilt für einen Zeitraum, der nicht länger als die Geltungsdauer der Akkreditierung ist. Sie kann auf Antrag verlängert werden, sofern die ITSEF die Anforderungen dieses Artikels noch immer erfüllt. Für eine Erneuerung der Zulassung sind keine Pilotevaluierungen erforderlich.

(6) Die nationale Behörde für die Cybersicherheitszertifizierung widerruft die Zulassung der ITSEF, wenn diese nicht mehr alle in diesem Artikel festgelegten Bedingungen erfüllt. Ab dem Widerruf der Zulassung darf die ITSEF sich selbst nicht mehr als zugelassene ITSEF bezeichnen.

**▼M1****▼B**

## KAPITEL V

## ÜBERWACHUNG, NICHTKONFORMITÄT UND NICHTEINHALTUNG

## ABSCHNITT 1

*Überwachung der Einhaltung der Vorschriften**Artikel 25***Überwachungstätigkeiten der nationalen Behörde für die Cybersicherheitszertifizierung**

(1) Unbeschadet des Artikels 58 Absatz 7 der Verordnung (EU) 2019/881 überwacht die nationale Behörde für die Cybersicherheitszertifizierung, dass

- a) die Zertifizierungsstelle und die ITSEF ihren Verpflichtungen gemäß der vorliegenden Verordnung und der Verordnung (EU) 2019/881 nachkommen;
- b) die Inhaber eines EUCC-Zertifikats ihren Verpflichtungen gemäß der vorliegenden Verordnung und der Verordnung (EU) 2019/881 nachkommen;
- c) die zertifizierten IKT-Produkte den im EUCC-System festgelegten Anforderungen entsprechen;
- d) die im EUCC-Zertifikat ausgedrückte Vertrauenswürdigkeit der sich wandelnden Bedrohungslage gerecht wird.

(2) Die nationale Behörde für die Cybersicherheitszertifizierung führt ihre Überwachungstätigkeiten insbesondere auf folgender Grundlage durch:

- a) Informationen von Zertifizierungsstellen, nationalen Akkreditierungsstellen und zuständigen Marktüberwachungsbehörden,
- b) Informationen aus eigenen Prüfungen und Untersuchungen und denen anderer Behörden,
- c) Stichprobenuntersuchungen gemäß Absatz 3,
- d) eingegangene Beschwerden.

**▼ B**

(3) Die nationale Behörde für die Cybersicherheitszertifizierung überprüft in Zusammenarbeit mit anderen Marktüberwachungsbehörden jährlich eine Stichprobe von mindestens 4 % der EUCC-Zertifikate, die anhand einer Risikobewertung ermittelt wird. Zertifizierungsstellen und nötigenfalls ITSEF unterstützen die zuständige nationale Behörde für die Cybersicherheitszertifizierung auf deren Verlangen und in deren Namen bei der Überwachung der Einhaltung der Vorschriften.

(4) Die nationale Behörde für die Cybersicherheitszertifizierung wählt die Stichprobe der zu überprüfenden zertifizierten IKT-Produkte anhand objektiver Kriterien aus, darunter:

- a) Produktkategorie,
- b) Vertrauenswürdigkeitsstufen der Produkte,
- c) Zertifikatsinhaber,
- d) Zertifizierungsstelle und gegebenenfalls beauftragte ITSEF,
- e) sonstige Informationen, die der Behörde zur Kenntnis gebracht werden.

(5) Die nationale Behörde für die Cybersicherheitszertifizierung unterrichtet die Inhaber der EUCC-Zertifikate über die ausgewählten IKT-Produkte und die Auswahlkriterien.

(6) Die Zertifizierungsstelle, die das in die Stichprobe einbezogene IKT-Produkt zertifiziert hat, führt im Auftrag der nationalen Behörde für die Cybersicherheitszertifizierung und mit Unterstützung der jeweiligen ITSEF zusätzliche Überprüfungen nach dem in Anhang IV Abschnitt IV.2 festgelegten Verfahren durch und übermittelt der nationalen Behörde für die Cybersicherheitszertifizierung die Ergebnisse.

(7) Wenn die nationale Behörde für die Cybersicherheitszertifizierung hinreichende Gründe zu der Annahme hat, dass ein zertifiziertes IKT-Produkt nicht mehr den Anforderungen dieser Verordnung oder der Verordnung (EU) 2019/881 genügt, kann sie Untersuchungen durchführen oder von anderen Überwachungsbefugnissen gemäß Artikel 58 Absatz 8 der Verordnung (EU) 2019/881 Gebrauch machen.

(8) Die nationale Behörde für die Cybersicherheitszertifizierung unterrichtet die betreffende Zertifizierungsstelle und die ITSEF über laufende Untersuchungen zu ausgewählten IKT-Produkten.

(9) Wenn die nationale Behörde für die Cybersicherheitszertifizierung feststellt, dass eine laufende Untersuchung IKT-Produkte betrifft, die von Zertifizierungsstellen in anderen Mitgliedstaaten zertifiziert wurden, setzt sie die nationalen Behörden für die Cybersicherheitszertifizierung in den betreffenden Mitgliedstaaten davon in Kenntnis, damit diese gegebenenfalls an den Untersuchungen mitwirken können. Außerdem unterrichtet diese nationale Behörde für die Cybersicherheitszertifizierung die Europäische Gruppe für die Cybersicherheitszertifizierung über die grenzübergreifenden Untersuchungen und deren Ergebnisse.

**▼ B***Artikel 26***Überwachungstätigkeiten der Zertifizierungsstelle**

- (1) Die Zertifizierungsstelle überwacht
  - a) die Erfüllung der Verpflichtungen aus der vorliegenden Verordnung und der Verordnung (EU) 2019/881 in Bezug auf das von der Zertifizierungsstelle ausgestellte EUCC-Zertifikat durch die Zertifikatsinhaber,
  - b) die Einhaltung der jeweiligen an die von ihr zertifizierten IKT-Produkte gestellten Sicherheitsanforderungen,
  - c) die in den zertifizierten Schutzprofilen ausgedrückte Vertrauenswürdigkeit.
- (2) Die Zertifizierungsstelle führt ihre Überwachungstätigkeiten auf folgender Grundlage durch:
  - a) Informationen, die der Zertifizierungsantragsteller aufgrund seiner Verpflichtungen nach Artikel 9 Absatz 2 vorgelegt hat;
  - b) Informationen, die sich aus Tätigkeiten anderer einschlägiger Marktüberwachungsbehörden ergeben;
  - c) eingegangene Beschwerden;
  - d) Informationen über Schwachstellen, die sich auf die von ihr zertifizierten IKT-Produkte auswirken könnten.
- (3) Die nationale Behörde für die Cybersicherheitszertifizierung kann unbeschadet ihrer Tätigkeiten im Zusammenhang mit anderen zuständigen Marktüberwachungsbehörden Vorschriften für einen regelmäßigen Dialog zwischen Zertifizierungsstellen und Inhabern von EUCC-Zertifikaten festlegen, um die Einhaltung der nach Artikel 9 Absatz 2 eingegangenen Verpflichtungen zu überprüfen und darüber Bericht zu erstatten.

*Artikel 27***Überwachungstätigkeiten des Zertifikatsinhabers**

- (1) Der Inhaber eines EUCC-Zertifikats nimmt folgende Aufgaben wahr, um die Konformität des zertifizierten IKT-Produkts mit den daran gestellten Sicherheitsanforderungen zu überwachen:
  - a) Überwachung von Informationen über Schwachstellen in Bezug auf das zertifizierte IKT-Produkt, einschließlich bekannter Abhängigkeiten, mit seinen eigenen Mitteln, aber auch unter Beachtung von
    - 1) Veröffentlichungen oder Mitteilungen mit Informationen über Schwachstellen von Nutzern oder Sicherheitsforschern gemäß Artikel 55 Absatz 1 Buchstabe c der Verordnung (EU) 2019/881;
    - 2) Mitteilungen von anderen Quellen;
  - b) Überwachung der im EUCC-Zertifikat ausgedrückten Vertrauenswürdigkeit.

**▼B**

(2) Der Inhaber eines EUCC-Zertifikats muss mit der Zertifizierungsstelle, der ITSEF und gegebenenfalls mit der nationalen Behörde für die Cybersicherheitszertifizierung zusammenarbeiten, um deren Überwachungstätigkeiten zu unterstützen.

*ABSCHNITT II****Konformität und Einhaltung****Artikel 28***Folgen der Nichtkonformität eines zertifizierten IKT-Produkts oder Schutzprofils**

(1) Wenn ein zertifiziertes IKT-Produkt oder Schutzprofil den Anforderungen der vorliegenden Verordnung und der Verordnung (EU) 2019/881 nicht genügt, benachrichtigt die Zertifizierungsstelle den Inhaber des EUCC-Zertifikats über die festgestellte Nichtkonformität und fordert ihn auf, Abhilfemaßnahmen zu ergreifen.

(2) Wenn sich eine Nichtkonformität mit den Bestimmungen dieser Verordnung auf die Einhaltung anderer einschlägiger Rechtsvorschriften der Union auswirken könnte, in denen die Möglichkeit vorgesehen ist, die Vermutung der Konformität mit den Anforderungen der betreffenden Vorschriften anhand des EUCC-Zertifikats nachzuweisen, setzt die Zertifizierungsstelle unverzüglich die nationale Behörde für die Cybersicherheitszertifizierung davon in Kenntnis. Die nationale Behörde für die Cybersicherheitszertifizierung unterrichtet unverzüglich die für diese anderen einschlägigen Rechtsvorschriften der Union zuständige Marktüberwachungsbehörde über die festgestellte Nichtkonformität.

(3) Nach Erhalt der in Absatz 1 genannten Informationen schlägt der Inhaber des EUCC-Zertifikats der Zertifizierungsstelle innerhalb der von ihr gesetzten Frist, die 30 Tage nicht überschreiten darf, die zur Beseitigung der Nichtkonformität erforderlichen Abhilfemaßnahmen vor.

(4) Die Zertifizierungsstelle kann das EUCC-Zertifikat im Notfall, oder falls der Inhaber des EUCC-Zertifikats nicht ordnungsgemäß mit ihr zusammenarbeitet, gemäß Artikel 30 unverzüglich aussetzen.

(5) Die Zertifizierungsstelle führt eine Überprüfung gemäß den Artikeln 13 und 19 durch, um zu bewerten, ob die Nichtkonformität mit den Abhilfemaßnahmen beseitigt wird.

(6) Wenn der Inhaber des EUCC-Zertifikats innerhalb der in Absatz 3 genannten Frist keine geeigneten Abhilfemaßnahmen vorschlägt, wird das Zertifikat gemäß Artikel 30 ausgesetzt oder gemäß Artikel 14 oder Artikel 20 widerrufen.

(7) Dieser Artikel findet keine Anwendung auf Schwachstellen, die ein zertifiziertes IKT-Produkt betreffen und gemäß Kapitel VI behandelt werden.

*Artikel 29***Folgen der Nichteinhaltung durch den Zertifikatsinhaber**

(1) Stellt die Zertifizierungsstelle fest, dass

a) der Inhaber des EUCC-Zertifikats oder der Zertifizierungsantragsteller seinen Zusagen und Verpflichtungen gemäß Artikel 9 Absatz 2, Artikel 17 Absatz 2, Artikel 27 und Artikel 41 nicht nachkommt oder

**▼B**

- b) der Inhaber des EUCC-Zertifikats gegen Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 oder Kapitel VI der vorliegenden Verordnung verstößt,

setzt sie ihm eine Frist von höchstens 30 Tagen, innerhalb deren der Inhaber des EUCC-Zertifikats Abhilfemaßnahmen ergreifen muss.

**▼MI**

- (2) Wenn der Inhaber des EUCC-Zertifikats innerhalb der in Absatz 1 genannten Frist keine geeigneten Abhilfemaßnahmen vorschlägt, wird das Zertifikat gemäß Artikel 30 ausgesetzt oder gemäß Artikel 14 oder Artikel 20 widerrufen.

**▼B**

- (3) Ein anhaltender oder wiederholter Verstoß des Inhabers des EUCC-Zertifikats gegen die in Absatz 1 genannten Verpflichtungen führt zum Widerruf des EUCC-Zertifikats gemäß Artikel 14 oder Artikel 20.

- (4) Die Zertifizierungsstelle unterrichtet die nationale Behörde für die Cybersicherheitszertifizierung über die in Absatz 1 genannten Feststellungen. Wenn der Verstoß die Einhaltung anderer einschlägiger Rechtsvorschriften der Union beeinträchtigt, unterrichtet die nationale Behörde für die Cybersicherheitszertifizierung unverzüglich die für diese anderen einschlägigen Rechtsvorschriften der Union zuständige Marktüberwachungsbehörde über die festgestellte Nichteinhaltung.

*Artikel 30***Aussetzung des EUCC-Zertifikats**

- (1) Bei einer Aussetzung eines EUCC-Zertifikats nach dieser Verordnung, setzt die Zertifizierungsstelle das betreffende EUCC-Zertifikat für einen Zeitraum aus, der den Umständen, die Anlass zu der Aussetzung geben, angemessen ist und 42 Tage nicht überschreitet. Der Aussetzungszeitraum beginnt an dem auf den Aussetzungsbeschluss der Zertifizierungsstelle folgenden Tag. Die Aussetzung lässt die Geltung des Zertifikats unberührt.

- (2) Die Zertifizierungsstelle unterrichtet den Zertifikatsinhaber und die nationale Behörde für die Cybersicherheitszertifizierung unverzüglich über die Aussetzung unter Angabe der Aussetzungsgründe, der verlangten Abhilfemaßnahmen und der Aussetzungsdauer.

- (3) Der Zertifikatsinhaber benachrichtigt die Käufer der betreffenden IKT-Produkte über die Aussetzung und die von der Zertifizierungsstelle angegebenen Aussetzungsgründe, mit Ausnahme der Teile der Begründung, deren Bekanntwerden ein Sicherheitsrisiko darstellen würde oder die sensible Informationen enthalten. Der Zertifikatsinhaber macht diese Informationen auch öffentlich zugänglich.

- (4) Wenn andere einschlägige Rechtsvorschriften der Union eine Konformitätsvermutung auf der Grundlage von Zertifikaten vorsehen, die nach den Bestimmungen der vorliegenden Verordnung ausgestellt wurden, so unterrichtet die nationale Behörde für die Cybersicherheitszertifizierung die für diese anderen einschlägigen Rechtsvorschriften der Union zuständige Marktüberwachungsbehörde über die Aussetzung.

- (5) Die Aussetzung eines Zertifikats wird der ENISA gemäß Artikel 42 Absatz 3 mitgeteilt.

- (6) In hinreichend begründeten Fällen kann die nationale Behörde für die Cybersicherheitszertifizierung eine Verlängerung der Aussetzung eines EUCC-Zertifikats genehmigen. Die Gesamtdauer der Aussetzung darf ein Jahr nicht überschreiten.

**▼B***Artikel 31***Folgen der Nichteinhaltung durch die Konformitätsbewertungsstelle**

(1) Wenn eine Zertifizierungsstelle ihren Verpflichtungen nicht nachkommt oder wenn im Falle der Feststellung eines Verstoßes durch eine ITSEF die zuständige Zertifizierungsstelle ihren Verpflichtungen nicht nachkommt, muss die nationale Behörde für die Cybersicherheitszertifizierung unverzüglich

- a) mit Unterstützung der ITSEF die möglicherweise davon betroffenen EUCC-Zertifikate ermitteln;
- b) erforderlichenfalls veranlassen, dass entweder die ITSEF, die die Evaluierung durchgeführt hatte, oder eine andere akkreditierte und gegebenenfalls zugelassene ITSEF, die fachlich besser dazu in der Lage ist, bestimmte Evaluierungstätigkeiten zu einem oder mehreren IKT-Produkten oder Schutzprofilen durchführt, um diese Ermittlung zu unterstützen;
- c) die Auswirkungen der Nichteinhaltung analysieren;
- d) den Inhaber des von der Nichteinhaltung betroffenen EUCC-Zertifikats benachrichtigen.

(2) Auf der Grundlage der in Absatz 1 genannten Maßnahmen fasst die Zertifizierungsstelle zu jedem betroffenen EUCC-Zertifikat einen der folgenden Beschlüsse:

- a) unveränderte Aufrechterhaltung des EUCC-Zertifikats,
- b) Widerruf des EUCC-Zertifikats gemäß Artikel 14 oder Artikel 20 und gegebenenfalls Ausstellung eines neuen EUCC-Zertifikats.

(3) Auf der Grundlage der in Absatz 1 genannten Maßnahmen muss die nationale Behörde für die Cybersicherheitszertifizierung

- a) erforderlichenfalls der nationalen Akkreditierungsstelle die Nichteinhaltung durch die Zertifizierungsstelle oder die betreffende ITSEF melden;
- b) gegebenenfalls die möglichen Auswirkungen auf die Zulassung prüfen.

## KAPITEL VI

**SCHWACHSTELLENMANAGEMENT UND OFFENLEGUNG VON SCHWACHSTELLEN***Artikel 32***Anwendungsbereich des Schwachstellenmanagements**

Dieses Kapitel gilt für IKT-Produkte, für die ein EUCC-Zertifikat ausgestellt wurde.

## ABSCHNITT 1

***Schwachstellenmanagement****Artikel 33***Schwachstellenmanagementverfahren**

(1) Der Inhaber eines EUCC-Zertifikats muss alle erforderlichen Verfahren für das Schwachstellenmanagement gemäß den Vorschriften dieses Abschnitts, die nötigenfalls durch die in der Norm EN ISO/IEC 30111 festgelegten Verfahren ergänzt werden, festlegen und aufrechterhalten.

**▼B**

- (2) Der Inhaber eines EUCC-Zertifikats unterhält und veröffentlicht geeignete Methoden für die Einholung von Informationen über Schwachstellen in Bezug auf sein Produkt aus externen Quellen, darunter auch von Nutzern, Zertifizierungsstellen und Sicherheitsforschern.
- (3) Wenn ein Inhaber eines EUCC-Zertifikats eine mögliche Schwachstelle in Bezug auf ein zertifiziertes IKT-Produkt feststellt oder Informationen hierüber erhält, zeichnet er diese Informationen auf und führt eine Analyse der Auswirkungen der Schwachstellen durch.
- (4) Wenn sich eine mögliche Schwachstelle auf ein zusammengesetztes Produkt auswirkt, informiert der Inhaber des EUCC-Zertifikats die Inhaber abhängiger EUCC-Zertifikate über die mögliche Schwachstelle.
- (5) Auf angemessenes Verlangen der Zertifizierungsstelle, die das Zertifikat ausgestellt hat, übermittelt der Inhaber eines EUCC-Zertifikats dieser Zertifizierungsstelle alle relevanten Informationen über mögliche Schwachstellen.

*Artikel 34***Analyse der Auswirkungen der Schwachstelle**

- (1) Die Analyse der Auswirkungen der Schwachstellen bezieht sich auf den Evaluierungsgegenstand und die im Zertifikat enthaltenen Aussagen zur Vertrauenswürdigkeit. Die Analyse der Auswirkungen der Schwachstelle wird innerhalb eines Zeitrahmens durchgeführt, der angesichts der Ausnutzbarkeit und Kritikalität der möglichen Schwachstelle des zertifizierten IKT-Produkts angemessen ist.
- (2) Soweit zutreffend wird eine Berechnung des Angriffspotenzials nach der einschlägigen Methodik durchgeführt, die in den in Artikel 3 genannten Normen und den in Anhang I aufgeführten einschlägigen Sachstandsdocumenten enthalten ist, um die Ausnutzbarkeit der Schwachstelle zu ermitteln. Dabei wird die AVA\_VAN-Stufe des EUCC-Zertifikats berücksichtigt.

*Artikel 35***Bericht über die Analyse der Auswirkungen der Schwachstelle**

- (1) Der Inhaber erstellt einen Bericht über die Analyse der Auswirkungen der Schwachstelle, wenn aus der Analyse der Auswirkungen hervorgeht, dass sich die Schwachstelle wahrscheinlich auf die Konformität des IKT-Produkts mit dessen Zertifikat auswirkt.
- (2) Der Bericht über die Analyse der Auswirkungen der Schwachstelle muss eine Bewertung folgender Elemente enthalten:
- a) die Auswirkungen der Schwachstelle auf das zertifizierte IKT-Produkt;
  - b) mögliche Risiken im Zusammenhang mit der Nähe oder Verfügbarkeit einer Angriffsmöglichkeit;
  - c) ob die Schwachstelle beseitigt werden kann;
  - d) falls die Schwachstelle beseitigt werden kann, mögliche Lösungen für die Beseitigung der Schwachstelle.
- (3) Der Bericht über die Analyse der Auswirkungen der Schwachstelle enthält, soweit zutreffend, Einzelheiten über mögliche Mittel der Ausnutzung der Schwachstelle. Informationen über mögliche Mittel der Ausnutzung der Schwachstelle werden unter Einhaltung geeigneter Sicherheitsvorkehrungen behandelt, um ihre Vertraulichkeit zu schützen und nötigenfalls ihre Verbreitung zu begrenzen.

**▼B**

(4) Der Inhaber eines EUCC-Zertifikats übermittelt der Zertifizierungsstelle oder der nationalen Behörde für die Cybersicherheitszertifizierung unverzüglich einen Bericht über die Analyse der Auswirkungen der Schwachstelle gemäß Artikel 56 Absatz 8 der Verordnung (EU) 2019/881.

(5) Wenn in dem Bericht über die Analyse der Auswirkungen der Schwachstelle festgestellt wird, dass die Schwachstelle kein verbleibendes Restrisiko im Sinne der in Artikel 3 genannten Normen darstellt und dass sie beseitigt werden kann, wird Artikel 36 angewandt.

(6) Wenn in dem Bericht über die Analyse der Auswirkungen der Schwachstelle festgestellt wird, dass die Schwachstelle kein verbleibendes Restrisiko darstellt und dass sie nicht beseitigt werden kann, wird das EUCC-Zertifikat gemäß Artikel 14 widerrufen.

(7) Der Inhaber des EUCC-Zertifikats überwacht ein etwaiges verbleibendes Restrisiko aus der Schwachstelle, um sicherzustellen, dass sie im Falle von Änderungen im betrieblichen Umfeld nicht doch ausgenutzt werden kann.

*Artikel 36***Beseitigung von Schwachstellen**

Der Inhaber eines EUCC-Zertifikats legt der Zertifizierungsstelle einen Vorschlag für geeignete Abhilfemaßnahmen vor. Die Zertifizierungsstelle überprüft das EUCC-Zertifikat gemäß Artikel 13. Der Umfang der Überprüfung hängt von der vorgeschlagenen Beseitigung der Schwachstelle ab.

*ABSCHNITT II***Offenlegung von Schwachstellen***Artikel 37***Weitergabe von Informationen an die nationale Behörde für die Cybersicherheitszertifizierung**

(1) Die von der Zertifizierungsstelle an die nationale Behörde für die Cybersicherheitszertifizierung übermittelten Informationen müssen alle Elemente enthalten, die erforderlich sind, damit die nationale Behörde für die Cybersicherheitszertifizierung die Auswirkungen der Schwachstelle und die an dem IKT-Produkt vorzunehmenden Änderungen erfassen kann, sowie gegebenenfalls Angaben der Zertifizierungsstelle über weiterreichende Auswirkungen der Schwachstelle auf andere zertifizierte IKT-Produkte.

(2) Die gemäß Absatz 1 übermittelten Informationen dürfen keine Einzelheiten über die Mittel der Ausnutzung der Schwachstelle enthalten. Diese Bestimmung lässt die Untersuchungsbefugnisse der nationalen Behörde für die Cybersicherheitszertifizierung unberührt.

*Artikel 38***Zusammenarbeit mit anderen nationalen Behörden für die Cybersicherheitszertifizierung**

(1) Die nationale Behörde für die Cybersicherheitszertifizierung leitet die einschlägigen Informationen, die sie gemäß Artikel 37 erhalten hat, an andere nationale Behörden für die Cybersicherheitszertifizierung und die ENISA weiter.

**▼B**

(2) Andere nationale Behörden für die Cybersicherheitszertifizierung können die Schwachstelle weiter analysieren oder nach Unterrichtung des Inhabers des EUCC-Zertifikats die zuständigen Zertifizierungsstellen auffordern zu bewerten, ob die Schwachstelle andere zertifizierte IKT-Produkte betreffen könnte.

*Artikel 39***Veröffentlichung von Schwachstellen**

Nach dem Widerruf eines Zertifikats muss der Inhaber des EUCC-Zertifikats alle öffentlich bekannten und beseitigten Schwachstellen in dem IKT-Produkt offenlegen und in der gemäß Artikel 12 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates<sup>(1)</sup> eingerichteten europäischen Schwachstellendatenbank oder in anderen Online-Registern gemäß Artikel 55 Absatz 1 Buchstabe d der Verordnung (EU) 2019/881 registrieren.

## KAPITEL VII

**AUFBEWAHRUNG, OFFENLEGUNG UND SCHUTZ VON INFORMATIONEN***Artikel 40***Aufbewahrung von Aufzeichnungen durch Zertifizierungsstellen und ITSEF**

(1) ITSEF und Zertifizierungsstellen führen ein Aufzeichnungssystem, das alle Unterlagen enthält, die im Zusammenhang mit jeder von ihnen durchgeführten Evaluierung und Zertifizierung erstellt werden.

(2) Zertifizierungsstellen und ITSEF speichern die Aufzeichnungen in sicherer Weise und bewahren diese Aufzeichnungen so lange auf, wie dies für die Zwecke dieser Verordnung erforderlich ist, mindestens aber für fünf Jahre nach Widerruf des betreffenden EUCC-Zertifikats. Wenn die Zertifizierungsstelle ein neues EUCC-Zertifikat gemäß Artikel 13 Absatz 2 Buchstabe c ausgestellt hat, bewahrt sie die Dokumentation des widerrufenen EUCC-Zertifikats so lange wie das neue EUCC-Zertifikat zusammen mit diesem auf.

*Artikel 41***Vom Zertifikatsinhaber zur Verfügung gestellte Informationen**

(1) Die in Artikel 55 der Verordnung (EU) 2019/881 genannten Informationen müssen in einer für die Nutzer leicht zugänglichen Sprache verfügbar sein.

(2) Der Inhaber eines EUCC-Zertifikats speichert die folgenden Informationen in sicherer Weise und so lange, wie dies für die Zwecke dieser Verordnung erforderlich ist, mindestens aber für fünf Jahre nach Widerruf des betreffenden EUCC-Zertifikats:

- a) Aufzeichnungen über die Informationen, die der Zertifizierungsstelle und der ITSEF während des Zertifizierungsverfahrens übermittelt wurden,
- b) ein Musterexemplar des zertifizierten IKT-Produkts.

<sup>(1)</sup> Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).

**▼B**

(3) Wenn die Zertifizierungsstelle ein neues EUCC-Zertifikat gemäß Artikel 13 Absatz 2 Buchstabe c ausgestellt hat, bewahrt der Inhaber die Dokumentation des widerrufenen EUCC-Zertifikats so lange wie das neue EUCC-Zertifikat zusammen mit diesem auf.

(4) Auf Verlangen der Zertifizierungsstelle oder der nationalen Behörde für die Cybersicherheitszertifizierung stellt der Inhaber eines EUCC-Zertifikats die in Absatz 2 genannten Aufzeichnungen und Kopien zur Verfügung.

*Artikel 42***Von der ENISA bereitzustellende Informationen**

(1) Die ENISA veröffentlicht die folgenden Informationen auf der in Artikel 50 Absatz 1 der Verordnung (EU) 2019/881 genannten Website:

- a) alle EUCC-Zertifikate,
- b) Angaben zum Status eines EUCC-Zertifikats, insbesondere, ob es in Kraft, ausgesetzt, widerrufen oder abgelaufen ist,
- c) Zertifizierungsberichte zu jedem EUCC-Zertifikat,
- d) eine Liste der akkreditierten Konformitätsbewertungsstellen,
- e) eine Liste der zugelassenen Konformitätsbewertungsstellen,
- f) die Sachstandsdokumente, die in Anhang I aufgeführt sind,
- g) die Stellungnahmen der Europäischen Gruppe für die Cybersicherheitszertifizierung gemäß Artikel 62 Absatz 4 Buchstabe c der Verordnung (EU) 2019/881,
- h) Berichte über die gegenseitige Beurteilung, die gemäß Artikel 47 erstellt werden.

(2) Die in Absatz 1 genannten Informationen sind zumindest in englischer Sprache bereitzustellen.

(3) Zertifizierungsstellen und gegebenenfalls nationale Behörden für die Cybersicherheitszertifizierung unterrichten die ENISA unverzüglich über ihre Entscheidungen, die sich auf den Inhalt oder den Status eines in Absatz 1 Buchstabe b genannten EUCC-Zertifikats auswirken.

(4) Die ENISA stellt sicher, dass aus den gemäß Absatz 1 Buchstaben a, b und c veröffentlichten Informationen eindeutig hervorgeht, welche Versionen eines zertifizierten IKT-Produkts von einem EUCC-Zertifikat erfasst werden.

*Artikel 43***Schutz von Informationen**

Die Konformitätsbewertungsstellen, die nationalen Behörden für die Cybersicherheitszertifizierung, die Europäische Gruppe für die Cybersicherheitszertifizierung, die ENISA, die Kommission und alle anderen Beteiligten gewährleisten die Sicherheit und den Schutz von Unternehmensgeheimnissen und anderen vertraulichen Informationen, einschließlich Geschäftsgeheimnissen, sowie die Wahrung der Rechte des geistigen Eigentums und ergreifen alle hierzu erforderlichen und geeigneten technischen und organisatorischen Maßnahmen.



## KAPITEL VIII

ABKOMMEN MIT DRITTLÄNDERN ÜBER DIE GEGENSEITIGE  
ANERKENNUNG*Artikel 44***Bedingungen**

- (1) Drittländer, die ihre Produkte gemäß dieser Verordnung zertifizieren und eine solche Zertifizierung innerhalb der Union anerkannt haben wollen, müssen mit der Union ein Abkommen über die gegenseitige Anerkennung schließen.
- (2) Ein Abkommen über die gegenseitige Anerkennung regelt die Vertrauenswürdigkeitsstufen, die für zertifizierte IKT-Produkte und gegebenenfalls für Schutzprofile gelten.
- (3) Ein Abkommen über die gegenseitige Anerkennung gemäß Absatz 1 kann nur mit Drittländern geschlossen werden, die folgende Bedingungen erfüllen:
  - a) Sie haben eine Behörde, die
    - 1) eine öffentliche Stelle ist, die unabhängig von den Einrichtungen ist, deren Organisations- und Rechtsstruktur, Finanzierung und Entscheidungsfindung sie beaufsichtigt und überwacht,
    - 2) über angemessene Überwachungs- und Aufsichtsbefugnisse zur Durchführung von Untersuchungen verfügt und befugt ist, geeignete Korrekturmaßnahmen zu ergreifen, um die Einhaltung der Vorschriften zu gewährleisten,
    - 3) über ein wirksames, verhältnismäßiges und abschreckendes Sanktionssystem verfügt, um die Einhaltung der Vorschriften zu gewährleisten,
    - 4) bereit ist, mit der Europäischen Gruppe für die Cybersicherheitszertifizierung und der ENISA zusammenzuarbeiten, um bewährte Verfahren und Informationen über wichtige Entwicklungen im Bereich der Cybersicherheitszertifizierung auszutauschen und auf eine einheitliche Auslegung der derzeit geltenden Evaluierungskriterien und -methoden hinzuwirken, indem sie unter anderem eine harmonisierte Dokumentation verwendet, die den in Anhang I aufgeführten Sachstandsdokumenten gleichwertig ist;
  - b) sie haben eine unabhängige Akkreditierungsstelle, die Akkreditierungen nach Normen durchführt, die den in der Verordnung (EG) Nr. 765/2008 genannten Normen gleichwertig sind;
  - c) sie gehen die Verpflichtung ein, dass die Evaluierungs- und Zertifizierungsverfahren ordnungsgemäß und professionell durchgeführt werden und dass dabei die in dieser Verordnung, insbesondere in Artikel 3, genannten internationalen Normen beachtet werden;
  - d) sie sind in der Lage, bislang nicht erkannte Schwachstellen zu melden, und haben ein festgelegtes, geeignetes Verfahren für das Schwachstellenmanagement und die Offenlegung von Schwachstellen;
  - e) sie haben festgelegte Verfahren, die eine wirksame Einreichung und Bearbeitung von Beschwerden ermöglichen und dem Beschwerdeführer einen wirksamen Rechtsbehelf bieten;

**▼B**

- f) sie schaffen einen Mechanismus für die Zusammenarbeit mit anderen Stellen der Union und der Mitgliedstaaten, die für die Cybersicherheitszertifizierung gemäß dieser Verordnung zuständig sind, einschließlich des Austauschs von Informationen über eine mögliche Nichtkonformität von Zertifikaten, der Beobachtung einschlägiger Entwicklungen im Bereich der Zertifizierung und der Gewährleistung eines gemeinsamen Herangehens an die Aufrechterhaltung und Überprüfung der Zertifizierung.
- (4) Zusätzlich zu den in Absatz 3 genannten Bedingungen kann ein in Absatz 1 genanntes Abkommen über die gegenseitige Anerkennung, das sich auf die Vertrauenswürdigkeitsstufe „hoch“ erstreckt, nur dann mit Drittländern geschlossen werden, wenn auch die folgenden Bedingungen erfüllt sind:
- a) Das Drittland hat eine unabhängige und öffentliche Behörde für die Cybersicherheitszertifizierung, die Evaluierungstätigkeiten selbst durchführt oder deren Durchführung delegiert, die erforderlich sind, um eine Zertifizierung auf der Vertrauenswürdigkeitsstufe „hoch“ zu ermöglichen, die den Anforderungen und Verfahren gleichwertig ist, die in der vorliegenden Verordnung und in der Verordnung (EU) 2019/881 für nationale Cybersicherheitsbehörden festgelegt sind;
- b) mit dem Abkommen über die gegenseitige Anerkennung wird ein gemeinsamer Mechanismus geschaffen, der einer gegenseitigen Beurteilung bei der EUCC-Zertifizierung gleichwertig ist, um den Austausch von Verfahren zu fördern und bei der Evaluierung und Zertifizierung auftretende Probleme gemeinsam zu lösen.

## KAPITEL IX

## GEGENSEITIGE BEURTEILUNG VON ZERTIFIZIERUNGSSTELLEN

*Artikel 45***Verfahren der gegenseitigen Beurteilung**

- (1) Eine Zertifizierungsstelle, die EUCC-Zertifikate auf der Vertrauenswürdigkeitsstufe „hoch“ ausstellt, wird regelmäßig, mindestens jedoch alle fünf Jahre, einer gegenseitigen Beurteilung unterzogen. Die verschiedenen Arten der gegenseitigen Beurteilung sind in Anhang VI aufgeführt.
- (2) Die Europäische Gruppe für die Cybersicherheitszertifizierung erstellt und pflegt einen Zeitplan für gegenseitige Beurteilungen, damit eine solche Periodizität eingehalten wird. Außer in hinreichend begründeten Fällen werden gegenseitige Beurteilungen vor Ort durchgeführt.
- (3) Die gegenseitige Beurteilung kann auf Nachweise gestützt werden, die im Rahmen früherer gegenseitiger Beurteilungen oder gleichwertiger Verfahren einer selbst der gegenseitigen Beurteilung unterzogenen Zertifizierungsstelle oder einer nationalen Behörde für die Cybersicherheitszertifizierung gesammelt wurden, sofern
- a) die Ergebnisse nicht älter als fünf Jahre sind;
- b) den Ergebnissen eine Beschreibung des für das betreffende System eingerichteten Verfahrens der gegenseitigen Beurteilung beigelegt wird, falls sich die Ergebnisse auf eine gegenseitige Beurteilung beziehen, die im Rahmen eines anderen Zertifizierungssystems durchgeführt wurde;
- c) aus dem in Artikel 47 genannten Bericht über die gegenseitige Beurteilung hervorgeht, welche Ergebnisse mit bzw. ohne weitere Bewertung weiterverwendet wurden.

**▼B**

- (4) Wenn sich eine gegenseitige Beurteilung auf einen technischen Bereich erstreckt, muss auch die betreffende ITSEF beurteilt werden.
- (5) Die der gegenseitigen Beurteilung unterzogene Zertifizierungsstelle und erforderlichenfalls die nationale Behörde für die Cybersicherheitszertifizierung sorgen dafür, dass dem Beurteilungsteam alle relevanten Informationen zur Verfügung gestellt werden.
- (6) Die gegenseitige Beurteilung wird von einem gemäß Anhang VI gebildeten Beurteilungsteam durchgeführt.

*Artikel 46***Phasen der gegenseitigen Beurteilung**

- (1) In der Vorbereitungsphase überprüfen die Mitglieder des Beurteilungsteams die Dokumentation der Zertifizierungsstelle zu ihren Vorgaben und Verfahren, einschließlich der Verwendung der Sachstandsdokumente.
- (2) In der Vor-Ort-Phase bewertet das Beurteilungsteam die fachliche Kompetenz der Stelle und gegebenenfalls die Kompetenz einer ITSEF, die mindestens eine von der gegenseitigen Beurteilung erfasste Evaluierung eines IKT-Produkts durchgeführt hat.
- (3) Die Dauer der Vor-Ort-Phase kann je nach Faktoren wie der Möglichkeit der Weiterverwendung vorhandener Nachweise und Ergebnisse gegenseitiger Beurteilungen oder der Zahl der ITSEFs und der technischen Bereiche, für die die Zertifizierungsstelle Zertifikate ausstellt, verlängert oder verkürzt werden.
- (4) Das Beurteilungsteam ermittelt – soweit zutreffend – die fachliche Kompetenz jeder ITSEF, indem es deren technische(s) Labor(e) besucht und ihre Evaluatoren zu den technischen Bereichen und den damit verbundenen spezifischen Angriffsmethoden befragt.
- (5) In der Berichtsphase dokumentiert das Beurteilungsteam seine Feststellungen in einem Bericht über die gegenseitige Beurteilung, der ein Urteil und gegebenenfalls eine Liste der festgestellten Nichtkonformitäten enthält, denen jeweils ein Kritikalitätsgrad zugeordnet wird.
- (6) Der Bericht über die gegenseitige Beurteilung wird zuerst mit der beurteilten Zertifizierungsstelle erörtert. Im Anschluss daran erstellt die beurteilte Zertifizierungsstelle einen Zeitplan für die Maßnahmen, die in Bezug auf die Feststellungen zu ergreifen sind.

*Artikel 47***Bericht über die gegenseitige Beurteilung**

- (1) Das Beurteilungsteam legt der beurteilten Zertifizierungsstelle zunächst einen Entwurf des Berichts über die gegenseitige Beurteilung vor.
- (2) Die beurteilte Zertifizierungsstelle übermittelt dem Beurteilungsteam ihre Anmerkungen zu den Ergebnissen und eine Liste von Verpflichtungszusagen zur Beseitigung der im Entwurf des Berichts über die gegenseitige Beurteilung festgestellten Mängel.

**▼B**

- (3) Das Beurteilungsteam übermittelt der Europäischen Gruppe für die Cybersicherheitszertifizierung den abschließenden Bericht über die gegenseitige Beurteilung, der auch die Anmerkungen und die Verpflichtungszusagen der beurteilten Zertifizierungsstelle enthält. Darin nimmt das Beurteilungsteam auch zu den Anmerkungen Stellung und dazu, ob diese Verpflichtungszusagen ausreichen, um die festgestellten Mängel zu beseitigen.
- (4) Wenn im Bericht über die gegenseitige Beurteilung Nichtkonformitäten festgestellt werden, kann die Europäische Gruppe für die Cybersicherheitszertifizierung der beurteilten Zertifizierungsstelle eine angemessene Frist zur Beseitigung der Nichtkonformitäten setzen.
- (5) Die Europäische Gruppe für die Cybersicherheitszertifizierung gibt zu dem Bericht über die gegenseitige Beurteilung eine Stellungnahme ab:
- a) Wenn im Bericht über die gegenseitige Beurteilung keine Nichtkonformitäten festgestellt werden oder wenn die Nichtkonformitäten von der beurteilten Zertifizierungsstelle angemessen beseitigt werden, kann die Europäische Gruppe für die Cybersicherheitszertifizierung eine positive Stellungnahme abgeben, die von der ENISA mit allen einschlägigen Dokumenten auf ihrer Website zur Cybersicherheitszertifizierung veröffentlicht wird;
  - b) wenn die beurteilte Zertifizierungsstelle die festgestellten Nichtkonformitäten nicht innerhalb der gesetzten Frist angemessen beseitigt, kann die Europäische Gruppe für die Cybersicherheitszertifizierung eine negative Stellungnahme abgeben, die zusammen mit dem Bericht über die gegenseitige Beurteilung und allen einschlägigen Dokumenten von der ENISA auf ihrer Website zur Cybersicherheitszertifizierung veröffentlicht wird.
- (6) Vor der Veröffentlichung der Stellungnahme werden alle sensiblen, personenbezogenen oder proprietären Informationen aus den zu veröffentlichenden Dokumenten entfernt.

## KAPITEL X

## AUFRECHTERHALTUNG DES SYSTEMS

*Artikel 48*

## Aufrechterhaltung des EUCC-Systems

- (1) Die Kommission kann die Europäische Gruppe für die Cybersicherheitszertifizierung ersuchen, eine Stellungnahme im Hinblick auf die Aufrechterhaltung des EUCC-Systems abzugeben und die erforderlichen vorbereitenden Arbeiten durchzuführen.
- (2) Die Europäische Gruppe für die Cybersicherheitszertifizierung kann Stellungnahmen zur Billigung von Sachstandsdokumenten abgeben.
- (3) Sachstandsdokumente, die von der Europäischen Gruppe für die Cybersicherheitszertifizierung gebilligt wurden, werden von der ENISA veröffentlicht.

**▼M1**

- (4) Sofern in Anhang I oder II nichts anderes bestimmt ist, gelten die Sachstandsdokumente ab dem Anwendungsbeginn des Änderungsrechtsakts, mit dem sie in Anhang I oder II aufgenommen wurden.

**▼B**

KAPITEL XI  
SCHLUSSBESTIMMUNGEN

*Artikel 49*

**Nationale Systeme, die unter das EUCC-System fallen**

- (1) Gemäß Artikel 57 Absatz 1 der Verordnung (EU) 2019/881 und unbeschadet des Artikels 57 Absatz 3 der Verordnung werden alle nationalen Systeme für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für IKT-Produkte und -Prozesse, die unter das EUCC-System fallen, 12 Monate nach dem Inkrafttreten der vorliegenden Verordnung unwirksam.
- (2) Abweichend von Artikel 50 kann ein Zertifizierungsprozess im Rahmen eines nationalen Systems für die Cybersicherheitszertifizierung innerhalb von zwölf Monaten nach dem Inkrafttreten der vorliegenden Verordnung noch eingeleitet werden, muss aber spätestens 24 Monate nach dem Inkrafttreten der vorliegenden Verordnung abgeschlossen sein.
- (3) Zertifikate, die im Rahmen nationaler Systeme für die Cybersicherheitszertifizierung ausgestellt wurden, können einer Überprüfung unterzogen werden. Neue Zertifikate, die die überprüften Zertifikate ersetzen, werden gemäß der vorliegenden Verordnung ausgestellt.

**▼MI**

- (4) Bei der Durchführung der in Absatz 3 genannten Überprüfung innerhalb von zwei Jahren nach der Ausstellung eines ersten Zertifikats und wenn eine solche Überprüfung zur Ausstellung eines neuen Zertifikats gemäß dieser Verordnung führt, können die in Artikel 3 Absatz 2 aufgeführten Normen angewandt werden. Als Ausstellungsdatum des ersten Zertifikats gilt das Datum der Ausstellung des letzten Zertifikats für ein IKT-Produkt oder ein Schutzprofil, auf dem die gegenwärtige Zertifizierung beruht.

**▼B**

*Artikel 50*

**Inkrafttreten**

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem 27. Februar 2025.

Kapitel IV und Anhang V sind jedoch ab dem Inkrafttreten dieser Verordnung anwendbar.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

▼ **M1**

## ANHANG I

**Sachstandsdokumente für bestimmte technische Bereiche und andere Sachstandsdokumente**

1. Sachstandsdokumente zur Unterstützung technischer Bereiche auf AVA\_VAN-Stufe 4 oder 5:
  - a) folgende Dokumente zur harmonisierten Evaluierung des technischen Bereichs „Chipkarten und ähnliche Geräte“:
    1. *Minimum ITSEF requirements for security evaluations of smart cards and similar devices* (ITSEF-Mindestanforderungen an die Sicherheitsevaluierung von Chipkarten und ähnlichen Geräten), Version 1.1,
    2. *Minimum Site Security Requirements* (Mindestsicherheitsanforderungen an den Standort), Version 1.1,
    3. *Application of Common Criteria to integrated circuits* (Anwendung der Gemeinsamen Kriterien auf integrierte Schaltungen), Version 1.1,
    4. *Security Architecture requirements (ADV\_ARC) for smart cards and similar devices* (Anforderungen an die Sicherheitsarchitektur (ADV\_ARC) von Chipkarten und ähnlichen Geräten), Version 1.1,
    5. *Certification of „open“ smart card products* (Zertifizierung von „offenen“ Chipkartenprodukten), Version 1.1,
    6. *Composite product evaluation for smart cards and similar devices* (Evaluierung von Chipkarten und ähnlichen Geräten als zusammengesetzte Produkte), Version 1.1,
    7. *Application of Attack Potential to Smartcards and Similar Devices* (Anwendung des Angriffspotenzials auf Chipkarten und ähnliche Geräte), Version 1.2;
  - b) folgende Dokumente zur harmonisierten Evaluierung des technischen Bereichs „Hardware-Geräte mit Sicherheitsboxen“:
    1. *Minimum ITSEF requirements for security evaluations of hardware devices with security boxes* (ITSEF-Mindestanforderungen an die Sicherheitsevaluierung von Hardware-Geräten mit Sicherheitsboxen), Version 1.1,
    2. *Minimum Site Security Requirements* (Mindestsicherheitsanforderungen an den Standort), Version 1.1,
    3. *Application of Attack Potential to hardware devices with security boxes* (Anwendung des Angriffspotenzials auf Hardware-Geräte mit Sicherheitsboxen), Version 1.2;
2. Sachstandsdokumente zur harmonisierten Akkreditierung von Konformitätsbewertungsstellen:
  - a) *Accreditation of ITSEFs for the EUCC* (Akkreditierung von ITSEFs für das EUCC), Version 1.1, für Akkreditierungen, die vor dem 8. Juli 2025 ausgestellt wurden,
  - b) *Accreditation of ITSEFs for the EUCC* (Akkreditierung von ITSEFs für das EUCC), Version 1.6c, für Akkreditierungen, die neu ausgestellt oder nach dem 8. Juli 2025 überprüft werden,
  - c) *Accreditation of CBs for the EUCC* (Akkreditierung von BS für das EUCC), Version 1.6b.

**▼B**

*ANHANG II*

**Auf AVA\_VAN-Stufe 4 oder 5 zertifizierte Schutzprofile**

1. Für die Kategorie „entfernte qualifizierte Signatur- und Siegelerstellungseinheiten“:
  - 1) EN 419241-2:2019 — Vertrauenswürdige Systeme, die Serversignaturen unterstützen — Teil 2: Schutzprofil für qualifizierte Signaturerstellungseinheiten zur Serversignierung;
  - 2) EN 419221-5:2018 — Schutzprofile für kryptographische Module von Vertrauensdiensteanbietern — Teil 5: Kryptographisches Modul für vertrauenswürdige Dienste.
2. Schutzprofile, die als Sachstandsdokumente angenommen wurden:

[LEER]

**▼B**

## ANHANG III

**Empfohlene Schutzprofile (zur Veranschaulichung der technischen Bereiche aus Anhang I)**

Schutzprofile, die bei der Zertifizierung von IKT-Produkten verwendet werden, die unter die angegebene IKT-Produktkategorie fallen:

- a) für die Kategorie „maschinenlesbare Reisedokumente“:
- 1) *PP for a Machine Readable Travel Document using Standard Inspection Procedure with PACE* (Schutzprofil für ein maschinenlesbares Reisedokument mit Standardprüfverfahren mit PACE), BSI-CC-PP-0068-V2-2011-MA-01,
  - 2) *PP for a Machine Readable Travel Document with “ICAO Application” Extended Access Control* (Schutzprofil für ein maschinenlesbares Reisedokument mit erweiterter Zugangskontrolle für ICAO-Anwendung), BSI-CC-PP-0056-2009,
  - 3) *PP for a Machine Readable Travel Document with “ICAO Application” Extended Access Control with PACE* (Schutzprofil für ein maschinenlesbares Reisedokument mit erweiterter Zugangskontrolle für ICAO-Anwendung mit PACE), BSI-CC-PP-0056-V2-2012-MA-02,
  - 4) *PP for a Machine Readable Travel Document with “ICAO Application” Basic Access Control* (Schutzprofil für ein maschinenlesbares Reisedokument mit grundlegender Zugangskontrolle für ICAO-Anwendung), BSI-CC-PP-0055-2009;
- b) für die Kategorie „sichere Signaturerstellungseinheiten“:
- 1) EN 419211-1:2014 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 1: Überblick,
  - 2) EN 419211-2:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 2: Einheiten mit Schlüsselerzeugung,
  - 3) EN 419211-3:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 3: Einheiten mit Schlüsselimport,
  - 4) EN 419211-4:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 4: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Zertifikaterzeugungsanwendung,
  - 5) EN 419211-5:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung,
  - 6) EN 419211-6:2014 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigen Kanal zur Signaturerstellungsanwendung;
- c) für die Kategorie „digitale Fahrtenschreiber“:
- 1) Digitaler Fahrtenschreiber — Fahrtenschreiberkarte, gemäß der Durchführungsverordnung (EU) 2016/799 der Kommission vom 18. März 2016 zur Durchführung der Verordnung (EU) Nr. 165/2014 (Anhang 1C),
  - 2) Digitaler Fahrtenschreiber — Fahrzeugeinheit, gemäß Anhang IB der Verordnung (EG) Nr. 1360/2002 der Kommission, zum Einbau in Straßentransportfahrzeuge vorgesehen,

**▼ B**

- 3) Digitaler Fahrtenschreiber — externe GNSS-Ausrüstung (EGF PP), gemäß Anhang 1C der Durchführungsverordnung (EU) 2016/799 der Kommission vom 18. März 2016 zur Durchführung der Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates,
  - 4) Digitaler Fahrtenschreiber — Bewegungssensor (MS PP), gemäß Anhang 1C der Durchführungsverordnung (EU) 2016/799 der Kommission vom 18. März 2016 zur Durchführung der Verordnung (EU) Nr. 165/2014 des Europäischen Parlaments und des Rates;
- d) für die Kategorie „sichere integrierte Schaltungen, Chipkarten und zugehörige Geräte“:
- 1) *Security IC Platform Protection Profile* (Schutzprofil für Sicherheitsplattform für integrierte Schaltungen), BSI-CC-PP-0084-2014,
  - 2) *Java Card System — Open Configuration* (JAVA-Kartensystem — offene Konfiguration) V3.0.5, BSI-CC-PP-0099-2017,
  - 3) *Java Card System — Closed Configuration* (JAVA-Kartensystem — geschlossene Konfiguration), BSI-CC-PP-0101-2017,
  - 4) *PP for a PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16* (Schutzprofil für eine PC-Client-spezifische TPM-Familie), ANSSI-CC-PP-2015/07,
  - 5) *PP Universal SIM card* (Schutzprofil für Universal-SIM-Karte), PU-2009-RT-79, ANSSI-CC-PP-2010/04,
  - 6) *Embedded UICC (eUICC) for Machine-to-Machine Devices* (eUICC für Maschine-zu-Maschine-Geräte), BSI-CC-PP-0089-2015;
- e) für die Kategorie „Interaktionspunkte (für Zahlungen) und Zahlungsterminals“:
- 1) *Point of Interaction “POI-CHIP-ONLY”* (Interaktionspunkt „Nur-POI-Chip“), ANSSI-CC-PP-2015/01,
  - 2) *Point of Interaction “POI-CHIP-ONLY and Open Protocol Package”* (Interaktionspunkt „Nur-POI-Chip und offenes Protokollpaket“), ANSSI-CC-PP-2015/02,
  - 3) *Point of Interaction “POI-COMPREHENSIVE”* (Interaktionspunkt „POI-Umfassend“), ANSSI-CC-PP-2015/03;
  - 4) *Point of Interaction “POI-COMPREHENSIVE and Open Protocol Package”* (Interaktionspunkt „POI-Umfassend und offenes Protokollpaket“), ANSSI-CC-PP-2015/04,
  - 5) *Point of Interaction “POI-PED-ONLY”* (Interaktionspunkt „Nur-POI-PED“), ANSSI-CC-PP-2015/05,
  - 6) *Point of Interaction “POI-PED-ONLY and Open Protocol Package”* (Interaktionspunkt „Nur-POI-PED und offenes Protokollpaket“), ANSSI-CC-PP-2015/06;

**▼B**

- f) für die Kategorie „Hardware-Geräte mit Sicherheitsboxen“:
- 1) *Cryptographic Module for CSP Signing Operations with Backup — PP CMCSOB* (Kryptografiemodul für CSP-Signierungsvorgänge mit Sicherheitskopie), PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08,
  - 2) *Cryptographic Module for CSP key generation services — PP CMCKG* (Kryptografiemodul für CSP-Schlüsselerstellungsdienste), PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09,
  - 3) *Cryptographic Module for CSP Signing Operations without Backup — PP CMCSO* (Kryptografiemodul für CSP-Signierungsvorgänge ohne Sicherheitskopie), PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

**▼B***ANHANG IV***Kontinuität der Vertrauenswürdigkeit und Überprüfung der Zertifikate****IV.1 Kontinuität der Vertrauenswürdigkeit: Anwendungsbereich**

1. Die folgenden Anforderungen an die Kontinuität der Vertrauenswürdigkeit gelten für Aufrechterhaltungstätigkeiten im Zusammenhang mit
  - a) einer Neubewertung, wenn ein unverändert zertifiziertes IKT-Produkt seinen Sicherheitsanforderungen noch genügt,
  - b) einer Evaluierung der Auswirkungen von Änderungen an einem zertifizierten IKT-Produkt auf dessen Zertifizierung,
  - c) der Anwendung von Patches nach einem bewerteten Patchverwaltungsprozess, sofern dies Teil der Zertifizierung ist,
  - d) der Überprüfung der Lebenszyklusmanagement- oder Produktionsprozesse des Zertifikatsinhabers.
2. Der Inhaber eines EUCC-Zertifikats kann die Überprüfung des Zertifikats beantragen, wenn
  - a) das EUCC-Zertifikat innerhalb der nächsten neun Monate abläuft,
  - b) das zertifizierte IKT-Produkt oder ein anderer Faktor, der sich auf dessen Sicherheitsfunktionen auswirken könnte, geändert worden ist,
  - c) der Zertifikatsinhaber beantragt, dass die Schwachstellenbewertung erneut durchgeführt wird, um die Vertrauenswürdigkeit des EUCC-Zertifikats in Bezug auf die Widerstandsfähigkeit des IKT-Produkts gegen aktuelle Cyberangriffe erneut zu bestätigen.

**IV.2 Neubewertung**

1. Wenn die Auswirkungen von Änderungen im Bedrohungsumfeld eines unveränderten zertifizierten IKT-Produkts zu bewerten sind, wird die Neubewertung bei der Zertifizierungsstelle beantragt.
2. Die Neubewertung wird von derselben ITSEF durchgeführt, die an der vorherigen Evaluierung beteiligt war, und alle noch gültigen Ergebnisse werden dabei weiterverwendet. Schwerpunkt der Evaluierung sind die Tätigkeiten in Bezug auf die Vertrauenswürdigkeit, die möglicherweise vom veränderten Bedrohungsumfeld des zertifizierten IKT-Produkts betroffen sind, insbesondere die relevante AVA\_VAN-Familie sowie zusätzlich der Lebenszyklus der Vertrauenswürdigkeit (ALC), wofür erneut ausreichende Belege für die Aufrechterhaltung der Entwicklungsumgebung zu sammeln sind.
3. Die ITSEF beschreibt die Änderungen und die Einzelheiten der Ergebnisse der Neubewertung in einer Aktualisierung des vorherigen technischen Evaluierungsberichts.
4. Die Zertifizierungsstelle überprüft den aktualisierten technischen Evaluierungsbericht und erstellt einen Neubewertungsbericht. Der Status des ursprünglichen Zertifikats wird danach gemäß Artikel 13 geändert.
5. Der Neubewertungsbericht und das aktualisierte Zertifikat werden der nationalen Behörde für die Cybersicherheitszertifizierung und der ENISA zur Veröffentlichung auf ihrer Website zur Cybersicherheitszertifizierung übermittelt.

**▼B****IV.3 Änderungen an einem zertifizierten IKT-Produkt**

1. Wenn Änderungen an einem zertifizierten IKT-Produkt vorgenommen wurden und der Zertifikatsinhaber das Zertifikat aufrechterhalten möchte, muss er der Zertifizierungsstelle einen Auswirkungsanalysebericht vorlegen.
2. Der Auswirkungsanalysebericht muss Folgendes enthalten:
  - a) eine Einleitung mit den erforderlichen Angaben zur Zuordnung des Auswirkungsanalyseberichts und des geänderten Evaluierungsgegenstands,
  - b) eine Beschreibung der Änderungen am Produkt,
  - c) die Angabe der betroffenen Entwicklernachweise,
  - d) eine Beschreibung der Änderungen der Entwicklernachweise,
  - e) die Ergebnisse und Schlussfolgerungen zu den Auswirkungen auf die Vertrauenswürdigkeit für jede einzelne Änderung.
3. Die Zertifizierungsstelle prüft die im Auswirkungsanalysebericht beschriebenen Änderungen, um deren Auswirkungen auf die Vertrauenswürdigkeit des zertifizierten Evaluierungsgegenstands zu validieren, wie in den Schlussfolgerungen des Auswirkungsanalyseberichts vorgeschlagen.
4. Im Anschluss an die Prüfung bestimmt die Zertifizierungsstelle das Ausmaß einer Änderung je nach ihren Auswirkungen als geringfügig oder erheblich.

**▼M1**

5. Wenn die Zertifizierungsstelle bestätigt, dass die Änderungen geringfügig sind, wird für das geänderte IKT-Produkt kein neues Zertifikat ausgestellt und der ursprüngliche Zertifizierungsbericht durch einen Aufrechterhaltungsbericht ergänzt.

Der Aufrechterhaltungsbericht wird in den Auswirkungsanalysebericht aufgenommen und enthält folgende Abschnitte:

- a) Einleitung,
  - b) Beschreibung der Änderungen,
  - c) betroffene Entwicklernachweise.
6. Der in Nummer 5 genannte Aufrechterhaltungsbericht wird der ENISA zur Veröffentlichung auf ihrer Website zur Cybersicherheitszertifizierung übermittelt.

**▼B**

7. Werden die Änderungen als erheblich bestätigt, wird eine erneute Evaluierung auf der Grundlage der vorherigen Evaluierung durchgeführt, wobei alle noch gültigen Ergebnisse der vorherigen Evaluierung weiterverwendet werden.
8. Nach Abschluss der Evaluierung des geänderten Evaluierungsgegenstands erstellt die ITSEF einen neuen technischen Evaluierungsbericht. Die Zertifizierungsstelle überprüft den aktualisierten technischen Evaluierungsbericht und stellt gegebenenfalls ein neues Zertifikat mit einem neuen Zertifizierungsbericht aus.
9. Das neue Zertifikat und der neue Zertifizierungsbericht werden der ENISA zur Veröffentlichung übermittelt.

**▼B****IV.4 Patchverwaltung**

1. Ein Patchverwaltungsverfahren gibt einen strukturierten Prozess zur Aktualisierung eines zertifizierten IKT-Produkts vor. Das Patchverwaltungsverfahren einschließlich des vom Zertifizierungsantragsteller in das IKT-Produkt implementierten Mechanismus kann nach der Zertifizierung des IKT-Produkts unter der Verantwortung der Konformitätsbewertungsstelle angewandt werden.
2. Der Zertifizierungsantragsteller kann in die Zertifizierung des IKT-Produkts einen Patchmechanismus als Teil eines in dem IKT-Produkt umgesetzten zertifizierten Verwaltungsverfahrens einbeziehen, wenn eine der folgenden Bedingungen erfüllt ist:
  - a) Die vom Patch betroffenen Funktionen gehören nicht zum Evaluierungsgegenstand des zertifizierten IKT-Produkts,
  - b) der Patch betrifft eine vorab festgelegte geringfügige Änderung des zertifizierten IKT-Produkts,
  - c) der Patch betrifft eine bestätigte Schwachstelle, die sich kritisch auf die Sicherheit des zertifizierten IKT-Produkts auswirkt.
3. Falls der Patch eine erhebliche Änderung des Evaluierungsgegenstands des zertifizierten IKT-Produkts in Bezug auf eine bislang nicht erkannte Schwachstelle betrifft, die sich nicht kritisch auf die Sicherheit des IKT-Produkts auswirkt, werden die Bestimmungen des Artikels 13 angewandt.
4. Das Patchverwaltungsverfahren für ein IKT-Produkt besteht aus
  - a) dem Prozess für die Entwicklung und Bereitstellung des Patches für das IKT-Produkt,
  - b) dem technischen Mechanismus und den technischen Funktionen für die Übernahme des Patches in das IKT-Produkt,
  - c) einer Reihe von Evaluierungstätigkeiten in Bezug auf die Wirksamkeit und Leistungsfähigkeit des technischen Mechanismus.
5. Während der Zertifizierung des IKT-Produkts
  - a) muss der Zertifizierungsantragsteller für das IKT-Produkt die Beschreibung des Patchverwaltungsverfahrens vorlegen;
  - b) muss die ITSEF nachprüfen, ob
    - 1) der Entwickler die Patchmechanismen im Einklang mit dem zur Zertifizierung eingereichten Patchverwaltungsverfahren in das IKT-Produkt integriert hat,
    - 2) der Evaluierungsgegenstand so abgegrenzt worden ist, dass die Änderungen an den eingegrenzten Prozessen die Sicherheit des Evaluierungsgegenstands nicht beeinträchtigen,
    - 3) der technische Patchmechanismus im Einklang mit den Bestimmungen dieses Abschnitts und den Angaben des Antragstellers funktioniert;
  - c) muss die Zertifizierungsstelle das Ergebnis der Bewertung des Patchverwaltungsverfahrens in den Zertifizierungsbericht aufnehmen.
6. Der Inhaber des Zertifikats kann den nach dem zertifizierten Patchverwaltungsverfahren erstellten Patch auf das betreffende zertifizierte IKT-Produkt anwenden und muss in den folgenden Fällen innerhalb von fünf Arbeitstagen die folgenden Schritte unternehmen:

**▼B**

- a) in dem in Nummer 2 Buchstabe a genannten Fall den betreffenden Patch der Zertifizierungsstelle melden, die das entsprechende EUCC-Zertifikat nicht ändert;
- b) in dem in Nummer 2 Buchstabe b genannten Fall den betreffenden Patch der ITSEF zur Prüfung vorlegen. Die ITSEF unterrichtet hiervon die Zertifizierungsstelle nach Erhalt des Patches, woraufhin die Zertifizierungsstelle geeignete Maßnahmen zur Ausstellung einer neuen Version des betreffenden EUCC-Zertifikats und zur Aktualisierung des Zertifizierungsberichts ergreift;
- c) in dem in Nummer 2 Buchstabe c genannten Fall den betreffenden Patch der ITSEF zur erforderlichen erneuten Evaluierung vorlegen, kann den Patch aber parallel dazu anwenden. Die ITSEF unterrichtet hiervon die Zertifizierungsstelle, die daraufhin mit den entsprechenden Zertifizierungstätigkeiten beginnt.

*ANHANG V***INHALT EINES ZERTIFIZIERUNGSBERICHTS****V.1 Zertifizierungsbericht**

1. Auf der Grundlage der von der ITSEF vorgelegten technischen Evaluierungsberichte erstellt die Zertifizierungsstelle einen Zertifizierungsbericht, der zusammen mit dem entsprechenden EUCC-Zertifikat veröffentlicht wird.
2. Der Zertifizierungsbericht enthält detaillierte und praktische Informationen über das IKT-Produkt oder die Kategorie von IKT-Produkten und über den sicheren Einsatz des IKT-Produkts und umfasst daher alle öffentlich zugänglichen und mitteilbaren Informationen, die für Nutzer und interessierte Kreise von Bedeutung sind. Auf öffentlich zugängliche und mitteilbare Informationen kann im Zertifizierungsbericht verwiesen werden.
3. Der Zertifizierungsbericht umfasst mindestens folgende Abschnitte:
  - a) Zusammenfassung,
  - b) Angabe des IKT-Produkts oder der IKT-Produktkategorie für Schutzprofile,
  - c) Sicherheitsdienste,
  - d) Annahmen und Klarstellung des Anwendungsbereichs,
  - e) Informationen zur Architektur,
  - f) zusätzliche Cybersicherheitsinformationen, sofern zutreffend,
  - g) IKT-Produkttests, sofern durchgeführt,
  - h) gegebenenfalls Angabe der Lebenszyklusmanagementprozesse und Produktionsanlagen des Zertifikatinhabers,
  - i) Ergebnisse der Evaluierung und Angaben zum Zertifikat,
  - j) Zusammenfassung des Sicherheitsziels des zu zertifizierenden IKT-Produkts,
  - k) falls verfügbar, mit dem System verbundenes Siegel oder Kennzeichen,
  - l) Literaturverzeichnis.
4. Die Zusammenfassung ist eine kurze Zusammenfassung des gesamten Zertifizierungsberichts. Die Zusammenfassung enthält einen klaren und prägnanten Überblick über die Evaluierungsergebnisse mit folgenden Informationen:
  - a) Name des evaluierten IKT-Produkts, Aufzählung der Produktkomponenten, die Gegenstand der Evaluierung sind, und Version des IKT-Produkts,
  - b) Name der ITSEF, die die Evaluierung durchgeführt hat, und gegebenenfalls Liste der Unterauftragnehmer,
  - c) Abschlussdatum der Evaluierung,
  - d) Verweis auf den von der ITSEF erstellten technischen Evaluierungsbericht,
  - e) Kurzbeschreibung der Ergebnisse des Zertifizierungsberichts, einschließlich:
    - 1) Version und gegebenenfalls Ausgabedatum der bei der Evaluierung angewandten Gemeinsamen Kriterien,
    - 2) das Vertrauenswürdigkeitspaket und die sicherheitsbezogenen Vertrauenswürdigkeitskomponenten der Gemeinsamen Kriterien (CC), einschließlich der bei der Evaluierung verwendeten AVA\_VAN-Stufe und der entsprechenden Vertrauenswürdigkeitsstufe gemäß Artikel 52 der Verordnung (EU) 2019/881, auf die sich das EUCC-Zertifikat bezieht,

**▼ B**

- 3) die Sicherheitsfunktionen des evaluierten IKT-Produkts,
  - 4) eine Zusammenfassung der Bedrohungen und der organisatorischen Sicherheitsvorgaben, die durch das evaluierte IKT-Produkt angegangen werden,
  - 5) besondere Konfigurationsanforderungen,
  - 6) Annahmen über die Betriebsumgebung,
  - 7) gegebenenfalls das Bestehen eines genehmigten Patchverwaltungsverfahrens gemäß Anhang IV Abschnitt IV.4,
  - 8) Haftungsausschlüsse.
5. Das evaluierte IKT-Produkt muss eindeutig gekennzeichnet sein, mindestens anhand der folgenden Angaben:
- a) Name des evaluierten IKT-Produkts,
  - b) Aufzählung der Komponenten des IKT-Produkts, die Teil der Evaluierung sind,
  - c) Versionsnummer der Komponenten des IKT-Produkts,
  - d) zusätzliche Anforderungen an die Betriebsumgebung des zertifizierten IKT-Produkts,
  - e) Name und Kontaktangaben des Inhabers des EUCC-Zertifikats,
  - f) gegebenenfalls das im Zertifikat vermerkte Patchverwaltungsverfahren,
  - g) Link zur Website des Inhabers des EUCC-Zertifikats, auf der zusätzliche Cybersicherheitsinformationen über das zertifizierte IKT-Produkt gemäß Artikel 55 der Verordnung (EU) 2019/881 bereitgestellt werden.
6. Die Informationen in diesem Abschnitt müssen möglichst genau sein, um eine vollständige und richtige Darstellung des IKT-Produkts zu gewährleisten, die dann bei künftigen Evaluierungen weiterverwendet werden kann.
7. Der Abschnitt über die Sicherheitskonzepte muss eine Beschreibung des Sicherheitskonzepts des IKT-Produkts sowie der Konzepte oder Vorschriften, die das bewertete IKT-Produkt durchsetzen oder einhalten muss, beinhalten. Er muss Verweise auf folgende Konzepte und deren Beschreibung enthalten:
- a) das Konzept des Zertifikatsinhabers für die Behandlung von Schwachstellen,
  - b) das Konzept des Zertifikatsinhabers für die Gewährleistung der Kontinuität der Vertrauenswürdigkeit.
8. Das Konzept kann gegebenenfalls die Bedingungen für die Anwendung eines Patchverwaltungsverfahrens während der Geltungsdauer des Zertifikats umfassen.
9. Der Abschnitt über die Annahmen und die Klarstellung des Anwendungsbereichs muss umfassende Informationen über die Umstände und Ziele im Zusammenhang mit der beabsichtigten Verwendung des Produkts gemäß Artikel 7 Absatz 1 Buchstabe c enthalten. Dazu gehören
- a) Annahmen in Bezug auf Verwendung und Einsatz des IKT-Produkts in Form von Mindestanforderungen, z. B. dass eine ordnungsgemäße Installation und Konfiguration mit geeigneter Hardware erfolgt,
  - b) Annahmen in Bezug auf die Umgebung für den ordnungsgemäßen Betrieb des IKT-Produkts.

**▼ B**

10. Die unter Nummer 9 aufgeführten Informationen müssen so verständlich wie möglich sein, damit die Nutzer des zertifizierten IKT-Produkts fundierte Entscheidungen über die mit der Verwendung verbundenen Risiken treffen können.
11. Der Abschnitt über Informationen zur Architektur muss eine allgemeine Beschreibung des IKT-Produkts und seiner Hauptkomponenten gemäß der in den Gemeinsamen Kriterien vorgesehenen Struktur von ADV\_TDS-Teilsystemen enthalten.
12. Es wird eine vollständige Liste der zusätzlichen Cybersicherheitsinformationen des IKT-Produkts gemäß Artikel 55 der Verordnung (EU) 2019/881 bereitgestellt. Alle einschlägigen Unterlagen müssen mit den Versionsnummern versehen sein.
13. Der Abschnitt über IKT-Produkttests muss folgende Informationen enthalten:
  - a) Name und Anlaufstelle der Behörde oder Stelle, die das Zertifikat ausgestellt hat, mit Angabe der zuständigen nationalen Behörde für die Cybersicherheitszertifizierung;
  - b) Name der ITSEF, die die Evaluierung durchgeführt hat, falls nicht identisch mit der Zertifizierungsstelle;
  - c) Angabe der verwendeten Vertrauenswürdigkeitskomponenten aus den in Artikel 3 genannten Normen;
  - d) Version des Sachstandsdocuments und weitere Sicherheitsbewertungskriterien, die bei der Evaluierung verwendet werden;
  - e) die vollständigen und genauen Einstellungen und Konfigurationen des IKT-Produkts während der Evaluierung, gegebenenfalls mit betrieblichen Hinweisen und Anmerkungen;
  - f) alle verwendeten Schutzprofile, einschließlich der folgenden Angaben:
    - 1) Verfasser des Schutzprofils,
    - 2) Name und Kennung des Schutzprofils,
    - 3) Kennung des Zertifikats des Schutzprofils,
    - 4) Name und Kontaktangaben der Zertifizierungsstelle und der ITSEF, die an der Evaluierung des Schutzprofils beteiligt waren,
    - 5) Vertrauenswürdigkeitspaket(e), das/die nach dem Schutzprofil für ein Produkt erforderlich sind.
14. Der Abschnitt über die Evaluierungsergebnisse und die Zertifikatsangaben muss folgende Informationen enthalten:
  - a) Bestätigung der erreichten Vertrauenswürdigkeitsstufe gemäß Artikel 4 der vorliegenden Verordnung und Artikel 52 der Verordnung (EU) 2019/881,
  - b) Anforderungen an die Vertrauenswürdigkeit laut den in Artikel 3 genannten Normen, denen das IKT-Produkt oder das Schutzprofil tatsächlich entspricht, einschließlich der AVA\_VAN-Stufe,
  - c) ausführliche Beschreibung der Anforderungen an die Vertrauenswürdigkeit mit Einzelheiten dazu, wie das Produkt die einzelnen Anforderungen erfüllt,
  - d) Ausstellungsdatum und Geltungsdauer des Zertifikats,
  - e) eindeutige Kennung des Zertifikats.

**▼ B**

15. Das Sicherheitsziel wird entweder in den Zertifizierungsbericht aufgenommen oder im Zertifizierungsbericht genannt, zusammengefasst und zusammen mit dem Zertifizierungsbericht zur Veröffentlichung übermittelt.
16. Das Sicherheitsziel kann gemäß Abschnitt VI.2 bereinigt werden.
17. Das mit dem EUCC verknüpfte Siegel oder Kennzeichen kann nach den Vorschriften und Verfahren des Artikels 11 in den Zertifizierungsbericht aufgenommen werden.
18. Das Literaturverzeichnis enthält Verweise auf alle bei der Erstellung des Zertifizierungsberichts verwendeten Dokumente und Unterlagen. Dazu gehören zumindest
  - a) die Sicherheitsbewertungskriterien, die Sachstandsdokumente und weitere einschlägige Spezifikationen und deren Version,
  - b) der technische Evaluierungsbericht,
  - c) der technische Evaluierungsbericht für ein zusammengesetztes Produkt, falls zutreffend,
  - d) die technische Referenzdokumentation,
  - e) die bei der Evaluierung verwendete Dokumentation des Entwicklers.
19. Um die Reproduzierbarkeit der Evaluierung zu gewährleisten, muss die gesamte Dokumentation eindeutig mit dem richtigen Ausgabedatum und der entsprechenden Versionsnummer gekennzeichnet sein.

**V.2 Bereinigung eines Sicherheitsziels zur Veröffentlichung**

1. Das Sicherheitsziel, das gemäß Abschnitt VI.1 Nummer 1 in den Zertifizierungsbericht aufzunehmen ist bzw. auf das darin zu verweisen ist, kann durch die Entfernung oder Umschreibung proprietärer technischer Informationen bereinigt werden.
2. Das daraus resultierende bereinigte Sicherheitsziel muss eine tatsächliche und vollständige Darstellung der Originalfassung sein. Das bedeutet, dass im bereinigten Sicherheitsziel keine Informationen weggelassen werden dürfen, die für das Verständnis der Sicherheitseigenschaften des Evaluierungsgegenstands und des Umfangs der Evaluierung erforderlich sind.
3. Der Inhalt des bereinigten Sicherheitsziels muss den folgenden Mindestanforderungen genügen:
  - a) Die Einleitung wird nicht bereinigt, da sie im Allgemeinen keine proprietären Informationen enthält;
  - b) das bereinigte Sicherheitsziel hat keine andere eindeutige Kennung als die vollständige Originalfassung;
  - c) die Beschreibung des Sicherheitsziels kann verkürzt werden, soweit sie proprietäre und detaillierte Informationen über das Sicherheitsziel enthält, die nicht veröffentlicht werden sollten;
  - d) die Beschreibung der Sicherheitsumgebung des Evaluierungsziels (Annahmen, Bedrohungen, organisatorische Sicherheitsvorgaben) darf nicht verkürzt werden, soweit diese Informationen für das Verständnis des Umfangs der Evaluierung erforderlich sind;
  - e) die Sicherheitsvorgaben werden nicht verkürzt, da alle Informationen öffentlich zugänglich gemacht werden müssen, um den Zweck des Sicherheitsziels und des Evaluierungsgegenstands verständlich zu machen;

**▼ B**

- f) alle Sicherheitsanforderungen werden veröffentlicht. Anwendungshinweise können Aufschluss darüber geben, wie die funktionalen Anforderungen der Gemeinsamen Kriterien gemäß Artikel 3 zum Verständnis des Sicherheitsziels heranzuziehen sind;
  - g) die zusammengefasste Spezifikation des Evaluierungsgegenstands enthält alle Sicherheitsfunktionen des Evaluierungsgegenstands, kann aber von zusätzlichen proprietären Informationen bereinigt werden;
  - h) die auf den Evaluierungsgegenstand angewandten Schutzprofile müssen genannt werden;
  - i) die Begründung kann bereinigt werden, um proprietäre Informationen zu entfernen.
4. Auch wenn das bereinigte Sicherheitsziel nicht nach den in Artikel 3 genannten Evaluierungsnormen förmlich evaluiert wird, gewährleistet die Zertifizierungsstelle, dass es dem vollständigen evaluierten Sicherheitsziel entspricht, und verweist im Zertifizierungsbericht sowohl auf das vollständige als auch auf das bereinigte Sicherheitsziel.



## ANHANG VI

### GEGENSTAND DER GEGENSEITIGEN BEURTEILUNG UND ZUSAMMENSETZUNG DES BEURTEILUNGSTEAMS

#### VI.1 Gegenstand der gegenseitigen Beurteilung

1. Folgende Arten der gegenseitigen Beurteilung sind vorgesehen:
  - a) Beurteilungsart 1: eine Zertifizierungsstelle führt Zertifizierungstätigkeiten auf AVA\_VAN.3-Stufe durch;
  - b) Beurteilungsart 2: eine Zertifizierungsstelle führt Zertifizierungstätigkeiten in Bezug auf einen technischen Bereich durch, der in Anhang I als Sachstandsdocument aufgeführt ist;
  - c) Beurteilungsart 3: eine Zertifizierungsstelle führt Zertifizierungstätigkeiten oberhalb der AVA\_VAN.3-Stufe unter Verwendung eines Schutzprofils durch, das in Anhang II oder III als Sachstandsdocument aufgeführt ist.
2. Die beurteilte Zertifizierungsstelle legt eine Liste der zertifizierten IKT-Produkte vor, die für die Überprüfung durch das Beurteilungsteam nach den folgenden Regeln infrage kommen:
  - a) Die fraglichen Produkte fallen in den technischen Geltungsbereich der Zulassung der Zertifizierungsstelle; zu analysieren sind im Rahmen der gegenseitigen Beurteilung mindestens zwei verschiedene Produktevaluierungen auf der Vertrauenswürdigkeitsstufe „hoch“ sowie ein Schutzprofil, falls die Zertifizierungsstelle ein Zertifikat auf der Vertrauenswürdigkeitsstufe „hoch“ ausgestellt hat;
  - b) in der Beurteilungsart 2 legt die Zertifizierungsstelle mindestens ein Produkt pro technischen Bereich und pro betroffener ITSEF vor;
  - c) in der Beurteilungsart 3 wird mindestens ein infrage kommendes Produkt anhand eines anwendbaren und relevanten Schutzprofils überprüft.

#### VI.2 Beurteilungsteam

1. Das Beurteilungsteam besteht aus mindestens zwei Sachverständigen, die von unterschiedlichen Zertifizierungsstellen, die Zertifikate der Vertrauenswürdigkeitsstufe „hoch“ ausstellen, aus verschiedenen Mitgliedstaaten ausgewählt werden. Die Sachverständigen sollten einschlägiges Fachwissen in Bezug auf die in Artikel 3 genannten Normen und Sachstandsdocumente, die für die gegenseitige Beurteilung von Belang sind, nachweisen.
2. Im Falle der Delegation der Zertifikatsausstellung oder vorherigen Zustimmung zur Zertifikatsausstellung gemäß Artikel 56 Absatz 6 der Verordnung (EU) 2019/881 wird ein Sachverständiger der für die betreffende Zertifizierungsstelle zuständigen nationalen Behörde für die Cybersicherheitszertifizierung zusätzlich zu dem gemäß Absatz 1 dieses Abschnitts ausgewählten Beurteilungsteam hinzugezogen.
3. Für die Beurteilungsart 2 werden die Teammitglieder aus Zertifizierungsstellen ausgewählt, die für den betreffenden technischen Bereich zugelassen sind.
4. Jedes Mitglied des Beurteilungsteams muss über mindestens zwei Jahre Erfahrung mit der Durchführung von Zertifizierungstätigkeiten in einer Zertifizierungsstelle verfügen.
5. Für die Beurteilungsart 2 oder 3 muss jedes Mitglied des Beurteilungsteams mindestens zwei Jahre Erfahrung mit der Durchführung von Zertifizierungstätigkeiten im betreffenden technischen Bereich oder in Bezug auf das betreffende Schutzprofil sowie bewährte Sachkenntnis und eine Beteiligung an der Zulassung einer ITSEF nachweisen.

**▼B**

6. Die nationale Behörde für die Cybersicherheitszertifizierung, die die beurteilte Zertifizierungsstelle überwacht und beaufsichtigt, und mindestens eine andere nationale Behörde für die Cybersicherheitszertifizierung, deren Zertifizierungsstelle keiner gegenseitigen Beurteilung unterzogen wird, nehmen als Beobachter an der gegenseitigen Beurteilung teil. Die ENISA kann ebenfalls als Beobachterin an der gegenseitigen Beurteilung teilnehmen.
7. Die Zusammensetzung des Beurteilungsteams wird der beurteilten Zertifizierungsstelle mitgeteilt. In begründeten Fällen kann sie Einspruch gegen die Zusammensetzung des Beurteilungsteams einlegen und deren Überprüfung beantragen.

*ANHANG VII***Inhalt eines EUCC-Zertifikats**

Ein EUCC-Zertifikat muss mindestens Folgendes enthalten:

- a) eine eindeutige Kennung, die von der Zertifizierungsstelle, die das Zertifikat ausstellt, vergeben wird;
- b) Angaben zum zertifizierten IKT-Produkt oder Schutzprofil und zum Zertifikatsinhaber, einschließlich:
  - 1) Name des IKT-Produkts oder des Schutzprofils und gegebenenfalls des Evaluierungsgegenstands,
  - 2) Art des IKT-Produkts oder des Schutzprofils und gegebenenfalls des Evaluierungsgegenstands,
  - 3) Version des IKT-Produkts oder des Schutzprofils,
  - 4) Name, Anschrift und Kontaktangaben des Zertifikatsinhabers,
  - 5) Link zur Website des Zertifikatsinhabers, die die in Artikel 55 der Verordnung (EU) 2019/881 genannten zusätzlichen Informationen über die Cybersicherheit enthält;
- c) Informationen über die Evaluierung und Zertifizierung des IKT-Produkts oder Schutzprofils, einschließlich:
  - 1) Name, Anschrift und Kontaktangaben der Zertifizierungsstelle, die das Zertifikat ausgestellt hat,
  - 2) Name der ITSEF, die die Evaluierung durchgeführt hat, falls nicht mit der Zertifizierungsstelle identisch,
  - 3) Name der zuständigen nationalen Behörde für die Cybersicherheitszertifizierung,
  - 4) Verweis auf diese Verordnung,
  - 5) Verweis auf den Zertifizierungsbericht in Bezug auf das in Anhang V genannte Zertifikat,
  - 6) Vertrauenswürdigkeitsstufe gemäß Artikel 4,
  - 7) Verweis auf die Fassungen der Normen, auf denen die Evaluierung gemäß Artikel 3 beruht,
  - 8) Angabe der Vertrauenswürdigkeitsstufe oder des Vertrauenswürdigkeitspakets nach den in Artikel 3 genannten Normen und im Einklang mit Anhang VIII, einschließlich der verwendeten Vertrauenswürdigkeitskomponenten und der abgedeckten AVA\_VAN-Stufe,
  - 9) gegebenenfalls Verweis auf ein oder mehrere Schutzprofile, denen das IKT-Produkt oder Schutzprofil entspricht,
  - 10) Ausstellungsdatum,
  - 11) Geltungsdauer des Zertifikats;
- d) Siegel oder Kennzeichen, das mit dem Zertifikat gemäß Artikel 11 verknüpft ist.



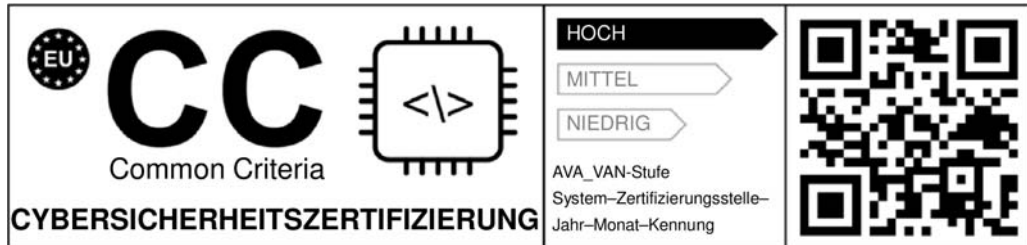
## ANHANG VIII

**Erklärung zum Vertrauenswürdigkeitspaket**

1. Entgegen den Definitionen der Gemeinsamen Kriterien wird eine Steigerung (*Augmentation*)
  - a) nicht mit der Abkürzung „+“ bezeichnet,
  - b) nicht mit einer Liste aller betroffenen Komponenten im Einzelnen aufgeführt,
  - c) nicht ausführlich im Zertifizierungsbericht dargelegt.
2. Die in einem EUCC-Zertifikat bestätigte Vertrauenswürdigkeitsstufe (*Assurance Level*) kann durch die Vertrauenswürdigkeitsstufe der Evaluierung gemäß Artikel 3 dieser Verordnung (*Evaluation Assurance Level*, EAL) ergänzt werden.
3. Wenn sich die in einem EUCC-Zertifikat bestätigte Vertrauenswürdigkeitsstufe nicht auf eine Steigerung bezieht, wird im EUCC-Zertifikat eines der folgenden Pakete angegeben:
  - a) „das spezifische Vertrauenswürdigkeitspaket“,
  - b) „das dem Schutzprofil entsprechende Vertrauenswürdigkeitspaket“, falls auf ein Schutzprofil ohne Vertrauenswürdigkeitsstufe der Evaluierung (EAL) verwiesen wird.

**▼ B***ANHANG IX***Siegel und Kennzeichen**

1. Form des Siegels und Kennzeichens:



2. Bei Verkleinerung oder Vergrößerung des Siegels und Kennzeichens müssen die sich aus der vorstehenden Abbildung ergebenden Proportionen eingehalten werden.
3. Ein materiell vorhandenes Siegel und Kennzeichen muss mindestens 5 mm hoch sein.