Amtsblatt
der Europäischen Union

DE
Reihe L

2025/2462

9.12.2025

DURCHFÜHRUNGSVERORDNUNG (EU) 2025/2462 DER KOMMISSION

vom 8. Dezember 2025

zur Änderung der Durchführungsverordnung (EU) 2024/482 im Hinblick auf Begriffsbestimmungen, die Zertifizierung von IKT-Produktreihen, die Kontinuität der Vertrauenswürdigkeit und Sachstandsdokumente

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) ([1]), insbesondere auf Artikel 49 Absatz 7,

in Erwägung nachstehender Gründe:

(1) In der Durchführungsverordnung (EU) 2024/482 der Kommission ([2]) werden die Rollen, Vorschriften und Verpflichtungen sowie die Struktur des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC) im Einklang mit dem in der Verordnung (EU) 2019/881 genannten europäischen Rahmen für die Cybersicherheitszertifizierung festgelegt.

(2) Die den Gemeinsamen Kriterien (CC) – einer internationalen Norm für die Evaluierung der Informationssicherheit – beigefügte gemeinsame Evaluierungsmethodik ermöglicht die Evaluierung der Sicherheit von IKT-Produkten für Zertifizierungszwecke. In diesem Zusammenhang können einige IKT-Produkte auf derselben funktionalen Basis beruhen, um ähnliche Sicherheitsfunktionen für verschiedene Plattformen oder Geräte zu bieten; dies wird auch als Produktreihe bezeichnet. Die Konzeption, Hardware, Firmware oder Software kann sich jedoch von einem IKT-Produkt zum anderen unterscheiden. Es ist Sache der Zertifizierungsstelle, im Einzelfall zu entscheiden, ob die Zertifizierung einer Produktreihe durchgeführt werden kann. Die Bedingungen für die Produktreihenzertifizierung könnten in den unterstützenden EUCC-Leitlinien näher erläutert werden.

(3) Um die Zuverlässigkeit zertifizierter Produkte aufrechtzuerhalten, muss festgelegt werden, was eine erhebliche und was eine geringfügige Änderung des Evaluierungsgegenstands oder seiner Umgebung, einschließlich seiner Betriebs- oder Entwicklungsumgebung, darstellt. Daher müssen diese Begriffe unter Berücksichtigung bestehender und weit verbreiteter technischer Spezifikationen der Gruppe hoher Beamter für Informationssicherheit (SOG-IS) und der Beteiligten der Anerkennungsvereinbarung für die nach den Gemeinsamen Kriterien ausgestellten Zertifikate auf dem Gebiet der IT-Sicherheit (CCRA) präzisiert werden.

(4) Geringfügige Änderungen sind häufig dadurch gekennzeichnet, dass sie nur begrenzte Auswirkungen auf die Produktvertrauenswürdigkeitserklärung des ausgestellten EUCC-Zertifikats haben. Geringfügige Änderungen sollten daher im Rahmen von Aufrechterhaltungsverfahren verwaltet werden und erfordern keine erneute Evaluierung der Sicherheitsfunktionen des Produkts. Zu geringfügigen Änderungen, die durch Aufrechterhaltung erfolgen sollten, zählen unter anderem redaktionelle Änderungen, Änderungen an der Umgebung des Evaluierungsgegenstands, die den zertifizierten Evaluierungsgegenstand nicht verändern, sowie Änderungen des zertifizierten Evaluierungsgegenstands, die sich nicht auf die Vertrauenswürdigkeitsnachweise auswirken. Änderungen in der Entwicklungsumgebung können ebenfalls als geringfügig angesehen werden, sofern sie keine Folgewirkungen auf bestehende Vertrauenswürdigkeitsmaßnahmen haben. In einigen Fällen können sie jedoch eine Teilevaluierung der einschlägigen Maßnahmen erfordern.

([1]) ABl. L 151 vom 7.6.2019, S. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) 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) (ABl. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(5) Eine erhebliche Änderung ist jede Änderung des zertifizierten Evaluierungsgegenstands oder seiner Umgebung, die die im EUCC-Zertifikat ausgedrückte Vertrauenswürdigkeit beeinträchtigen kann und daher eine erneute Evaluierung nach sich ziehen sollte. Beispiele für wesentliche Änderungen sind unter anderem Änderungen der beanspruchten Anforderungen an die Vertrauenswürdigkeit, mit Ausnahme der Anforderungen an die Vertrauenswürdigkeit der CC ALC_FLR-Familie (Mängelbeseitigung), sowie Änderungen der Vertraulichkeits- oder Integritätskontrollen der Entwicklungsumgebung, wenn solche Änderungen die sichere Entwicklung oder Herstellung des Evaluierungsgegenstands beeinträchtigen könnten oder Änderungen des Evaluierungsgegenstands eine ausnutzbare Schwachstelle beseitigen. Darüber hinaus kann auch eine Reihe geringfügiger Änderungen, die zusammen erhebliche Auswirkungen auf die Sicherheit haben, als erhebliche Änderung eingestuft werden. Es ist auch wichtig anzuerkennen, dass sich eine Fehlerbehebung zwar möglicherweise nur auf einen bestimmten Aspekt des Evaluierungsgegenstands auswirkt, ihre Unvorhersehbarkeit und mögliche Auswirkungen auf die Vertrauenswürdigkeit sie jedoch zu einer erheblichen Änderung machen kann, wenn sie die mit der Zertifizierung gebotene sicherheitsbezogene Vertrauenswürdigkeit beeinträchtigt.

(6) Änderungen im Bedrohungsumfeld eines unveränderten zertifizierten IKT-Produkts könnten eine Neubewertung erforderlich machen. Die möglichen Ergebnisse eines solchen Neubewertungsverfahrens sollten eindeutig festgelegt werden, insbesondere seine Auswirkungen auf das EUCC-Zertifikat. Bei erfolgreichem Abschluss einer Neubewertung sollte die Zertifizierungsstelle das Zertifikat bestätigen oder ein neues Zertifikat mit verlängerter Geltungsdauer ausstellen. Ist das Neubewertungsverfahren nicht erfolgreich, sollte die Zertifizierungsstelle das Zertifikat widerrufen oder ein neues Zertifikat mit verändertem Anwendungsbereich ausstellen. Diese Bestimmungen sollten für die Neubewertung von Schutzprofilen entsprechend gelten.

(7) In Anhang I der Durchführungsverordnung (EU) 2024/482 sind die für die Evaluierung von IKT-Produkten und Schutzprofilen geltenden Sachstandsdokumente aufgeführt. Diese Sachstandsdokumente sollten aktualisiert werden, um den jüngsten Entwicklungen Rechnung zu tragen, z. B. im Zusammenhang mit technologischen Entwicklungen, der Cyberbedrohungslandschaft, Branchenpraktiken oder internationalen Normen. Eine solche Aktualisierung ist angebracht bei den Sachstandsdokumenten in Bezug auf Mindestsicherheitsanforderungen an den Standort, die Anwendung des Angriffspotenzials auf Chipkarten, die Anwendung des Angriffspotenzials auf Hardware-Geräte mit Sicherheitsboxen, die Anwendung der Gemeinsamen Kriterien auf integrierte Schaltungen und die Evaluierung von Chipkarten und ähnlichen Geräten als zusammengesetzte Produkte. Sachstandsdokumente in Bezug auf die Evaluierung und Zertifizierung zusammengesetzter Produkte unter Verwendung der neuesten Version der Gemeinsamen Kriterien, die Weiterverwendung der Evaluierungsergebnisse von Standortprüfungen und Klarstellungen zur Auslegung von Schutzprofilen in Bezug auf qualifizierte elektronische Signaturerstellungseinheiten, Fahrtenschreiber und Hardware-Sicherheitsmodule sind nicht eingeschlossen. Zur Gewährleistung einer einheitlichen Evaluierung von IKT-Produkten im Rahmen des EUCC sollte Anhang I geändert werden, um diese aktualisierten und neuen Sachstandsdokumente nach ihrer Billigung durch die Europäische Gruppe für die Cybersicherheitszertifizierung (ECCG) aufzunehmen.

(8) Darüber hinaus sollte das Sachstandsdokument *„ADV_SPM.1 Interpretation for CC:2022 transition“* (ADV_SPM.1 Auslegung für den CC:2022-Übergang) in das System aufgenommen werden, damit für Zertifizierungsverfahren, die auf spezifischen Schutzprofilen beruhen, weiterhin die formale Modellierung (ADV_SPM.1) eingesetzt werden kann, bis die entsprechenden Schutzprofile aktualisiert werden, z. B. durch Hinzufügung einer CC:2022-konformen Schutzprofilkonfiguration für mehrfache Vertrauenswürdigkeit, die ADV_SPM.1 unterstützt. Um dem Markt ausreichend Zeit für den Übergang zu den aktualisierten Gemeinsamen Kriterien zu geben, müssen besondere Übergangsvorschriften für die Schutzprofile „Security IC Platform PP with Augmentation Packages“ (Schutzprofil für Sicherheitsplattform mit Erweiterungspaketen) (v1.0), BSI-CC-PP-0084-2014, „Java Card System – Closed Configuration“ (Java-Kartensystem – geschlossene Konfiguration) (v3.1), BSI-CC-PP-0101-V2-2020, oder „Java Card System – Open Configuration“ (Java-Kartensystem – offene Konfiguration) (v3.1), BSI-CC-0099-V2-2020, vorgesehen werden. Zur Vermeidung von Marktstörungen sollte festgelegt werden, dass das Sachstandsdokument *„ADV_SPM.1 interpretation for CC:2022 transition“* (ADV_SPM.1 Auslegung für den CC:2022-Übergang) für Zertifizierungsverfahren gilt, die vor der Annahme dieser Verordnung eingeleitet wurden. Die Anwendung dieses Dokuments sollte jedoch angesichts der Zeit, die für die endgültige Aktualisierung der entsprechenden Schutzprofile erforderlich ist, strikt auf das notwendige Maß beschränkt werden. Genauer gesagt sollte bei Zertifizierungsverfahren unter Verwendung der Schutzprofile „Security IC Platform PP with Augmentation Packages“ (Schutzprofil für Sicherheitsplattform mit Erweiterungspaketen) (v1.0), BSI-CC-PP-0084-2014, oder „Java Card System – Closed Configuration“ (Java-Kartensystem – geschlossene Konfiguration) (v3.1), BSI-CC-PP-0101-V2-2020, das Sachstandsdokument für diejenigen Verfahren, die vor dem 1. Oktober 2026 eingeleitet wurden, gelten. Bei Zertifizierungsverfahren unter Verwendung des Schutzprofils „Java Card System – Open Configuration“ (Java-Kartensystem – offene Konfiguration) (v3.1), BSI-CC-PP-0099-V2-2020, sollte das Sachstandsdokument nur für die Verfahren gelten, die vor dem Inkrafttreten dieser Verordnung eingeleitet wurden, da bereits eine neue Version des Schutzprofils „Java Card System – Open Configuration“ (Java-Kartensystem – offene Konfiguration) verfügbar ist.

(9) Eine Änderung der Sachstandsdokumente während eines Zertifizierungsverfahrens könnte die Evaluierung des Produkts stören und die Ausstellung des Zertifikats verzögern. Daher müssen für neue oder aktualisierte Sachstandsdokumente geeignete Übergangsbestimmungen festgelegt werden, damit Anbieter, ITSEFs, Zertifizierungsstellen und andere Beteiligte die erforderlichen Anpassungen vornehmen können. Die geltenden aktualisierten und neuen Sachstandsdokumente sollten bei neuen Zertifizierungsanträgen zugrunde gelegt werden, auch bei Anträgen auf Neubewertung und erneute Evaluierung, wogegen es bei laufenden Zertifizierungsverfahren möglich sein sollte, weiterhin frühere Versionen der Sachstandsdokumente zu verwenden.

(10) In Anhang II bzw. Anhang III der Durchführungsverordnung (EU) 2024/482 sind die auf AVA_VAN-Stufe 4 oder 5 zertifizierten Schutzprofile bzw. die empfohlenen Schutzprofile aufgeführt. Infolge einer Aktualisierung der Schutzprofile sind mehrere Verweise unvollständig oder überholt. Diese Verweise sollten ergänzt werden und außerdem sollten neue Verweise aufgenommen werden, um eine umfassendere Abdeckung sicherer integrierter Schaltungen, Chipkarten und zugehöriger Geräte sowie von Trusted Computing zu gewährleisten.

(11) Artikel 19 der Durchführungsverordnung (EU) 2024/482 muss geändert werden, um klarzustellen, dass Anhang IV – mit den erforderlichen Änderungen – für die Überprüfung von EUCC-Zertifikaten für Schutzprofile gilt.

(12) Da das Sicherheitsziel ein Schlüsselelement für das Verständnis des Anwendungsbereichs eines Zertifizierungsverfahrens ist, muss die ENISA ferner das Sicherheitsziel für jedes EUCC-Zertifikat auf ihrer Website veröffentlichen.

(13) Darüber hinaus sollten die Zertifizierungsstellen der ENISA gemäß Artikel 42 Absatz 2 der Durchführungsverordnung (EU) 2024/482 eine Fassung des Sicherheitsziels und des Zertifizierungsberichts in englischer Sprache bereitstellen, damit die Agentur diese Informationen in englischer Sprache auf der entsprechenden Website zur Verfügung stellen kann. Aus diesem Grund sollten die Zertifizierungsantragsteller den Zertifizierungsstellen auf Anfrage eine Fassung des Sicherheitsziels in englischer Sprache übermitteln.

(14) Es ist nicht erforderlich, dass der Name der Zertifizierungsstelle in der eindeutigen Kennung des Zertifikats erscheint, da die Kennnummer der Zertifizierungsstelle ausreicht, um diese Stelle eindeutig zu identifizieren. Auch der Monat der Ausstellung muss nicht erscheinen, da die Zertifikate jährlich gezählt werden. Daher sollte diese Anforderung zur Vereinfachung gestrichen werden. Da das Jahr der Ausstellung des Zertifikats der Ausstellung des ersten Zertifikats entspricht, sollte dieses Datum in der eindeutigen Kennung der nach einer Überprüfung ausgestellten Zertifikate angegeben werden, um die Rückverfolgbarkeit zu gewährleisten.

(15) Die Durchführungsverordnung (EU) 2024/482 sollte daher entsprechend geändert werden.

(16) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des nach Artikel 66 der Verordnung (EU) 2019/881 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Die Durchführungsverordnung (EU) 2024/482 wird wie folgt geändert:

1. In Artikel 2 werden die folgenden Nummern 16, 17 und 18 angefügt:

„16. ‚Produktreihe' eine Reihe von IKT-Produkten eines Antragstellers, die auf derselben funktionalen Basis beruhen, um denselben Sicherheitsbedarfen gerecht zu werden, und deren Konzeption, Hardware, Firmware oder Software sich von einem IKT-Produkt zum anderen unterscheiden können;

17. ‚geringfügige Änderung' eine Änderung des zertifizierten Evaluierungsgegenstands oder seiner Umgebung, die die im EUCC-Zertifikat ausgedrückte Vertrauenswürdigkeit nicht beeinträchtigt;

18. ‚erhebliche Änderung' eine Änderung des zertifizierten Evaluierungsgegenstands oder seiner Umgebung, die die im EUCC-Zertifikat ausgedrückte Vertrauenswürdigkeit beeinträchtigen kann."

2. In Artikel 5 wird folgender Absatz 3 angefügt:

„(3) Eine Zertifizierungsstelle kann die Zertifizierung einer Produktreihe gestatten."

3. Artikel 9 Absatz 2 Buchstabe a erhält folgende Fassung:

„a) der Zertifizierungsstelle und der ITSEF alle erforderlichen vollständigen und korrekten Informationen zu übermitteln und auf Anfrage zusätzliche erforderliche Informationen bereitzustellen, einschließlich einer Fassung des Sicherheitsziels in englischer Sprache;"

4. Artikel 11 Absatz 3 Buchstabe b erhält folgende Fassung:

„b) die eindeutige Kennung des Zertifikats, bestehend aus

1) dem Namen des Systems,

2) der Kennnummer gemäß Artikel 3 der Durchführungsverordnung (EU) 2024/3143 der Zertifizierungsstelle, die das Zertifikat ausgestellt hat,

3) dem Jahr der Ausstellung des ursprünglichen Zertifikats,

4) der Kennnummer, die von der Zertifizierungsstelle, die das Zertifikat ausgestellt hat, vergeben wurde."

5. Artikel 19 Absatz 1 erhält folgende Fassung:

„(1) Auf Antrag des Zertifikatsinhabers oder aus anderen triftigen Gründen kann die Zertifizierungsstelle ein EUCC-Zertifikat für ein Schutzprofil überprüfen. Die Überprüfung erfolgt gemäß Anhang IV. 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."

6. Artikel 42 wird wie folgt geändert:

a) In Absatz 1 wird folgender Buchstabe i angefügt:

„i) das Sicherheitsziel zu jedem EUCC-Zertifikat,"

b) Absatz 2 erhält folgende Fassung:

„(2) Die in Absatz 1 genannten Informationen sind zumindest in englischer Sprache bereitzustellen. Dazu stellen die Zertifizierungsstellen der ENISA die Fassungen der Zertifizierungsberichte und Sicherheitsziele in der Originalsprache zur Verfügung und übermitteln darüber hinaus unverzüglich auch die Fassung dieser Dokumente in englischer Sprache."

7. Artikel 48 Absatz 4 erhält folgende Fassung:

„(4) Sofern in Anhang I oder II nichts anderes bestimmt ist, gelten die Sachstandsdokumente für Zertifizierungsverfahren, einschließlich Neubewertungen und erneuter Evaluierungen, die ab dem Anwendungsbeginn des Änderungsrechtsakts, mit dem die Sachstandsdokumente in Anhang I oder II aufgenommen wurden, eingeleitet wurden."

8. Anhang I erhält die Fassung des Anhangs I der vorliegenden Verordnung.

9. Anhang II erhält die Fassung des Anhangs II der vorliegenden Verordnung.

10. Anhang III erhält die Fassung des Anhangs III der vorliegenden Verordnung.

11. Anhang IV wird gemäß Anhang IV der vorliegenden Verordnung geändert.

12. Anhang V wird gemäß Anhang V der vorliegenden Verordnung geändert.

13. Anhang IX erhält die Fassung des Anhangs VI der vorliegenden Verordnung.

Artikel 2

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

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

Brüssel, den 8. Dezember 2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG I

„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 2,
      (3) *Reusing evaluation results of site audits (STAR)* (Weiterverwendung der Evaluierungsergebnisse von Standortprüfungen), Version 1,
      (4) *Application of Common Criteria to integrated circuits* (Anwendung der Gemeinsamen Kriterien auf integrierte Schaltungen), Version 2,
      (5) *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,
      (6) *Certification of ‚open' smart card products* (Zertifizierung von ‚offenen' Chipkartenprodukten), Version 1.1,
      (7) *Composite product evaluation for smart cards and similar devices for CC3.1* (Evaluierung von Chipkarten und ähnlichen Geräten als zusammengesetzte Produkte für CC3.1), Version 2,
      (8) *Composite product evaluation and certification for CC:2022* (Evaluierung und Zertifizierung zusammengesetzter Produkte für CC:2022), Version 1,
      (9) *Application of Attack Potential to Smartcards and Similar Devices* (Anwendung des Angriffspotenzials auf Chipkarten und ähnliche Geräte), Version 2,
      (10) *Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices* (Evaluierung und Zertifizierung der Sicherheit qualifizierter elektronischer Signatur-/Siegelerstellungseinheiten), Version 1,
      (11) *ADV_SPM.1 interpretation for CC:2022 transition* (ADV__SPM.1 Auslegung für den CC:2022-Übergang), Version 1.1, für Zertifizierungsverfahren unter Verwendung der folgenden Schutzprofile:
         a) Schutzprofile *Security IC Platform PP with Augmentation Packages* (Schutzprofil für Sicherheitsplattform mit Erweiterungspaketen) (v1.0), BSI-CC-PP-0084-2014, oder *Java Card System — Closed Configuration* (Java-Kartensystem — geschlossene Konfiguration) (v3.1), BSI-CC-PP-0101-V2-2020, vor dem 1. Oktober 2026 eingeleitet,
         b) Schutzprofil *Java Card System — Open Configuration* (Java-Kartensystem — offene Konfiguration) (v3.1), BSI-CC-PP-0099-V2-2020, vor dem 29. Dezemer 2025 eingeleitet;
   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 2,
      (3) *Reusing evaluation results of site audits (STAR)* (Weiterverwendung der Evaluierungsergebnisse von Standortprüfungen), Version 1,
      (4) *Application of Attack Potential to hardware devices with security boxes* (Anwendung des Angriffspotenzials auf Hardware-Geräte mit Sicherheitsboxen), Version 2,
      (5) *Hardware assessment in EN 419221-5* (Hardwarebewertung in der Norm EN 419221-5) (HSM PP), Version 1,
      (6) *JIL Tachograph MS PP Clarification* (Klarstellung des Schutzprofils für JIL-Fahrtenschreiber), Version 1.
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."

ANHANG II

„ANHANG II

Auf AVA_VAN-Stufe 4 oder 5 zertifizierte Schutzprofile

1. Für entfernte qualifizierte Signatur- und Siegelerstellungseinheiten:

   a) EN 419241-2:2019 — Vertrauenswürdige Systeme, die Serversignaturen unterstützen — Teil 2: Schutzprofil für qualifizierte Signaturerstellungseinheiten zur Serversignierung (v0.16), ANSSI-CC-PP-2018/02-M01;

   b) EN 419221-5:2018 — Schutzprofile für kryptographische Module von Vertrauensdiensteanbietern — Teil 5: Kryptographisches Modul für vertrauenswürdige Dienste (v0.15), ANSSI-CC-PP-2016/05-M01.

2. Schutzprofile, die als Sachstandsdokumente angenommen wurden:

   [LEER].“

ANHANG III

„ANHANG III

Empfohlene Schutzprofile

Schutzprofile, die bei der Zertifizierung von IKT-Produkten verwendet werden, einschließlich Produkten in den technischen Bereichen:

1. Chipkarten und ähnliche Geräte
   a) Reisedokumente:
      (1) *PP for a Machine Readable Travel Document with 'ICAO Application' Basic Access Control* (Schutzprofil für ein maschinenlesbares Reisedokument mit grundlegender Zugangskontrolle für ICAO-Anwendung) (v1.10), BSI-CC-PP-0055-2009,
      (2) *PP for a Machine Readable Travel Document using Standard Inspection Procedure with PACE* (Schutzprofil für ein maschinenlesbares Reisedokument mit Standardprüfverfahren mit PACE) (PACE_PP) (v1), BSI-CC-PP-0068-V2-2011-MA-01,
      (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) (v1.3), BSI-CC-PP-0056-V2-2012-MA-02;
   b) Sichere Signaturerstellungseinheiten (SSCD):
      (1) EN 419211-2:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 2: Einheiten mit Schlüsselerzeugung (v1.03), BSI-CC-PP-0059-2009-MA-02,
      (2) EN 419211-3:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 3: Einheiten mit Schlüsselimport (v1.0.2), BSI-CC-PP-0075-2012-MA-01,
      (3) EN 419211-4:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 4: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigem Kanal zur Zertifikaterzeugungsanwendung (v1.0.1), BSI-CC-PP-0071-2012-MA-01,
      (4) EN 419211-5:2013 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 5: Erweiterung für Einheiten mit Schlüsselerzeugung und vertrauenswürdigem Kanal zur Signaturerstellungsanwendung (v1.0.1), BSI-CC-PP-0072-2012-MA-01,
      (5) EN 419211-6:2014 — Schutzprofile für sichere Signaturerstellungseinheiten — Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigem Kanal zur Signaturerstellungsanwendung (v1.0.4), BSI-CC-PP-0076-2013-MA-01;
   c) Fahrtenschreiber: Digitaler Fahrtenschreiber — Fahrtenschreiberkarte (TC PP) (v1.0), BSI-CC-PP-0091-2017;
   d) Sichere integrierte Schaltungen, Java-Kartenplattform und eUICC:
      (1) *Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations* (Universelles Schutzprofil für eine SIM-Java-Kartenplattform — Grund- und SCWS-Konfigurationen) (v2.0.2), ANSSI-CC-PP-2010/04 (Grundkonfiguration), ANSSI-CC-PP-2010/05 (Grund- und SCWS-Konfigurationen);
      (2) *Security IC Platform PP with Augmentation Packages* (Schutzprofil für Sicherheitsplattform mit Erweiterungspaketen) (v1.0), BSI-CC-PP-0084-2014,
      (3) *Embedded UICC (eUICC) for Machine-to-Machine Devices* (eUICC für Maschine-zu-Maschine-Geräte) (v1.1), BSI-CC-PP-0089-2015,
      (4) *Cryptographic Service Provider — CSP* (Kryptografiediensteanbieter — CSP) (v0.9.8), BSI-CC-PP-0104-2019,
      (5) *Cryptographic Service Provider — Time Stamp Service and Audit* (Kryptografiediensteanbieter — Zeitstempeldienst und Prüfung) (PPC-CSP-TS-Au) Version 0.9.5, BSI-CC-PP-0107-2019,
      (6) *Cryptographic Service Provider — Time Stamp Service, Audit and Clustering* (Kryptografiediensteanbieter — Zeitstempeldienst, Prüfung und Clustering) (PPC-CSP-TS-Au) Version 0.9.4, BSI-CC-PP-0108-2019,
      (7) *Java Card System — Closed Configuration* (JAVA-Kartensystem — geschlossene Konfiguration) (v3.1), BSI-CC-PP-0101-V2-2020,
      (8) *Secure Element Protection Profile* (Schutzprofil für sichere Elemente) — GPC_SPE_174 (v1.0), CCN-CC-PP-5-2021,
      (9) *Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile* (Schutzprofil für sichere Untersysteme in Ein-Chip-Systemen) (v1.8), BSI-CC-PP-0117-V2-2023,
      (10) *Java Card System — Open Configuration* (JAVA-Kartensystem — offene Konfiguration) (v3.2), BSI-CC-PP-0099-V3-2024,
      (11) *Embedded UICC (eUICC) for Consumer Devices Protection Profile* (Schutzprofil für eUICC für Verbrauchergeräte) (v2.1), BSI-CC-PP-0100-V2-2025;
   e) Trusted Platform Module (TPM): *Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0* (Schutzprofil für eine PC-Client-spezifische TPM-Modulspezifikationsfamilie), Stufe 0, Revision 1.59 (v1.3), ANSSI-CC-PP-2021/02.

2. Hardwaregeräte mit Sicherheitsboxen

   a) Interaktionspunkte (für Zahlungen) und Zahlungsterminals:

      (1) *Point of Interaction 'POI-CHIP-ONLY'* (Interaktionspunkt ‚Nur-POI-Chip') (v4.0), ANSSI-CC-PP-2015/01,

      (2) *Point of Interaction 'POI-CHIP-ONLY and Open Protocol Package'* (Interaktionspunkt ‚Nur-POI-Chip und offenes Protokollpaket') (v4.0), ANSSI-CC-PP-2015/02,

      (3) *Point of Interaction 'POI-COMPREHENSIVE'* (Interaktionspunkt ‚POI-Umfassend') (v4.0), ANSSI-CC-PP-2015/03,

      (4) *Point of Interaction 'POI-COMPREHENSIVE and Open Protocol Package'* (Interaktionspunkt ‚POI-Umfassend und offenes Protokollpaket') (v4.0), ANSSI-CC-PP-2015/04,

      (5) *Point of Interaction 'POI-PED-ONLY'* (Interaktionspunkt ‚Nur-POI-PED') (v4.0), ANSSI-CC-PP-2015/05,

      (6) *Point of Interaction 'POI-PED-ONLY and Open Protocol Package'* (Interaktionspunkt ‚Nur-POI-PED und offenes Protokollpaket') (v4.0), ANSSI-CC-PP-2015/06;

   b) Hardware-Sicherheitsmodul:

      (1) *Cryptographic Module for CSP Signing Operations with Backup* (Kryptografiemodul für CSP-Signierungsvorgänge mit Sicherheitskopie) — PP CMCSOB 14167-2 (v0.35), ANSSI-CC-PP-2015/08,

      (2) *Cryptographic Module for CSP Key Generation Services* (Kryptografiemodul für CSP-Schlüsselerstellungsdienste) — PP CMCKG 14167-3 (v0.20), ANSSI-CC-PP-2015/09,

      (3) *Cryptographic Module for CSP Signing Operations without Backup* (Kryptografiemodul für CSP-Signierungsvorgänge ohne Sicherheitskopie) — PP CMCSO 14167-4 (v0.32), ANSSI-CC-PP-2015/10;

   c) Fahrtenschreiber:

      (1) Digitaler Fahrtenschreiber — Bewegungssensor (MS PP) (v1.0), BSI-CC-PP-0093-2017,

      (2) Digitaler Fahrtenschreiber — Fahrzeugeinheit (VU PP) (v1.15), BSI-CC-PP-0094-V2-2021,

      (3) Digitaler Fahrtenschreiber — externe GNSS-Ausrüstung (EGF PP) (v1.10), BSI-CC-PP-0092-V2-2021;

3. Sonstige: *Trusted Execution Environment Protection Profile* (Schutzprofil für eine vertrauenswürdige Ausführungsumgebung) — GPD_SPE_021 (v1.3), ANSSI-CC-PP-2014/01-M02."

ANHANG IV

Anhang IV der Durchführungsverordnung (EU) 2024/482 wird wie folgt geändert:

1. Abschnitt IV.2 Nummer 4 erhält folgende Fassung:

„4. Die Zertifizierungsstelle überprüft den aktualisierten technischen Evaluierungsbericht und erstellt einen Neubewertungsbericht. Der Status des ursprünglichen Zertifikats wird danach gemäß Artikel 13 oder Artikel 19 geändert. Ist das Neubewertungsverfahren erfolgreich, gilt Artikel 13 Absatz 2 Buchstabe a oder c im Falle der Zertifizierung eines Produkts und Artikel 19 Absatz 2 Buchstabe a oder c im Falle der Zertifizierung eines Schutzprofils. Ist das Neubewertungsverfahren nicht erfolgreich, gilt Artikel 13 Absatz 2 Buchstabe b oder d im Falle der Zertifizierung eines Produkts und Artikel 19 Absatz 2 Buchstabe b oder d im Falle der Zertifizierung eines Schutzprofils."

2. Abschnitt IV.3 wird wie folgt geändert:

a) Überschrift IV.3 erhält folgende Fassung:

„IV.3 **Änderungen an einem zertifizierten IKT-Produkt — Aufrechterhaltung und erneute Evaluierung**".

b) Die Nummern 4 und 5 erhalten folgende Fassung:

„4. Im Anschluss an die Prüfung bestimmt die Zertifizierungsstelle das Ausmaß einer Änderung je nach ihren Auswirkungen auf die im EUCC-Zertifikat ausgedrückte Vertrauenswürdigkeit als geringfügig oder erheblich.

5. Wenn die Zertifizierungsstelle bestätigt, dass die Änderungen geringfügig sind, wird für das geänderte IKT-Produkt kein neues Zertifikat gemäß Artikel 13 Absatz 2 Buchstabe a oder Artikel 19 Absatz 2 Buchstabe a ausgestellt und der ursprüngliche Zertifizierungsbericht durch einen Aufrechterhaltungsbericht ergänzt."

c) Die folgende Nummer 5a wird eingefügt:

„5a. Bei Änderungen der Vertrauenswürdigkeitsmaßnahmen in der Entwicklungsumgebung, einschließlich der Hinzufügung von Anforderungen an die Vertrauenswürdigkeit der CC ALC_FLR-Familie (Mängelbeseitigung), kann die Zertifizierungsstelle die ITSEF auffordern, eine Teilevaluierung der betreffenden Vertrauenswürdigkeitsmaßnahmen durchzuführen. Die ITSEF muss einen technischen Bericht über die Teilevaluierung erstellen, auf dessen Grundlage die Zertifizierungsstelle bestätigt, dass die Änderungen geringfügig oder erheblich sind. Wenn die Zertifizierungsstelle bestätigt, dass die Änderungen geringfügig sind, findet Abschnitt IV.3 Nummer 5 Anwendung. Wenn die Zertifizierungsstelle bestätigt, dass die Änderungen erheblich sind, findet Abschnitt IV.3 Nummer 7 Anwendung."

ANHANG V

Anhang V Abschnitt V.1 der Durchführungsverordnung (EU) 2024/482 erhält folgende Fassung:

„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 und Sicherheitsziel veröffentlicht wird.

2. Der Zertifizierungsbericht enthält detaillierte und praktische Informationen über das IKT-Produkt und über den sicheren Einsatz des IKT-Produkts. Er 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 muss zumindest die folgenden Informationen enthalten:
   a) Zusammenfassung,
   b) Angabe des IKT-Produkts,
   c) Kontaktangaben in Bezug auf die Evaluierung des IKT-Produkts,
   d) Sicherheitskonzepte,
   e) Annahmen und Klarstellung des Anwendungsbereichs,
   f) Informationen zur Architektur,
   g) zusätzliche Cybersicherheitsinformationen, sofern zutreffend,
   h) Zusammenfassung der Evaluierung des IKT-Produkts und evaluierte Konfiguration,
   i) Ergebnisse der Evaluierung und Angaben zum Zertifikat,
   j) gegebenenfalls Bemerkungen und Empfehlungen,
   k) gegebenenfalls Anhänge,
   l) Verweis auf das Sicherheitsziel des zu zertifizierenden IKT-Produkts,
   m) falls verfügbar, mit dem System verbundenes Siegel oder Kennzeichen,
   n) gegebenenfalls ein Glossar,
   o) Literaturverzeichnis.

4. Die in Absatz 3 Buchstabe a genannte Zusammenfassung ist eine kurze Zusammenfassung des gesamten Zertifizierungsberichts. Sie enthält einen klaren und prägnanten Überblick über die Evaluierungsergebnisse mit folgenden Informationen:
   a) Name des evaluierten IKT-Produkts,
   b) Name der ITSEF, die die Evaluierung durchgeführt hat,
   c) Abschlussdatum der Evaluierung,
   d) Datum der Ausstellung des Zertifikats,
   e) Datum der Ausstellung des ursprünglichen Zertifikats, falls zutreffend,
   f) Geltungsdauer,
   g) eindeutige Kennung des Zertifikats gemäß Artikel 11,
   h) Kurzbeschreibung der Ergebnisse des Zertifizierungsberichts, einschließlich:
      i) Version und gegebenenfalls Ausgabedatum der bei der Evaluierung angewandten Gemeinsamen Kriterien,
      ii) Vertrauenswürdigkeitspaket oder Liste der sicherheitsbezogenen Vertrauenswürdigkeitskomponenten der Gemeinsamen Kriterien (CC), bei der Evaluierung verwendete AVA_VAN-Stufe und entsprechende Vertrauenswürdigkeitsstufe gemäß Artikel 52 der Verordnung (EU) 2019/881, auf die sich das EUCC-Zertifikat bezieht,
      iii) das/die Schutzprofil(e), mit dem/denen das IKT-Produkt die Konformität beansprucht,
      iv) Verweis auf das Sicherheitskonzept des evaluierten IKT-Produkts,
      v) gegebenenfalls Haftungsausschluss/Haftungsausschlüsse.

5. Das evaluierte IKT-Produkt muss aus den Angaben gemäß Nummer 3 Buchstabe b eindeutig hervorgehen, einschließlich der folgenden Informationen:

   a) eindeutige Kennung des evaluierten IKT-Produkts,

   b) Aufzählung der Komponenten des IKT-Produkts, die Teil der Evaluierung sind, einschließlich der Versionsnummer jeder einzelnen Komponente,

   c) Verweis auf zusätzliche Anforderungen an die Betriebsumgebung des zertifizierten IKT-Produkts.

6. Die Kontaktangaben gemäß Nummer 3 Buchstabe c umfassen mindestens die folgenden Angaben:

   a) Name des Entwicklers,

   b) Name und Kontaktangaben des Inhabers des EUCC-Zertifikats,

   c) Name der Zertifizierungsstelle, die das Zertifikat ausgestellt hat,

   d) zuständige nationale Behörde für die Cybersicherheitszertifizierung,

   e) Name der ITSEF, die die Evaluierung durchgeführt hat, und, falls zutreffend, Liste der Unterauftragnehmer.

7. Das Sicherheitskonzept gemäß Nummer 3 Buchstabe d beinhaltet die Beschreibung des Sicherheitskonzepts des IKT-Produkts als Gesamtheit der Sicherheitsdienste sowie der Konzepte oder Vorschriften, die das bewertete IKT-Produkt durchsetzen oder einhalten muss. Es muss außerdem folgende Angaben enthalten:

   a) eine Beschreibung der Verfahren des Zertifikatsinhabers für das Schwachstellenmanagement und die Offenlegung von Schwachstellen, die ausschließlich Informationen enthält, die öffentlich zugänglich gemacht werden können;

   b) das Konzept des Zertifikatsinhabers zur Gewährleistung der Kontinuität, falls zutreffend, einschließlich der Beschreibung der Lebenszyklusmanagement- oder Produktionsprozesse des Zertifikatsinhabers gemäß Anhang IV Abschnitt IV.1;

   c) falls zutreffend, das Bestehen eines Patchverwaltungsverfahrens und das Ergebnis seiner Bewertung gemäß Anhang IV Abschnitt IV.4.

8. Die Annahmen und die Klarstellung des Anwendungsbereichs gemäß Nummer 3 Buchstabe e muss umfassende Informationen über die Umstände und Ziele im Zusammenhang mit der beabsichtigten Verwendung des Produkts gemäß Artikel 7 Absatz 1 Buchstabe c sowie Folgendes enthalten:

   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,

   c) Beschreibung etwaiger Bedrohungen für das IKT-Produkt, denen die evaluierten Sicherheitsfunktionen des Produkts je nach der beabsichtigten Verwendung nicht entgegenwirken, sofern dies für einen potenziellen IKT-Produktnutzer als relevant erachtet wird.

   Die in Unterabsatz 1 genannten Informationen müssen so klar und verständlich wie möglich sein, damit die Nutzer des zertifizierten IKT-Produkts fundierte Entscheidungen über die mit dessen Verwendung verbundenen Risiken treffen können.

9. Die Informationen zur Architektur gemäß Nummer 3 Buchstabe f müssen eine allgemeine Beschreibung des IKT-Produkts und seiner Hauptkomponenten auf der Grundlage der in den Gemeinsamen Kriterien für die Vertrauenswürdigkeitsfamilie *Development — TOE-Design* (Entwicklung — Konzeption des Evaluierungsgegenstands) (ADV_TDS) festgelegten Vorgaben enthalten.

10. Die zusätzlichen Cybersicherheitsinformationen gemäß Nummer 3 Buchstabe g müssen den Link zur Website des Inhabers des EUCC-Zertifikats gemäß Artikel 55 der Verordnung (EU) 2019/881 enthalten.

11. Die Evaluierung und Konfiguration des IKT-Produkts gemäß Nummer 3 Buchstabe h müssen den Testaufwand sowohl des Entwicklers als auch des Evaluierers wiedergeben, einschließlich des Testansatzes, der Testkonfiguration und der Testtiefe. Sie enthalten zumindest die folgenden Angaben:

    a) Angabe der verwendeten Vertrauenswürdigkeitskomponenten aus den in Artikel 3 genannten Normen;

    b) Version des Sachstandsdokuments und weitere Sicherheitsbewertungskriterien, die bei der Evaluierung verwendet werden;

    c) Einstellungen und Konfigurationen des für die Tests und die Schwachstellenanalyse verwendeten Evaluierungsgegenstands;

    d) alle verwendeten Schutzprofile, einschließlich der folgenden Angaben: Name, Version, Datum und Zertifikat des Schutzprofils.

12. Die Ergebnisse der Evaluierung und die Angaben zum Zertifikat gemäß Nummer 3 Buchstabe i müssen Angaben zur erreichten Vertrauenswürdigkeitsstufe gemäß Artikel 4 der vorliegenden Verordnung und Artikel 52 der Verordnung (EU) 2019/881 enthalten.

13. Die Bemerkungen und Empfehlungen gemäß Nummer 3 Buchstabe j dienen dazu, zusätzliche Informationen über die Evaluierungsergebnisse zu geben. Diese Bemerkungen und Empfehlungen können Mängel des IKT-Produkts betreffen, die bei der Evaluierung entdeckt wurden, oder die Form von Hinweisen auf Merkmale, die besonders nützlich sind, annehmen.

14. Die Anhänge gemäß Nummer 3 Buchstabe k werden verwendet, um zusätzliche Informationen darzulegen, die für das Zielpublikum des Berichts nützlich sein können, aber aus logischer Sicht nicht in die vorgeschriebenen Abschnitte des Berichts passen, auch im Falle einer vollständigen Beschreibung des Sicherheitskonzepts.

15. Das Sicherheitsziel gemäß Nummer 3 Buchstabe l bezieht sich auf das evaluierte Sicherheitsziel. Das evaluierte Sicherheitsziel wird zusammen mit dem Zertifizierungsbericht für die Zwecke der Veröffentlichung auf der in Artikel 50 Absatz 1 der Verordnung (EU) 2019/881 genannten Website bereitgestellt. Ist vor der Veröffentlichung eine Bereinigung des evaluierten Sicherheitsziels erforderlich, so erfolgt diese gemäß Anhang V Abschnitt V.2 dieser Verordnung.

16. Die mit dem EUCC-System verknüpften Siegel oder Kennzeichen gemäß Nummer 3 Buchstabe m werden nach den Vorschriften und Verfahren des Artikels 11 in den Zertifizierungsbericht aufgenommen.

17. Das Glossar gemäß Nummer 3 Buchstabe n wird verwendet, um die Lesbarkeit des Berichts zu verbessern, indem Definitionen von Akronymen oder Begriffen bereitgestellt werden, deren Bedeutung möglicherweise nicht ohne Weiteres ersichtlich ist.

18. Das Literaturverzeichnis gemäß Nummer 3 Buchstabe o 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, die verwendet wurden,

    b) der technische Evaluierungsbericht,

    c) der technische Evaluierungsbericht für ein zusammengesetztes Produkt, falls zutreffend,

    d) die technische Referenzdokumentation,

    e) Sicherheitsleitlinien für Entwickler,

    f) Konfigurationsliste für Entwickler.

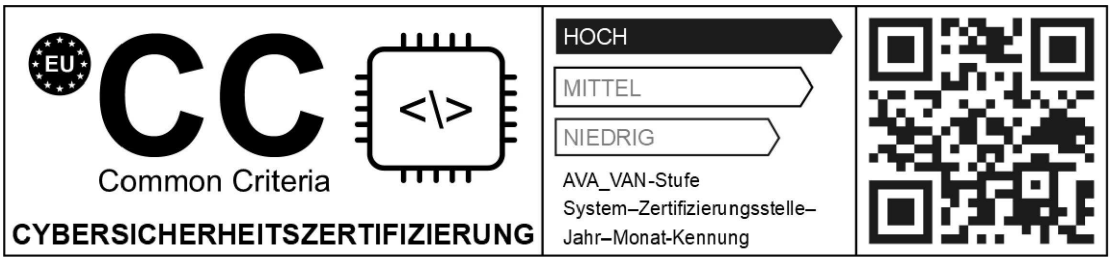
    Um die Reproduzierbarkeit der Evaluierung zu gewährleisten, muss die gesamte Dokumentation eindeutig mit dem richtigen Ausgabedatum und der entsprechenden Versionsnummer gekennzeichnet sein.“

ANHANG VI

„ANHANG IX

Siegel und Kennzeichen

1. Form des Siegels und Kennzeichens:



2. Bei Verkleinerung oder Vergrößerung des Siegels und Kennzeichens müssen die in Nummer 1 angegebenen Proportionen eingehalten werden.

3. Ein materiell vorhandenes Siegel und Kennzeichen muss mindestens 5 mm hoch sein.“