

**Teil 2 - "INFORMATIONSSICHERHEIT"**

Anmerkung 1: Die Erfassung von Einrichtungen, "Software", Systemen, anwenderspezifischen "elektronischen Baugruppen", Modulen, integrierten Schaltungen, Bauteilen oder Funktionen der "Informationssicherheit" richtet sich nach Kategorie 5, Teil 2 auch dann, wenn es sich um Komponenten oder "elektronische Baugruppen" anderer Einrichtungen handelt.

Anmerkung 2: Die Kategorie 5, Teil 2 erfasst keine Güter, wenn diese von ihrem Benutzer für den persönlichen Gebrauch mitgeführt werden.

Anmerkung 3: Kryptotechnik-Anmerkung:  
Die Nummern 5A002 und 5D002 erfassen keine Güter, die alle folgenden Voraussetzungen erfüllen:

- a) die Güter sind frei erhältlich und werden im Einzelhandel ohne Einschränkungen mittels einer der folgenden Geschäftspraktiken verkauft:
  1. Barverkauf,
  2. Versandverkauf,
  3. Verkauf über elektronische Medien oder
  4. Telefonverkauf;
- b) die kryptografische Funktionalität der Güter kann nicht mit einfachen Mitteln durch den Benutzer geändert werden;
- c) die Güter sind entwickelt, um vom Benutzer ohne umfangreiche Unterstützung durch den Anbieter installiert zu werden, und
- d) um die Übereinstimmung mit den unter a) bis c) beschriebenen Voraussetzungen feststellen zu können, sind detaillierte technische Beschreibungen der Güter vorzulegen und auf Verlangen der zuständigen Behörde des Mitgliedsstaates, in dem der Ausführer niedergelassen ist, vorzulegen.

Technische Anmerkung:  
Der in der Kategorie 5, Teil 2 verwendete Begriff der Schlüssellänge schließt Paritätsbits nicht mit ein.

**5A2 Systeme, Ausrüstung und Bestandteile**

5A002\* Systeme für "Informationssicherheit", Geräte und Bestandteile hierfür wie folgt:  
[W]

- a) Systeme, Geräte, anwenderspezifische "elektronische Baugruppen", Module und integrierte Schaltungen für "Informationssicherheit", wie folgt und andere besonders entwickelte Bestandteile hierfür:

Ergänzende Anmerkung:  
Bezüglich der Erfassung von GNSS (Global Navigation Satellite Systems)-Empfangseinrichtungen mit "Kryptotechnik" (z. B. GPS oder GLONASS) siehe Nummer 7A005.

1. entwickelt oder geändert zum Einsatz von "Kryptotechnik" unter Verwendung digitaler Verfahren, soweit es sich nicht um Authentisierung oder Digitale Signatur handelt, und mit einer der folgenden Eigenschaften:

5A002 a) 1. (Fortsetzung)

Technische Anmerkungen:

1. Funktionen der Authentisierung und Digitalen Signatur schließen zugehörige Schlüsselmanagementfunktionen ein.
2. Der Begriff der Authentisierung schließt alle Elemente der Zugangskontrolle ein, welche nicht die Verschlüsselung von Dateien oder Texten ermöglichen, mit Ausnahme derer, die im direkten Zusammenhang mit dem Schutz von Passwörtern, persönlicher Identifikationsnummern (PIN) oder vergleichbarer Daten stehen und den unbefugten Zugriff verhindern.
3. Der Begriff "Kryptotechnik" beinhaltet nicht "feste" Datenkompressions- oder Codierungstechniken.

Anmerkung: Die Unternummer 5A002a1 schließt Einrichtungen, entwickelt oder geändert zum Einsatz analoger "Kryptotechnik", ein, wenn deren Funktion auf der Verwendung digitaler Verfahren beruht.

- a) Verwendung "symmetrischer Algorithmen" mit einer Schlüssellänge größer 56 Bit oder
- b) Verwendung "asymmetrischer Algorithmen", deren Sicherheit auf einem der folgenden Verfahren beruht:
  1. Faktorisierung ganzer Zahlen, die größer als  $2^{512}$  sind (z.B. RSA-Verfahren),
  2. Berechnung des diskreten Logarithmus in der Multiplikationsgruppe eines endlichen Körpers mit mehr als  $2^{512}$  Elementen (z.B. Diffie-Hellman-Verfahren über  $Z/pZ$ ) oder
  3. Berechnung des diskreten Logarithmus in anderen Gruppen als den unter 5A002a1b2 aufgeführten mit größerer Ordnung als  $2^{112}$  (z.B. Diffie-Hellman-Verfahren über einer elliptischen Kurve),
2. entwickelt oder geändert zur Ausführung kryptoanalytischer Funktionen,
3. nicht belegt,
4. besonders entwickelt oder geändert, um kompromittierende Abstrahlung von Informationssignalen über das Maß hinaus zu unterdrücken, das aus Gründen des Gesundheitsschutzes, der Sicherheit oder der Einhaltung von Standards zur elektromagnetischen Verträglichkeit (EMV) erforderlich ist,
5. entwickelt oder geändert, um kryptografische Verfahren zur Erzeugung eines Spreizungscodes für Systeme mit "Gespreiztem-Spektrum-Verfahren", die nicht von Unternummer 5A002a6 erfasst sind, einschließlich der Erzeugung von Sprung-Codes für Systeme mit "Frequenzsprungverfahren", zu verwenden,
6. entwickelt oder geändert, um kryptografische Verfahren zur Erzeugung von Channelization-, Scrambling- oder Netzwerkidentifizierungscodes zu verwenden, für Systeme, die Ultrabreitbandmodulationsverfahren verwenden, und mit einer der folgenden Eigenschaften:
  - a) Bandbreite größer als 500 MHz oder
  - b) "normierte Bandbreite" (fractional bandwidth) größer/gleich 20 %,
7. nicht -kryptografische Sicherheitssysteme und Baugruppen der Informations- und Kommunikationstechnik (IuK), die über die Vertrauenswürdigkeitsstufe EAL-6 (Evaluation Assurance Level) der Common Criteria (CC) oder gleichwertiger Kriterien bewertet wurden,
8. Kommunikations-Kabelsysteme, entwickelt oder geändert, um unter Einsatz von mechanischen, elektrischen oder elektronischen Mitteln heimliches Eindringen zu erkennen,
9. entwickelt oder geändert für die Verwendung von "Quantenkryptografie".

Technische Anmerkung:

"Quantenkryptografie" ist auch bekannt als Quantum Key Distribution (QKD).

5A002 (Fortsetzung)

Anmerkung: Nummer 5A002 erfasst nicht folgende Güter:

- a) "personenbezogene Mikroprozessor-Karten" (personalised smart cards) mit einer der folgenden Eigenschaften:
1. ihre kryptografische Funktionalität ist beschränkt auf die Verwendung in Geräten oder Systemen, die gemäß den Buchstaben b) bis g) dieser Anmerkung von der Erfassung ausgenommen sind, oder
  2. für allgemeine Anwendungen im öffentlichen Bereich, bei denen die kryptografischen Funktionen dem Anwender nicht zugänglich sind und die besonders entwickelt sowie darauf beschränkt sind, intern gespeicherte personenbezogene Daten zu schützen,

Anmerkung: Falls eine "personenbezogene Mikroprozessor-Karte" über verschiedene Funktionen verfügt, ist jede einzelne Funktion hinsichtlich der Erfassung zu prüfen.

- b) Empfangseinrichtungen für Rundfunk, Pay-TV oder ähnliche Verteildienste mit eingeschränktem Empfängerkreis, für den allgemeinen Gebrauch, ohne digitale Verschlüsselungsfunktionen, ausgenommen derer, die ausschließlich für die Übermittlung von Zahlungs- bzw. programmbezogenen Informationen an den Dienstanbieter benutzt werden,
- c) Einrichtungen, deren kryptografische Funktionalität nicht anwenderzugänglich ist und die für folgende Anwendungen sowohl besonders entwickelt als auch beschränkt sind:
1. Ausführung kopiergeschützter "Software",
  2. Zugriff auf:
    - a) kopiergeschützte Inhalte, gespeichert auf nur mit Leseberechtigung versehenen Medien (read-only media), oder
    - b) in verschlüsselter Form gespeicherte Informationen (z.B. in Verbindung mit dem Schutz von Urheberrechten), wenn die entsprechenden Medien in jeweils identischer Form zum Verkauf im Einzelhandel angeboten werden,
  3. Sicherung der Urheberrechte (copyrights) beim Kopieren von Audio/Video-Daten oder
  4. Verschlüsselung und/oder Entschlüsselung zum Schutz von Bibliotheken, Design-Attributen oder zugehörigen Daten für den Entwurf von Halbleiterbauelementen oder integrierten Schaltungen,
- d) Kryptoeinrichtungen, besonders entwickelt für den Bankgebrauch oder 'Geldtransaktionen', soweit sie nur für diese Anwendungen einsetzbar sind,

Technische Anmerkung:

'Geldtransaktionen' im Sinne der Anmerkung d) zur Nummer 5A002 schließen auch die Erfassung und den Einzug von Gebühren sowie Kreditfunktionen ein.

- e) tragbare oder mobile Funktelefone für zivilen Einsatz (z.B. für den Einsatz in kommerziellen zivilen zellularen Funksystemen), die weder eine Möglichkeit zur Übertragung verschlüsselter Daten direkt zu einem anderen Funktelefon oder zu Einrichtungen (andere als Radio Access Network (RAN)-Einrichtungen) bieten noch eine Möglichkeit zur Durchleitung verschlüsselter Daten durch die RAN-Einrichtung (z.B. Radio Network Controller (RNC) oder Base Station Controller (BSC)) bieten,

5A002 Anmerkung (Fortsetzung)

- f) Ausrüstung für schnurlose Telefone, die keine Möglichkeit der End-zu-End-Verschlüsselung bieten und deren maximal erzielbare einfache Reichweite (das ist die Reichweite zwischen Terminal und Basisstation ohne Maßnahmen zur Reichweitenerhöhung) nach Angaben des Herstellers kleiner ist als 400 m, oder
- g) tragbare oder mobile Funktelefone sowie ähnliche nicht drahtgebundene Endgeräte bzw. Baugruppen (client wireless devices) für Anwendungen im zivilen Bereich, die ausschließlich veröffentlichte oder kommerziell erhältliche kryptographische Standardverfahren anwenden (ausgenommen sind dem Kopierschutz dienende Funktionen, diese dürfen auch unveröffentlicht sein) und die die Voraussetzungen b) und c) der Kryptotechnik-Anmerkung (Anmerkung 3 zur Kategorie 5, Teil 2) erfüllen, die für eine spezielle zivile Industrieanwendung ausschließlich in Bezug auf Funktionen, die die kryptographischen Funktionalitäten der ursprünglichen unveränderten Endgeräte bzw. Baugruppen nicht beeinflussen, angepasst wurden.
- h) Ausrüstung, besonders konstruiert für die Wartung tragbarer oder mobiler Funktelefone sowie ähnlicher nicht drahtgebundener Endgeräte bzw. Baugruppen (client wireless devices), die alle Voraussetzungen der Kryptotechnik-Anmerkung (Anmerkung 3 zur Kategorie 5, Teil 2) erfüllen, sofern die Wartungsausrüstung alle folgenden Voraussetzungen erfüllt:
1. die Kryptografiefunktion der Wartungsausrüstung kann vom Nutzer der Ausrüstung nicht ohne Weiteres geändert werden,
  2. die Wartungsausrüstung ist dazu entwickelt, ohne umfangreiche Unterstützung durch den Anbieter installiert zu werden, und
  3. die Kryptografiefunktion des zu wartenden Gerätes kann mit der Wartungsausrüstung nicht geändert werden,
- i) Ausrüstung für ein nicht drahtgebundenes "Personal Area Network", die ausschließlich veröffentlichte oder kommerziell erhältliche kryptografische Standardverfahren anwendet und deren kryptografische Funktionalität nominell auf einen Betriebsbereich beschränkt ist, der nach Angaben des Herstellers 30 m nicht überschreitet.

## 5B2 Prüf-, Test- und Herstellungseinrichtungen

5B002 [W] Prüf-, Test- und "Herstellungs" ausrüstung für "Informationssicherheit" wie folgt:

- a) Einrichtungen, besonders entwickelt für die "Entwicklung" oder "Herstellung" von Geräten die von Nummer 5A002 oder Unternummer 5B002b erfasst werden;
- b) Messeinrichtungen, besonders entwickelt, um "Informationssicherheits"-Funktionen von Geräten, die von Nummer 5A002 erfasst werden, oder von "Software", die von Unternummer 5D002a oder 5D002c erfasst wird, auszuwerten und zu bestätigen.

## 5C2 Werkstoffe und Materialien

Kein Eintrag.

**5D2 Datenverarbeitungsprogramme (Software)**

5D002\*  
[W] "Software" wie folgt:

- a) "Software", besonders entwickelt oder geändert für die "Entwicklung", "Herstellung" oder "Verwendung" von Einrichtungen, die von Nummer 5A002, oder von "Software", die von Unternummer 5D002c erfasst wird;
- b) "Software", besonders entwickelt oder geändert zur Unterstützung der von Nummer 5E002 erfassten "Technologie";
- c) "Software" wie folgt:
  1. "Software", die die Eigenschaften der von Nummer 5A002 erfassten Geräte besitzt oder deren Funktionen ausführt oder simuliert,
  2. "Software" zur Zertifizierung der von Unternummer 5D002c1 erfassten "Software".

Anmerkung: Nummer 5D002 erfasst nicht "Software" wie folgt:

- a) "Software", erforderlich für die "Verwendung" von Einrichtungen, die gemäß der Anmerkung zu Nummer 5A002 von der Erfassung ausgenommen sind,
- b) "Software", die Funktionen von Einrichtungen bereitstellt, die gemäß der Anmerkung zu Nummer 5A002 von der Erfassung ausgenommen sind.

**5E2 Technologie**

5E002\*  
[W] "Technologie" entsprechend der Allgemeinen Technologie-Anmerkung für die "Entwicklung", "Herstellung" oder "Verwendung" von Einrichtungen, die von Nummer 5A002 oder 5B002 erfasst werden, oder von "Software", die von Unternummer 5D002a oder 5D002c erfasst wird.