Teil 2 — "INFORMATIONSSICHERHEIT"

Anmerkung 1: *Nicht belegt.*

Anmerkung 2: *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, 5D002a1, 5D002b und 5D002c1 erfassen keine Güter mit folgenden Eigenschaften:

a) Güter, die alle folgenden Voraussetzungen erfüllen:

1. Die Güter sind frei erhältlich und werden im Einzelhandel ohne Einschränkungen mittels einer der folgenden Geschäftspraktiken verkauft:

a) Barverkauf,

b) Versandverkauf,

c) Verkauf über elektronische Medien oder

d) Telefonverkauf.

2. Die kryptografische Funktionalität der Güter kann nicht mit einfachen Mitteln durch den Benutzer geändert werden.

3. Sie wurde so konzipiert, dass der Benutzer sie ohne umfangreiche Unterstützung durch den Anbieter installieren kann, und

4. Um die Übereinstimmung mit den unter 1. bis 3. beschriebenen Voraussetzungen feststellen zu können, sind detaillierte technische Beschreibungen der Güter vorzuhalten und auf Verlangen der zuständigen Behörde des Mitgliedstaats, in dem der Ausführer niedergelassen ist, vorzulegen.

b) Hardwarekomponenten oder 'ausführbare Software' von unter Buchstabe a dieser Anmerkung beschriebenen Gütern, die für diese bestehenden Güter entwickelt wurden, mit allen folgenden Eigenschaften:

1. "Informationssicherheit" ist nicht die Hauptfunktion oder Teil der Menge der Hauptfunktionen der Komponente oder der 'ausführbaren Software',

2. die Komponente oder 'ausführbare Software' verändert keine kryptografischen Funktionen der bestehenden Güter und fügt diesen keine neuen kryptografischen Funktionen hinzu,

3. die Funktionsmerkmale der Komponente oder 'ausführbaren Software' sind feststehend und wurden nicht entsprechend einer Kundenvorgabe entwickelt oder geändert und

4. sofern erforderlich gemäß der Festlegung durch die zuständigen Behörden des Mitgliedstaats, in dem der Ausführer niedergelassen ist, sind detaillierte technische Beschreibungen der Komponente oder der 'ausführbaren Software' sowie der betreffenden Endgüter vorzuhalten und auf Verlangen der zuständigen Behörde vorzulegen, um die Übereinstimmung mit den oben beschriebenen Voraussetzungen überprüfen zu können.

Technische Anmerkung:

Im Sinne der Kryptotechnik-Anmerkung bedeutet 'ausführbare Software' "Software" in ausführbarer Form von bestehenden Hardware-Komponenten, die gemäß der Kryptotechnik-Anmerkung nicht von Nummer 5A002 erfasst werden.

Anmerkung: 'Ausführbare Software' schließt vollständige Binärabbilder (binary images) der auf einem Endprodukt laufenden "Software" nicht ein.

Anmerkung zur Kryptotechnik-Anmerkung:

1. Um die Voraussetzungen von Anmerkung 3 Buchstabe a zu erfüllen, müssen alle folgenden Bedingungen erfüllt sein:

a) das Gut ist von potenziellem Interesse für ein breites Spektrum an Einzelpersonen und Unternehmen und

b) der Preis und die Informationen zur Hauptfunktion des Guts sind vor ihrem Erwerb verfügbar, ohne dass hierfür eine Anfrage an den Verkäufer oder Lieferanten erforderlich ist. Eine einfache Preisauskunft gilt nicht als Anfrage.

2. Zur Bestimmung der Anwendbarkeit von Anmerkung 3 Buchstabe a können die zuständigen Behörden relevante Faktoren berücksichtigen wie Menge, Preis, erforderliche fachliche Kompetenz, bestehende Vertriebswege, typische Kunden, typische Verwendung oder etwaiges wettbewerbsausschließendes Verhalten des Lieferanten.

5A2 Systeme, Ausrüstung und Bestandteile

5A002 Systeme für "Informationssicherheit", Geräte und Bestandteile wie folgt:

Anmerkung: Bezüglich der Erfassung von GNSS (Global Navigation Satellite Systems)-Empfangseinrichtungen mit "Kryptotechnik" siehe Nummer 7A005 und zu verwandter Entschlüsselungs-"Software" und -"Technologie" siehe die Nummern 7D005 und 7E001.

a) Konstruiert oder geändert für die Verwendung von 'Kryptotechnik für die Vertraulichkeit von Daten' mit einer 'symmetrischen Schlüssellänge größer 56 Bit oder gleichwertig', sofern diese kryptografische Funktionalität ohne "kryptografische Freischaltung" verwendbar ist oder bereits freigeschaltet worden ist, wie folgt:

1. Güter mit "Informationssicherheit" als eine Hauptfunktion,

2. Digitale Kommunikations- oder Netzwerksysteme, Ausrüstung und Bestandteile, die nicht von Unternummer 5A002a1 erfasst werden,

3. Rechner, andere Güter, bei denen Informationsspeicherung oder -verarbeitung eine Hauptfunktion ist, und deren Bestandteile, die nicht von den Unternummern 5A002a1 oder 5A002a2 erfasst werden,

Anmerkung: Zu Betriebssystemen siehe auch die Unternummern 5D002a1 und 5D002c1.

4. Güter, die nicht von den Unternummern 5A002a1 bis 5A002a3 erfasst werden, sofern die 'Kryptotechnik für die Vertraulichkeit von Daten' mit einer 'symmetrischen Schlüssellänge größer 56 Bit oder gleichwertig' alle folgenden Kriterien erfüllt:

a) sie unterstützt eine Funktion, die keine Hauptfunktion des Guts ist, und

b) sie wird von einer eingebauten Ausrüstung oder "Software" ausgeführt, die als eigenständiges Gut von Kategorie 5 – Teil 2 erfasst wäre.

Technische Anmerkungen:

1. Im Sinne von Unternummer 5A002a bezeichnet 'Kryptotechnik für die Vertraulichkeit von Daten' "Kryptotechnik" unter Verwendung digitaler Verfahren, die andere kryptografische Funktionen als folgende ausführt:

a) "Authentisierung",

b) digitale Signatur,

c) Datenintegrität,

d) Nachweisbarkeit (non-repudiation),

e) digitales Rechtemanagement, einschließlich der Ausführung kopiergeschützter "Software",

f) Ver- oder Entschlüsselung, die dem Entertainment, kommerziellen Massenübertragungen oder dem Management von medizinischen Datensätzen dienen, oder

g) Schlüsselverwaltung, die einer der unter Buchstabe a bis f beschriebenen Funktionen dient.

2. Im Sinne der Unternummer 5A002a bezeichnet 'symmetrische Schlüssellänge größer 56 Bit oder gleichwertig' eine der folgenden Eigenschaften:

a) einen "symmetrischen Algorithmus" mit einer Schlüssellänge größer 56 Bit, Paritätsbits nicht mit eingeschlossen, oder

5A002 a. 2. (*Fortsetzung*)

b) einen "asymmetrischen Algorithmus", dessen Sicherheit auf einem der folgenden Verfahren beruht:

1. Faktorisierung ganzer Zahlen, die größer als 512 Bit sind (z. B. RSA-Verfahren),

2. Berechnung des diskreten Logarithmus in der Multiplikationsgruppe eines endlichen Körpers mit mehr als 512 Bit (z. B. Diffie-Hellman-Verfahren über Z/pZ) oder

3. Berechnung des diskreten Logarithmus in anderen Gruppen als den unter Buchstabe b Nummer 2 aufgeführten größer als 112 Bit (z. B. Diffie-Hellman-Verfahren über einer elliptischen Kurve).

Anmerkung 1: Sofern gemäß der Festlegung durch die zuständige Behörde des Landes des Ausführers erforderlich, sind detaillierte technische Beschreibungen der Güter vorzuhalten und dieser Behörde auf Verlangen vorzulegen, damit sie überprüfen kann,

a) ob die Güter die Kriterien der Unternummern 5A002a1 bis 5A002a4 erfüllen oder

b) ob die in Unternummer 5A002a beschriebene kryptografische Funktionalität für die Vertraulichkeit von Daten ohne „kryptografische Freischaltung" verwendbar ist.

Anmerkung 2: Unternummer 5A002a erfasst weder eines der folgenden Güter noch für diese besonders konstruierte Bestandteile für „Informationssicherheit":

a) Mikroprozessor-Karten (smart cards) und 'Schreib/ Lesegeräte' hierfür wie folgt:

1. Mikroprozessor-Karten oder elektronisch lesbare persönliche Dokumente (z. B. Wertmarke, ePass) mit einer der folgenden Eigenschaften:

a) die kryptografische Funktionalität erfüllt alle folgenden Eigenschaften:

1. sie ist beschränkt auf eine der folgenden Verwendungen:

a) Ausrüstung oder Systeme, die nicht von den Unternummern 5A002a1 bis 5A002a4 erfasst sind,

b) Ausrüstung oder Systeme, die keine 'Kryptotechnik für die Vertraulichkeit von Daten' mit einer 'symmetrischen Schlüssellänge größer 56 Bit oder gleichwertig' verwenden, oder

c) Ausrüstung oder Systeme, die gemäß den Buchstaben b bis f der vorliegenden Anmerkung nicht von Unternummer 5A002a erfasst sind; und

2. sie kann nicht für andere Zwecke umprogrammiert werden; oder:

b) mit allen folgenden Eigenschaften:

1. besonders entwickelt, um darauf gespeicherte 'personenbezogene Daten' zu schützen, und sind auf diese Funktion beschränkt,

2. sie wurden nur für öffentliche oder kommerzielle Transaktionen oder zur individuellen Identifizierung personalisiert oder können nur hierfür personalisiert werden, und

3. ihre kryptografische Funktionalität ist nicht anwenderzugänglich.

Technische Anmerkung:

'Personenbezogene Daten' beinhalten alle spezifischen Daten einer bestimmten Person oder eines Objekts, wie z. B. gespeicherter Geldbetrag oder zur "Authentisierung" benötigte Daten.

2. 'Schreib/Lesegeräte', die besonders für die in Buchstabe a Nummer 1 dieser Anmerkung beschriebenen Güter konstruiert oder geändert und auf diese beschränkt sind.

Technische Anmerkung:

'Schreib/Lesegeräte' beziehen Geräte ein, die mit einer Mikroprozessor-Karte oder einem elektronisch lesbaren Dokument über ein Netzwerk kommunizieren.

b) Kryptoeinrichtungen, besonders entwickelt für den Bankgebrauch oder 'Geldtransaktionen', soweit sie nur für diese Anwendungen einsetzbar sind.

Technische Anmerkung:

'Geldtransaktionen' im Sinne des Buchstaben b der Anmerkung 2 zur Unternummer 5A002a schließen auch die Erfassung und den Einzug von Gebühren sowie Kreditfunktionen ein.

5A002 a. *Anmerkung 2:* (*Fortsetzung*)

c) 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) noch eine Möglichkeit zur Durchleitung verschlüsselter Daten durch die RAN-Einrichtung (z. B. Radio Network Controller (RNC) oder Base Station Controller (BSC)) bieten,

d) 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,

e) 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 a2 bis a4 der Kryptotechnik-Anmerkung (Anmerkung 3 zur Kategorie 5, Teil 2) erfüllen, die für eine spezielle zivile Industrieanwendung ausschließlich in Bezug auf Leistungsmerkmale, die die kryptographischen Funktionalitäten der ursprünglichen unveränderten Endgeräte bzw. Baugruppen nicht beeinflussen, angepasst wurden,

f) Güter, bei denen die Funktionalität der "Informationssicherheit" auf die Funktionalität eines drahtlosen "Personal Area Network" beschränkt ist und die alle folgenden Kriterien erfüllen:

1. ausschließlicher Einsatz veröffentlichter oder kommerziell erhältlicher kryptographischer Standardverfahren, und

2. die kryptografische Funktionalität ist nominell auf einen Betriebsbereich beschränkt, der nach Angaben des Herstellers 30 m nicht überschreitet, oder der nach Angaben des Herstellers bei Ausrüstung, die Verbindungen mit maximal sieben Geräten aufbauen kann, 100 m nicht überschreitet,

g) Ausrüstung für den Mobilfunkzugang (RAN), konstruiert für Anwendungen im zivilen Bereich, die auch die Voraussetzungen der Absätze a2 bis a4 der Kryptografie-Anmerkung erfüllt (Teil 2, Kategorie 5, Anmerkung 3), mit einer auf 0,1 W (20 dBm) oder weniger begrenzten HF-Ausgangsleistung und die simultan bis zu 16 Nutzer unterstützen kann.

h) Router, Switche oder Repeater (relay), bei denen die Funktionalität der "Informationssicherheit" auf die Aufgaben von "Betrieb, Verwaltung oder Wartung" (Operations, Administration or Maintenance ("OAM")) beschränkt ist und die ausschließlich veröffentlichte oder kommerziell erhältliche kryptografische Standardverfahren anwenden; oder

i) Rechner für allgemeine Anwendungen oder Server, bei denen die Funktion der "Informationssicherheit" alle folgenden Kriterien erfüllt:

1. sie wendet ausschließlich veröffentlichte oder kommerziell erhältliche kryptographische Standardverfahren an, und

2. sie besitzt eine der folgenden Eigenschaften:

a) sie ist Bestandteil einer CPU, die die Kriterien der Anmerkung 3 von Kategorie 5, Teil 2, erfüllt,

b) sie ist Bestandteil eines Betriebssystems, das nicht in Nummer 5D002 erfasst wird, oder

c) sie ist auf "Betrieb, Verwaltung oder Wartung" ("OAM") der Einrichtung beschränkt.

b) entwickelt oder geändert, um bei einem Gut mittels "kryptografischer Freischaltung" das Leistungsniveau, das in Unternummer 5A002a beschrieben wird und das nicht anderweitig erreicht wird, zu erzielen oder zu übertreffen.

c) entwickelt oder geändert für die Verwendung oder Ausführung von "Quantenkryptografie".

Technische Anmerkung:

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

5A002 (*Fortsetzung*)

d) 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:

1. Bandbreite größer als 500 MHz oder

2. "normierte Bandbreite" (fractional bandwidth) größer/gleich 20 %.

e) entwickelt oder geändert, um kryptografische Verfahren zur Erzeugung eines Spreizungscodes für Systeme mit "Gespreiztem-Spektrum-Verfahren", die nicht von Unternummer 5A002d erfasst sind, einschließlich der Erzeugung von Sprung-Codes für Systeme mit "Frequenzsprungverfahren", zu verwenden.

5A003 Systeme, Ausrüstung und Bestandteile für nicht-kryptografische "Informationsicherheit" wie folgt:

a) Kommunikations-Kabelsysteme, entwickelt oder geändert, um unter Einsatz von mechanischen, elektrischen oder elektronischen Mitteln heimliches Eindringen zu erkennen,

Anmerkung: Unternummer 5A003a erfasst nur die Sicherheit der physikalischen Schicht (physical layer security). Im Sinne der Unternummer 5A003a beinhaltet die physikalische Schicht auch Schicht 1 (Layer 1) des OSI-Modells (Open Systems Interconnection) (ISO/IEC 7498-1).

b) 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.

5A004 Systeme, Ausrüstung und Bestandteile für die Überwindung, die Schwächung oder die Umgehung von "Informationssicherheit" wie folgt:

a) entwickelt oder geändert zur Ausführung 'kryptoanalytischer Funktionen',

Anmerkung: Die Unternummer 5A004a schließt Systeme und Ausrüstung ein, die zur Ausführung 'kryptoanalytischer Funktionen' durch Reverse Engineering entwickelt oder geändert wurden.

Technische Anmerkung:

'Kryptoanalytische Funktionen' sind Funktionen, die zum Brechen kryptografischer Verfahren entwickelt wurden, um vertrauliche Variablen oder sensitive Daten einschließlich Klartext, Passwörter oder kryptografische Schlüssel abzuleiten.

5B2 Prüf-, Test- und Herstellungseinrichtungen

5B002 Prüf-, Test- und "Herstellungs-"einrichtungen für "Informationssicherheit" wie folgt:

a) Einrichtungen, besonders entwickelt für die "Entwicklung" oder "Herstellung" von Geräten, die von Nummer 5A002, 5A003, 5A004 oder Unternummer 5B002b erfasst werden;

b) Messeinrichtungen, besonders entwickelt, um "Informationssicherheits"-Funktionen von Einrichtungen, die von Nummer 5A002, 5A003 oder 5A004 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 "Software" wie folgt:

a) "Software", besonders entwickelt oder geändert für die "Entwicklung", "Herstellung" oder "Verwendung" folgender Güter:

1. Ausrüstung, die von Nummer 5A002 erfasst ist, oder „Software", die von Unternummer 5D002c1 erfasst ist,

5D002 a. (*Fortsetzung*)

2. Ausrüstung, die von Nummer 5A003 erfasst ist, oder „Software“, die von Unternummer 5D002c2 erfasst ist, oder

3. Ausrüstung, die von Nummer 5A004 erfasst ist, oder „Software“, die von Unternummer 5D002c3 erfasst ist,

b) "Software", entwickelt oder geändert, um bei einem Gut mittels "kryptografischer Freischaltung" die Kriterien, die in Unternummer 5A002a beschrieben werden und die nicht anderweitig erreicht werden, zu erfüllen.

c) “Software”, die die Eigenschaften folgender Güter besitzt oder deren Funktionen ausführt oder simuliert, wie folgt:

1. Ausrüstung, die von den Unternummern 5A002a, 5A002c, 5A002d oder 5A002e erfasst ist.

Anmerkung: Unternummer 5D002c1 erfasst keine "Software", deren Aufgaben auf “Betrieb, Verwaltung oder Wartung” (“OAM”) beschränkt sind und die ausschließlich veröffentlichte oder kommerziell erhältliche kryptographische Standardverfahren anwendet.

2. Ausrüstung, die von Nummer 5A003 erfasst wird, oder

3. Ausrüstung, die von Nummer 5A004 erfasst wird,

d) nicht belegt.

5E2 Technologie

5E002 “Technologie” wie folgt:

a) “Technologie” entsprechend der Allgemeinen Technologie-Anmerkung für die "Entwicklung", "Herstellung" oder "Verwendung" von Einrichtungen, die von Nummer 5A002, 5A003, 5A004 oder 5B002 erfasst werden, oder von “Software”, die von Unternummer 5D002a oder 5D002c erfasst wird.

b) "Technologie", entwickelt oder geändert, um bei einem Gut mittels "kryptografischer Freischaltung" die Kriterien, die in Unternummer 5A002a beschrieben werden und die nicht anderweitig erreicht werden, zu erfüllen.

Anmerkung: Nummer 5E002 erfasst technische Daten zur “Informationssicherheit”, die durch Verfahren erfasst wurden, die zur Evaluierung oder Bestimmung der Umsetzung von in Kategorie 5, Teil 2, beschriebenen Funktionen, Leistungsmerkmalen oder Techniken durchgeführt wurden.