Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anwendungshinweise und Interpretationen zum Schema (AIS)

AIS B7, Version 1.0

Stand:	01.10.2023
Status:	Verbindlich für Geltungsbereich Highspeed-Konnektor
Thema:	Anforderungen an einen Highspeed-Konnektor
Herausgeber:	Zertifizierungsstelle des BSI
Verteiler:	Anerkannte BSZ Prüfstellen BSI intern Internet-Seite des BSI

Änderungshistorie

Version	*Datum*	*Name/Org.-Einheit*	*Änderungen*
1.0	2023-10-01	BSI und gematik GmbH	Erstausgabe der AIS B7: Anforderungen an einen Highspeed-Konnektor

Tabelle 1: Änderunghistorie

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

Inhalt

1 Hintergrund

1 In diesem Dokument werden die für den Geltungsbereich spezifischen Anforderungen an Evaluierungsgegenstand und Antragstellerdokumente im Geltungsbereich Highspeed Konnektor (HSK) der Beschleunigten Sicherheitszertifizierung(BSZ) beschrieben.

2 Die Vorgaben zum Highspeed-Konnektor wurden von der gematik GmbH als Nationale Agentur für Digitale Medizin in Form von Spezifikationen erstellt. Dieses Dokument wurde von der gematik GmbH in Abstimmung mit dem BSI erstellt.

3 Die in diesem Dokument beschriebenen Anforderungen beziehen sich auf die Bereitstellung des Evaluierungsgegenstands inklusive der notwendigen Betriebsumgebung, auf die Sicherheitsfunktionalität, die Schnittstellen, das Bedrohungsmodell und die Betriebsumgebung des Highspeed-Konnektors (HSK) und enthalten zusätzliche Aufgaben für Evaluierung durch die Prüfstelle.

4 Die Anforderungen an die Bereitstellung des Evaluierungsgegenstands sind in Kapitel 3 beschrieben.

5 Die Anforderungen an Sicherheitsfunktionalität, Schnittstellen, Bedrohungsmodell und Betriebsumgebung sind auf Vorgaben für das Dokument Sicherheitsvorgaben (eng. Security Target, ST) für die BSZ abgebildet und ergänzen somit das Dokument [AIS B1]. Sie sind in den Kapiteln 4 und 5 beschrieben.

6 Die Anforderungen für die zusätzlichen Evaluierungsaufgaben sind in Kapitel 6 beschrieben.

7 Die anderen in diesem Geltungsbereich gültigen Anforderungsdokumente, die in Kapitel 2 aufgeführt sind, bleiben unverändert gültig.

2 Für den Geltungsbereich HSK gültige Anforderungsdokumente

1 [BSZ-Prod] Produktzertifizierung: Programm Beschleunigte Sicherheitszertifizierung (BSZ), BSZ-Produkte, BSI

2 [BSZ-Prüf] Anerkennung von Prüfstellen: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ), BSZ-Prüfstellen, BSI

3 [BSZ-EP] Programm [BSZ-Prüfstellen]: BSZ-Evaluierungsprozess, BSZ-EP, BSI

4 [AIS B1] Requirements for Security Targets, BSI

5 [AIS B2] Requirements for the evaluation of cryptographic mechanisms according to the BSZ, BSI

6 [AIS B3] Requirements for user guidance, BSI

7 [AIS B4] Requirements for evaluation according to the BSZ, BSI

8 [AIS B6] Requirements for a TOE, BSI

9 [BSZ-ETR] BSZ – Vorlage für den Evaluierungsreport, BSI

10 [BSZ-ADA] BSZ - Agenda der Auftaktbesprechung, BSI

3 Vorgaben für die Bereitstellung des Evaluierungsgegenstands

8 Im Geltungsbereich Highspeed-Konnektor (HSK) gilt grundlegend die Anforderung der [BSZ-Prod] zur Bereitstellung des Evaluierungsgegenstands inklusive der notwendigen Betriebsumgebung. Das heißt, der Hersteller muss der Prüfstelle drei Evaluierungsgegenstände für die Durchführung der Evaluierung übergeben. Die Evaluierung muss in den Räumlichkeiten der Prüfstelle stattfinden

9 Der Antragsteller muss der Prüfstelle zusätzlich zum Evaluierungsgegenstand eine „Debugging-Variante“ des Evaluierungsgegenstands übergeben. Zweck der Debugging-Variante ist unter anderem, ein effizientes Testen der Client-Dienste zu ermöglichen. Die genaue Spezifikation der Debugging-Variante wird im Einzelfall zwischen Antragsteller und Prüfstelle mit Einvernehmen der Zertifizierungsstelle vereinbart.

10 Die Debugging-Variante kann zusätzlich auf der Hardware der Evaluierungsgegenstände installiert und betrieben werden.

11 Die Debugging-Variante muss alle Funktionen des Evaluierungsgegenstands enthalten. Die Funktionen müssen in gleicher Art und Weise und Version umgesetzt sein.

4 Vorgaben an die Sicherheitsvorgaben für einen HSK

12 Die hier beschriebenen Anforderungen an das Dokument Sicherheitsvorgaben für einen HSK ergänzen und spezifizieren die allgemeinen Anforderungen an die Sicherheitsvorgaben für die BSZ aus [AIS B1]. Die folgenden Abschnitte orientieren sich an der in [AIS B1] vorgegebenen Struktur und definieren die jeweiligen Anforderungen an den Inhalt der einzelnen Kapitel und Unterkapitel.

13 Der Platzhalter < Produktname > in den Anforderungen muss im ST sinnvoll mit dem Namen, der Kurzbezeichnung oder Abkürzung des Evaluierungsgegenstands (eng. Target of Evaluation, TOE) ersetzt werden. Es können auch passende Artikel, Präpositionen oder Pronomen ergänzt werden.

4.1 Einleitung

4.1.1 Kontext des Dokuments

14 In diesem Unterkapitel muss der Geltungsbereich HSK benannt werden.

4.1.2 Identifikation des Produkts

15 Produkt und Version müssen den in anderen Teilen des Zulassungsprozesses der gematik entsprechen.

4.1.3 Referenzen Abkürzungsverzeichnis

16 In diesem Unterkapitel sollen insbesondere auch die referenzierten Spezifikationen der gematik und Standards aufgezählt werden.
Beispiele sind in Kapitel 5 aufgeführt.

4.2 Produktbeschreibung

4.2.1 Allgemeine Beschreibung

17 Im Unterkapitel allgemeine Produktbeschreibung muss das Produkt (HSK) beschrieben werden.
Beispiel: < Produktname > ist ein Highspeed-Konnektors (HSK) für die Telematikinfrastruktur. Ein HSK ist eine performante und skalierbare Lösung für die Anbindung an die Telematikinfrastruktur des deutschen Gesundheitswesens (TI) und die Nutzung ihrer Anwendungen.

4.2.2 Eigenschaften / Funktionen

18 Die Beschreibung der Eigenschaften des HSK muss die folgenden Punkte enthalten:

- Der HSK bietet dem Nutzer über seine Außenschnittstellen sowohl Grundfunktionalitäten wie die Erstellung und Prüfung von Signaturen oder die Ver- und Entschlüsselung von Dokumenten, als auch die Nutzung von medizinischen Anwendungen der TI wie bspw. die elektronische Patientenakte an. Die dafür teilweise notwendige Nutzung von Smartcards von Versicherten und Leistungserbringern über eHealth-Kartenterminals (eHKT) wird ebenfalls vom HSK gesteuert.
- Zur Administration verfügt der HSK über eine Management-Schnittstelle, die mittels TLS abgesichert ist und eine Authentifizierung des Administrators per Username und Passwort verlangt.

- Der HSK kann so konfiguriert werden, dass die fachliche Nutzung der Außenschnittstellen nur über einen TLS-Kanal und nach Client-Authentisierung möglich ist. Dies ist die Konfiguration in der der HSK im Rahmen der BSZ geprüft wird.

19 Die Auflistung der Schnittstellen muss die folgenden Schnittstellen beinhalten:

- Netzwerkschnittstelle ins lokale Netz
  - als Server
    - Management-Schnittstelle über https (ggf. mehrere, getrennte Schnittstellen)
    - SOAP-Schnittstelle (je nach Konfiguration über http/https)
    - LDAP-Schnittstelle (je nach Konfiguration LDAP/LDAPS)
    - DNS-Server
    - NTP-Server
  - als Client
    - SICCT-Verbindungen zum eHealth-Kartenterminal
    - TLS-Verbindungen zum eHealth-Kartenterminal
    - Fehlermeldungen an Clients (je nach Konfiguration über http/https)
- Netzwerkschnittstelle zur TI
  - als Server
    - keine
  - als Client
    - TLS-Verbindungen (https) zu TI-Diensten
    - plain http-Verbindungen zu TI-Diensten

Hinweis: Diese Liste ist eine Liste der mindestens in einem HSK enthaltenen Schnittstellen und keine direkte Vorlage für das Security Target die wie oben dargestellt kopiert werden soll. Grundsätzlich gelten für die Auflistung der Schnittstellen die entsprechenden Anforderungen der [AIS B1].

20 Weitere Schnittstellen sind nicht vorgesehen. Sollte der HSK eines Herstellers dennoch weitere Schnittstellen besitzen, sind diese im Security Target zu beschreiben. Eine frühzeitige Abstimmung diesbezüglich mit der Prüfstelle und der gematik wird dringend empfohlen. Insbesondere ist es empfehlenswert vorab zu klären, ob eine Untersuchung im Rahmen der BSZ notwendig und möglich ist.
Hinweis: Wenn die Evaluierung von zusätzlichen Schnittstellen und Diensten zu erheblichen Mehraufwänden führt, kann es sein, dass eine Evaluierung und somit auch eine Zertifizierung im Rahmen der BSZ nicht möglich ist.

21 Bei zusätzlichen Schnittstellen müssen Verwendungszweck und Erreichbarkeit der Schnittstelle beschrieben und auch in „Umfang der Sicherheitsleistungen“ (siehe Abschnitt 4.3) abgebildet werden. Das heißt, es ist zu prüfen, ob jenseits der in Abschnitt 4.3 aufgeführten Werte, Schutzziele, Angreifer, Sicherheitsfunktionen, Bedrohungen und Annahmen weitere notwendig sind. Falls es keine Vorgaben der gematik zu diesen Schnittstellen gibt, sollen die aktuellen Empfehlungen des BSI zu Kryptographische Verfahren (TR-02102) beachtet werden.
Hinweis: Der HSK wird in der Produktivumgebung über zwei Varianten an die TI angebunden. Variante a) ist einen sogenannten SZZP-light-plus zu welchem der HSK einen gesicherten, authentisierten Kanal aufbauen muss. Dies ist eine Funktion des SZZP-light-plus, die der HSK bedienen muss, um mit Diensten in der TI kommunizieren zu können. Es ist keine Funktion zum Schutz des HSK selbst. Dies wird im Absatz

Grenzen der Evaluierung nochmals thematisiert. Die Variante b) ist ein SZZP oder SZZP-light, bei welchem kein gesicherter, authentisierter Kanal aufgebaut werden muss. Je nach Betriebsumgebung – also je nach vorhandenem SZZP - wird vom Hersteller bei der Inbetriebnahme einmalig konfiguriert, ob vom HSK der sichere, authentisierte Kanal verwendet wird oder nicht.

4.2.3 Produktnutzung

22 Im Unterkapitel Produktnutzung muss der Einsatz des HSK beschrieben werden.
Beispiel: Der HSK ist für große Leistungserbringerinstitutionen mit einer sehr hohen Zahl von Nutzern gedacht. Diese Umgebungen werden mit den bisher verfügbaren Einboxkonnektoren aufgrund ihrer naturgemäß geringeren Leistung nicht ausreichend bedient.

4.2.4 Einsatzumgebung

23 Im Unterkapitel Einsatzumgebung des HSK muss die Einsatzumgebung des Produkts wie folgt beschrieben werden:
< Produktname > wird in einer Rechenzentrumsumgebung betrieben, in der das HSK-Produkt vor physischem Zugriff geschützt ist. Für den Zugang zu Diensten der TI ist < Produktname > mit einem < SZZP/SZZP-light/SZZP-light-plus > verbunden. Diese vom < Produktname > genutzten Dienste der TI sind als vertrauenswürdig anzusehen. Für die Ansteuerung von Smartcards der Nutzer ist der < Produktname > mit eHealth-Kartenterminals verbunden, welche als vertrauenswürdig anzusehen sind. An seiner Management-Schnittstelle muss sich der < Produktname > vor unauthentisierten Nutzern schützen. Da die fachlichen Schnittstellen des < Produktname > von einer großen Anzahl an verschiedenen Nutzer und Clients genutzt werden, sollen diese Schnittstellen grundsätzlich nicht angreifbar sein, dürfen also genau nur nach spezifiziertem Funktionsumfang ansprechbar sein und reagieren.

4.3 Umfang der Sicherheitsleistung

24 Das ST muss die in diesem Unterkapitel dargestellten Sicherheitsleistungen beinhalten.

25 Die Beschreibung von Nutzern, Annahmen, Werte, Angreifer und Sicherheitsfunktionen sowie die Abbildung der Sicherheitsfunktionen auf das Bedrohungsmodel im Security Target muss wie in den jeweiligen Abschnitten beschrieben erfolgen.
Hinweis: Hinweise und einleitende Sätze müssen nicht in das ST übernommen werden

26 Den Annahmen in Abschnitt 4.3.2 sollen grundsätzlich keine weitere Annahme hinzugefügt werden. Falls weitere Annahmen vorgesehen sind, wird eine frühzeitige Abstimmung diesbezüglich mit der Prüfstelle, Zertifizierungsstelle und der gematik dringend empfohlen.

27 Es ist möglich weitere Nutzer, Werte, Angreifer, Bedrohungen und Sicherheitsfunktionen hinzuzufügen bzw. genauer zu spezifizieren.
Hinweis: Diese müssen dann in Unterabschnitt 4.3.7 Abdeckung entsprechend ergänzt werden.

4.3.1 Nutzer

28 < Produktname > unterscheidet grundsätzlich zwei Nutzergruppen, Administratoren und fachliche Nutzer. Sollte der HSK eines Herstellers dennoch Nutzergruppen adressieren, sind diese im Security Target zu beschreiben. Eine frühzeitige Abstimmung diesbezüglich mit der Prüfstelle und der gematik wird dringend empfohlen.

29 Administrator: Nutzung der Web-/REST-Interface über https mit Authentisierung per Username und Passwort; berechtigt für genau definierte Konfigurationsmöglichkeiten; keine tiefergreifenden Systemrechte.
Hinweis: Der HSK kann unterschiedliche Administratorrollen enthalten. Diese müssen jeweils einzeln beschrieben werden.

30 Fachliche Nutzer: Nutzung des http(s)/SOAP- und LDAP(S)-Interface, je nach Konfiguration über TLS mit Clientauthentisierung; nicht berechtigt für Konfigurationsänderungen und keine tiefergehenden Systemrechte.

4.3.2 Annahmen

31 **Ann.1** < Produktname > wird in einer Umgebung betrieben, in der er vor unberechtigtem physischem Zugriff geschützt ist. Betrachtet werden müssen daher nur logische Schnittstellen des HSK. Die Umsetzung von entsprechenden Maßnahmen wird durch ein Produktgutachten nachgewiesen, welches der Hersteller durch einen unabhängigen Gutachter anfertigen lässt und bei der gematik einreicht, die es hinsichtlich Vollständigkeit und Nachvollziehbarkeit prüft.
Hinweis: Der Schutz vor unberechtigtem physischem Zugriff bezieht sich konkret auf das Produkt, nicht jedoch auf das in der Betriebsumgebung vorliegende Netzwerk. Angriffe aus diesem Netzwerk, müssen mit betrachtet werden.

32 **Ann.2** Um den physischen Schutz von Beginn an zu gewährleisten, wird < Produktname > vom Hersteller sicher in Betrieb genommen.

33 **Ann.3** Der < Produktname > wird von geschultem Personal sicher administriert.

34 **Ann.4** Die Dienste der TI und die eHealth-Kartenterminals sind als vertrauenswürdig und sicher anzusehen.

35 **Ann.5** Aktive Angriffe aus dem Netz der TI sind ausgeschlossen. Dies gilt nicht für passive Versuche, Datenverkehr mitzulesen oder zu manipulieren bzw. Identitäten bspw. von Fachdiensten vorzutäuschen.

4.3.3 Werte

#	*Beschreibung*	*Schutzziele*
W.1	Primärdaten: Nutzerdaten und Metadaten die vom Nutzer an < Produktname > gesendet, ggf. durch den HSK von Fachdiensten abgerufen, im HSK verarbeitet und vom HSK an den Nutzer ausgegeben werden.	Vertraulichkeit, Integrität
W.2	Sekundärdaten: Artefakte, die für den Schutz von Primärdaten benötigt werden, wie bspw. Schlüssel und Zugriffs-Token	Vertraulichkeit, Integrität
W.3	Authentisierungsdaten: Daten mit denen Zugriff auf den < Produktname > bzw. seine Schnittstellen möglich wird, wie bspw. Passwörter, Client-Credentials und UserID	Vertraulichkeit, Integrität
W.4	Vertrauensanker: TSL-Signer-CA-Zertifikat, CV-Root-Zertifikate	Integrität
W.5	Konfigurationsdaten: Daten bzw. Konfigurationen, deren Änderung den sicheren Betrieb des HSK beeinträchtigen können.	Integrität

Tabelle 1: Übersicht zu schützender Werte

4.3.4 Angreifer

#	*Beschreibung*
A.1	Ein unauthentisierter Nutzer aus dem lokalen Netz, der Zugriff auf die Management-Schnittstelle des HSK erlangen will.
A.2	Ein Nutzer von einem unauthentisierten Client aus dem lokalen Netz, der bei Konfiguration von zwingender Client-Authentisierung (zertifikatbasierte Client-Authentisierung im TLS-Handshake oder Username/Passwort nach TLS-Handshake) Zugriff auf die fachlichen Schnittstellen des < Produktname > erlangen will.

A.3	Ein Nutzer aus dem lokalen Netz, der bei Konfiguration von zwingendem TLS als Man-in-the-Middle (MitM) die Verbindung eines anderen Nutzers abhören und manipulieren will.
A.4	Ein Nutzer aus dem lokalen Netz, der den HSK aus Versehen oder bewusst manipulieren will.
A.5	Ein unauthentisierter Nutzer mit Zugang zum Netz der TI, der die Kommunikation zwischen dem < Produktname > und Diensten der TI abfangen oder manipulieren will.

Tabelle 2: Übersicht Angreifer

4.3.5 Bedrohungen

#	*Beschreibung*
B.1	Es findet ein unberechtigter Zugriff auf die Management-Schnittstelle statt.
B.2	Es findet ein unberechtigter Zugriff auf fachliche Schnittstellen trotz konfiguriertem zwingendem TLS mit Client-Authentisierung statt.
B.3	Verbindungen von berechtigten Nutzern werden trotz konfiguriertem zwingendem TLS abgehört oder manipuliert.
B.4	< Produktname > wird an seinen Schnittstelle durch Übermittlung fehlerhafter oder schadhafter Aufrufe / Daten manipuliert.
B.5	Dienste der TI, welche nur per TLS erreichbar sind, werden mittels falscher Identitäten vorgetäuscht mit dem Ziel Daten unberechtigt zur Kenntnis zu nehmen oder zu ändern (kein aktives Hacking).

Tabelle 3: Übersicht Bedrohungen

4.3.6 Sicherheitsfunktionen

#	*Beschreibung*
SF.1	< Produktname > führt eine sichere Authentifizierung von Nutzern an der Management-Schnittstelle mittels Username und Passwort gemäß TIP1-A_4808-01 durch.
SF.2	TLS Umsetzung: < Produktname > setzt das TLS-Protokoll entsprechend [gemSN_HSK] Absatz 2.2.3.1 „Robustheit“ und 2.2.3.2 „TLS-Version, Ciphersuiten“ um.
SF.3	TLS durchsetzen: < Produktname > erlaubt die Kommunikation für die in [gemSN_HSK] Absatz 2.2.3.3 „Durchsetzen von TLS an allen notwendigen Stellen“ geforderten Kommunikationswege über seine Schnittstellen nur unter Verwendung von TLS (siehe SF.2).
SF.4	< Produktname > führt eine sichere Authentifizierung von Kommunikationspartnern bei TLS-Verbindungen, wie es nach [gemSN_HSK] Absatz „Korrekte Implementierung und Robustheit des TLS-Protokolls“ gefordert ist, durch.
SF.5	Robuste Schnittstellen: < Produktname > setzt seine Schnittstellen robust um und verhindert unautorisierten Zugriff.

Tabelle 4: Übersicht Sicherheitsfunktionen

4.3.7 Abdeckung

Angreifer	*Bedrohung*	*Werte*	*Sicherheitsfunktionen*
A.1	B.1	W.3, W.5	SF.1
A.2	B.2	W.1, W.2	SF.2, SF.3, SF.4
A.3	B.3	W.1, W.2	SF.2, SF.3
A.4	B.4	W.1, W.2, W.3, W.4, W5	SF.5,SF.1, SF.2, SF.3, SF.4
A.5	B.5	W.1, W.2	SF.2, SF.3, SF.4

Tabelle 5: Abbildung der Sicherheitsfunktionen auf das Bedrohungsmodell

4.4 Grenzen der Evaluierung

36 Das ST muss im Kapitel Grenzen der Evaluierung die folgenden Punkte beinhalten:

- Angriffe auf die Hardware von < Produktname > werden nicht betrachtet, da < Produktname > vor unberechtigtem physischem Zugriff geschützt ist.
  Hinweis: Der Schutz vor unberechtigtem physischem Zugriff bezieht sich konkret auf das Produkt, nicht jedoch auf das in der Betriebsumgebung vorliegende Netzwerk. Angriffe aus diesem Netzwerk, müssen mit betrachtet werden.
- Die sichere Umsetzung der fachlichen Funktionen von < Produktname > sowie weitere Sicherheitsprotokolle auf Anwendungsebene innerhalb von TLS-Kanälen sind nicht Gegenstand der Betrachtung. Diese Funktionen werden durch ein anderes Prüfverfahren validiert.
- Die Schnittstelle zum SZZP/SZZP-light/SZZP-light-plus muss – wie jede andere Schnittstelle – hinsichtlich Robustheit berücksichtigt werden. Jedoch ist die Funktionalität für den sicheren, authentischen Kanal zum SZZP-light-plus (wenn das Produkt für die Anbindung an eben solch einen SZZP-light-plus konfiguriert ist) nicht Teil des Prüfumfangs, da es keine Funktion zum Schutz des/der < Produktname > ist. Ebenso ist die Funktionalität, bestimmte Kommunikationen genau nur durch den sicheren, authentischen Kanal zum SZZP-light-plus zu senden, nicht Teil der Prüfungen in der BSZ.
- Aktive Angriffe aus dem Netz der TI sind ausgeschlossen. Es werden daher lediglich aktive Angriffe mit lokalem Zugriff auf die logischen Schnittstellen des/der < Produktname > betrachtet. Passive Versuche, Datenverkehr mitzulesen oder zu manipulieren bzw. Identitäten bspw. von Fachdiensten vorzutäuschen, werden auch bzgl. dem Netz der TI mitbetrachtet.
- Ein mit < Produktname > zusammen verwendetes HSM ist nicht Teil der Untersuchung. Entsprechend der bestehenden Vorgaben der gematik kommen nur geeignete, zertifizierte HSMs zum Einsatz. Daher müssen diese nicht erneut evaluiert werden.
  Hinweis: Sofern die Schnittstelle des HSK zu einem solchen HSM im Netzwerk exponiert ist, also nicht vom Schutz vor unberechtigtem physischem Zugriff umfasst ist, muss diese Schnittstelle des HSK im Rahmen der Evaluierung betrachtet werden.

5 Spezifikation kryptographischer Vorgaben

37 Für ein BSZ-Verfahren ist eine detaillierte, tabellarische Darstellung aller in den betrachteten Sicherheitsfunktionen verwendeten kryptographischen Algorithmen und Verfahren erforderlich. Dies soll nach Schnittstellen bzw. Diensten Aufgeteilt sein und ist im Folgenden beispielhaft dargestellt ist

#	*Zweck*	*Kryptographischer Mechanismus*	*Implementierungsstandard*	*Schlüssellänge in Bit*	*Anwendungsstandard*
	Verbindung zur Management-Schnittstelle via HTTPS mit TLS 1.2 [RFC 8446]				
1	Authentizität	RSA Verifikation von Signaturen für TLS sha256withRSAEncryption (OID 1.2.840.113549.1.1.	[RFC-8017] (PKCS#1) [FIPS 180-4] (SHA)	2048 Bit	[gemSpec_Krypt] Kap. 3.3.2
2	Authentisierung	RSA Signatur Erzeugung und Verifikation für TLS sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	[RFC-8017] (RSASSA- PKCS1-v1_5) [FIPS 180-4] (SHA)	2048 Bit	[gemSpec_Krypt], Kap. 3.3.2
3	Schlüsselaushandlung	Diffie-Hellman Schlüsselaushandlung (DH) und Elliptic Curve Diffie-Hellman Schlüsselaushandlung (ECDH) für TLS	[RFC-5246] (TLS v1.2) [RFC-3268] (DHE_RSA) [RFC-4492] (ECDHE_RSA)	DH: Gruppe 14 2048 Bit Exponentenlänge = 2048 Bits ECDH: Schlüssellänge entsprechend der verwendeten elliptischen Kurven P-{256,384} ([FIPS186-4]) und brainpoolP{256,384}r1 ([RFC7027])	[gemSpec_Krypt], Kap. 3.3.2
4	Schlüsselableitung	Schlüsselableitung für TLS 1.2	[RFC-5246] (TLS v1.2) [FIPS-180-4] (SHA), [RFC-2104] (HMAC)	128 Bit und 256 Bit	[gemSpec_Krypt], Kap. 3.3.2
5	Integrität	HMAC Berechnung und Prüfung für TLS HMAC mit SHA-1, SHA-256 und SHA-384	[FIPS 180-4] (SHA) [RFC-2104] (HMAC)	160 Bit, 256 Bit und 384 Bit	[gemSpec_Krypt], Kap. 3.3.2

#	*Zweck*	*Kryptographischer Mechanismus*	*Implementierungsstandard*	*Schlüssellänge in Bit*	*Anwendungsstandard*
			[RFC-5246] (TLS v1.2)		
6	Vertraulichkeit	Symmetrische Verschlüsselung und Entschlüsselung für TLS 1.2 AES-128 und AES-256 in CBC	[FIPS 197] (AES) [RFC-3268] (AES-TLS mit DH) [RFC-4492] (AES-TLS mit ECDH)	128 Bit und 256 Bit	[gemSpec_Krypt], Kap. 3.3.2
7	Vertraulichkeit mit Nachrichten-authentizität (Authenticated Encryption)	AES-128 und AES-256 in GCM Mode für TLS 1.2	[FIPS 197] (AES) [RFC-3268] (AES-TLS) [SP 800-38D] (GCM) [RFC-5289] (AES-GCM-TLS) [RFC-5116] (AEAD)	128 Bit und 256 Bit	[gemSpec_Krypt], Kap. 3.3.2
8	Sichere Kanäle	TLS v1.2	[RFC-5246] (TLS v1.2)	-	[gemSpec_Krypt], Kap. 3.3.2

Tabelle 6: Beispiel für nach Schnittstellen gegliederte Kryptotabelle

6 Zusätzliche Anforderungen an die Evaluierung

38 Die zusätzlichen Anforderungen an die Evaluierung und Evaluierungsaufgaben sind den jeweiligen Abschnitten in dem Dokument [AIS B4] „Requirements for Evaluation according to the BSZ“ zugeordnet.

39 In Phase 1, Step 1 – Review the TOE, the ST and the cryptographic documentation muss die Prüfstelle sicherstellen, dass sie den Evaluierungsgegenstand, wie in Kapitel 3 gefordert, erhalten hat.

40 In Phase 1, Step 2 - Estimate the evaluation effort and duration muss die Prüfstelle überprüfen, dass die durch den Antragsteller gelieferten Evaluierungsgegenstände in der für die Evaluierung vorgesehenen Version und in der Debugging-Variante in den vorgesehenen Laborräumen der Prüfstelle aufgestellt ist und der Betrieb aller Evaluierungsgegenstände in der vorgesehenen Umgebung ordnungsgemäß funktioniert.
Hinweis: Hier ist grundsätzlich keine Vorabversion des Evaluierungsgegenstandes sondern die zu zertifizierende Version gemeint. Wenn die zu zertifizierende Version noch nicht vorliegt, kann dies zunächst mit einer vorab Version geschehen. Allerdings besteht, wenn die zu zertifizierende Version erst kurz vor oder kurz nach dem Auftaktgespräch geliefert wird, ein Risiko, dass sich die Evaluierung verzögert.

41 In Phase 1, Step 2 - Estimate the evaluation effort and duration muss die Prüfstelle bei der Aufwandsplanung berücksichtigen, dass bei einer Erstzertifizierung aufgrund der Komplexität eines Highspeed-Konnektors typischerweise 60 Personentage angesetzt werden. Falls der Evaluierungsgegenstand mehr Schnittstellen und Dienste als die für einen Highspeed-Konnektor verpflichtend vorgesehen enthält und dies erheblichen Mehraufwand bei der Evaluierung zur Folge hat, muss die Prüfstelle dies vor der Auftaktbesprechung an die Zertifizierungsstelle und den Antragsteller melden. Die Zertifizierungsstelle und Prüfstelle stimmen daraufhin ab, ob eine Evaluierung im Rahmen einer BSZ möglich ist.

42 In Phase 2, Step 1 - Preparation muss die Prüfstelle bei der Vorbereitung der Präsentation für die Auftaktbesprechung beachten, dass die Präsentation eine Darstellung und Beschreibung der Testumgebung und Testsaufbaus enthalten muss.

43 In Phase 3 the Evaluation muss die Prüfstelle, wenn sie bei Tests mittels der Debugging-Variante des Evaluierungsgegenstands Schwachstellen oder relevante Abweichungen feststellt, untersuchen und bewerten, ob die Befunde auch für Evaluierungsgegenstand gelten.

44 In Phase 3, Step 5 - Preparation of the evaluation report muss die Prüfstelle im Evaluierungsreport klarstellen, welche Test an der Debugging-Variante des Evaluierungsgegenstands durchgeführt wurden. Die Prüfstelle muss mit kurzer Begründung darstellen, inwieweit Testergebnisse auf den Evaluierungsgegenstand übertragbar sind.

7 Referenzdokumente

1 [FIPS-180-4] FIPS PUB 180-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard (SHS), NIST

2 [FIPS-186-4] FIPS PUB 186-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Digital Signature Standard (DSS), NIST

3 [FIPS-197] FIPS PUB 197, Federal Information Processing Standards Publication 197: ADVANCED ENCRYPTION STANDARD (AES), NIST

4 [FIPS-202] FIPS PUB 202, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, NIST

5 [gemSN_HSK] „Sicherheitsnachweis Highspeed-Konnektor“ (gemSicherheitsnachweis_HSK), gematik

6 [RFC-2104] RFC 2104, Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication"

7 [RFC-3268] RFC 3268, Chown, P., Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)

8 [RFC-4492] RFC 4492, Blake-Wilson, et al.: Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)

9 [RFC-5116] RFC 5116, D. McGrew: An Interface and Algorithms for Authenticated Encryption

10 [RFC-5246] RFC 5246, T. Dierks: The Transport Layer Security (TLS) Protocol, Version 1.2

11 [RFC-5289] RFC 5289, E. Rescorla, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)

12 [RFC-5639] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, M. Lochter, J. Merkle

13 [RFC-8017] RFC 8017, K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch: PKCS #1: RSA Cryptography Specifications Version 2.2

14 [SP800-38D] NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST

15 [TR-02102-2] BSI TR-02102-1 Technische Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Bundesamt für Sicherheit in der Informationstechnik