Inhaltsverzeichnis

1 Einführung

1.1 Stand

Das Dokument beruht auf den Steckbriefen

- gemProdT_Kon_Highspeed_PTV_1.4.1-0_V1.0.0 (14.06.2024) und
- gemAnbT_Kon_Highspeed_ATV_1.5.0_V1.0.0 (14.06.2024).

1.2 Überblick

1.2.1 Art der Nachweise

Für einen vollständigen Sicherheitsnachweis für das Produkt Highspeed-Konnektor (HSK), sind vom Hersteller insgesamt drei Verfahren zu durchlaufen:

- eine Beschleunigte Sicherheitszertifizierung (BSZ),
- eine Prüfung durch Common-Criteria-Prüfstelle (CC-Prüfstelle) und
- ein Produktgutachten.

Die BSZ ist eine Zertifizierung durch das BSI. Durch den Blackbox-Ansatz, der größten Teils für die BSZ gilt und den grundsätzlichen Fokus auf Penetrationstests, gibt es Aspekte die weniger gut in diesem Verfahren beleuchtet werden können. Daher wird es flankiert durch die Prüfung durch eine CC-Prüfstelle mit Konnektor-Erfahrung, welche Quellcode-Analysen und funktionale Tests im Whitebox-Ansatz durchführt. Themen die die Vertrauenswürdige Ausführungsumgebung (VAU) betreffen, werden per Produktgutachten geprüft, wie dies bspw. auch beim ePA-Aktensystem und dem E-Rezept-Fachdienst gemacht wird.

Durch diese Kombination von Prüfverfahren wird insgesamt ein sehr hohes Vertrauensniveau für den Sicherheitsnachweis erreicht.

Im Folgenden wird der fachliche Umfang der einzelnen Verfahren in Form von Themenblöcken beschrieben, und konkrete, zu prüfende Sicherheitsfunktionalitäten benannt, wobei jeweils die mit einer Prüfung abgedeckten Anforderungen referenziert werden. Dabei findet zum Teil in der Spalte „Details zur Anforderung an HSK" eine Fokussierung für das jeweilige Prüfverfahren statt. Dies ist insbesondere relevant für umfangreiche Anforderungen, die neben der Sicherheit auch funktionale Aspekte abdecken, die hier gerade nicht im Umfang der Prüfungen sein sollen. Insgesamt werden bei den jeweiligen Nachweisverfahren alle Anforderungen referenziert, die auch im Produkttypsteckbrief bei diesem Verfahren enthalten sind. In welchen Dokumenten die Anforderungen nachzulesen sind, ergibt sich wiederum aus dem Produkttypsteckbrief und wird aus Platzgründen hier nicht aufgeführt.

1.2.2 Aufrechterhaltung der Nachweise

Die **Beschleunigte Sicherheitszertifizierung** gilt, sofern keine Änderungen am Produkt vorgenommen werden, für zwei Jahre und muss in jedem Fall vor Ablauf dieses Zeitraums wiederholt werden. Bei Änderungen am Produkt wird durch die Prüfstelle

anhand des IAR bewertet, ob diese Änderungen über die (evtl. auch neuen) Außenschnittstellen des HSK erreich- und testbar sind, sich voraussichtlich dort auswirken und somit den Scope der BSZ betreffen. Ist dieses der Fall, muss eine Delta-Evaluierung durchgeführt werden. Beispiele für solche Änderungen können neu spezifizierte und umgesetzte Schnittstellen oder grundlegende Anpassung durch den Hersteller durch andere Architektur / Technologie / Bibliotheken oder auch größere HW-Änderung sein. Entscheidend ist jeweils die Prüfstelleneinschätzung.

Die **Prüfung durch die CC-Prüfstelle** und das **Produktgutachten** sind grundsätzlich alle drei Jahre zu wiederholen. In der Zwischenzeit werden jährlich die bis dahin vorgenommenen Änderungen in Form eines Delta-Gutachtens betrachtet (sofern Änderungen vorgenommen wurden). In jedem Fall sind Änderungen stets der gematik zu melden. Bei massiven Änderungen an sicherheitsrelevanten Eigenschaften (bspw. neuer Ansatz für die Umsetzung der vertrauenswürdigen Ausführungsumgebung, VAU) kann eine unmittelbare Sicherheitsprüfung noch vor der Umsetzung in der PU auch bei Themen, die CC-Prüfstelle oder Produktgutachten betreffen, notwendig werden.

1.3 Bedrohungsmodell

Das Bedrohungsmodell für den Highspeed-Konnektor ähnelt in vielen Punkten dem des Einboxkonnektors, unterscheidet sich jedoch an zwei Stellen stark. Dies ist zum einen der nicht vorhandene Angriffsvektor aus dem Internet, da der HSK direkt per SZZP ans TI-Netz angeschlossen ist, und zum anderen der für den HSK geforderte Betreiberausschluss, der mittels einer VAU durchgesetzt werden soll. Die Notwendigkeit der Robustheit der Schnittstellen und der korrekten und somit sicheren Umsetzung von Protokollen und Sicherheitsfunktionalität ist beim HSK identisch zum Einboxkonnektor.

Zu schützen sind die im HSK verarbeiteten Daten von Versicherten, konkret deren Vertraulichkeit und Integrität (Primärdaten). Dies umfasst jedoch automatisch auch Assets, mit denen Zugriff auf solche Daten erlangt werden kann (bspw. Schlüssel und Token; Sekundärdaten).

Folgende grobe Sicherheitsziele ergeben sich für die jeweiligen Prüfverfahren:

- BSZ:
  - Sämtliche Außenschnittstellen des HSK müssen robust sein gegenüber schadhafter Nutzung durch nicht authentisierte Nutzer.
  - Fachliche Schnittstellen an der Clientseite müssen – auch bei authentisierter Nutzung – robust sein gegen fehlerhafte und schadhafte Verwendung.
  - "Außenliegende" Protokolle für die Authentifizierung von Kommunikationspartnern und den Schutz von Daten (hier konkret TLS) müssen korrekt umgesetzt und robust sein gegenüber Angreifern.
- CC-Prüfstelle:
  - Die im Dokument geforderten Sicherheitsfunktionen müssen spezifikationskonform umgesetzt sein und geforderte Sicherheitsprüfungen dürfen nicht umgangen werden können.
  - Kommunikations-Protokolle auf Anwendungsebene Richtung Fachdienste (hier konkret VAU- und SGD-Protokoll) müssen spezifikationskonform umgesetzt sein.
- Produktgutachten: Der HSK muss sich vor Zugriffen des Betreibers auf die verarbeiteten Daten von Versicherten schützen.

1.4 Legende

(A_12345)	Anforderungs-IDs in Klammern bedeuten, dass die betroffene Anforderung implizit mit geprüft wird, ohne einen konkreten eigenen Prüfschritt zu erfordern.
A_12345(+)	Anforderungs-IDs in kursiver Formatierung gefolgt von (+) bedeuten, dass die betroffene Anforderung nicht im Steckbrief gelistet ist, jedoch entweder durch Verweise innerhalb einer anderen Anforderung normativ wird oder zumindest weitere relevante Informationen zur entsprechenden Sicherheitsfunktion enthält.

2 Beschleunigte Sicherheitszertifizierung (BSZ)

2.1 Beschreibung des Verfahrens

Die allgemeine Herangehensweise und die Prüfmethoden sind durch das BSI für die BSZ festgelegt. Es handelt sich grundsätzlich um einen Blackbox-Ansatz mit einem starken Fokus auf Penetrationstests. Jedoch findet insbesondere für den Bereich Kryptographie auch in der BSZ eine Prüfung anhand von Quellcode statt.

Bei untersuchten Sicherheitsprotokollen (hier konkret TLS) wird neben der Prüfung auf Robustheit auch die Prüfung der korrekten Implementierungen des Protokolls vorgenommen.

Festlegungen zum BSZ-Geltungsbereich HSK finden grundsätzlich in BSI-Dokumenten statt und sind dort weniger detailliert, als die folgenden Absätze. Jedoch ist geplant ein Begleitdokument bereitzustellen, auf das die BSZ-Dokumente verweisen und welches in etwa die Inhalte dieses Kapitels umfassen wird.

Das Vorgehen bei Pentests liegt bei einer BSZ im Ermessen der Prüfstelle bzw. des Prüfers. Nichtsdestotrotz sind hier bei „Robustheitsprüfungen" teilweise beispielhaft Prüfungen genannt um einen Eindruck vom angedachten Vorgehen zu gewinnen.

2.2 Zu prüfende Sicherheitsfunktionen

2.2.1 Robustheit der Client-Schnittstellen auf Anwendungsebene

Es ist zu prüfen, dass der TOE an seinen Schnittstellen zu Clients auf Anwendungsebene (also nach dem TLS-Verbindungsaufbau) resistent ist gegen manipulierte Aufrufe. Dies betrifft grundsätzlich alle vorhandenen Schnittstellen.

Für die Management-Schnittstelle reduziert sich der Umfang jedoch auf die Robustheit der Schnittstelle vor der Authentisierung also gegenüber unauthentisierten Nutzereingaben.

Die neben der Management-Schnittstelle im HSK vorhandenen fachlichen Schnittstellen bzw. die darüber angebotenen Operationen sind in der Spezifikation [gemSpec_Kon] jeweils in den Abschnitten „Operationen an der Außenschnittstelle" definiert (abzüglich einiger im HSK nicht umgesetzter Operationen des Netzkonnektors).

Es ist ebenso zu prüfen, dass darüber hinaus keine weiteren Außenschnittstellen – insbesondere keine weiteren Admin-Zugänge zur Server-Plattform – vorhanden sind (A_21988-01).

Die Prüfungen können bspw. Fuzzing, für SOAP-Schnittstellen bekannten Angriffe, Angriffe auf die relevanten Parser (bspw. XML) oder relevante Angriffe aus den OWASP Top 10 umfassen. Das konkrete Prüfvorgehen ist durch die BSZ definiert bzw. liegt wie o.g. im Ermessen der für die Durchführung einer BSZ akkreditierten Prüfstelle.

Thema	Details zur Anforderung an HSK	AFO-IDs

Keine zusätzlichen Schnittstellen	Prüfung, dass keine zusätzlichen Schnittstellen (insbesondere Admin-Zugänge zur Server-Plattform) existieren	A_21988-01
Robustheit Schnittstellen	Robustheit aller Client-Schnittstellen (siehe Fließtext in diesem Absatz) HSM zu berücksichtigen falls extern nutzbar	*keine AFO(+)* A_23474
Robustheit während Bootup	Keine Dienste erreichbar während Bootup	TIP1-A_4507

2.2.2 Nutzer-Authentifizierung an der Management-Schnittstelle

Es muss geprüft werden, dass der HSK die Authentifizierung des Administrators sicher umgesetzt hat, sodass diese nicht umgangen werden kann.

Thema	Details zur Anforderung an HSK	**AFO-IDs**
Sichere Authentifizierung vor Zugriff auf/Änderung von Konfigurationen	Sämtliche Konfigurationsänderungen dürfen nur durch berechtigte Nutzer nach Authentifizierung möglich sein. Entsprechend darf es nicht möglich sein die Authentisierung zu umgehen.	TIP1-A_4808-01 TIP1-A_5661 (VSDM-A_2637) (TIP1-A_4814-02) (TIP1-A_4818) (TIP1-A_4517-02) (A_21697-01) (A_21698) (A_21699-02) (A_21701) (A_21702) (A_21760-01)

2.2.3 Korrekte Implementierung und Robustheit des TLS-Protokolls

2.2.3.1 Robustheit

Es ist zu prüfen, dass der HSK – sowohl im Rahmen des TLS-Verbindungsaufbaus als auch bei der anschließenden TLS-Kommunikation – resistent ist gegen bspw. manipulierte Pakete, Pakete die unerwartet sind (wiederholte Einspielung oder falsche Reihenfolge; Fehlerhandling) und bekannte Angriffe gegen das TLS-Protokoll.

2.2.3.2 TLS-Version, Ciphersuiten usw.

Die Vorgaben zu TLS-Verbindungen, die der HSK durchsetzen muss, sind durch die Prüfstelle für eine Stichprobe von Verbindungen zu prüfen.

Thema	Details zur Anforderung an HSK	AFO-IDs
TLS-Versionen	(allgemein)	(A_17322)
	nicht SSL	GS-A_5035
	nicht TLS1.0	GS-A_4387
	nicht TLS 1.1	A_18464
	TLS1.2 muss unterstützt werden	GS-A_4385
	TLS1.3 kann unterstützt werden	A_18467
Vorgaben zu TLS-Ciphersuiten, ECC-Kurven, DH-Exponenten	Umsetzung der in den referenzierten Anforderungen definierten Vorgaben zu TLS	GS-A_5345-01 GS-A_4384-01 A_17124-01 A_17094-01 (A_17322) A_23226-01
Session-Resumption & Renegotiation	allgemeine Vorgaben	GS-A_5322[a)]
	Es darf nur „Secure Renegotiation" unterstützt werden.	GS-A_5525
Hash-Funktionen in TLS	Mindestens SHA-256 muss unterstützt werden, nichts darunter	A_21275-01

[a)] Hinweis: TLS-Session-Resumption wird verwendet bei VSDM-A_2225.

2.2.3.3 Durchsetzen von TLS an allen notwendigen Stellen

Es muss geprüft werden, dass mit den genannten Kommunikationspartnern vor der fachlichen Nutzung immer erst eine per TLS gesicherte Verbindung aufgebaut wird.

Hinweis: Im Falle der Kommunikation mit Clientsystemen ist die Verpflichtung zum Durchsetzen von TLS von der Konfiguration durch den Administrator abhängig.

Schnittstelle	Details zur Anforderung an HSK	AFO-IDs
Zum Kartenterminal		TIP1-A_4545-03

Zum TSL-Dienst	Für Download BNetzA-VL-Hash	TIP1-A_5662
	Für Download TSL-Hash	A_17661
Zu Clientsystemen	Varianten	TIP1-A_5009
	Unabhängig von der Konfiguration, müssen immer auch TLS-Verbindungen angenommen werden	TIP1-A_4515
Für Management-Schnittstellen	Web-GUI	TIP1-A_4806-01
	automatisierte Schnittstelle	TIP1-A_5661
Für CETP zu Clientsystemen	Übermittlung von Fehlermeldungen wobei die Rollen getauscht sind (HSK ist Client)	TIP1-A_4595
Zum Verzeichnisdienst		TIP1-A_5517-02 TIP1-A_5566
Zum KSR		TIP1-A_4834
Für VSDM	konkret zum Intermediär	VSDM-A_3003
Für ePA	zu den SGDs	A_18011
	zur ePA Dokumentenverwaltung	A_15532
	zur ePA Zugangsgateway des Versicherten	A_14930
	zur ePA Autorisierung	A_14223
	In allen Fällen: Anwendungsfall abbrechen bei TLS-Verbindungsaufbau-Fehlern	A_17948

2.2.3.4 Authentisierung & Authentifizierung / Zertifikatsprüfung

Es ist für die in 2.2.3.3- Durchsetzen von TLS an allen notwendigen Stellen aufgeführten Verbindungen zu prüfen, dass der HSK die Authentifizierung des Kommunikationspartners im TLS-Handshake (oder bei Primärsystemen auch per http basic Auth) umsetzt und – je nach Verbindung – die eigene Authentisierung durchführt. Insbesondere ist zu prüfen, dass die Verbindung nicht zustande kommt, wenn Prüfungen im Rahmen der Authentifizierung des Kommunikationspartners fehlschlagen.

Thema	Details zur Anforderung an HSK	AFO-IDs
Zertifikatsprüfung	Das vom Kommunikationspartner übergebene Zertifikat muss geprüft werden. Die Zertifikatsprüfung wird in 3.2.4.1-Zertifikatsprüfung behandelt.	siehe 3.2.4.1-Zertifikatsprüfung
	Prüfung der aufgerufenen FQDN gegen die im Zertifikat hinterlegte FQDN für zentrale Dienste & Fachdienste	GS-A_5077
	Prüfung des Sperrstatus des Zertifikats per OCSP für zentrale Dienste & Fachdienste	TIP1-A_7254
Zertifikatsprüfung: Prüfung auf Zertifikatstyp und Rolle	Kartenterminal	TIP1-A_4545-03
	TSL-Dienst	TIP1-A_5662 A_17661
	KSR	TIP1-A_4834
	Verzeichnisdienst	TIP1-A_5517-02 TIP1-A_5566
	Fachdienste	TIP1-A_4720-02
	ePA SGD	A_18012
	ePA Dokumentenverwaltung	A_15532
	ePA Authentisierung	A_14930
	ePA Autorisierung	A_14223
TLS zu Clientsystemen	Varianten Authentifizierung Clients (Zertifikat, Passwort, ohne)	TIP1-A_4518-02
	Authentifizierung Clients durchsetzen	TIP1-A_4516 TIP1-A_4524-03
Authentisierung des HSKs	Als Client ggü. Fachdiensten (aktuell nur Intermediär)	TIP1-A_4720-02
	Als Client ggü. Kartenterminal	TIP1-A_4545-03

	Als Server ggü. Clientsystemen (im Falle von CETP als Client)	A_21760-01 A_21702 A_21698
	Als Server an der Management-Schnittstelle	TIP1-A_4806-01

3 Prüfung durch Common-Criteria-Prüfstelle (CC-Prüfstelle)

3.1 Beschreibung des Verfahrens

Ziel dieses Prüfverfahrens ist es, mittels Quellcode-Analyse und funktionalen Tests die Umsetzung der Sicherheitsfunktionen zu prüfen, deren Umsetzung sich weniger gut durch den Pentest-Ansatz der BSZ überprüfen lässt. Es handelt es sich explizit nicht um ein Verfahren nach Common Criteria, zielt aber auf Prüfstellentätigkeiten ab, die am ehesten mit den CC-Aspekten ADV_IMP, ATE_IND (mit ATE_FUN) und AVA_VAN zu vergleichen sind. Weitere Pentests sind in diesem Verfahren allerdings ausgeschlossen, da diese Prüfmethode umfassend in der BSZ angewendet wird.

Eine Prüfung von Dokumenten (über den Quellcode hinaus) ist nicht vorgesehen, jedoch sind Dokumentationen des Herstellers zwingend erforderlich um der Prüfstelle die ausreichenden Kenntnisse zum Produkt zu vermitteln.

Der Prüfansatz ist anforderungsbasiert und eher mit dem Vorgehen bei einem Produktgutachten zu vergleichen. Entscheidend ist hier jedoch, dass Evaluatoren mit Konnektor-Erfahrung die Prüfungen durchführen müssen, da explizit die langjährigen Erfahrungen auch aus dem Zusammenspiel mit den BSI-Zertifizierern als Expertise für diese Prüfungen gewünscht ist. Neben der Anerkennung als CC-Evaluator ist entsprechend auch die Konnektor-Erfahrung durch Benennung von konkreten Projekttätigkeiten nachzuweisen.

Das Verfahren wurde grundsätzlich schon als Sicherheitsnachweis bei Minor-Releases-Verfahren von Einboxkonnektoren angewendet, weist jedoch auch Abweichungen vom dortigen Vorgehen auf. Es wird kein Security-Target geben, das vom Hersteller erstellt/fortgeschrieben werden muss. Vorgaben sind die Anforderungen aus dem Steckbrief und die darauf wirkenden, in diesem Dokument dargelegten Fokussierungen zu den Anforderungen. Eine Prüfung über diese Anforderungen bzw. deren Fokussierung hinaus ist nicht vorgesehen. Bei der Herangehensweise an die Prüfung der zum Großteil aus den Konnektor-Schutzprofilen sowie den bisherigen Security Targets der Hersteller bekannten Sicherheitsfunktionen soll die Prüfstelle aber gerade die Erfahrungen aus den bisherigen Konnektor-Evaluierungen mit einbringen.

Die Ergebnisse der Prüfungen werden nachvollziehbar in einem Prüfbericht aufbereitet, welcher an die gematik übermittelt wird (Vorgehen wie bei einem Minor-Release-Verfahren).

3.1.1 Nachnutzen bestehender Prüfungsergebnisse und Zertifizierungen

Es ist der Prüfstelle explizit gestattet auf Ergebnisse von bereits zuvor durch diese Prüfstelle durchgeführten Prüfungen zurückzugreifen, wenn nachweislich die gleiche Implementierung auch im zu prüfenden HSK verwendet wird.

Werden Fachmodule, die bereits im Einboxkonnektor geprüft und zertifiziert wurden, unverändert im HSK übernommen, kann die bestehende TR-Zertifizierung des Fachmoduls nachgenutzt werden. Sollten sich bei Basis-Diensten Änderungen ergeben, die auch deren Nutzung durch Fachmodule betrifft, ist dies bei der Prüfung des HSK zu berücksichtigen. Alle restlichen Anforderungen, die von der TR für das jeweilige Fachmodul abgedeckt sind (entsprechend Produkttypsteckbrief des Einboxkonnektors),

entfallen dann aber für die Prüfung beim HSK. Dazu muss jedoch die Nutzung der unveränderten Implementierung durch die Prüfstelle verifiziert werden.

3.1.2 Zuarbeiten des Herstellers

Folgende Zuarbeiten des Herstellers für die Prüfstelle sind zwingend notwendig in diesem Verfahren:

- Die Bereitstellung einer Architekturbeschreibung, die der Prüfstelle ein ausreichendes Verständnis zum HSK ermöglicht, wie es für einen Whitebox-Ansatz notwendig ist,
- die Bereitstellung von Quellcode mit Kommentierung hinsichtlich der Erfüllung der notwendigen Anforderungen (Mapping Anforderungen auf Quellcode),
- die Durchführung von Herstellertests zu den Anforderungen und die Bereitstellung der Testfälle, der Testberichte und ggf. der Testumgebungen/-tools und
- die Bereitstellung einer aktuellen CVE-Analyse.

3.1.3 Beteiligung der gematik

Das Prüfverfahren „Prüfung durch CC-Prüfstelle" erfolgt in der Hoheit der gematik, wobei es jedoch im Kern auf die Kompetenz der CC-Prüfstelle baut. Die Prüfstellen haben bereits mehrere erfolgreiche CC-Evaluierungen von Einboxkonnektoren durchgeführt, weshalb von einer gründlichen Prüfung ausgegangen werden kann.

Da die gematik jedoch in der Verantwortung steht und den Sicherheitsnachweis abnimmt, muss sie entsprechende Möglichkeiten zur Teilnahme am Verfahren haben. Dies ist zwar grundsätzlich durch die Abnahme des Prüfberichtes gegeben, was jedoch zu einem sehr späten Zeitpunkt im Verfahren stattfindet. Mängel die dann ggf. noch gefunden werden, können zu großen Verzögerungen führen. Daher sollen bereits zu Beginn – in Form eines „Kick-Offs" – und auch im laufenden Verfahren – durch die jederzeit mögliche Kommunikation zwischen Prüfstelle und gematik – nach Möglichkeit alle Unklarheiten ausgeräumt werden.

3.2 Zu prüfende Sicherheitsfunktionen

3.2.1 Korrekte Implementierung des VAU-Protokoll

Bei der Kommunikation mit dem Verarbeitungskontext einer ePA in der Dokumentenverwaltung eines ePA-Aktensystems wird ein Schutz auf Anwendungsebene durch das „VAU-Protokoll" durchgesetzt, wobei der Konnektor als Client agiert. Das Protokoll dient zur Gewährleistung der Authentizität der Kommunikationspartner und schützt vor dem unberechtigten Mitlesen oder unbemerkten Ändern von Informationen die über den Kanal gesendet werden.

Die Umsetzung der Vorgaben zum VAU-Protokoll durch den HSK in der Rolle Client ist zu prüfen. Dies beinhaltet die Prüfung, dass:

- der HSK die kryptographischen Vorgaben für das Protokoll sowohl selbst erfüllt als auch deren Erfüllung bei Server-Nachrichten verifiziert,
- der Protokollablauf auf Clientseite vom HSK korrekt umgesetzt ist (Reihenfolge der Nachrichten sowie Aufbau und Inhalt der Client-Nachrichten) und

- der Protokollablauf seitens des HSK abgebrochen wird, wenn eine der vom Client durchzuführenden Prüfungen von Server-Nachrichten fehlschlägt.

Hinweis: Explizit nicht geprüft werden muss die Robustheit der VAU-Protokoll-Implementierung vor einem aktiven Angreifer auf Server-Seite. Der Fokus liegt allein auf der spezifikationskonformen Umsetzung des Protokolls.

Thema	Details zur Anforderung an HSK	AFO-IDs
Durchsetzen des VAU-Protokolls	keine Schlüssel/Daten im Klartext	A_15199-01 A_15549
Zertifikatsprüfung	allgemein	3.2.4.1-Zertifikatsprüfung
	Prüfung Zertifikatstyp & Rolle	A_17225-01 A_15210
kryptographische Vorgaben	CipherConfiguration "AES-256-GCM-BrainpoolP256r1-SHA-256"	A_15549
	Neuer Sitzungsschlüssel nach 24 h	A_15549
	brainpoolP256r1 für Server PublicKey	A_16852-01
	ECDH-Keys mit BrainpoolP256r1	A_16883-01
	ECDH nach [NIST-800-56-A][a)]	A_16852-01
	HKDF nach [RFC-5869] mit SHA256[a)]	A_16943-01
	Verschlüsseln mit AES-GCM	A_16945-02 A_17070-02
	Signieren mit AUT-Identität	A_17081
Protokollablauf allgemein und Erstellen & Prüfen von Nachrichten	allgemein: Arten von Nachrichten	A_16884
	Ignorieren zusätzlicher JSON-Datenfelder	A_17074
	Signaturen immer über Base64-Daten	A_23282
	ECDH-Schlüsselpaar erzeugen	A_16883-01

	VAUClientHello – erzeugen & senden	A_15592-03 A_16883-01
	VAUServerHello – Hash prüfen	A_16903
	VAUServerHello – Signatur prüfen	A_16941-01
	VAUServerHello – Sign.-Zertifikat prüfen	A_16941-01
	VAUServerHello – Gültigkeit OCSP-Resp.	A_23273
	VAUServerHello – Certificate-Hash prüfen	A_16941-01
	Empfangenen Kurvenpunkt prüfen	A_16852-01
	ECDH durchführen[a)]	A_16852-01
	HKDF durchführen[a)]	A_16943-01
	VAUClientSigFin – erzeugen & senden	A_17070-02 A_17071
	VAUServerFin – "FinishedData" prüfen	A_17084
	Nutzdaten verschlüsseln & senden	A_16945-02
	Nutzdaten empfangen – KeyID prüfen	A_16957-01
	Nutzdaten empfangen – Entschlüsselung	A_16957-01
	Nutzdaten empfangen – Zähler prüfen	A_16957-01
	Zählerüberlauf verhindern	A_17069
	VAUServerError – Abbruch nur bei korrekter Signatur	A_16900

[a)] Hinweis: Die Umsetzung beider Punkte ist nicht einzeln prüfbar, da nur das Gesamtergebnis (direkt die KeyID und indirekt die AES-Schlüssel über deren Nutzung) sichtbar wird.

3.2.2 Korrekte Implementierung des SGD-Protokoll

Bei der Kommunikation mit den Schlüsselgenerierungsdiensten (SGD; ePA) wird ein Schutz auf Anwendungsebene durch das „SGD-Protokoll" durchgesetzt, wobei der Konnektor als Client agiert. Das Protokoll dient zur Gewährleistung der Authentizität der Kommunikationspartner und schützt vor dem unberechtigten Mitlesen oder unbemerkten Ändern von Informationen die über den Kanal gesendet werden.

Die Umsetzung der Vorgaben zum SGD-Protokoll durch den HSK in der Rolle Client ist zu prüfen. Dies beinhaltet die Prüfung, dass:

- der HSK die kryptographischen Vorgaben für das Protokoll sowohl selbst erfüllt als auch deren Erfüllung bei Server-Nachrichten verifiziert,
- der Protokollablauf auf durch den HSK als Client korrekt umgesetzt ist (Reihenfolge der Nachrichten sowie Aufbau und Inhalt der Client-Nachrichten) und
- der Protokollablauf seitens des HSK abgebrochen wird, wenn eine der vom HSL als Client durchzuführenden Prüfungen von Server-Nachrichten fehlschlägt.

Hinweis: Explizit nicht geprüft werden muss die Robustheit der SGD-Protokoll-Implementierung vor einem aktiven Angreifer auf Server-Seite. Der Fokus liegt allein auf der spezifikationskonformen Umsetzung des Protokolls.

Thema	Details zur Anforderung an HSK	AFO-IDs
Durchsetzen des SGD-Protokolls	keine Schlüssel/Daten im Klartext	A_17777
Zertifikatsprüfung	Prüfung ob in TSL und zeitlich gültig	A_17847
	Prüfung korrekte Rolle für SGD 1 bzw. 2	A_17848
kryptographische Vorgaben	ECDH nach [NIST-800-56-A]	A_17875
	HKDF nach [RFC-5869] mit SHA256a)	A_17875
	ECIES: Schlüssel auf BrainpoolP256r1	A_17874
	ECIES: Verfahren nach [SEC1-2009]	A_17875
	ECIES: AES-256-GCM mit 96 Bit IV	A_17872 A_17875
	ECIES-Keys: Signieren mit ECDSA	A_17874
	ECIES-Keys: Signieren mit AUT-Identität	A_17874

	ECIES-Keys: Nur einmal nutzen Oder Option Mehrfachnutzung: ECIES-Keys und zugehöriges AuthenticiationToken vom SGD vor Ablauf deren Gültigkeit (15 Minuten) löschen	A_18005 A_22497
	SHA-256 für Signaturerstellung/-prüfung	A_19971
Protokollablauf allgemein und Erstellen & Prüfen von Nachrichten	Durchsetzen des Protokollablaufs	A_17966
	Ignorieren zusätzlicher Key-Value-Paare	A_17892
	Bei Erhalt Nachricht prüfen, ob HTTP-Variable Namens "SGD-Userpseudonym" enthalten; wenn ja Variable inkl. Wert im nächsten Request an SGD aufführen	A_22494
	GetPublicKey-Request	A_17897 *A_17895-02(+)*
	GetPublicKey-Response auswerten	A_17899
	GetPublicKey-Response – Signatur prüfen	A_18024
	GetPublicKey-Response – SGD-HSM-Zertifikat prüfen	A_17847 A_17848 A_18024
	ECIES-Schlüsselpaar erzeugen	A_18032 A_17874
	GetAuthenticationToken-Request	A_18025-01 A_17900 A_17901 A_17902 A_17875
	GetAuthenticationToken-Response entschlüsseln und auswerten	A_18028 A_17903 A_17875

	KeyDerivation-Request	A_18029 A_17888 *A_17898(+)* A_17900 A_17901 A_17902 A_17924-01 *A_17922(+)* A_18003 A_18006
	KeyDerivation-Response entschlüsseln und auswerten	A_18031-01 A_17903 A_20977

3.2.3 Zufall & Schlüsselerzeugung

Die Konformität des Zufallszahlengenerators und der Schlüsselerzeugung zur TR-03116-1 ist zu prüfen. Zudem muss geprüft werden, dass die konforme Zufallszahlenquelle/Schlüsselgenerierung auch für die verschiedenen Anwendungsfälle korrekt genutzt wird.

Thema	Details zur Anforderung an HSK	AFO-IDs
Zufallszahlengenerator	Erfüllung BSI-TR-03116-1 Absatz 3.8	GS-A_4367
Schlüsselerzeugung	Erfüllung BSI-TR-03116-1 Absatz 3.9	GS-A_4368
Korrekte Nutzung	Der HSK muss die konforme Erzeugung von Zufall und Schlüsseln für folgende Anwendungsfälle korrekt nutzen:	
	TLS: DH / ECDH durchführen	GS-A_4384-01 GS-A_5345-01 A_17094-01
	Dokumentenverschlüsselung (Erzeugung Schlüssel und IV)	A_17220 A_17221-01 GS-A_4373 GS-A_4389 GS-A_5016 TIP1-A_4616-03
	ePA: Akten- und Kontextschlüssel erzeugen	A_15705 (A_14742) (A_15867)

	ePA: Dokumentenschlüssel erzeugen	A_14975-01 A_18001 (A_15867)
	ePA: Dokumentverschlüsselung IV erzeugen	A_18004
	ePA: Schlüsselverschlüsselung IV erzeugen	A_17872
	VAU-Protokoll: ECDH-Schlüssel erzeugen	A_16883-01 (A_15894) (A_15895)
	VAU-Protokoll: IV erzeugen	A_16945-02
	SGD-Protokoll: ECDH-Schlüssel erzeugen	A_18032 (A_18165)
	SGD-Protokoll: Challenge für Request GetAuthenticationToken erzeugen	A_18025-01
	SGD-Protokoll: Request-ID für Request KeyDerivation erzeugen	A_18029
	KT-Pairing: Shared Secret erzeugen	TIP1-A_4548-02
	KT-Verbindungsaufbau: Challenge erzeugen	TIP1-A_4545-03
	Clientsystem-TLS-Zertifikate erzeugen	TIP1-A_4517-02
	Konnektor-TLS-Zertifikat erzeugen	A_21699-02
	Jobnummer erzeugen	TIP1-A_4642

3.2.4 Zertifikatsdienst

3.2.4.1 Zertifikatsprüfung

Es muss geprüft werden, dass der HSK die im folgenden aufgeführten Prüfschritte durchführt und er das korrekte Prüfergebnis ausgibt, also insbesondere nur Zertifikate als gültig ausweist, bei denen alle notwendigen Prüfungen positiv durchlaufen wurden. Bei Zertifikatsprüfungen innerhalb von Anwendungsfällen erfolgt die Rückgabe eines positiven bzw. negativen Prüfergebnis implizit durch die weitere Ausführung bzw. den Abbruch des Anwendungsfalls.

Thema	Details zur Anforderung an HSK	AFO-IDs
Kryptographische Vorgaben	siehe in 3.2.4.2- Zertifikate und Schlüssel	
Zertifikatsprüfung X.509	Ablauf der Prüfung allgemein	TIP1-A_4696-03 (GS-A_4829)
	Prüfung beim Stecken HBA & SMC-B Fokus ist nur, dass auch hier eine korrekte Prüfung stattfindet	A_23311 A_23702 (A_23702)
X.509 nonQES	(Ablauf der Prüfung allgemein, TUC_PKI_018)	*(GS-A_4652-01(+))*
	Prüfung zeitliche Gültigkeit	*GS-A_4653-01(+)*
	Prüfung Vorhandensein CA in TSL	*GS-A_4654-01(+)*
	Prüfung Zertifikatssignatur mit CA	*GS-A_4655-01(+)*
	Prüfung Sperrstatus per OCSP unter Berücksichtigung der Graceperiod	*GS-A_4657-03(+)* GS-A_4943
	Ermittlung Rolle & Rückgabe an Aufrufer	*GS-A_4660-02(+)*
	Prüfung auf vom Aufrufer geforderten Zertifikatstyp	*GS-A_4652-01(+)* *GS-A_4749-01(+)*
X.509 QES	(Ablauf der Prüfung allgemein, TUC_PKI_030)	*(GS-A_4750-01(+))*
	Prüfung zeitliche Gültigkeit	*GS-A_4653-01(+)*
	Prüfung Vorhandensein CA in BNetzA-VL	*GS-A_4750-01(+)*
	Prüfung Gültigkeit CA bei Erstell. Zertifikat	*GS-A_4750-01(+)*
	Prüfung Zertifikatssignatur mit CA	*GS-A_4750-01(+)*
	Prüfung Sperrstatus per OCSP	*GS-A_4750-01(+)*
	Ermittlung Rolle & Rückgabe an Aufrufer	*GS-A_4750-01(+)*
Zertifikatsprüfung CVC	Ablauf der Prüfung allgemein	TIP1-A_5482-01 (GS-A_4829)

	Prüfung der mathematischen Korrektheit	*GS-A_5009(+)* *GS-A_5010(+)*
	Prüfung Gültigkeit CVC nach Schalenmodel	*GS-A_5011(+)* *GS-A_5012(+)*

3.2.4.2 Zertifikate und Schlüssel

Es ist zu prüfen, dass die Vorgaben zu Zertifikatssignaturen und den im Zertifikat bestätigten Schlüssel vom HSK umgesetzt bzw. bei der Prüfung von Zertifikaten durchgesetzt werden. Das heißt bei der Verwendung und Prüfung von Zertifikaten müssen solche, die Signaturen und Schlüssel enthalten, die auf anderen als den erlaubten kryptographischen Verfahren/Algorithmen und Schlüssellängen basieren, vom HSK abgelehnt werden.

Hinweis: CV-Zertifikate werden meist von den beteiligten Karten selbst geprüft. Lediglich das CV-Zertifikat der eGK wird vom Konnektor selbst geprüft.

Thema	Details zur Anforderung an HSK	AFO-IDs
Vorgaben für X.509 nonQES Zertifikate	RSA: Schlüssel: RSA-Schlüsselpaar mit 2048 Bit Signatur: sha256withRSAEncryption	GS-A_4357-01 GS-A_4359 GS-A_4361 GS-A_4362
	ECC: Schlüssel: ECC-Schlüsselpaar basierend auf brainpoolP256r1 oder P-256 Signatur: ecdsa-with-SHA256	GS-A_4357-01 GS-A_4359 GS-A_4361 GS-A_4362
Vorgaben für X.509 QES Zertifikate	RSA-Signaturerstellung: Schlüssel: RSA-Schlüsselpaar mit 2048 Bit Signatur: sha256withRSAEncryption oder id-RSASSA-PSS	GS-A_4358
	RSA-Signaturprüfung: Schlüssel: RSA-Schlüsselpaar mit 1976 bis 4096 Bit	GS-A_5071-01
	ECC: Schlüssel: ECC-Schlüsselpaar basierend auf brainpoolP256r1 Signatur: ecdsa-with-SHA256	GS-A_4358
Vorgaben für CV-Zertifikate	Schlüssel: ECC-Schlüsselpaar basierend auf brainpoolP256r1 Signatur: ecdsa-with-SHA256	GS-A_4365 GS-A_4366 GS-A_4379

Hashwert für Fingerprints	Erzeugen von Zertifikat-Fingerprints immer mit SHA-256	GS-A_4393

3.2.5 Signaturdienst

3.2.5.1 Signaturverfahren und kryptographische Vorgaben

Es ist zu prüfen, dass die Vorgaben zu Signaturverfahren und den erlaubten kryptographischen Verfahren/Algorithmen vom HSK durchgesetzt werden. Diese gelten für die Signaturerstellung und die Signaturprüfung. Die Erstellung und Prüfung von Signaturen, die auf anderen als den zu unterstützenden Verfahren beruhen, sind vom HSK abzulehnen.

Thema	Details zur Anforderung an HSK	AFO-IDs
Unterstützte Signaturverfahren und kryptographische Vorgaben Dokumentensignaturen (nonQES und QES)	XML-ECC-Signaturerstellung/-prüfung: ECDSA / brainpoolP256r1 / SHA-256 / „http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256" / XAdES	A_17206 A_17360
	XML-RSA-Signaturerstellung/-prüfung: RSASSA-PSS / SHA-256 / XAdES	GS-A_4371 GS-A_4372 *GS-A_5091(+)*
	PDF-ECC-Signaturerstellung/-prüfung: ECDSA / brainpoolP256r1 / SHA-256 / PAdES-3 & PDF/A-2	A_17208
	PDF-RSA-Signaturerstellung/-prüfung: RSASSA-PSS / SHA-256 / PAdES-3	GS-A_5081
	CMS-ECC-Signaturerstellung/-prüfung: ECDSA / brainpoolP256r1 / SHA-256 / CAdES	A_17207 A_17359
	CMS-RSA-Signaturerstellung/-prüfung: RSASSA-PSS / SHA-256 / CAdES	GS-A_5080
Zusätzlich zu unterstützende kryptographische Verfahren für QES-Dokumentensignaturen-Prüfung	Für RSA-QES-Signaturprüfung zusätzlich: · SHA-256, SHA-384, SHA-512 · RSASSA-PSS · RSASSA-PKCS1-v1_5	GS-A_5071-01
Kryptographische Vorgaben für externe Authentisierung	Signaturerstellung per ExternalAuthenticate:	A_17209

	RSASSA-PKCS1-v1_5, RSASSA-PSS, ECDSA	
Zulässige Signaturverfahren	Allgemein nonQES und QES: XAdES, PAdES, CAdES	TIP1-A_4623-02 TIP1-A_4627
	Unterstützung Signaturverfahren nur entsprechend TAB_KON_778 und dabei insbesondere QES XAdES Signaturerstellung und -prüfung nur mit Signaturrrichtlinie	TIP1-A_5447
	Signaturrichtlinie bei QES XAdES Signaturerstellung bzw. -prüfung einbetten bzw. berücksichtigen/durchsetzen	TIP1-A_5538
	Keine Unterstützung von nonQES XAdES Signaturerstellung und -prüfung	A_18756[a)]
Vorgaben für konkrete Anwendungsfälle durchsetzen	Prüfung ECC-XML-Signatur TSL ECDSA / brainpoolP256r1 / SHA-256 / „http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256“	A_17205
	Signaturprüfung Shared Secret bei KT-Pairing mit RSASSA-PSS bzw. ECDSA brainpoolP256r1	GS-A_5207 *A_17090-01(+)*
	Card-to-Card-Authentisierung ECC-Schlüssel basierend auf brainpoolP256r1	GS-A_4379
Vorgaben ExternalAuthenticate	· Nur für HBA und SMC-B AUT Zertifikat · Bitstrings mit maximal 512 Bit	TIP1-A_5437-02

[a)] Hinweis: Die Anforderung macht die Unterstützung von nonQES XadES Signaturen nur optional, fordert jedoch die Betrachtung bei der Sicherheitszertifizierung. Da hier kein CC-Verfahren durchlaufen wird, ist eine ausreichende Betrachtung nicht möglich, weshalb eine solche Funktionalität nicht umgesetzt werden darf.

3.2.5.2 Signaturprüfung

Es muss geprüft werden, dass der HSK die im folgenden aufgeführten Prüfschritte durchführt und er das korrekte Prüfergebnis ausgibt, also insbesondere nur Dokumentensignaturen als gültig ausweist, bei denen alle notwendigen Prüfungen positiv durchlaufen wurden.

Thema	Details zur Anforderung an HSK	AFO-IDs
Kryptographische Vorgaben und Vorgaben zu Signatur-Verfahren	siehe 3.2.5.1- Signaturverfahren und kryptographische Vorgaben	siehe 3.2.5.1- Signaturverfahren und kryptographische Vorgaben
Signaturprüfung nonQES	Informativ: Unterstütze Signatur-Varianten	(TIP1-A_5447)
	Ablauf der Prüfung allgemein	TIP1-A_4654-05
	Ermittlung Signaturzeitpunkt	TIP1-A_5545
	Dokumentvalidierung	TIP1-A_4527-04
	kryptographische Prüfung der Signatur	TIP1-A_4654-05
	Prüfung des Signaturzertifikats siehe 3.2.4.1 - Zertifikatsprüfung	TIP1-A_4654-05 siehe 3.2.4.1 - Zertifikatsprüfung
	Prüfung Signaturformat und -richtlinie	TIP1-A_4654-05
Signaturprüfung QES	Informativ: Unterstütze Signatur-Varianten	(TIP1-A_5447)
	Ablauf der Prüfung allgemein	TIP1-A_4672-05
	Ermittlung Signaturzeitpunkt	TIP1-A_5540-01
	Dokumentvalidierung (inkl. XML-Schema)	TIP1-A_4527-04
	kryptographische Prüfung der Signatur	TIP1-A_4672-05
	Prüfung des Signaturzertifikats siehe 3.2.4.1 - Zertifikatsprüfung	TIP1-A_4672-05 siehe 3.2.4.1 - Zertifikatsprüfung
	Prüfung Signaturformat und -richtlinie	TIP1-A_4672-05
Vorgaben für konkrete Anwendungsfälle durchsetzen	Prüfung ECC-XML-Signatur TSL ECDSA / brainpoolP256r1 / SHA-256 / „http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256“	A_17205

	Signaturprüfung Shared Secret bei KT-Pairing mit RSASSA-PSS bzw. ECDSA brainpoolP256r1	GS-A_5207 *A_17090-01(+)*

3.2.5.3 Signaturerzeugung

Es muss geprüft werden, dass die Vorgaben zur Signaturerstellung vom HSK umgesetzt bzw. durchgesetzt werden. Für die eigentliche Signaturerstellung (Nutzung des Schlüssels) ist dabei in den meisten Fällen jedoch eine Smartcard zuständig, in der auch der entsprechende private Schlüssel gespeichert ist. Der HSK muss hier aber die erlaubten Signaturverfahren und dafür unterstützen Karten durchsetzen, die Smartcard korrekt ansteuern, ggf. die Jobnummern-Verwaltung vornehmen, auf den Abbruch von Stapelsignaturen reagieren und die von der Karte zurückgegebene Signatur auf Korrektheit prüfen.

Thema	Details zur Anforderung an HSK	AFO-IDs
Kryptographische Vorgaben und Vorgaben zu Signatur-Verfahren	siehe 3.2.5.1- Signaturverfahren und kryptographische Vorgaben	siehe 3.2.5.1- Signaturverfahren und kryptographische Vorgaben
Korrekte Kartenkommandos	Setzen von algId und keyRef und korrekte Nutzung PSO Compute Digital Signature	TIP1-A_4581
Jobnummer	Anzeige Job-Nummer am KT-Display bei Eingabe PIN.QES für qualifizierte Einzel- und Stapelsignatur	TIP1-A_4639 TIP1-A_4640
	Jobnummer muss eindeutig sein (keine Wiederholung) über 1000 Aufrufe	TIP1-A_4644
	Nutzer-Information im Handbuch zum Abgleich der Jobnummer vom KT-Display mit Anzeige Primärsystem vor PIN-Eingabe	TIP1-A_4992-02
Signaturerstellung	Erstellung nonQES- und QES-Signatur nur wenn Signaturzertifikat gültig	TIP1-A_4647-03 TIP1-A_4649-02
	OCSP-Prüfung Signaturzertifikat	A_23536
	nonQES-Signaturerstellung nur mit SMC-B bzw. für Fachmodule auch mit eGK	TIP1-A_4653-03

	QES-Signaturerstellung nur mit HBA	TIP1-A_4655-03
	C2C-Authentisierung und Secure Messaging zum HBA für QES (außer „Einzelsignatur“)	TIP1-A_4651-02 TIP1-A_4670
	Rückgabe erstellter nonQES- und QES-Signatur nur nachdem diese erfolgreich mathematisch geprüft wurde	TIP1-A_4648 TIP1-A_4651-02 TIP1-A_4652-02
	Durchsetzen Vorgaben aus TAB_KON_192 bei Abbruch einer Stapelsignatur	TIP1-A_4651-02 TIP1-A_4671
Vorgaben ExternalAuthenticate	· Nur für HBA und SMC-B-AUT-Zertifikat · Bitstrings mit maximal 512 Bit	TIP1-A_5437-02

3.2.5.4 Komfortsignatur

Es ist zu prüfen, dass der HSK die für die Komfortsignatur spezifischen Anforderungen korrekt umsetzt. Komfortsignaturen (qualifizierte Signaturen ohne Eingabe der PIN.QES) dürfen nur ausgelöst werden, wenn die dafür notwendigen Prüfungen positiv durchlaufen wurden.

Thema	Details zur Anforderung an HSK	AFO-IDs
UserID durchsetzen	Auslösen Komfortsignatur nur bei Angabe der korrekten UserID, mit der auch der Komfort-signaturmodus unter Eingabe der PIN.QES aktiviert wurde	TIP1-A_4524-03
	Prüfung korrekte Länge der UserID	A_20073-01
	Prüfung Eindeutigkeit der UserID	A_20074
Timer und Zähler	Keine Komfortsignatur mehr möglich nach Ablauf des Timers	A_18686-01 A_19103-07
	Keine Komfortsignatur mehr möglich nach Erreichen der Maximalanzahl (Zähler)	A_19100-01 A_19102-04
	Default-Werte Timer (=6) und Zähler (=100)	TIP1-A_4680-03

Handbuchhinweis	Vorhandensein eines Handbuch-Hinweis zur Relevanz der Nutzer-Authentifizierung	A_19101
Globale Konfiguration (SAK_COMFORT_ SIGNATURE)	Keine Komfortsignatur möglich wenn Disabled	A_19104-04 A_19103-07
	Default-Wert Disabled	TIP1-A_4680-03
	Aktivieren nur möglich, wenn zwingendes TLS mit Client-Authentisierung konfiguriert ist	TIP1-A_4680-03
DeactivateComfortSignature	Nach Aufruf der Operation keine Komfortsignatur mehr möglich	A_19105
Secure Messaging durchsetzen	Zu signierende Daten werden ausschließlich geschützt an HBA gesendet	A_19258
Hinweis: Parallele Sessions	Mehrere Komfortsignatursessions pro HBA erlaubt (mindestens zwei Sessions gefordert)	(A_22344)
	Unabhängige Timer je Session	(A_22352)
	Unabhängige Zähler je Session	(A_22459)

3.2.6 Verschlüsselung und Entschlüsselung

Es muss geprüft werden, dass der HSK die Vorgaben zur Ver- und Entschlüsselung korrekt umsetzt. Dies beinhaltet insbesondere, dass der HSK nur die unterstützten Verfahren und Algorithmen zur Ver- und Entschlüsselung unterstützt und diese insbesondere bei der Verschlüsselung korrekt umgesetzt hat um den Schutz der Vertraulichkeit von den zu verschlüsselnden Informationen durchzusetzen.

Thema	Details zur Anforderung an HSK	AFO-IDs
Kryptographische Vorgaben und Vorgaben zu hybriden Ver- und Entschlüsselungsverfahren	CMS-ECC-Ver-/Entschlüsselung CMS nach RFC-5626 / AES-GCM 256 Bit / AES-Key mit ECIES nach gemSpec_COS und gemSpec_Krypt#5.7	A_17220 GS-A_4389

	CMS-RSA-Ver-/Entschlüsselung AES-GCM 256 Bit / RSAES-OAEP mit MGF 1 mit SHA-256	GS-A_4389 GS-A_4390 GS-A_5016
	XML-ECC-Ver-/Entschlüsselung XML nach „http://gematik.de/ecies/2019" bzw. gemSpec_Krypt#5.7 / AES-GCM 256 Bit / AES-Key mit ECIES nach gemSpec_COS und gemSpec_Krypt#5.7	A_17221-01 GS-A_4389
	XML-RSA-Ver-/Entschlüsselung XMLEnc-1.1 / AES-GCM 256 Bit / RSAES-OAEP	GS-A_4373 GS-A_4374 GS-A_4376-02
Details zu kryptographischen Vorgaben zur symmetrische Ver- und Entschlüsselung	AES nach FIPS-197 mit 256 Bit Schlüsseln im GCM nach NIST-SP-800-38D mit Tag-Länge von 128 Bit und zufälligem 96 Bit IV	GS-A_4389 GS-A_4373 A_17872
	Nur für hybride Entschlüsselung wird im symmetrischen Teil zusätzlich AES-GCM mit 128 und 192 Bit Schlüsseln unterstützt	TIP1-A_4617-02
Vorgaben für konkrete Anwendungsfälle durchsetzen	hybride Dokumentenverschlüsselung (EncryptDocument) · Verschlüsselungszertifikat vor Verschlüsselung auf Gültigkeit prüfen · Keine Verschlüsselung verschachtelter XML-Elemente · symmetrischen Schlüssel erzeugen · Dokument symmetrisch verschlüsseln · symmetrischen Schlüssel asymmetrisch verschlüsseln	TIP1-A_4616-03
	ePA: Verschlüsseln von Akten- und Kontextschlüssel	A_18007 A_17872 A_17868
	ePA: Verschlüsseln Dokumentenschlüssel	A_14976-02 A_17872
	ePA: Verschlüsseln von Dokumenten	A_14975-01 (A_13907) A_18008 A_17872

	ePA: allgemein: symmetrische Verschlüsselung mit AES/GCM mit 256 Bit Schlüsseln und 96 Bit IV	A_15705 A_18001 A_17872
	ePA: korrekte Chiffrat-Struktur	A_18004
	ePA: Prüfung der Schlüssellänge von Akten- und Kontextschlüssel; Abbruch bei falscher Länge	A_16193
Korrekte Kartenkommandos	Setzen von algId und keyRef und korrekte Nutzung PSO Decipher	TIP1-A_4582 (TIP1-A_4617-02)

3.2.7 Schutz sensibler/vertraulicher Daten

Es ist zu prüfen, dass der HSK schützenswerte Objekte vertraulich behandelt, also diese nur so lange vorhält, wie sie für die Verarbeitung notwendig sind (bzw. wie es per Spezifikation gefordert ist) und diese nur an berechtigte Kommunikationspartner mit ggf. notwendiger Verschlüsselung und/oder unter dem ggf. notwendigen Transportschutz weitergibt. Allgemein dürfen Versichertendaten sowie kryptographische Schlüssel, nicht persistiert werden, es sei denn es wird ausdrücklich von der Spezifikation gefordert.

Thema	Details zur Anforderung an HSK	AFO-IDs
Keine Protokollierung personen-bezogener (medizinischer) Daten	Übergreifendes Verbot	TIP1-A_4710-02
	FM AMTS	AMTS-A_2140
	FM NFDM	NFDM-A_2095 NFDM-A_2097
	FM ePA	A_14155
Keine Schlüssel protokollieren	FM AMTS	AMTS-A_2139
	FM NFDM	NFDM-A_2096
	FM ePA	A_14154
	FM VSDM	VSDM-A_2789
Kein persistieren von Schlüsseln oder personen-bezogener Daten	FM ePA: Daten	A_14173 A_14722
	FM ePA: Schlüssel	A_14174

	FM AMTS: Daten	AMTS-A_2189
	FM NFDM: Daten	NFDM-A_2105
Löschen vertraulicher Assets wenn nicht mehr benötigt	FM AMTS: Löschen temporärer Daten bei Ziehen der eGK	AMTS-A_2648
	FM AMTS: KVNR löschen nach Sitzung	AMTS-A_2169
	ePA: Dokumentenschlüssel löschen nach Ver-/Entschlüsselung des Dokuments	A_13903 A_14959
	ePA: Session löschen nach 20 Timeouts	A_14651
	ePA: Session löschen bei Ziehen der eGK	A_17949-01
	ePA: VAU-Session-Key nach 24 löschen	A_15549
	ePA: VAU KeyID und zugehörige Session-Keys bei Protokollabbruch löschen	A_16849
	ePA: SGD-Protokoll ECIES-Keys und SGD-Authentication-Token spätestens vor deren Ablauf (15 min) löschen	(A_18005) A_22497
	HBA/SMC-B Daten nach 24 h löschen	TIP1-A_4558
	eGK-Daten nach Ziehen löschen	TIP1-A_4558
	TLS-Session-Keys löschen wenn nicht mehr benötigt	*keine AFO(+)*
Schutz von vertraulichen Assets	Session-Keys der Protokolle TLS, VAU, SGD und C2C Trusted Channel sind hinsichtlich Vertraulichkeit und Integrität zu schützen und dürfen genau nur für die Kommunikation mit der Gegenstelle genutzt werden, mit der die Schlüssel ausgehandelt/abgeleitet wurden	*keine AFO(+)*
	Keine Ausgabe der UserID an Clients (insbesondere bei der Komfortsignatur)	A_19106-02 A_19109-02

	ePA: Akten-/Kontextschlüssel nicht an PS	A_14175
	ePA: Akten-/Kontextschlüssel dürfen nur verschlüsselt an Dokumentenverwaltung übertragen werden	*keine AFO(+)*
	ePA: Kontextschlüssel darf nur innerhalb des VAU-Kanals und nur direkt in den Verarbeitungskontext der VAU übertragen werden	*keine AFO(+)*

3.2.8 Aufrechterhaltung des Vertrauensraums (TSL/BNetzA-VL)

Es ist zu prüfen, dass der HSK die im folgenden aufgeführten Überwachungen seines bestehenden Vertrauensraums sowie die Aktualisierungen der TSL und der BNetzA-VL und dabei insbesondere die notwendigen Prüfungen durchführt. Der HSK darf keiner TSL und keiner BNetzA-VL vertrauen und diese auch nicht nutzen oder übernehmen, bei der eine der notwendigen Prüfungen fehlgeschlagen ist.

Thema	Details zur Anforderung an HSK	AFO-IDs
Vertrauensanker	Bei Verwendung von gSMC-Ks Nutzung des in EF.C.TSL.CA_1 personalisierten Vertrauensankers	TIP1-A_4682
	TSL-Signer-CA-Zertifikat sicher speichern	A_17548-02
Nutzung ECC-TSL	Verwendung der ECC-TSL	A_17688
TSL-Graceperiod durchsetzen	TSL ungültig nach Ablauf TSL-Graceperiod (max. 30 Tage nach Ablauf TSL)	GS-A_4898
Vertrauensraum Aktualisierung	Tägliche Prüfung auf Aktualisierung der TSL	A_22338 (GS-A_4899)
	Ablauf Aktualisierung der TSL allgemein	TIP1-A_4693-03 GS-A_4642
	Download neue TSL (falls nicht übergeben)	*GS-A_4647(+)*
	Prüfung TSL im System auf Aktualität gegen neue TSL (oder Vergleich Hash	GS-A_4648

	der TSL im System gegen runtergeladenen Hash)	
	Validierung TSL (XML)	*GS-A_4649(+)*
	Prüfung TSL-Signer-Zertifikat gegen vorhandenes TSL-Signer-CA-Zertifikat	GS-A_4650
	Prüfung Sperrstatus TSL-Signer-Zertifikat	GS-A_4642
	Prüfung Signatur TSL · Signatur basierend auf ECC · ggf. auch Signatur basierend auf RSA	GS-A_4651 A_17205 *GS-A_5340(+)*
	Wenn in neuer TSL vorhanden, neues TSL-Signer-CA-Zertifikat prüfen und importieren	GS-A_4643 *GS-A_4653-01(+)*
	Abschluss: Neuen Vertrauensraum bilden	GS-A_4642
BNetzA-VL Aktualisierung	· Wohlgeformtheit prüfen und validieren gegen XML-Schema ETSI_TS_119_612#Annex C.2 · Zeitliche Gültigkeit prüfen · BNetzA-VL-Signer-Zertifikat auf Vorhandensein in TSL prüfen · XadES-Signatur BNetzA-VL gegen Signer-Zertifikat aus TSL prüfen	TIP1-A_6729 GS-A_5484

3.2.9 Informationsmodell

Es ist zu prüfen, dass der HSK das konfigurierte Informationsmodell durchsetzt. Der HSK muss den Zugriff auf die im Aufrufkontext vom Client angegebenen Ressourcen unterbinden, wenn dieser Zugriff nicht nach dem Informationsmodell gestattet ist.

Thema	Details zur Anforderung an HSK	AFO-IDs
Prüfung Zugriffsberechtigung	SMC-B darf nur vom zugeordneten Mandanten genutzt werden	TIP1-A_4524-03 A_13941
	Lokale und Remote-KTs (und dort gesteckte Karten) dürfen nur vom zugeordneten Mandanten und Arbeitsplätzen genutzt werden	TIP1-A_4524-03 TIP1-A_4565 A_13941

	Karten-Zugriff nur mit korrektem CardHandle	TIP1-A_4565
	Durchsetzen exklusiver Zugriff auf Karte, insbesondere für den HBA bei QES sowie für die eGK bei ePA und VSDM	TIP1-A_4571 TIP1-A_4566 A_20157
	Ein bestimmtes Client-Auth-Merkmal darf auch nur von dem Clientsystem (Aufrufkontext) akzeptiert werden, dem das Merkmal zugeordnet ist (Informationsmodell)	TIP1-A_4524-03 Ablauf Auth. siehe 2.2.3.3-Durchsetzen von TLS an allen notwendigen Stellen
	Durchsetzen der UserID bei Komfortsignatur	siehe 3.2.5.4-Komfortsignatur

3.2.10 Fachmodul ePA

Es muss geprüft werden, dass das Fachmodul ePA im HSK die folgenden Vorgaben umsetzt.

Thema	Details zur Anforderung an HSK	AFO-IDs
Trennung Akten-Sessions	Strikte Trennung von Aktensessions nach Nutzern (Telematik-ID/KVNR) die auf eine Akte zugreifen und Akten (Record Identifier) auf die zugegriffen wird	A_13677
PIN vor Berechtigungsvergabe	Immer Abfrage der PIN.CH des Versicherten bei RequestFacilityAuthorization	A_14769
Beidseitiges C2C	Wenn C2C notwendig, dann immer beidseitig	A_15215
Vorgaben zum SAML-Token	Erfüllung Vorgaben für SAML-Token	A_14927
	Erfüllung Vorgaben für Claims in SAML-Token	A_15638
Vorgaben Policy-Dokument	Erfüllung Vorgaben für Policy-Dokument ePA1	A_15693

	Erfüllung Vorgaben für Policy-Dokument ePA2	A_15693-05
Nutzung Konnektor-Basis-Dienste durch Fachmodul	Protokollierungsdienst	A_14710
	Namensdienst	A_15135
	Zugriffsberechtigungsdienst	A_15136
	Kartendienst	A_15194
	TLS-Dienst	A_15535
	Zeitdienst	A_15677
	Zertifikatsdienste	A_15891
	Signaturdienste	A_15892
	Verschlüsselungsdienst	A_14748
Nur erlaubte Kommunikation	Einhalten des definierten Außenverhaltens von PHRService und PHRManagementService, insbesondere keine anderweitigen Nachrichten an Komponenten außerhalb des Fachmoduls	A_17879
Korrekte SGD-Ableitungsregel	Bestimmung korrekter Ableitungsregel entsprechend Rolle des Berechtigten	A_17988

3.2.11 Fachmodule AMTS & NFDM

Es muss geprüft werden, dass die Fachmodule NFDM und AMTS im HSK neben den hier genannten Anforderungen auch die folgenden Vorgaben umsetzen.

Thema	Details zur Anforderung an HSK	AFO-IDs
FM NFDM – Berechtigungsregeln	Regeln für ReadNFD durchsetzen	NFDM-A_2112
	Regeln für WriteNFD durchsetzen	NFDM-A_2115
	Regeln für EraseNFD durchsetzen	NFDM-A_2118
	Regeln für ReadDPE durchsetzen	NFDM-A_2122
	Regeln für WriteDPE durchsetzen	NFDM-A_2125

	Regeln für EraseDPE durchsetzen	NFDM-A_2128
FM AMTS – nicht MRPIN.home	MRPIN.home darf nicht genutzt werden	AMTS-A_2167
FM AMTS – Korrekte PIN-Objekt	Nutzung eGK PIN-Objekt entsprechend Eingangsparameter UsingPIN (Read&Write)	AMTS-A_2192 AMTS-A_2202

3.2.12 Management-Schnittstelle & Konfigurationsdaten

Es ist zu prüfen, dass im HSK die Vorgaben für dessen Management-Schnittstelle umgesetzt sind und der HSK insbesondere die Vorgaben zur Nutzer-Verwaltung und zur Trennung von Nutzer-Rollen bzgl. des Management/Konfiguration des HSK erfüllt.

Thema	Details zur Anforderung an HSK	AFO-IDs
Nutzerverwaltung	Trennung Administrator und Super-Administrator, dass nur letzterer weitere Nutzer einrichten und Nutzer löschen darf (es muss entsprechend jeder Zeit einen Super-Administrator geben)	TIP1-A_4810-02
	Durchsetzen Berechtigungen und Trennung Admin-Rollen Basissystem	A_23359-03
	Trennung Rolle für Kopplung mit HSM: Kein Zugriff der „normalen" Administratorrollen entsprechend TIP1-A_4810 auf Funktion zur Kopplung des HSK an den SZZP und ein HSM; Schutz der Kopplungs-Funktion durch zusätzliche unabhängige Admin-Rolle	A_21987-02
	Trennung Admin-Rolle für Erstellen / Löschen von HSK-Instanzen von Admin-Rolle einer bestehenden HSK-Instanz	TIP1-A_4820-02
	Berechtigungen bzgl. HSM-B	A_23628 A_23629 A_23631 A_23632 A_23757

Sicheres Löschen HSK-Instanz	Beim Löschen einer HSK-Instanz müssen alle Daten der Instanz gelöscht werden.	TIP1-A_4820-02
Schutz Integrität Sicherheitsprotokoll	Kein Admin einer HSK-Instanz darf das Sicherheitsprotokoll verändern oder löschen können	TIP1-A_4716 TIP1-A_4709
Selbstauskunft	Administrator muss Versions-informationen einsehen können	TIP1-A_4812
Sicheres Persistieren von Konfigurationsdaten	Konfigurationsdaten sicher speichern (Verfügbarkeit, Integrität, Vertraulichkeit)	TIP1-A_4813
Sicherer Export / Import von Konfigurationsdaten	Signatur des Export-Datensatzes sowie Signaturprüfung und Bestätigung des Administrators bei Import	TIP1-A_4815
	Verschlüsselung des Export-Datensatzes	TIP1-A_4816
	Import von KT-Daten erst nach weiterer Bestätigung des Administrators	TIP1-A_5011
	Backup Instanz-Konfigurationen über Basissystem nur geschützt vor unberechtigtem Zugriff	A_23395
Remote-Administration (falls vorhanden)	Authentifizierung	TIP1-A_7277 TIP1-A_7278 TIP1-A_7279
	Einschränkung Rechte	TIP1-A_7280
Sicherung & Wiederherstellung	Back & Restore für Basissystem	A_23397
Nicht von Instanz-Admin änderbare Konfigurationen wenn global am Basissystem aktiviert	Zwingende zertifikatbasierte Client-Authentisierung bei TI-Gateway	A_23303
	Automatische Updates	A_23432

3.2.13 HSM-B

Das Feature HSM-B (Personalisierung und Nutzung von SM-B-Identitäten im HSM des HSK) ist zunächst optional. Wenn Hersteller es umsetzen ist die Umsetzung der folgenden Anforderungen zu prüfen.

Thema	Details zur Anforderung an HSK	AFO-IDs
Optionalität	Zur Info: Aktuell Feature optional	A_23654
Schlüsselerzeugung für Institutionsidentitäten	Schlüsselerzeugung im HSM; Qualität der Schlüssel nach gemSpec_Krypt; nicht im Klartext exportierbar	A_23628
Import von Zertifikaten zu Institutionsidentitäten	Entschlüsselung inkl. Integritätsprüfung (AES-GCM); sichere Speicherung Aktivierungscode (nur für HSK zugreifbar)	A_23629
Zuordnung von Institutionsidentitäten zu vInstanzen	Genau nur zugeordnete vInstanz darf HSM-B verwenden	A_23631
Mandantenzuordnung mit Aktivierungscode	Zuordnung im Infomodell stets nur nach erfolgreicher Eingabe und Abgleich Aktivierungscode (auch bei erneuter Zuordnung nach etwaigem Entfernen); Maßnahmen gegen Brute-Force bei Eingabe Aktivierungscode	A_23632
Export von CSR	ECDSA-Signatur mit Identität HSK.SIG im HSM analog zu gemSpec_Kon#A_21185*	A_23655
Management von C.HSK.SIG und C.HSK.ENC	Erzeugung ECC-Schlüssel im HSM; Erzeugung Schlüssel nur durch Hersteller; Qualität der ECC-Schlüssel nach gemSpec_Krypt; Import Zertifikate auch durch Schlüsselverwalter / Zugangsmodul	A_23757
Kein Zugriff des Betreibers auf das HSM	Wenn HSM-B, dann keine Nutzung des HSMs durch weitere Komponenten (A_23475 entfällt somit), da Identitäten auf HSM deutlich schützenswerter werden und Trennung über Credentials zu schwach	A_24016

3.2.14 Weitere Prüfungen

Es ist zu prüfen, dass die folgenden Punkte im HSK umgesetzt sind.

Thema	Details zur Anforderung an HSK	AFO-IDs
Firmware-Aktualisierung	Vor Anwenden eines Update-Pakets muss der HSK dessen Authentizität und Integrität prüfen und darf das Paket nur bei positivem Prüfergebnis anwenden.	TIP1-A_4832-03
Protokollierung	Sicherheitsrelevante Ereignisse müssen im Sicherheitsprotokoll protokolliert werden.	TIP1-A_4715 TIP1-A_5654
KT-Verbindungsaufbau	Nach TLS-Verbindungsaufbau zum KT muss vor fachlicher Nutzung das vom KT präsentierte Shared Secret geprüft werden, ob es zum fürs KT hinterlegte ShS passt	TIP1-A_4545-03
Kartenterminal Pairing	Das Pairing mit einem KT muss im HSK korrekt umgesetzt sein. Dabei sind folgende Punkte durchzuführen wobei die genannten Prüfungen durchzuführen sind und bei negativen Ergebnissen der Vorgang abgebrochen werden muss: · TLS-Verbindung aufbauen · dabei Prüfung Zertifikat C.SMKT.AUT · Anzeige Fingerprint für Admin und warten auf Bestätigung des Admin · Shared Secret generieren und mit Display Message an KT senden · Signatur des KT über das Shared Secret prüfen gegen C.SMKT.AUT	TIP1-A_4548-02
KT-Kommandos wenn KT nicht verbunden	Es dürfen nur erlaubte Kommandos zu KTs gesendet werden, die nicht verbunden sind (CT.CONNECTED=Nein)	TIP1-A_6478
Kein Zugriff auf DF.KT (gSMC-KT)	Keine Zugriffe auf DF.KT der gSMC-KT	TIP1-A_4559

Verbot direkter Zugriff auf eGK über Außenschnittstellen	Keine Entschlüsselung mit eGK bei DecryptDocument	A_17746
	Keine Authentisierung mit eGK bei ExternalAuthenticate	TIP1-A_5437-02
	Keine Nutzung von eGK CH.AUT für Signaturen an Außenschnittstelle	A_17768
	Keine PIN-Eingabe eGK per VerifyPin	TIP1-A_4567 *TIP1-A_4587(+)*
Beidseitige C2C Authentisierung Prüfung CVC der eGK	Bei beidseitiger C2C-Authentisierung mit eGK muss HSK Prüfung CVC der eGK gegen bekannte CV-Root-CA-Zertifikate (mittels CVC-CA der eGK) und Prüfung eGK auf Besitzt des privaten Schlüssels zum CVC durchführen	TIP1-A_4572
eGK Sperrung prüfen	Für die Prüfung der eGK muss das Zertifikat C.CH.AUT geprüft werden (siehe 3.2.4.1- Zertifikatsprüfung)	TIP1-A_4579
Verwaltung Kartensitzungen	Zugriff auf durch PIN/C2C geschützte Objekte nur innerhalb der Kartensitzung, in der die Freischaltung durchgeführt wurde	TIP1-A_4560
	Erhöhter Sicherheitszustand einer Karte muss zurückgesetzt werden, wenn dies von einem Fachmodule angefordert wird	TIP1-A_4584
Remote-PIN Verfahren	Kein Remote-PIN Eingabe für eGK	TIP1-A_5012
	Korrekte Ansteuerung von Karten/KTs für C2C-Authentisierung mit Aufbau Trusted Channel zwischen gSMC-KT (PIN-Sender) und HBA/SMC-B (PIN-Empfänger)	TIP1-A_5012
Durchsetzen kritischer Fehlerzustände	Fehlerzuständen müssen erfasst und die jeweils definierten Anwendungsfälle bei kritischen Fehlerzuständen unterbunden werden	TIP1-A_4509 TIP1-A_4510-05
Verhalten bei Zeitabweichung	Keine fachliche Nutzung des HSK bei Abweichung von über 1h zwischen Systemzeit zu per ntp erhaltener Zeit	TIP1-A_4788

Manuell importierte CA-Zertifikate	Zertifikate (bzw. Schlüssel darin), die nur gegen manuell importierte CAs prüfbar sind, dürfen genau nur für hybride Verschlüsslung genutzt werden	TIP1-A_5433
Prüfung/Verarbeitung Dokumente	Ablehnen nicht zulässiger Dateien	A_19052-01 A_22673
	Referenzen in Dokumenten nicht auflösen	TIP1-A_5541-01
	schemaLocation Attribute nicht auswerten	A_22923
Nutzung gSMC-K oder HSM	Private Schlüssel zu Identitäten ID.AK.AUT, ID.SAK.AUT und C.SAK.AUTD_CVC des HSK müssen auf einer gSMC-K oder einem HSM gespeichert sein.	TIP1-A_4503-03
Sichere Trennung Instanzen	Es muss eine sichere Technologie zur Trennung virtueller Konnektor-Instanzen auf einem HSK verwendet werden. Die eingesetzte Lösung muss über einen längeren Zeitraum vom Hersteller der Lösung mit Updates versorgt werden. Hinweis: Eine detaillierte Prüfung der Virtualisierungslösung ist nicht notwendig, sofern diese aus Sicht des Prüfers ausgereift ist und dem Stand der Technik entspricht.	A_22041
Kommunikationsregeln für TI-Netze	Kommunikation zu zentralen Diensten und gesicherten Fachdiensten nur vom Konnektor aus.	TIP1-A_4730-02 TIP1-A_4731-02
	Keine Kommunikation zu Netz „Dezentral“.	TIP1-A_4732-02
Kopplung an TI-Gateway Zugangsmodul	Kopplung / sicherer Kanal für Zugangsmodul (Admin-Rolle Basissystem)	A_23360

3.2.15 CVE-Analyse

Es ist zu prüfen, dass die vom Hersteller für den HSK vorgelegte CVE-Analyse vollständig ist, die Bewertung von relevanten CVEs stattgefunden hat und nachvollziehbar ist sowie eine Umsetzung ggf. notwendiger Patches im HSK vorgenommen wurde.

Thema	Details zur Anforderung an HSK	AFO-IDs
CVE-Analyse	Der Hersteller muss die in seiner HSK-Implementierung genutzte Software, Firmware, Treiber und Bibliotheken hinsichtlich bekannter Schwachstellen (CVEs) überwachen. Wenn Schwachstellen bekannt sind, müssen diese Bewertet und je nach Bewertung gepatcht werden.	*keine AFO(+)*

4 Produktgutachten

4.1 Beschreibung des Verfahrens

Die Anforderungen an ein Produktgutachten sowie an Sicherheits- und Produktgutachter sind in gemRL_PruefSichEig_DS (siehe gematik-Fachportal) beschrieben.

4.2 Zu prüfende Sicherheitsfunktionen

4.2.1 Vertrauenswürdige Ausführungsumgebung (VAU)

Die Umsetzung folgender Anforderungen ist zu prüfen.

Thema	Details zur Anforderung an HSK	AFO-IDs
Vertrauenswürdige Ausführungsumgebung (VAU)	VAU muss alle physikalischen und Software-Komponenten umfassen, die dem Schutz der im Klartext verarbeiteten Versichertendaten dienen	A_17346-02
	Keine persistente Speicherung von Versichertendaten	A_17347-02
	Akten- und Kontextschlüssel nur an ePA-Aktensystem und nur in sicherem Kanal	A_17348-02
	Trennung Datenverarbeitung in VAU von allen anderen Datenverarbeitungen des Anbieters (Betreiberausschluss)	A_17350-02
	Schutz Integrität Software vor Manipulation durch Anbieter (Betreiberausschluss)	A_17351-02
	Schutz Integrität Hardware vor Manipulation durch Anbieter (Betreiberausschluss)	A_17352-02

	Schutz vor Manipulation der Software und Hardware muss dauerhaft wirksam sein	A_17353-02
	Kein physischer Zugriff auf Komponenten in denen Versichertendaten verarbeitet werden und/oder Nutzung CPU-Level-Verschlüsselung (bspw. Intel TME oder AMD SME), die auch bei physischem Zugang nicht deaktiviert werden kann	A_17354-02
	Physischer Zugriff nur nach Löschen verarbeiteter Klartext-Versichertendaten (bzw. Nutzung CPU-Level-Verschlüsselung, die auch bei physischem Zugang nicht deaktiviert werden kann)	A_17355-02
	Löschen aller Daten bei Beenden eines Verarbeitungsvorgangs (nicht nur ePA)	A_17356-03
	Zugriff auf VAU nur durch Hersteller	A_21987-02
	Kein Zugriff auf HSK und HSK-Identitäten im HSM über ggf. extern nutzbares HSK-HSM	A_23474
	Protokollierung jedes phys. Zugriffs (berechtigte und unberechtigte)	A_23495-01
	Dokumentenprüfung: Wenn berechtigte Zugriff durch Betreiber möglich sind (vgl. A_17354-02), dann dazu Sicherheitskonzept, Doku für Betreiber inkl. Verweis auf A_24295, Eingrenzung Wartungsarbeiten	A_24294

4.2.2 HSM und Kopplung HSK mit HSM

Die Umsetzung folgender Anforderungen ist zu prüfen.

Thema	Details zur Anforderung an HSK	AFO-IDs
Qualität des HSM	Nur HSMs mit Zertifizierung nach FIPS 140-2 Level 3 oder Common Criteria EAL 4	A_17598-01

Kopplung HSM	Kein Zugriff des Betreibers auf Schlüssel im HSM (kryptographische Koppelung und nur Vertraulichkeits- und Integritätsgeschützte, beidseitig authentisierte Verbindung)	A_21886
Bei HSM-B kein Zugriff des Betreibers auf das HSM	Wenn HSM-B, dann keine Nutzung des HSMs durch weitere Komponenten (A_23475 entfällt somit), da Identitäten auf HSM deutlich schützenswerter werden und Trennung über Credentials zu schwach	A_24016

5 Sicherheitsgutachten Hersteller

5.1 Beschreibung des Verfahrens

Die Anforderungen an ein Sicherheitsgutachten sowie an Sicherheitsgutachter sind in gemRL_PruefSichEig_DS (siehe gematik-Fachportal) beschrieben.

5.2 Zu prüfende Sicherheitsprozesse

5.2.1 Personalisierung HSK/HSM

Setzt der Hersteller HSMs statt gSMC-Ks ein, muss er dies in seiner Entwicklungsumgebung personalisieren. Die Umsetzung folgender Anforderungen zur Personalisierung des HSMs ist in diesem Fall zu prüfen.

Thema	Details zur Anforderung an HSK	AFO-IDs
Einbringen Vertrauensraum	Validierung TSL-Signer-CA vor Einbringen	GS-A_4640
	Einbringen TSL-Signer-CA	GS-A_4641 A_22336
	Einbringen ECC-TSL	GS-A_4748 A_17688 A_22336
Personalisierung HSM mit Konnektor-Identitäten	Personalisierung mit sicheren Personalisierungsprozessen in sicherer Produktionsumgebung	A_21885 A_23906 A_23907
Rollentrennung	Trennung Personalisierung HSM und Betrieb HSK	A_23470
Identitäten für HSM-B Personalisierung (C.HSK.SIG/ENC)	Selbe Pseudo-ICCSN für alle Identitäten eines HSK	A_23906
	Sicherer Prozess bei „Nach"-Personalisierung im Feld, Erzeugung Schlüssel im HSM und nur durch Hersteller	A_23906
	Schlüsselerzeugung im HSM 4-Augenprinzip für	A_23907

	Schlüsselerzeugung und Zertifikatsbeantragung	
Personalisierungsanforderungen	Weitere Anforderungen zur Personalisierung	siehe Steckbrief

5.2.2 Sichere Softwareentwicklungsprozesse

Der Hersteller des HSK muss diesen in einer sicheren Entwicklungsumgebung mittels sicherer Software-Entwicklungsprozesse implementieren. Dies kann durch eine positiv abgeschlossene Evaluierung der Entwicklungsumgebung im Rahmen des CC-Verfahrens für einen Einboxkonnektor (Aspekt ALC) nachgewiesen werden, wobei von der Prüfstelle die Nutzung der gleichen Entwicklungsumgebung zu bestätigen ist.

Wird eine andere Entwicklungsumgebung genutzt ist ein Sicherheitsgutachten über die sicheren Softwareentwicklungsprozesse des Herstellers einzureichen. Auch hier können bestehende Gutachten nachgenutzt werden, sofern – durch den Gutachter bestätigt – die gleiche Entwicklungsumgebung genutzt wird.

Thema	Details zur Anforderung an HSK	AFO-IDs
Sichere Softwareentwicklungsprozesse	Hersteller HSK muss CC-evaluierten oder sicherheitsbegutachtete Software-Entwicklungsumgebung/-prozesse nutzen	A_22046
Anforderungen zu Software-Entwicklungs-Prozessen	Anforderungen zur Software-Entwicklung aus gemSpec_DS_Hersteller	siehe Steckbrief

6 Sicherheitsgutachten Anbieter

Es wird hier ausschließlich der Anbieter HSK betrachtet. Für den Anbieter TI-Gateway, welcher auch einen HSK betreibt, ist aber entsprechend dessen Anbietertypsteckbriefs ebenso ein Sicherheitsgutachten notwendig. Normativ sind immer die Steckbriefe.

6.1 Beschreibung des Verfahrens

Die Anforderungen an ein Sicherheitsgutachten sowie an Sicherheitsgutachter sind in gemRL_PruefSichEig_DS (siehe gematik-Fachportal) beschrieben.

6.2 Zu prüfende betriebliche Sicherheitsaspekte

Die Umsetzung folgender Anforderungen ist zu prüfen.

Thema	Details zur Anforderung an HSK	AFO-IDs
Betreiber HSK kein Betreiber ePA	Betreiber HSK darf nicht auch ePA Aktensystem betreiben	A_21248-02
Betrieb in EU/EWR	Betrieb HSK muss in EU/EWR stattfinden	GS-A_5551
Befolgen von Herstellervorgaben	Betreiber muss herstellerspezifische Sicherheitsvorgaben und -empfehlungen befolgen	GS-A_4984-01
Betrieb ausschließlich für die eigene Organisation	Nur Eigennutzung, kein Betrieb für datenschutzrechtlich verantwortliche Dritte	A_24073
	Betrieb in den eigenen Räumlichkeiten	A_24323
	Nachweise zum Eigenbetrieb	A_25476
Kein Zugriff auf SM-B Identitäten	Kein voller Zugriff des Betreibers auf SM-B-Identitäten	A_21990
VAU	Kein physischer Zugriff auf Komponenten in denen Versichertendaten verarbeitet werden	A_17354-01
	Physischer Zugriff nur nach Löschen verarbeiteter Versichertendaten	A_17355-01
	Löschen aller Daten bei Beenden eines Verarbeitungskontextes	A_17356-02

Routing- & Firewall-Regeln (falls nicht vom Produkt HSK umgesetzt)	für Pakete aus Bereich NET_TI_DEZENTRAL	TIP1-A_4732-02
	für Pakete aus Bereich ANLW_AKTIVE_BESTANDSNETZE	TIP1-A_4733-02
HSM-B	Benennung Schlüsselverwalter gegenüber gematik	A_23634
	Registrierung bei TSP entsprechend dessen Vorgaben	A_23635
	Rechtzeitige Beauftragung neuer C.HSK-Identitäten beim Hersteller HSK	A_23760
	Löschen von HSM-Bs, die nicht mehr verwendet werden	A_24017
	Prüfung Validität der Anfrage (Antragsteller bekannt?), vor Erzeugung von Schlüsseln und CSRs	A_25240