Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

Fachdienst National Contact Point for eHealth

Produkttyp Version:	1.5.0-0
Produkttyp Status:	freigegeben

Version:	1.0.0
Revision:	720438
Stand:	20.09.2023
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemProdT_NCPeH_FD_PTV_1.5.0-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

Die Produkttypversion ändert sich, wenn sich die normativen Festlegungen für den Produkttyp ändern und die Umsetzung durch Produktentwicklungen ebenfalls betroffen ist.

Produkttypversion	Beschreibung der Änderung	Referenz
1.0.0	Initiale Version auf Dokumentenebene	gemProdT_NCPeH_FD_PTV_1.0.0-0
1.5.0	Anpassung aufgrund der Einarbeitung der Änderung aus NCPeH_23.1	gemProdT_NCPeH_FD_PTV_1.5.0-0

Historie Produkttypsteckbrief

Die Dokumentenversion des Produkttypsteckbriefs ändert sich mit jeder inhaltlichen oder redaktionellen Änderung des Produkttypsteckbriefs und seinen referenzierten Dokumenten. Redaktionelle Änderungen haben keine Auswirkung auf die Produkttypversion.

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	20.09.23		freigegeben	gematik

Inhaltsverzeichnis

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die normativen Festlegungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps oder verweist auf Dokumente, in denen verbindliche normative Festlegungen mit ggf. anderer Notation zu finden sind. Die normativen Festlegungen bilden die Grundlage für die Erteilung von Zulassungen, Zertifizierungen bzw. Bestätigungen durch die gematik. (Wenn im weiteren Dokument vereinfachend der Begriff „Zulassung" verwendet wird, so ist dies der besseren Lesbarkeit geschuldet und umfasst übergreifend neben dem Verfahren der Zulassung auch Zertifizierungen und Bestätigungen der gematik-Zulassungsstelle.)

Die normativen Festlegungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die normativen Festlegungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

1.2 Zielgruppe

Der Produkttypsteckbrief richtet sich an die Anbieter, Hersteller sowie Betreiber des Produkttyps NCPeH-Fachdienst.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens,
- dem Bundesamt für Sicherheit in der Informationstechnik (BSI),
- Auditoren.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens und dem NCPeH-FD.

An einigen Stellen wird im Dokument auf übergreifende Anforderungen in anderen Dokumenten der TI verwiesen. In diesen referenzierten Anforderungen können teilweise Formulierungen auftauchen wie z.B. "Produkt der TI", "Produkttypen der TI", "Dienste der TI". Mit Nennung dieser Anforderungen in diesem Dokument gelten diese auch für den NCPeH-FD, unabhängig davon, ob der NCPeH-Fachdienst als Produkt der TI gilt oder nicht.

1.4 Abgrenzung des Dokumentes

Dieses Dokument macht keine Aussagen zur Aufteilung der Produktentwicklung bzw. Produktherstellung auf verschiedene Hersteller und Anbieter.

Die vom NCPeH-Fachdienst bereitzustellenden Schnittstellen, über die die grenzüberschreitende Datenübertragung mit NCPeHs anderer europäischen Mitgliedsstaaten erfolgt, sind normativdurch die eHDSI spezifiziert. Für diese Schnittstellen erfolgen hier allenfalls zusätzliche normative Ergänzungen.

1.5 Methodik

Die im Dokument verzeichneten normativen Festlegungen werden tabellarisch dargestellt. Die Tabellenspalten haben die folgende Bedeutung:

ID: Identifiziert die normative Festlegung eindeutig im Gesamtbestand aller Festlegungen der gematik.

Bezeichnung: Gibt den Titel einer normativen Festlegung informativ wieder, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der normativen Festlegung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

Quelle (Referenz): Verweist auf das Dokument, das die normative Festlegung definiert.

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Festlegungen.

Tabelle 1: Dokumente mit normativen Festlegungen

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.145.10
gemSpec_DS_Hersteller	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller	1.45.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.268.0
gemSpec_SGD_ePA	Spezifikation Schlüsselgenerierungsdienst ePA	1.56.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.327.0
gemSpec_Systemprozesse_dezTI	Spezifikation Systemprozesse der dezentralen TI	1.3.1
gemSpec_NCPeH_FD	Spezifikation NCPeH-Fachdienst	1.05.0
gemKPT_Test	Testkonzept der TI	2.8.68
gemSpec_TBAuth	Übergreifende Spezifikation Tokenbasierte Authentisierung	1.2.0
gemSpec_DM_ePA_EU-Pilot	Datenmodell ePA	1.53.1_EU-Pilot
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.234.0
gemSpec_TSL	Spezifikation TSL-Dienst	1.20.0

Weiterhin sind die in folgender Tabelle aufgeführten Dokumente und Web-Inhalte in Gänze (d.h. nicht nur die hier im Dokument aufgeführten Anwendungsfälle, Akzeptanzkriterien und Anforderungen etc.) **normativ und gelten mit** (vgl. Kapitel 1.5 Methodik in der jeweiligen Spezifikation)**.**

Tabelle 2: Mitgeltende Dokumente und Web-Inhalte

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag
gemSpec_NCPeH_FD	Spezifikation NCPeH-Fachdienst	
gemRL_PrüfSichEig_DS		2.2.0
gemTestTriggerNCPeH	gematik: Schnittstelle zum Triggern von eHDSI-Anwendungsfällen für den NCPeH-FD Die Definition der Schnittstelle "ncpeh-simulation-td-api-1.5.0.yaml" ist zu finden in https://repo1.maven.org/maven2/de/gematik/api/ncpeh-simulation-td-api/ Weiterführende Informationen sind in github zu finden: https://github.com/gematik/NCPeH-Simulation-API	1.5.0

3 Normative Festlegungen

Die folgenden Abschnitte verzeichnen alle für den Produkttypen normativen Festlegungen, die für die Herstellung und den Betrieb von Produkten des Produkttyps notwendig sind. Die Festlegungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung bei Abnahme des Produktes durch die gematik.

3.1 Festlegungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

In diesem Abschnitt sind alle funktionalen und nicht funktionalen Festlegungen an den technischen Teil des Produkttyps verzeichnet, deren Umsetzung durch Tests nachgewiesen werden müssen.

Tabelle 3: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

ID	Bezeichnung	Quelle (Referenz)
A_23998	Definition AccessCode	gemSpec_DM_ePA_EU-Pilot
AF_10107	LE-EU kann auf demographische Daten des Versicherten lesend zugreifen	gemSpec_NCPeH_FD
AF_10121	Verfügbare Versichertendatensätze des ePKA MIO auflisten	gemSpec_NCPeH_FD
AF_10122	Versichertendatensatz abrufen	gemSpec_NCPeH_FD
AF_10123	Versichertendatensatz als PDF abrufen	gemSpec_NCPeH_FD
A_17688	Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)	gemSpec_PKI
GS-A_4646	TUC_PKI_017: Lokalisierung TSL Download-Adressen	gemSpec_PKI
GS-A_4647	TUC_PKI_016: Download der TSL-Datei	gemSpec_PKI
GS-A_4648	TUC_PKI_019: Prüfung der Aktualität der TSL	gemSpec_PKI
GS-A_4649	TUC_PKI_020: XML-Dokument validieren	gemSpec_PKI
GS-A_4650	TUC_PKI_011: Prüfung des TSL-Signer-Zertifikates	gemSpec_PKI
GS-A_4651	TUC_PKI_012: XML-Signatur-Prüfung	gemSpec_PKI

ID	Bezeichnung	Quelle (Referenz)
GS-A_4652-01	TUC_PKI_018: Zertifikatsprüfung in der TI	gemSpec_PKI
GS-A_4653-01	TUC_PKI_002: Gültigkeitsprüfung des Zertifikats	gemSpec_PKI
GS-A_4654-01	TUC_PKI_003: CA-Zertifikat finden	gemSpec_PKI
GS-A_4655-01	TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur	gemSpec_PKI
GS-A_4656	TUC_PKI_005: Adresse für Status- und Sperrprüfung ermitteln	gemSpec_PKI
GS-A_4657-03	TUC_PKI_006: OCSP-Abfrage	gemSpec_PKI
GS-A_4660-02	TUC_PKI_009: Rollenermittlung	gemSpec_PKI
GS-A_4661-01	kritische Erweiterungen in Zertifikaten	gemSpec_PKI
GS-A_4663	Zertifikats-Prüfparameter für den TLS-Handshake	gemSpec_PKI
GS-A_4749-01	TUC_PKI_007: Prüfung Zertifikatstyp	gemSpec_PKI
GS-A_4750-01	TUC_PKI_030 „QES-Zertifikatsprüfung“	gemSpec_PKI
GS-A_4751	Fehlercodes bei TSL- und Zertifikatsprüfung	gemSpec_PKI
GS-A_4899	TSL Update-Prüfintervall	gemSpec_PKI
GS-A_4957-01	Beschränkungen OCSP-Request	gemSpec_PKI
GS-A_5077	FQDN-Prüfung beim TLS-Handshake	gemSpec_PKI
GS-A_5336	Zertifikatsprüfung nach Ablauf TSL-Graceperiod	gemSpec_PKI
GS-A_5484	TUC_PKI_036 „BNetzA-VL-Aktualisierung“	gemSpec_PKI
A_21980	Performance - Rohdaten - Leerlieferung (Rohdatenerfassung v.02)	gemSpec_Perf
A_22000	Performance - Rohdaten - zu liefernde Dateien (Rohdatenerfassung v.02)	gemSpec_Perf
A_22001-01	Performance - Rohdaten - Name der Berichte (Rohdatenerfassung v.02)	gemSpec_Perf
A_22002	Performance - Rohdaten - Übermittlung (Rohdatenerfassung v.02)	gemSpec_Perf

ID	Bezeichnung	Quelle (Referenz)
A_22004	Performance - Rohdaten - Korrektheit (Rohdatenerfassung v.02)	gemSpec_Perf
A_22429	Performance - Rohdaten - Inhalt der Selbstauskunft (Rohdatenerfassung v.02)	gemSpec_Perf
A_23118-01	Performance - Rohdaten - Spezifika NCPeH-Fachdienst - Message (Rohdatenerfassung v.02)	gemSpec_Perf
A_17925	SGD-Client, Parallele Anfrage SGD1 und SGD2	gemSpec_SGD_ePA
GS-A_5502	Ausstellung im Format SAML 2.0	gemSpec_TBAuth
GS-A_5504	Geltende Präfixe und Namensräume	gemSpec_TBAuth
~~A_23118~~	~~Performance - Rohdaten - Spezifika NCPeH-Fachdienst - Message (Rohdatenerfassung v.02)~~	~~gemSpec_Perf~~

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nicht funktionalen Festlegungen an den technischen Teil des Produkttyps verzeichnet, deren durchgeführte bzw. geplante Umsetzung und Beachtung der Hersteller bzw. der Anbieter durch eine Herstellererklärung bestätigt bzw. zusagt.

Tabelle 4: Festlegungen zur funktionalen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
A_20059	Festlegung von Konfiguration von Produktinstanzen durch die gematik	gemKPT_Test
GS-A_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	gemKPT_Test
TIP1-A_2720	RU/TU: Funktionales Abbild der Produktivumgebung	gemKPT_Test
TIP1-A_2722-01	TBI integriert die Produkttypen in seine Systemumgebung	gemKPT_Test
TIP1-A_2724	TBI verantwortet Betrieb RU und TU	gemKPT_Test
TIP1-A_2775	Performance in RU	gemKPT_Test
TIP1-A_2805	Zeitnahe Anpassung von Produktkonfigurationen	gemKPT_Test

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_2806	Zeitnahe Anpassung der Konfiguration der Testumgebung	gemKPT_Test
TIP1-A_3017	Systemumgebungsmanagement RU sowie TU	gemKPT_Test
TIP1-A_4191	Keine Echtdaten in RU und TU	gemKPT_Test
TIP1-A_4923	Dauerhafte Verfügbarkeit RU und TU	gemKPT_Test
TIP1-A_4930	Automatisierung von Tests	gemKPT_Test
TIP1-A_5052	Dauerhafte Verfügbarkeit in der RU	gemKPT_Test
TIP1-A_6079	Updates von Referenzobjekten	gemKPT_Test
TIP1-A_6086	Unterstützung bei Anbindung eines Produktes	gemKPT_Test
TIP1-A_6088	Unterstützung bei Fehlernachstellung	gemKPT_Test
TIP1-A_6093	Ausprägung der Referenzobjekte	gemKPT_Test
TIP1-A_6517-01	Eigenverantwortlicher Test: TBI	gemKPT_Test
TIP1-A_6518	Eigenverantwortlicher Test: TDI	gemKPT_Test
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_7330	Tracedaten von echten Außenschnittstellen	gemKPT_Test
TIP1-A_7358	Qualität des Produktmusters	gemKPT_Test
A_16958	VAU-Protokoll: Client, Neuinitiieren einer Schlüsselaushandlung	gemSpec_Krypt
A_17124-01	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
A_17775	TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)	gemSpec_Krypt
A_21888	VAU-Client, Nichtproduktivumgebung, vorgegebene ECDH-Schlüssel	gemSpec_Krypt

ID	Bezeichnung	Quelle (Referenz)
A_21977	VAU-Client, Nichtproduktivumgebung, vorgegebene ECDH-Schlüssel, optionale Konfigurierbarkeit	gemSpec_Krypt
GS-A_5080-01	Signaturen binärer Daten (Dokumente)	gemSpec_Krypt
AF_10124	Service Metadata auf eHDSI Configuration Service verwalten	gemSpec_NCPeH_FD
AF_10125	Konfigurationsparameter verwalten	gemSpec_NCPeH_FD
AF_10126	Evidences & Audit Trails aus Audit Repository abrufen	gemSpec_NCPeH_FD
AF_10127	MTC vom eHDSI Terminology Service herunterladen	gemSpec_NCPeH_FD
GS-A_4009	Übertragungstechnologie auf OSI-Schicht LAN	gemSpec_Net
GS-A_4053	Ingress und Egress Filtering	gemSpec_Net
GS-A_4054	Paketfilter Default Deny	gemSpec_Net
GS-A_4805	Abstimmung angeschlossener Produkttyp mit dem Anbieter Zentrales Netz	gemSpec_Net
GS-A_4831	Standards für IPv4	gemSpec_Net
GS-A_4884	Erlaubte ICMP-Types	gemSpec_Net
A_17690	Nutzung der Hash-Datei für TSL (ECC-Migration)	gemSpec_PKI
A_17700	TSL-Auswertung ServiceTypeIdentifier "unspecified"	gemSpec_PKI
GS-A_4640	Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung	gemSpec_PKI
GS-A_4642	TUC_PKI_001: Periodische Aktualisierung TI-Vertrauensraum	gemSpec_PKI
GS-A_4643	TUC_PKI_013: Import TI-Vertrauensanker aus TSL	gemSpec_PKI
GS-A_4898	TSL-Grace-Period einer TSL	gemSpec_PKI
GS-A_5215	Festlegung der zeitlichen Toleranzen in einer OCSP-Response	gemSpec_PKI

ID	Bezeichnung	Quelle (Referenz)
A_21975	Performance - Rohdaten - Default-Werte für Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_21976	Performance - Rohdaten - Konfigurierbarkeit der Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_21978	Performance - Rohdaten - Trennung der Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_21979	Performance - Rohdaten - Bezug der Lieferverpflichtung (Rohdatenerfassung v.02)	gemSpec_Perf
A_21981-02	Performance - Rohdaten - Format des Rohdaten-Performance-Berichtes (Rohdatenerfassung v.02)	gemSpec_Perf
A_21982-01	Performance - Rohdaten - Message-Block (Rohdatenerfassung v.02)	gemSpec_Perf
A_22005	Performance - Rohdaten - Frist für Nachlieferung (Rohdatenerfassung v.02)	gemSpec_Perf
A_22047	Performance - Rohdaten - Änderung der Konfiguration der Lieferintervalle (Rohdatenerfassung v.02)	gemSpec_Perf
A_22482	Performance - Rohdaten - Erfassung von Rohdaten (Rohdatenerfassung v.02)	gemSpec_Perf
A_22500-01	Performance - Rohdaten - Status-Block (Rohdatenerfassung v.02)	gemSpec_Perf
A_22513-01	Performance - Rohdaten - Message-Block im Fehlerfall (Rohdatenerfassung v.02)	gemSpec_Perf
A_23011	Performance - Rohdaten - Spezifika NCPeH-Fachdienst - Operation (Rohdatenerfassung v.02)	gemSpec_Perf
A_23012	Performance - Rohdaten - Spezifika NCPeH-Fachdienst - Duration (Rohdatenerfassung v.02)	gemSpec_Perf
A_23013	Performance - Rohdaten - Spezifika NCPeH-Fachdienst - Status (Rohdatenerfassung v.02)	gemSpec_Perf
A_23016	Performance - NCPeH-Fachdienst - Last- und Bearbeitungszeiten	gemSpec_Perf

ID	Bezeichnung	Quelle (Referenz)
A_23067	Performance - NCPeH-Fachdienst - Messung von Bearbeitungszeiten	gemSpec_Perf
A_17847	Prüfung eines SGD-HSM-Zertifikats (1/2)	gemSpec_SGD_ePA
A_17848	Prüfung eines SGD-HSM-Zertifikats (2/2)	gemSpec_SGD_ePA
A_17930	interoperables Austauschformat Schlüsselableitungsfunktionalität ePA	gemSpec_SGD_ePA
A_18005	SGD-Client, nur Einmalverwendung des kurzlebigen ECIES-Client-Schlüsselpaars	gemSpec_SGD_ePA
A_18024	SGD-Client, Prüfung SGD-HSM-ECIES-Schlüssel	gemSpec_SGD_ePA
A_18032	SGD-Client, kurzlebigen ECIES-Client-Schlüsselpaar	gemSpec_SGD_ePA
A_22497	SGD-Client, Mehrfachableitung (kurzlebiges ECIES-Client-Schlüsselpaar)	gemSpec_SGD_ePA
A_18072	Ablauf der Zertifikatsprüfung in der TI	gemSpec_Systemprozesse_dezTI
TIP1-A_6991	Leistung zur Prüfung eines Zertifikats in der TI	gemSpec_Systemprozesse_dezTI
TIP1-A_6992-01	Aufrufparameter der Zertifikatsprüfung in der TI	gemSpec_Systemprozesse_dezTI
TIP1-A_6993	Ergebnis der Zertifikatsprüfung in der TI	gemSpec_Systemprozesse_dezTI
TIP1-A_5120	Clients des TSL-Dienstes: HTTP-Komprimierung unterstützen	gemSpec_TSL

3.2 Festlegungen zur sicherheitstechnischen Eignung

3.2.1 Produktgutachten

Die in diesem Abschnitt verzeichneten Festlegungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL_PruefSichEig_DS]. Das entsprechende Produktgutachten ist der gematik vorzulegen.

Tabelle 5: Festlegungen zur sicherheitstechnischen Eignung "Produktgutachten"

ID	Bezeichnung	Quelle (Referenz)
A_15549	VAU-Client: Kommunikation zwischen VAU-Client und VAU	gemSpec_Krypt
A_15705	Vorgaben Aktenschlüssel (RecordKey) und Kontextschlüssel (ContextKey)	gemSpec_Krypt
A_16849	VAU-Protokoll: Aktionen bei Protokollabbruch	gemSpec_Krypt
A_16852-01	VAU-Protokoll: ECDH durchführen	gemSpec_Krypt
A_16883-01	VAU-Protokoll: Aufbau VAUClientHello-Nachricht	gemSpec_Krypt
A_16884	VAU-Protokoll: Nachrichtentypen und HTTP-Content-Type	gemSpec_Krypt
A_16897	VAU-Protokoll: Versand der VAUClientHello-Nachricht	gemSpec_Krypt
A_16900	VAU-Protokoll: Client, Behandlung von Fehlernachrichten	gemSpec_Krypt
A_16903	VAU-Protokoll: Client, Prüfung des VAUClientHelloDataHash-Werts (aus VAUServerHelloData)	gemSpec_Krypt
A_16941-01	VAU-Protokoll: Client, Prüfung der Signatur der VAUServerHelloData	gemSpec_Krypt
A_16943-01	VAU-Protokoll: Schlüsselableitung (HKDF)	gemSpec_Krypt
A_16945-02	VAU-Protokoll: Client, verschlüsselte Kommunikation (1)	gemSpec_Krypt
A_16957-01	VAU-Protokoll: Client, verschlüsselte Kommunikation (2)	gemSpec_Krypt
A_17069	VAU-Protokoll: Client Zählerüberlauf	gemSpec_Krypt
A_17070-02	VAU-Protokoll: Aufbau der VAUClientSigFin-Nachricht	gemSpec_Krypt
A_17071	VAU-Protokoll: Versand der VAUClientSigFin-Nachricht	gemSpec_Krypt
A_17074	VAU-Protokoll: Ignorieren von zusätzlichen Datenfeldern in Protokoll-Nachrichten	gemSpec_Krypt
A_17081	VAUProtokoll: zu verwendende Signaturschlüssel	gemSpec_Krypt

ID	Bezeichnung	Quelle (Referenz)
A_17084	VAU-Protokoll: Empfang der VAUServerFin-Nachricht	gemSpec_Krypt
A_17872	Ver- und Entschlüsselung der Akten und Kontextschlüssel (Schlüsselableitungsfunktionalität ePA)	gemSpec_Krypt
A_17874	SGD-Client, Client-authentisiertes ECIES-Schlüsselpaar	gemSpec_Krypt
A_17875	ECIES-verschlüsselter Nachrichtenversand zwischen SGD-Client und SGD-HSM	gemSpec_Krypt
A_18004	Vorgaben für die Kodierung von Chiffraten (innerhalb von ePA)	gemSpec_Krypt
A_18464	TLS-Verbindungen, nicht Version 1.1	gemSpec_Krypt
A_18465-01	VAU-Protokoll: MTOM/XOP-HTTP-Header-Informationen	gemSpec_Krypt
A_18466-01	VAU-Protokoll: zusätzliche HTTP-Header-Informationen	gemSpec_Krypt
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt
A_19971	SGD und SGD-Client, Hashfunktion für Signaturerstellung und -prüfung	gemSpec_Krypt
A_20549	VAU-Protokoll: Einbringen der ursprünglich intendierten Content-Type-Variable	gemSpec_Krypt
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	gemSpec_Krypt
A_21888	VAU-Client, Nichtproduktivumgebung, vorgegebene ECDH-Schlüssel	gemSpec_Krypt
A_21977	VAU-Client, Nichtproduktivumgebung, vorgegebene ECDH-Schlüssel, optionale Konfigurierbarkeit	gemSpec_Krypt
A_23273	VAU-Protokoll: Client, Prüfung der Signatur der VAUServerHelloData, Gültigkeit von OCSP-Antworten	gemSpec_Krypt
A_23282	VAU-Protokoll: Signaturen im VAU-Protokoll	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt

ID	Bezeichnung	Quelle (Referenz)
GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
A_21915-02	Verarbeitungskontext der VAU	gemSpec_NCPeH_FD
A_21917-02	Geschützte Weitergabe von Daten an autorisierte Nutzer durch die VAU	gemSpec_NCPeH_FD
A_21918-02	Transportverschlüsselte Übertragung von Daten	gemSpec_NCPeH_FD
A_21922-02	Isolation der VAU von Datenverarbeitungsprozessen des Anbieters	gemSpec_NCPeH_FD
A_21923-02	Ausschluss von Manipulationen an der Software der VAU	gemSpec_NCPeH_FD
A_21924-02	Ausschluss von Manipulationen an der Hardware der VAU	gemSpec_NCPeH_FD
A_21925-02	Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU	gemSpec_NCPeH_FD
A_21926-02	Kein physischer Zugang des Anbieters zu Systemen der VAU	gemSpec_NCPeH_FD
A_21927-02	Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU	gemSpec_NCPeH_FD
A_21928-02	Gute Prüfbarkeit der Sicherheitseigenschaften von Code in der VAU	gemSpec_NCPeH_FD
A_21934-02	Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU	gemSpec_NCPeH_FD
A_21935-02	Managementprozesse des HSM	gemSpec_NCPeH_FD
A_22385-02	Keine Speicherung von schützenswerten Daten	gemSpec_NCPeH_FD
A_22389-02	Private Schlüssel der TI im HSM	gemSpec_NCPeH_FD
A_22390-02	Integritätsprüfung der VAU	gemSpec_NCPeH_FD
A_22391-02	HSM-Kryptographieschnittstelle verfügbar nur für Verarbeitungskontexte der VAU	gemSpec_NCPeH_FD
A_22517-02	Umsetzung des NCPeH-Fachdienstes in einer Vertrauenswürdigen Ausführungsumgebung (VAU)	gemSpec_NCPeH_FD

ID	Bezeichnung	Quelle (Referenz)
A_22912	Anbieter des NCPeH-Fachdienstes - Verbot vom dynamischen Inhalt	gemSpec_NCPeH_FD
A_22973	TLS Endpunkt in der VAU	gemSpec_NCPeH_FD
A_23135	Akzeptieren der Identity Assertion des anfragenden LE-EU	gemSpec_NCPeH_FD
A_23136	Eingabevalidierung von Operationen	gemSpec_NCPeH_FD
A_23138	Tamper Proof Audit	gemSpec_NCPeH_FD
A_23140	Korrekte Zuordnung der NCPeH Land-B Identitäten	gemSpec_NCPeH_FD
A_23166	Keine Zwischenspeicherung ePKA MIO	gemSpec_NCPeH_FD
A_23176	Eingeschränkte Nutzung des Audit Repositories	gemSpec_NCPeH_FD
A_23178	Sicherheitsprüfung sicherheitsrelevante Anforderung	gemSpec_NCPeH_FD
A_23184	Private Schlüssel der eHDSI im HSM	gemSpec_NCPeH_FD
A_23189	Isolation der I_Management_Configuration Schnittstelle	gemSpec_NCPeH_FD
A_23190	Isolation der „Audit Trails Abrufen“ Schnittstelle	gemSpec_NCPeH_FD

3.2.2 Herstellererklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Festlegungen verzeichnet sind, muss der Hersteller bzw. der Anbieter deren Umsetzung und Beachtung zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung bestätigen bzw. zusagen.

Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"

ID	Bezeichnung	Quelle (Referenz)
GS-A_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	gemKPT_Test
TIP1-A_4191	Keine Echtdaten in RU und TU	gemKPT_Test
A_19163	Rechte der gematik zur sicherheitstechnischen Prüfung des Produktes	gemSpec_DS_Hersteller
A_19164	Mitwirkungspflicht bei Sicherheitsprüfung	gemSpec_DS_Hersteller

ID	Bezeichnung	Quelle (Referenz)
A_19165	Auditrechte der gematik zur Prüfung der Herstellerbestätigung	gemSpec_DS_Hersteller
A_17124-01	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	gemSpec_Krypt
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
A_17775	TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)	gemSpec_Krypt
A_18986	Fachdienst-interne TLS-Verbindungen	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5080-01	Signaturen binärer Daten (Dokumente)	gemSpec_Krypt
GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt
GS-A_5526	TLS-Renegotiation-Indication-Extension	gemSpec_Krypt
GS-A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	gemSpec_Krypt
GS-A_5580-01	TLS-Klient für betriebsunterstützende Dienste	gemSpec_Krypt
A_22914	Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im Handbuch	gemSpec_NCPeH_FD
A_17688	Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)	gemSpec_PKI
A_17690	Nutzung der Hash-Datei für TSL (ECC-Migration)	gemSpec_PKI
GS-A_4640	Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung	gemSpec_PKI
GS-A_4641	Initiale Einbringung TI-Vertrauensanker	gemSpec_PKI
GS-A_4642	TUC_PKI_001: Periodische Aktualisierung TI-Vertrauensraum	gemSpec_PKI

ID	Bezeichnung	Quelle (Referenz)
GS-A_4643	TUC_PKI_013: Import TI-Vertrauensanker aus TSL	gemSpec_PKI
GS-A_4748	Initiale Einbringung TSL-Datei	gemSpec_PKI
GS-A_4750-01	TUC_PKI_030 „QES-Zertifikatsprüfung"	gemSpec_PKI
GS-A_5077	FQDN-Prüfung beim TLS-Handshake	gemSpec_PKI
GS-A_5215	Festlegung der zeitlichen Toleranzen in einer OCSP-Response	gemSpec_PKI
GS-A_5484	TUC_PKI_036 „BNetzA-VL-Aktualisierung"	gemSpec_PKI
A_17847	Prüfung eines SGD-HSM-Zertifikats (1/2)	gemSpec_SGD_ePA
A_17848	Prüfung eines SGD-HSM-Zertifikats (2/2)	gemSpec_SGD_ePA
A_17930	interoperables Austauschformat Schlüsselableitungsfunktionalität ePA	gemSpec_SGD_ePA
A_18005	SGD-Client, nur Einmalverwendung des kurzlebigen ECIES-Client-Schlüsselpaars	gemSpec_SGD_ePA
A_18024	SGD-Client, Prüfung SGD-HSM-ECIES-Schlüssel	gemSpec_SGD_ePA
A_18032	SGD-Client, kurzlebigen ECIES-Client-Schlüsselpaar	gemSpec_SGD_ePA
A_22494	SGD-Client, HTTP-Variable SGD-Userpseudonym	gemSpec_SGD_ePA
A_22497	SGD-Client, Mehrfachableitung (kurzlebiges ECIES-Client-Schlüsselpaar)	gemSpec_SGD_ePA
A_18072	Ablauf der Zertifikatsprüfung in der TI	gemSpec_Systemprozesse_dezTI
TIP1-A_6992-01	Aufrufparameter der Zertifikatsprüfung in der TI	gemSpec_Systemprozesse_dezTI
TIP1-A_6993	Ergebnis der Zertifikatsprüfung in der TI	gemSpec_Systemprozesse_dezTI

4 Produkttypspezifische Merkmale

Es liegen keine optionalen Ausprägungen des Produkttyps vor.

5 Anhang – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
ID	Identifikation
CC	Common Criteria
NCPeH	National Contact Point for eHealth

5.2 Tabellenverzeichnis

5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[CC]	Internationaler Standard: Common Criteria for Information Technology Security Evaluation https://www.commoncriteriaportal.org/cc/
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung