Änderung in gemProdT_eRp_FD

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
A_19302	E-Rezept-Fachdienst - Protokolleintrag Versichertenprotokoll leicht verständlich	Der E-Rezept-Fachdienst MUSS in jedem zu tätigenden Eintrag des Protokolls für Versicherte einen lesbaren Text in einfacher Sprache (deutsch und englisch) erzeugen, der mindestens den Namen des Zugreifenden, die auslösende Operation und das Ergebnis der Operation umfasst, damit Versicherte ohne technisches Vorwissen den Inhalt des Zugriffsprotokolls verstehen können.	gemSpec_FD_eRp	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung: Test
A_19391	E-Rezept-Fachdienst - Authentifizierung Nutzername	Der E-Rezept-Fachdienst MUSS den Namen eines Nutzers in jedem Operationsaufruf anhand der Attribute "given_name", "family_name" und "organizationName" im übergebenen IDP-Token im HTTP-Header "Authorization" feststellen und für die Protokollierung des Zugriffs auf personenbezogene medizinische Daten je Operationsaufruf verwenden.	gemSpec_FD_eRp	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung: Test

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
A_19392	E-Rezept-Fachdienst - Authentifizierung Nutzerkennung	Der E-Rezept-Fachdienst MUSS die Nutzerkennung (10-stelliger Teil der KVNR, Telematik-ID für Leistungserbringerinstitutionen) eines Nutzers in jedem Operationsaufruf anhand des Attributs "idNummer" im übergebenen IDP-Token im HTTP-Header "Authorization" feststellen und für die Protokollierung des Zugriffs auf personenbezogene medizinische Daten je Operationsaufruf verwenden.	gemSpec_FD_eRp	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung: Test
A_19719	E-Rezept-Fachdienst – Verarbeitungskontexte der VAU über gemeinsame Host-Adressen erreichbar	Die VAU des E-Rezept-Fachdienstes MUSS ihre Verarbeitungskontexte über gemeinsame IP-Adressen und Ports des Eingangspunkts des Fachdienstes erreichbar machen.	gemSpec_FD_eRp	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung
A_19720	E-Rezept-Fachdienst – Verbindungen von Clients zu Verarbeitungskontexten der VAU über den Eingangspunkt	Der Eingangspunkt des E-Rezept-Fachdienstes MUSS Verbindungen von Clients (Internet oder TI) ausschließlich über TLS akzeptieren. Er MUSS die TLS-Verbindung terminieren und HTTP Requests und Responses zwischen dem Client und dem für die jeweilige Sitzung zugeordneten Verarbeitungskontext der	gemSpec_FD_eRp	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung: Test

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
		VAU vermitteln.			
A_19721	E-Rezept-Fachdienst – Sicherer Kanal zum Verarbeitungskontext der VAU auf Inhaltsebene	Der Eingangspunkt des E-Rezept-Fachdienstes MUSS Clients den Aufbau eines sicheren Kanals auf Inhaltsebene, d. h. einen Verbindungsaufbau gemäß [gemSpec_Krypt#3.16] und [gemSpec_Krypt#7], zum Verarbeitungskontext ermöglichen.	gemSpec_FD_eRp	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung
A_19724	E-Rezept-Fachdienst – Identität des Verarbeitungskontextes für Clients	Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sich gegenüber Clients mittels der Fachdienstidentität oid_erp-vau mit Zertifikatsprofil C.FD.ENC ausweisen.	gemSpec_FD_eRp	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung: Test

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
A_19726-01	E-Rezept-Fachdienst – Unabhängige Skalierung der Dienst-Ressourcen für verschiedene Anwendergruppen	Die VAU des E-Rezept-Fachdienstes MUSS für die Anwendergruppen Leistungserbringer (E-Rezepte ausstellen, E-Rezepte einlösen) und Versicherte (E-Rezepte einsehen, zuweisen und löschen) sicherstellen dass eine Überlastung aufgrund außergewöhnlich hoher Aktivität einer Anwendergruppe (primär der Versicherten) keine Beeinträchtigung der Arbeitsfähigkeit der anderen Anwendergruppen (primär der Ärzte und Apotheker) zur Folge hat.	gemSpec_FD_eRp	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung
A_19823	E-Rezept-Fachdienst – Richtlinien zum TLS-Verbindungsaufbau	Der Eingangspunkt des E-Rezept-Fachdienstes MUSS sich beim TLS-Verbindungsaufbau über das Transportnetz gegenüber dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] authentisieren. Das Zertifikat MUSS an die jeweilige Schnittstelle des Eingangspunkts für Primärsysteme und Frontends der Versicherten des E-Rezept-Fachdienstes gebunden werden, damit Clientsysteme beim TLS-Verbindungsaufbau eine vereinfachte Zertifikatsprüfung mit TLS-Standardbibliotheken durchführen können.	gemSpec_FD_eRp	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
A_20023	E-Rezept-Fachdienst - Bereitstellung TSL	Der E-Rezept-Fachdienst MUSS folgende Vorgaben umsetzen: * Er MUSS mindestens einmal täglich aus der TI (TI-interne Verbindung) die "TSL(ECC-RSA)" und deren zugehörigen Hashwert aus der TI herunterladen. * Er MUSS unter dem Pfadnamen "/TSL.xml" über das vom E-Rezept-FdV genutzte HTTPS-Interface die "TSL(ECC-RSA)" der TI zur Verfügung stellen (HTTP-GET, HTTP Content-Type: text/xml). * Er MUSS unter dem Pfadnamen "/TSL.sha2" über das vom E-Rezept-FdV genutzte HTTPS-Interface den vom TSL-Dienst heruntergeladenen SHA-256 Hashwert der Datei TSL.xml aus Spiegelstrich 2 zur Verfügung stellen (HTTP Content-Type: text/plain, Hashwert als hexdump kodiert (64 Byte + Newline))	gemSpec_FD_eRp	sicherheitstechnische Eignung: Produktgutachten, funktionale Eignung: Test	funktionale Eignung: Test
A_20019	Blacklisting von IP-Adressen	Der Fachdienst MUSS eine Blacklist führen, in welcher er IP-Adressen oder ganze Subnetze einträgt, wenn Angriffsszenarien von diesen Adressen oder Netzen erfolgen.	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten, funktionale Eignung: Test	sicherheitstechnische Eignung: Produktgutachten

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
A_20020	Bereinigung der "IP-Adress"-Blacklist Host-Adressen	Fachdienste MÜSSEN Host-Adressen mit einer Verzögerung von einer Stunde aus der Blacklist streichen, wenn von der gefilterten IP-Adresse keine weiteren Angriffe mehr verzeichnet werden.	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten, funktionale Eignung: Test	funktionale Eignung: Test
A_20362	"ACCESS_TOKEN" generelle Struktur	Fachdienste MÜSSEN die gemäß [RFC7519 # section-7.1 <https://tools.ietf.org/html/rfc7519#section-7.1>] vorgeschriebene Struktur der "ACCESS_TOKEN" gemäß [RFC7519 # section-7.2 <https://tools.ietf.org/html/rfc7519#section-7.2>] validieren.	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten, funktionale Eignung: Test	funktionale Eignung: Test
A_20363-01	"ACCESS_TOKEN" sind verschlüsselt	Der Fachdienst MUSS die für ihn vom Anwendungsfrontend verschlüsselten "ACCESS_TOKEN" entsprechend dem für diese Übertragung vorgesehenen Verfahren entschlüsseln.	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten, funktionale Eignung: Test	funktionale Eignung Test
A_20364	Unverschlüsselt eingehende	Fachdienste DÜRFEN unverschlüsselt eingehende "ACCESS_TOKEN" NICHT	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten,	funktionale Eignung Test

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
	ACCESS_TOKEN sind ungültig	annehmen.		funktionale Eignung: Test	
A_20365-01	Die Signatur des "ACCESS_TOKEN" ist zu prüfen	Fachdienste MÜSSEN die Signatur der "ACCESS_TOKEN" gegen den öffentlichen Schlüssel des Token-Endpunktes "PUK_IDP_SIG" prüfen. Fachdienste MÜSSEN den öffentliche Schlüssel „PUK_IDP_SIG“ dabei dem Discovery Dokument des IDP-Dienstes entnehmen.	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten , funktionale Eignung: Test	sicherheitstechnische Eignung: Produktgutachten
A_20367	Fehlermeldungen bei Übertragungsfehler des "ACCESS_TOKEN" melden	Fachdienste MÜSSEN Fehler, welche bei der Annahme des "ACCESS_TOKEN" entstehen, melden. Die Fehlermeldung MUSS mit dem privaten Schlüssel "PRK_FD" signiert sein. Die Fehlermeldungen MÜSSEN für den Anwender verständlich formuliert sein.	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten , funktionale Eignung: Test	funktionale Eignung Test
A_20369-01	Abbruch bei unerwarteten Inhalten	Der Fachdienst MUSS die im "ACCESS_TOKEN" übertragenen Attribute mit denen vergleichen, die mit dem IdP-Dienst bei der Registrierung vereinbart wurden und alle mit dem "ACCESS_TOKEN" in Verbindung stehenden Vorgänge abbrechen, wenn dem "ACCESS_TOKEN" für die Verarbeitung notwendige Claims fehlen oder aber andere als die mit dem IdP-	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
		Dienst vereinbarten personenbezogenen Attribute vorhanden sind.			
A_20370	Abbruch bei falschen Datentypen der Attribute	Fachdienste MÜSSEN "ACCESS_TOKEN" ablehnen, wenn die in einem Attribut vorgetragenen Werte nicht dem schematisch erwarteten Datentyp des Attributes entsprechen.	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten, funktionale Eignung: Test	funktionale Eignung Test
A_20373	Prüfung der Gültigkeit des "ACCESS_TOKEN" für den Zugriff auf Fachdienste ohne "nbf"	Fachdienste MÜSSEN sicherstellen, dass der Zeitraum der Verwendung des Tokens zwischen den im Token mitgelieferten Werten der Attribute "iat" und "exp" liegt.	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten, funktionale Eignung: Test	funktionale Eignung Test
A_20374	Prüfung der Gültigkeit des "ACCESS_TOKEN" für den Zugriff auf Fachdienste mit "nbf"	Fachdienste MÜSSEN sicherstellen, dass der Zeitraum der Verwendung des Tokens zwischen den im Token mitgelieferten Werten der Attribute "nbf" und "exp" liegt.	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten, funktionale Eignung: Test	funktionale Eignung Test
A_20631	Einschränkung zur Bereinigung der "IP-Adress"-Blacklist Subnetze	Fachdienste DÜRFEN Netzadressen NICHT aus der Blackliste streichen, wenn es sich hierbei um Blacklisting auf Basis von Geo-IP-Adressbereichen handelt.	gemSpec_IDP_FD	sicherheitstechnische Eignung: Produktgutachten, funktionale Eignung: Test	funktionale Eignung Test

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
A_17124	TLS-Verbindungen (ECC-Migration)	Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN die folgenden Vorgaben erfüllen: * Zur Authentifizierung MUSS eine X.509-Identität gemäß [gemSpec_Krypt#GS-A_4359] verwendet werden. * Als Ciphersuiten MÜSSEN TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0,0x2B) und TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0,0x2C) unterstützt werden. * Falls der Produkttyp in der Rolle als TLS-Client agiert, so MUSS er die eben genannten Ciphersuiten gegenüber evtl. ebenfalls von ihm unterstützen RSA-basierte Ciphersuiten (vgl. GS-A_4384) bevorzugen (in der Liste "cipher_suites" beim ClientHello vorne an stellen, vgl. [RFC-5246#7.4.1.2 Client Hello]). * Als Basis für den ephemeren ECDH MÜSSEN die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt und verwendet werden.	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN sicherstellen, dass sie nur (durch andere Anforderungen) zugelassene TLS-Ciphersuiten bzw. TLS-Versionen anbieten bzw. verwenden.	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung
A_17775	TLS-Verbindungen Reihenfolge Ciphersuiten (ECC-Migration)	Alle Produkttypen, die Übertragungen mittels TLS durchführen und in der Rolle TLS-Server agieren, SOLLEN die Reihenfolge der Ciphersuiten in der Liste "cipher_suites" aus dem TLS-ClientHello bei der Auswahl der Ciphersuite befolgen.	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung
A_18464	TLS-Verbindungen, nicht Version 1.1	Alle Produkttypen, die Übertragungen mittels TLS durchführen, DÜRFEN NICHT die TLS-Version 1.1 [RFC-4346] unterstützen.	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test
A_18467	TLS-Verbindungen, Version 1.3	Alle Produkttypen, die Übertragungen mittels TLS durchführen, KÖNNEN die TLS-Version 1.3 [RFC-8446] unterstützen, falls sie * dabei nur nach [BSI-TR-02102-2] empfohlene Verbindungskonfigurationen (Handshake-Modi, (EC)DH-Gruppen, Signaturverfahren, Ciphersuiten etc.) verwenden, und * mindestens die Ciphersuite	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
		"TSL_AES_128_GCM_SHA256" dabei unterstützen.			
A_18986	Fachdienst-interne TLS-Verbindungen	Alle Produkttypen, die Übertragungen mittels TLS durchführen, die nur innerhalb ihres Produkttypen verlaufen (bspw. ePA-Aktensystem interne TLS-Verbindungen zwischen dem Zugangsgateway und der Komponente Authentisierung), KÖNNEN für diese TLS-Verbindungen neben den in GS-A_4384 und ggf. A_17124 festgelegten TLS-Vorgaben ebenfalls alle weiteren in [TR-02102-2] empfohlenen TLS-Versionen und TLS-Ciphersuiten mit den jeweiligen in [TR-02102-2] dafür aufgeführten Domainparametern (Kurven, Schlüssellängen etc.) verwenden.	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN sicherstellen, dass * sie im Rahmen der Erstellung und Prüfung von digitalen Signaturen im Rahmen des TLS-Handshakes ausschließlich folgende kryptographisch geeignete Hashfunktionen verwenden: * SHA-256, SHA-384, SHA-512 [FIPS-180-4] * SHA3-256, SHA3-384, SHA3-512 [FIPS-202] * sie dabei mindestens SHA-256 unterstützen, (Bitte die Umsetzungshinweise in Bezug auf die "signature_algorithms"-Extension in gemSpec_Krypt#A_21275-* beachten.)	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung
GS-A_4385	TLS-Verbindungen, Version 1.2	Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN die TLS-Version 1.2 [RFC-5246] unterstützen.	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	Alle Produkttypen, die Übertragungen mittels TLS durchführen, DÜRFEN NICHT die TLS-Version 1.0 unterstützen.	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
GS-A_5035	Nichtverwendung des SSL-Protokolls	Alle Produkttypen, die Daten über Datenleitungen übertragen wollen, DÜRFEN NICHT das SSL-Protokoll unterstützen.	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test

GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN u. a. folgende Vorgaben erfüllen: * Falls der Produkttyp als Klient oder als Server im Rahmen von TLS an einer Session-Resumption mittels SessionID (vgl. [RFC-5246, Abschnitt 7.4.1.2]) teilnimmt, MUSS er sicherstellen, dass nach spätestens 24 Stunden das über den Diffie-Hellman-Schlüsselaustausch ausgehandelte Schlüsselmaterial und alles davon abgeleitete Schlüsselmaterial (vgl. [RFC-5246, Abschnitt 8.1 und 6.3]) bei ihm sicher gelöscht wird. * Falls der Produkttyp als Klient im Rahmen von TLS an einer Session-Resumption nach [RFC-5077] teilnimmt, MUSS er sicherstellen, dass nach spätestens 24 Stunden das über den Diffie-Hellman-Schlüsselaustausch ausgehandelte Schlüsselmaterial und alles davon abgeleitete Schlüsselmaterial (vgl. [RFC-5246, Abschnitt 8.1 und 6.3]) bei ihm sicher gelöscht wird. Damit verbundene SessionTickets MUSS er ebenfalls sicher löschen. * Falls der Produkttyp als Server im Rahmen von TLS an einer Session-Resumption nach [RFC-5077] teilnimmt, MUSS er sicherstellen, dass nach spätestens 24 Stunden das über den	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test

		Diffie-Hellman-Schlüsselaustausch ausgehandelte Schlüsselmaterial und alles davon abgeleitete Schlüsselmaterial (vgl. [RFC-5246, Abschnitt 8.1 und 6.3]) bei ihm sicher gelöscht wird. Damit verbundene SessionTickets MUSS er, falls bei ihm vorhanden, sicher löschen. Das Schlüsselmaterial, dass bei der Erzeugung des SessionTickets (für die Sicherung von Vertraulichkeit und Authentizität der SessionTickets) verwendet wird, MUSS spätestens alle 48 Stunden gewechselt werden und das alte Material MUSS sicher gelöscht werden. Als kryptographische Verfahren zur Erzeugung/Sicherung der SessionTickets MÜSSEN ausschließlich nach [BSI-TR-03116-1] zulässige Verfahren verwendet werden und das Schlüsselmaterial muss die Entropieanforderungen gemäß [gemSpec_Krypt#GS-A_4368] erfüllen. * Falls ein Produkttyp als Klient oder Server im Rahmen von TLS die Renegotiation unterstützt, so MUSS er dies ausschließlich nach [RFC-5746] tun. Ansonsten MUSS er die Renegotiation-Anfrage des Kommunikationspartners ablehnen.			

GS-A_5339	TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität	Alle Produkttypen, die TLS verwenden und bei denen insbesondere Webbrowser-Interoperabilität (Webportale, Download-Punkte o. Ä.) wichtig ist, MÜSSEN zur Absicherung der TLS-Übertragung neben der in [gemSpec_Krypt#GS-A_4384] aufgeführten Vorgaben zusätzlich Folgendes sicherstellen: * Der Produkttyp MUSS zusätzlich folgende Ciphersuiten unterstützen: * TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC0, 0x14), * TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC0, 0x13), * TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30) und * TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F). * Der TLS-Server KANN weitere Cipher-Suiten aus [TR-02102-2, Abschnitt 3.3.1 Tabelle 1] unterstützen. * Bei dem ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch MÜSSEN	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test

		die Kurven P-256 oder P-384 [FIPS-186-4] unterstützt werden. Daneben KÖNNEN die Kurven brainpoolP256r1, brainpoolP384r1 oder brainpoolP512r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt werden. Andere Kurven SOLLEN NICHT verwendet werden (Hinweis: die Intention des letzten Satzes ist insbesondere, dass die Ordnung des Basispunktes in E(F_p) nicht zu klein werden darf).			

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
GS-A_5526	TLS-Renegotiation-Indication-Extension	Alle Produkttypen, die das TLS-Protokoll verwenden, SOLLEN den RFC 5746 (TLS-Renegotiation-Indication-Extension [RFC-5746]) unterstützen.	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test
GS-A_5541	TLS-Verbindungen als TLS-Klient zur Störungsampel oder SM	Alle Produkttypen, die das TLS-Protokoll als TLS-Klient zur Störungsampel oder zum Service-Monitoring verwenden, KÖNNEN (1) auf die explizite Prüfung, dass der TLS-Server die (EC)DH-Gruppe für den ephemeren (EC)DH-Schlüsselaustausch spezifikationskonform gewählt hat (vgl. GS-A_4384 und A_17124 Punkt 4), verzichten, und (2) davon ausgehen, dass der TLS-Server die Auswahl der TLS-Verbindungsparameter (TLS-Version, TLS-Ciphersuite etc.) korrekt, i.S.v. spezifikationskonform, durchführt.	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung
GS-A_5542	TLS-Verbindungen (fatal Alert bei Abbrüchen)	Alle Produkttypen, die das TLS-Protokoll verwenden, MÜSSEN sicherstellen, dass alle von ihnen durchgeführten Verbindungsabbrüche (egal ob im noch laufenden TLS-Handshake oder in einer schon etablierten TLS-Verbindung) mit einer im TLS-Protokoll aufgeführten Fehlermeldung (fataler Alert) angekündigt werden, außer das TLS-Protokoll untersagt dies	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
		explizit.			
GS-A_5580-01	TLS-Klient für betriebsunterstützende Dienste	Alle Produkttypen, die das TLS-Protokoll als TLS-Klient für Betriebsunterstützende Dienste (Service-Monitoring, Betriebsdaten-Erfassung etc.) verwenden, MÜSSEN das vom Betriebsunterstützenden Dienst präsentierte Zertifikat prüfen. Für diese Prüfung MUSS entweder TUC_PKI_018 oder die vereinfachte Zertifikatsprüfung (GS-A_5581 „TUC vereinfachte Zertifikatsprüfung“ (Komponenten-PKI)) verwendet werden.	gemSpec_Krypt	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung
A_20574	Beachtung der ISI-LANA für Übergänge zu Fremdnetzen	Zentrale Produkttypen SOLLEN für Übergänge zu Fremdnetzen die Empfehlungen der [BSI ISI-LANA] befolgen. Übergänge zum Transportnetz mittels SZZP-light und Sicherheitsgateway Bestandsnetze sind von dieser Regelung ausgenommen.	gemSpec_Net	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung

Afo-ID	Titel	Beschreibung	Quelle (Referenz)	altes Prüfverfahren	neues Prüfverfahren
GS-A_4763	Einsatz von Hochverfügbarkeitsprotokollen	Fachanwendungsspezifische Dienste und zentrale Dienste MÜSSEN bei Nutzung von Hochverfügbarkeitsprotokollen am Anschluss an das zentrale Netz TI durch geeignete Maßnahmen (z. B. Authentisierung der Kommunikationspartner) sicherstellen, dass andere Netzwerkkomponenten nicht beeinflusst werden.	gemSpec_Net	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test
GS-A_4640	Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung	Hersteller von Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der initialen Einbringung das aktuell gültige TSL-Signer-CA-Zertifikat eindeutig identifizieren und mittels Fingerprint validieren, bevor dieses Zertifikat als TI-Vertrauensanker in die Komponente eingebracht werden darf.	gemSpec_PKI	sicherheitstechnische Eignung: Produktgutachten	sicherheitstechnische Eignung: Herstellererklärung
GS-A_4643	TUC_PKI_013: Import TI-Vertrauensanker aus TSL	Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_013 zum Import neuer TI-Vertrauensanker umsetzen.	gemSpec_PKI	sicherheitstechnische Eignung: Produktgutachten	funktionale Eignung Test

© gematik – öffentlich_Entwurf