Elektronische Gesundheitskarte und Telematikinfrastruktur

Errata 1 zum Fachdienst KOM-LE

Version:	1.0.0
Stand:	02.10.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemErrata_1_KOM-LE]

betroffener Produkttyp	**neue Produkttypversion:**
gemProdT_CM_KOMLE	PTV1.2.2-0
gemProdT_FD_KOMLE	PTV1.2.3-0

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	**Anpassungen** an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6968	gemSpec_Krypt gemSpec_KT	GS-A_4386 GS-A_5530 TIP1-A_4962	**Abkündigung der Verwendung von TLS 1.1** Das TLS-Protokoll in der Version 1.1 verwendet beim Verbindungsaufbau das schwache Hash-Verfahren SHA-1. Aus diesem Grund wird das IETF die TLS Version 1.1 abkündigen [1]. Darüber hinaus haben die namenhaften Webbrowser-Hersteller angekündigt ab 2020 TLS 1.1 nicht mehr zu unterstützen [2]. Des Weiteren schätzt die gematik ein (nach aktuellen Gesprächen mit dem BSI zu dem Thema), dass das BSI in der nächsten Aktualisierung der für die TI normativen TR-03116-1 TLS Version 1.1 für die TI verbieten wird. Ziel der gematik ist es frühzeitig diese Entwicklung (Abkündigung von TLS 1.1) auch in der Spezifikation widerzuspiegeln. Primärsysteme können ab dem 01.04.2020 nicht mehr davon ausgehen, dass alle Konnektoren TLS in der Version 1.1 unterstützen. [1]: https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-05 [2]: https://blog.qualys.com/ssllabs/2018/11/19/grade-change-for-tls-1-0-and-tls-1-1-protocols	siehe Anlage C_6968	gemSpec_Krypt, gemSpec_KT, gemILF_PS, gemProdT_Intermediär_VSDM gemProdT_KSR gemProdT_ZeitD gemProdT_ZentrNetz gemProdT_VZD gemProdT_VPN_ZugD gemProdT_NamD gemProdT_SG_BestNetze gemAnbT_VPN_ZugD Produttypsteckbriefe von Konnektor + alle Dienste die TLS verwenden gemProdT_ePA-Modul_FdV gemProdT_KTR-AdV
C_7032	gemSpec_Krypt	Kap. 3.3.2	**Zulassung von TLS Version 1.3 per KANN-Anforderung** Als KANN-Anforderung wird TLS in der Version 1.3 für alle Produkttypen der TI zugelassen.	1) Es wird in Kap. 3.3.2 nach GS_4385 folgende neue Anforderung hinzufügt: "A_18467 - TLS-Verbindungen, Version 1.3 Alle Produkttypen, die Übertragungen mittels TLS durchführen, KÖNNEN die TLS-Version 1.3 [RFC-8446] unterstützen, falls 1. sie dabei nur nach [BSI-TR-02102-2] empfohlene Verbindungskonfigurationen (Handshake-Modi, (EC)DH-Gruppen, Signaturverfahren, Ciphersuiten etc.) verwenden, und 2. mindestens die Ciphersuite "TSL_AES_128_GCM_SHA256" dabei unterstützen. <=" 2) Die Afo A_17322 wird wegen der Hinzufügung von Version 1.3 erweitert: "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, Produttypsteckbriefe von Konnektor (PTV4) + alle Dienste die TLS verwenden gemILF_PS Änderung beschrieben in C_6968
C_7040	gemSpec_Perf	Anhang C	**Korrektur: Performance_Kennzahlen für KOM-LE** Bei den Performance-Kennzahlen für den KOM-LE-Fachdienst wurden falsche Schnittstellen definiert. Diese werden korrigiert.	Es werden folgende Werte in der Tabelle: Tab_gemSpec_Perf_Performance-Kenngroessen angepasst: PDT24-S17-D2-G27 -> PDT24-S01-D2-G27 PDT24-S17-D2-G03 -> PDT24-S01-D2-G03 PDT24-S17-D2-G28 -> PDT24-S01-D2-G28	gemSpec_Perf
C_7047	gemProdT_FD_KOMLE_PTV gemAnbT_FD_KOMLE_ATV	KOM-LE-A_2185 KOM-LE-A_2189 KOM-LE-A_2162 KOM-LE-A_2164 KOM-LE-A_2166	**KOM-LE Fachdienst - Falsche Zuordnung von Anforderungen zu Prüfverfahren** Sicherheitsrelevante Anforderungen aus der Spezifikation des Fachdienstes für KOM-LE wurden nicht dem Sicherheitsgutachten (oder in zwei Fällen nicht zumindest dem funktionalen Test) zugeordnet, sondern nur der Hersteller-/Anbietererklärung oder Test.	Fünf Anforderungen werden in den Steckbriefen (Anbieter und Produkt) einem anderen bzw. teilweise einem weiteren Prüfverfahren zugeordnet: KOM-LE-A_2185 - ProdT: SiGu statt HE ; AnbT: neu SiGu KOM-LE-A_2189 - ProdT: Test statt HE KOM-LE-A_2162 - ProdT: Test statt HE KOM-LE-A_2164 - ProdT: SiGu statt HE ; AnbT: neu SiGu KOM-LE-A_2166 - ProdT: SiGu zusätzlich zu Test ; AnbT: neu SiGu	gemProdT_FD_KOMLE_PTV gemAnbT_FD_KOMLE_ATV

Änderungen in [gemSpec_Krypt]

3.3.2 TLS-Verbindungen

GS-A_4385 - TLS-Verbindungen, Version 1.2
Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN die TLS-Version 1.2 [RFC-5246] unterstützen. <=

~~Nach [RFC-5246, Abschnitt 7.4.1.2] muss ein TLS-Client beim Aufbau einer TLS-Verbindung (Handshake) die höchste von ihm unterstützte Version, also Version 1.2, als „favorite choice“ angeben. Mit [RFC-5246, Abschnitt 7.4.1.3] muss ein TLS-Server mit der höchsten von beiden Kommunikationspartnern unterstützten Version antworten, also nach GS-A_4385 Version 1.2. Damit wird zwischen Komponenten und Diensten, die GS-A_4385 umsetzen, nur noch die TLS-Version 1.2 verwendet.~~

~~Mittelfristig wird eine vollständige Migration auf TLS Version 1.2 angestrebt (vgl. auch [BSI-TR-02102-2, Abschnitt 3.2]), d. h. außer für den Konnektor und das KOM-LE-CM (s. u. GS-A_5530) wird die grundsätzliche Unterstützung von TLS-Version 1.1 freigestellt, und in einer späteren Migrationsphase wird diese Unterstützung (bzw. die Verwendung) untersagt.~~

~~**GS-A_4386 - TLS-Verbindungen, optional Version 1.1**~~
~~Alle Produkttypen, die Übertragungen mittels TLS durchführen, KÖNNEN die TLS-Version 1.1 [RFC-4346] unterstützen (oder auch nicht).~~
<=

~~Da alle aktuellen Webbrowser (vgl. Übersicht unter https://www.ssllabs.com/ssltest/clients.html und https://en.wikipedia.org/wiki/Comparison_of_TLS_implementations) seit längerem TLS-Version 1.2 unterstützen ist eine Forderung der Unterstützung von TLS-Version 1.1 bei Diensten innerhalb der TI, die u. Um. von einem Primärsystem aus mittels eines Webbrowsers kontaktiert werden (bspw. VZD), nicht notwendig.~~

~~Komponenten, die direkt mit einem Primärsystem per TLS in Verbindung treten, sollen zunächst weiterhin die TLS-Version 1.1 unterstützen, um eine größtmögliche Interoperabilität zu erreichen.~~

~~**GS-A_5530 - TLS-Verbindungen, Version 1.1**~~
~~Der Konnektor und das KOM-LE-CM MÜSSEN die TLS-Version 1.1 unterstützen.~~<=

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.<=

GS-A_4387 - TLS-Verbindungen, nicht Version 1.0
Alle Produkttypen, die Übertragungen mittels TLS durchführen, DÜRFEN NICHT die TLS-Version 1.0 unterstützen.<=

[…]

Änderungen in [gemILF_PS]

In Kap. 4.1.1

TIP1-A_4962 - Nutzung von TLS-Authentisierungsmethoden

Das Primärsystem SOLL ~~gemäß TLS Version 1.2~~ die TLS-Authentisierungsmethoden der Stufen 2 oder 4 aus Tabelle Tab_ILF_PS_Konfigurationsvarianten_HTTP und Stufe 2 aus Tabelle Tab_ILF_PS_Konfigurationsvarianten_CETP verwenden, d. h. TLS mit Server-Authentisierung mit oder ohne Client-Authentisierung. ~~Solange der Konnektor TLS-Version 1.1 anbietet, kann das PS auch TLS-Version 1.1 verwenden.~~

Der Konnektor kann nur noch in den Produkttypversionen 1 und 2 die TLS-Version 1.1 anbieten. Nur mit diesen Produkttypversionen kann das PS auch TLS-Version 1.1 verwenden. Ab der Konnektor-Produkttypversion 3 bietet der Konnektor TLS nur noch gemäß TLS Version 1.2 oder 1.3 an. Ab PTV3 MUSS das PS für TLS-gesicherte Verbindungen TLS Version 1.2 verwenden, es KANN auch TLS Version 1.3 verwenden .

<=

Änderungen in [gemSpec_KT]

2.4.5.1 Sicherung der administrativen TLS-Verbindung

Nach [TIP1-A_3415] sind Netzwerkverbindungen grundsätzlich mit den in [gemSpec_Krypt] genannten Verfahren zu sichern. ~~Die Verbindung zu den Netzwerk-basierten Managementschnittstellen ist immer mit TLS 1.1 gemäß [RFC4346] zu sichern [gemSpec_Krypt#GS-A_4386]. Um die Zukunftsfä higkeit zu gewährleisten sollen sie auch mittels TLS 1.2 gemäß [RFC5246] gesichert werden können [gemSpec_Krypt#GS-A_4385].~~

TIP1-A_3231_01 - TLS-Verbindung: einseitige Authentisierung
Das eHealth-Kartenterminal MUSS als Authentisierungsverfahren für administrative TLS-Verbindungen ~~gemäß [GS-A_4386]~~ mindestens einseitige Authentisierung einsetzen.
<=

2.4.4 Sicherheitsanforderungen LAN-gekoppelter Terminals

(…)
Für die Sicherung der hierfür notwendigen Netzwerkkommunikation sind~~ist~~ für alle Kartenterminals die in [gemSpec_Krypt] genannten Verfahren ~~TLS 1.1 (Transport Layer Security) gemäß [RFC4346] [gemSpec_Krypt#GS-A_4386]~~ als einheitliches auf Zertifikaten basierendes Verfahren vorgegeben. ~~Um die Zukunftsfähigkeit zu gewährleisten, soll zusätz-lich auch TLS 1.2 gemäß [RFC5246] unterstützt werden [gemSpec_Krypt#GS-A_4385].~~
(…)