Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

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 .

<=