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.

Änderungsbedarf in gemSpec_Krypt

⌦ **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 ~~(die Störungsampel ist also TLS-Server)~~ verwenden, KÖNNEN

(1) auf die explizite Prüfung der vom TLS-Server gesendeten DH-Gruppe und des öffentlichen DH-Schlüssels des TLS-Servers verzichten (vgl. GS-A_4384, Spiegelstrich 3), und

(2) davon ausgehen, dass der TLS-Server die Auswahl der TLS-Ciphersuite korrekt, i.S.v. spezifikationskonform, durchführt. ⌫

⌦ **GS-A_5580 TLS-Klient zur Störungsampel oder zum SM (Zertifikatsprüfung)**

Alle Produkttypen, die das TLS-Protokoll als TLS-Klient zur Störungsampel oder zum Service Monitoring (die Störungsampel/der Service-Monitoring-Server ist also TLS-Server) verwenden, MÜSSEN das von der Störungsampel/SM 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. ⌫

Bei bestimmten Produkttypen, bspw. TSPs, beschränkt sich die Prüfung von Zertifikaten beim TLS-Verbindungsaufbau in Bezug auf die TI ausschließlich auf die Prüfung des Zertifikats der Störungsampel oder des Service Monitorings. Dafür ist der TUC_PKI_018 unangemessen leistungsstark und komplex. Deshalb wird folgend mit GS-A_5581 eine passgenauere Zertifikatsprüfung als Alternative definiert.

⌦ **GS-A_5581 „TUC vereinfachte Zertifikatsprüfung“ (Komponenten-PKI)**

Alle Produkttypen, die eine Zertifikatsprüfung konform zu in dieser Anforderung definierten „TUC vereinfachte Zertifikatsprüfung“ durchführen wollen, erreichen dies indem sie folgende Vorgaben erfüllen.

(1) Es MUSS einen Prozess geben der authentisch und integer die Komponenten-CA-Zertifikate der TI regelmäßig (mindestens einmal pro Monat) ermittelt. Diese sind Basis für die folgenden Prüfschritte.

(2) Es MUSS geprüft werden, ob im vom TLS-Server präsentierten Zertifikat der korrekte (i. S. v. vom TLS-Client erwartete) FQDN enthalten ist (bspw. monitoring-update.stampel.telematik).

(3) Es MUSS geprüft werden, ob das präsentierte Zertifikat per Signaturprüfung rückführbar ist zu einem der CA-Zertifikate aus (1).

(4) Es MUSS geprüft werden, ob das präsentierte Zertifikat zeitlich gültig ist.

Wenn einer der Prüfschritte aus (2) bis (4) fehlschlägt, MUSS der Verbindungsaufbau abgebrochen werden.

© gematik – öffentlich_Entwurf

Es gibt GS-A_5581 folgend in gemSpec_Krypt Anwendungshinweise.⌫

Als Hilfestellung: für die Umsetzung von GS-A_5581 Spiegelstrich (1) kann man bspw. folgende Maßnahmen wählen.

(a) Übergabe bei einem Vororttermin in der gematik,

(b) Regelmäßiger Download über https://download.tsl.ti-dienste.de/

(c) Verwendung einer dedizierten Software zum Download, Signaturprüfung und Auswertung der TI-TSL (es existiert dafür jeweils mindestens eine Open-Source-Lösung und eine kommerzielle Lösung)

(d) oder andere Lösung, die die Integrität und Authentizität der Zertifikate sicherstellt.

Ziel ist es, dass für die Verbindung zur Störungsampel oder zum Service Monitoring auch einfach verfügbare und einfach verwendbare HTTPS-Clienten wie wget oder curl verwendet werden können.

Unter der Annahme, dass

(a) im Verzeichnis /etc/TI-Komponten-CAs die in GS-A_5581 Punkt (1) aufgeführten Zertifikate liegen und

(b) die an die Störungsampel zu sendende Information (i. d. R. unsignierte XML-Daten) in der Datei SOAP_Daten liegen,

erfüllen folgende Aufrufe die Punkt (2)-(4) aus GS-A_5581.

I. `wget --ca-directory=/etc/TI-Komponten-CAs --post-file=SOAP_Daten https://monitoring-update.stampel.telematik:8443/I_Monitoring_Message`

II. `curl --capath /etc/TI-Komponten-CAs –d SOAP_Daten https://monitoring-update.stampel.telematik:8443/I_Monitoring_Message`

© gematik – öffentlich_Entwurf