
Inhaltsverzeichnis

| | |
|---|----------|
| 1 Änderungsbeschreibung..... | 2 |
| 2 Änderung bzgl. gemF_TI-Gateway..... | 3 |
| 2.1 Zugangsmodul..... | 3 |
| 2.2 Zugangsmodul..... | 3 |
| 2.3 Zugangsmodul..... | 3 |
| 2.4 Zugangsmodul..... | 4 |
| 2.5 Anbieter TI-Gateway - A_23487..... | 4 |
| 2.6 Anbieter TI-Gateway..... | 4 |
| 2.7 Anbieter TI-Gateway und Zugangsmodul..... | 5 |

1 Änderungsbeschreibung

Der Disclaimer zum Thema WireGuard als VPN-Protokoll beim Zugangsmodul wird entfernt, da eine Nutzung von WireGuard für diesen Einsatzzweck nach Analyse final als zulässig beschieden wurde.

Bzgl. der Verwendung von TLS für die geforderte VPN-Strecke wird klargestellt, dass die Anforderung aus [gemSpec_Krypt] gilt und die in [gemF_TI-Gateway] getroffenen Anforderungen sich auf IPsec und WireGuard beziehen.
(Änderung 2.1)

Es erfolgt eine Klarstellung, dass neben den Clientsystemschnittstellen (SOAP usw.) auch die KT-Schnittstelle (SICCT) nur aus dem Nutzernetz erreichbar sein darf, wie es auch im informativen Teil bereits festgelegt ist.
(Änderung 2.2)

Zudem werden einige Sicherheitsanforderungen (Zugangsmodul und Anbieter) entsprechend der Erfahrungen aus den ersten Umsetzungen und deren Begutachtung angepasst bzw. entfernt sowie auch zwei neue Anforderung aufgenommen.
(Änderungen 2.3 - 2.7)

2 Änderung bzgl. gemF_TI-Gateway

Im Folgenden jeweils [alt] und [neu] direkt untereinander:

2.1 Zugangsmodul

Entfernen WireGuard-Disclaimer und Klarstellung zu Vorgaben für TLS

Absatz 5.2 unterhalb von A_23379-01

[alt] Als Protokolle sind aktuell IPsec/IKEv2, TLS und WireGuard vorgesehen.

Eingerahmter Disclaimer darunter beginnend mit "Hinweis bzgl. WireGuard"

[neu] Bei Verwendung der von TLS zur Erfüllung von A_23379* gilt bzgl. kryptographischer Vorgaben [gemSpec_Krypt#A_24779*]. Die folgenden Anforderungen beziehen sich auf IPsec und WireGuard.

Disclaimer darunter wird ersatzlos gestrichen

2.2 Zugangsmodul

SICCT Protokoll zur Einschränkung bzgl. fachlichen Interface hinzufügen

[alt] **A_23394 - Routing zum fachlichen Interface einer HSK-Instanz**

Das TI-GW-Zugangsmodul MUSS sicherstellen, dass das fachliche Interface (SOAP, LDAP, CETP) einer HSK-Instanz nur aus dem Netz der zugeordneten LE-Institution möglich ist - also auch explizit nicht aus einem möglicherweise vom Leistungserbringer für die Administration freigegebenen DVO-Netz. <=

[neu] **A_23394-01 - Routing zum fachlichen Interface einer HSK-Instanz**

Das TI-GW-Zugangsmodul MUSS sicherstellen, dass das fachliche Interface (SOAP, LDAP, CETP, **SICCT**) einer HSK-Instanz nur aus dem Netz der zugeordneten LE-Institution möglich ist - also auch explizit nicht aus einem möglicherweise vom Leistungserbringer für die Administration freigegebenen DVO-Netz. <=

2.3 Zugangsmodul

Präzisierung / Klarstellung bzgl. Vorgehen bei "Komponentenausfall"

[alt] **A_23344 - TI-GW-Zugangsmodul - Verbindungen bei Komponentenausfall beenden**

Das TI-GW-Zugangsmodul MUSS sicherstellen, dass alle bestehenden VPN-Verbindungen beendet werden und keine neuen Verbindungen zugelassen werden, wenn nachgelagerte Komponenten vollständig ausgefallen sind und dadurch die Nutzung des TI-Gateways nicht mehr möglich ist. <=

[neu] **A_23344-01 - TI-GW-Zugangsmodul - Sicherer Zustand bei Komponentenausfall**

Das TI-GW-Zugangsmodul MUSS sicherstellen, dass **beim Ausfall von**

sicherheitsrelevanten Komponenten des Zugangsmoduls oder des Highspeed-Konnektors keine Zugriffe aus angeschlossenen Netzen auf die TI-Gateway-Services, für die die ausgefallenen Komponenten notwendig sind, mehr möglich sind, bspw. in dem alle Zugriffe durch eine Firewall blockiert oder alle VPN-Verbindungen getrennt werden. <=

2.4 Zugangsmodul

Aufnahme A_23364 in die AFO zum Sicherheitsnachweis für den VPN-Client (Der VPN-Client eines TI-Gateway-Zugangsmoduls MUSS den VPN-Server gegen eine ihm vorliegende Prüfbasis authentifizieren.)

[alt] **A_23365 - TI-Gateway-Zugangsmodul - VPN-Client - VPN-Protokoll**

Der Hersteller des VPN-Client eines TI-Gateway-Zugangsmoduls MUSS das VPN-Protokoll im Client entsprechend A_23375*, A_23376*, A_23377*, A_23378*, A_23379* und A_23381* umsetzen und dies im Rahmen des Sicherheitsnachweis (Produktgutachten) mindestens durch entsprechende Tests inkl. Negativ-Testfälle im Blackbox-Ansatz verifizieren lassen. <=

[neu] **A_23365-01 - TI-Gateway-Zugangsmodul - VPN-Client - VPN-Protokoll**

Der Hersteller des VPN-Client eines TI-Gateway-Zugangsmoduls MUSS das VPN-Protokoll im Client entsprechend A_23364*, A_23375*, A_23376*, A_23377*, A_23378*, A_23379* und A_23381* umsetzen und dies im Rahmen des Sicherheitsnachweis (Produktgutachten) mindestens durch entsprechende Tests inkl. Negativ-Testfälle im Blackbox-Ansatz verifizieren lassen. <=

2.5 Anbieter TI-Gateway - A_23487

Änderung Prüfverfahren

AFO-Text zur Info:

A_23487 - Aktualisierbarkeit von VPN-Clients

Der Anbieter des TI-Gateways MUSS Maßnahmen umsetzen, um die Aktualität der eingesetzten VPN-Clients und weiterer ggf. ausgelieferter Client-Software sicherzustellen. <=

[alt] Prüfverfahren: organ./betriebl. Eignung: Anbietererklärung

[neu] Prüfverfahren: Sich.techn. Eignung: Gutachten

2.6 Anbieter TI-Gateway

Entfernen von AFOs aus Anbietertypsteckbrief

[neu] Es werden die folgenden AFOs vom Anbietertyp entfernt: GS-A_4057-01, GS-A_4777-01, GS-A_4778-01 (jeweils aus gemSpec_Net)

2.7 Anbieter TI-Gateway und Zugangsmodul

[neu] *neue AFO + informativer Text*

AFO NEU - Technische Prüfung von Produkthanforderungen auch bei Umsetzung durch den Anbieter

Der Anbieter TI-Gateway und der Hersteller des Zugangsmoduls MÜSSEN, wenn Anforderungen, die grundsätzlich dem Produkt und dort dem Produktgutachten zugeordnet sind, nicht im Produkt, sondern durch den Anbieter umgesetzt werden, im Rahmen des Sicherheitsgutachtens des Anbieters oder im Rahmen des Produktgutachtens des Herstellers, den technischen Nachweis (Prüfmethode eines Produktgutachtens) zur Umsetzung dieser Anforderungen erbringen. Dieser Nachweis ist relevant für die Produktzulassung, welche dann nur anbieterspezifisch erteilt werden kann. <= (Anbieter:Sicherheitsgutachten; Zugangsmodul:Produktgutachten)

Grundsätzlich sind dem Produkt zugeordnete Anforderungen auch im Produkt umzusetzen. Das in der vorhergehenden Anforderung beschriebene Szenario stellt somit eine Ausnahme dar. In solchen Fällen muss der Hersteller für die Produktzulassungen benennen, welche Anforderungen nicht durch das Produkt, sondern durch die Betriebsumgebung des Anbieters zu erfüllen sind. Dafür muss dann der Nachweis der Umsetzung durch technische Prüfungen am Gesamtsystem (Produkt + Betriebsumgebung des Anbieters) erfolgen und mittels Gutachten bereitgestellt werden. Die Produktzulassung kann dementsprechend erst erteilt werden, wenn ein bestätigendes Gutachten vorgelegt wurde. Die Produktzulassung ist dann beschränkt auf die Betriebsumgebung, für die auch der Nachweis erbracht wurde und den zugehörigen Anbieter dieser Umgebung. Entsprechend müssen Änderungen an Komponenten der Betriebsumgebung wie Änderungen am Produkt behandelt werden. Sollten zu einem späteren Zeitpunkt weitere Anbieter das Produkt verwenden wollen, muss auch für deren Betriebsumgebung der technische Nachweis erbracht werden und die Produktzulassung würde dann im Positivfall auf diese Anbieter und deren Betriebsumgebung erweitert werden.