Änderung für Basis- und KTR-Consumer

1 Anforderungen aus gemSpec_HSMProxy

Die drei Anforderungen **A_17714, A_17715, A_17716** aus gemSpec_HSMProxy **werden von den Consumern gelöst, d.h, aus dem Produkttypsteckbrief des KTR- und Basis-Consumer entfernt**. Die Umsetzung eines solchen expliziten Proxys hat sich nicht als sinnvoll erwiesen.

Die gemSpec_HSMProxy wäre damit auch überflüssig, da sie genau nur diese drei AFOs enthält und neben den Consumern nur die KTR-AdV diesen AFOs zugewiesen war. Consumer sind mit diesem Change dann nicht mehr zugewiesen und die KTR-AdV wird nicht umgesetzt und vermutlich abgekündigt.

2 Anforderungen aus gemSpec_Basis_KTR_Consumer

Als Ersatz werden in gemSpec_Basis_KTR_Consumer entsprechend auf Consumer zugeschnittene Anforderungen hinzugefügt.

Folgende Anforderungen werden im Absatz 5.3 zwischen den bestehenden Anforderungen A_17598 und A_18195 eingefügt:

A_24024 - HSM - Sicherer Zugriff auf Identitäten
Der Basis- und KTR-Consumer MUSS private Schlüssel der TI-Identitäten der Nutzer des Consumers im HSM eindeutig referenzieren und durchsetzen, dass Nutzer des Consumers jeweils genau nur Ihre Identitäten (private Schlüssel) verwenden können.**[**<=**]**

A_24025 - Authentisierte, vertrauliche und integritätsgeschützte Kommunikation
Der Basis- und KTR-Consumer MUSS durchsetzen, dass Operationsaufrufe zu einem HSM nur nach Authentisierung gegenüber dem HSM und unter Wahrung von Vertraulichkeit und Integrität stattfinden, sodass Unberechtigte weder Schlüssel auf dem HSM nutzen können, noch die Kommunikation mit dem HSM abhören oder manipulieren können. Die Maßnahmen dienen primär dem sicheren Betrieb des HSMs, MÜSSEN aber ebenso eine sichere Personalisierung (A_17599*) ermöglichen bzw. unterstützen.**[**<=**]**

2.1 Anforderungen bzgl. Firewall und Routing

Die Anforderungen zur Routing und Firewall als verpflichtender Teil des Produkts haben sich nicht als sinnvoll erwiesen. Diese Leistungen sind notwendig und werden auch umgesetzt jedoch durch den Betreiber als Umgebungsleistung. Dem wird Rechnung getragen, indem die Anforderungen entsprechend angepasst und neu zugeordnet werden.

A_17397 wird ersetzt durch A_173974-01:

A_17397-01 - IP-Pakete mit Source Route Option
Der Basis- und KTR-Consumer als Produkt oder dessen Anbieter über die Betriebsumgebung MUSS durchsetzen, dass nicht ~~DARF NICHT~~ IP-Pakete mit gesetzter Source Route Option gemäß [RFC791] erzeugt ~~en~~ oder weitergeleitet~~n~~ werden. In beiden Sicherheitsnachweisen muss klar dargestellt werden, wo die Sicherheitsleistung umgesetzt ist.
[<=]

fkt. Eig. HE, ProGu, SiGu(Anbieter)

A_17400-01 wird ersetzt durch A_17400-02:

A_17400-02 - NAT-Umsetzung
Der Basis- und KTR-Consumer als Produkt oder dessen Anbieter über die Betriebsumgebung MUSS für die Kommunikation mit Adressbereichen der TI sowie WANDA Basic und WANDA Smart eine Network Address Translation (NAT) gemäß [RFC3022#2.2, 3, 4.1-4.3] vornehmen. Für die Umsetzung der Private Local Address aus den Adressbereichen der Einsatzumgebung MUSS die verwendete IP-Adresse aus dem vom Anbieter Zentrale Plattform Dienste (AZPD) bereitgestellten Adress-Pool entnommen werden und als Global Address genutzt werden.**[<=]**

~~ProGu~~ fkt. Eig. Test, Betriebshandbuch

=> funktionale Anforderung

A_17405 wird ersetzt durch A_17405-01:

A_17405-01 - Nur IPv4. IPv6 nur hardwareseitig vorbereitet
Der Basis- und KTR-Consumer als Produkt oder dessen Anbieter über die Betriebsumgebung MUSS die IP Version 4 (IPv4) für alle seine IP-Schnittstellen unterstützen. Die eingesetzte Hardware~~des Basis- und KTR-Consumer~~ MUSS für den Einsatz von IPv4 und IPv6 im Dual-Stack-Mode geeignet sein. Bis zu einer Migration von IPv4 auf IPv6 MUSS der Basis- und KTR-Consumer als Produkt oder dessen Anbieter über die Betriebsumgebung sämtliche empfangenen IP-Pakete der Version 6 (IPv6) verwerfen. In beiden Sicherheitsnachweisen muss klar dargestellt werden, wo die Sicherheitsleistung umgesetzt ist.**[<=]**

fkt. Eig. HE, ProGu, SiGu(Anbieter)

A_17406 wird ersetzt durch A_17406-01:

A_17406-01 - Kein dynamisches Routing
Basis- und KTR-Consumer als Produkt oder dessen Anbieter über die Betriebsumgebung MUSS durchsetzen, dass nicht ~~DÜRFEN NICHT~~ Dynamische Routing-Protokolle eingesetzt ~~en~~ werden. In beiden Sicherheitsnachweisen muss klar dargestellt werden, wo die Sicherheitsleistung umgesetzt ist. **[<=]**

ProGu, SiGu(Anbieter)

A_17411 wird ersetzt durch A_17411-01:

A_17411-01 - Kommunikation mit NET_TI_Offene_FD
Der Basis- und KTR-Consumer als Produkt oder dessen Anbieter über die Betriebsumgebung MUSS sicherstellen, dass IP-Pakete mit dem Ziel NET_TI_Offene_FD und NET_WANDA_Smart weitergeleitet werden.**[<=]**

~~ProGu~~ fkt. Eig. Test, Betriebshandbuch

=> funktionale Anforderung

A_17514 wird ersetzt durch A_17514-01:

A_17514-01 - Kommunikation mit NET_TI_Gesicherte_FD
Der KTR-Consumer als Produkt oder dessen Anbieter über die Betriebsumgebung MUSS sicherstellen, dass IP-Pakete mit dem Ziel NET_TI_Gesicherte_FD nur durch das im KTR-Consumer vorhandene jeweilige Fachmodul in Richtung TI mit dem Ziel NET_TI_Gesicherte_FD weitergeleitet werden. In beiden Sicherheitsnachweisen muss klar dargestellt werden, wo die Sicherheitsleistung umgesetzt ist.**[<=]**

ProGu, SiGu(Anbieter)

A_17415 wird ersetzt durch A_17415-01:

A_17415-01 - Kommunikation mit NET_TI_ZENTRAL
Der Basis- und KTR-Consumer als Produkt oder dessen Anbieter über die Betriebsumgebung MUSS sicherstellen, dass IP-Pakete in Richtung NET_TI_ZENTRAL ~~mit dem Ziel TI-Namens- und Zeitdienst nur~~ ausschließlich vom Basis- und KTR-Consumer ausgehen~~ weitergeleitet werden~~. In beiden Sicherheitsnachweisen muss klar dargestellt werden, wo die Sicherheitsleistung umgesetzt ist.**[<=]**

ProGu, SiGu(Anbieter)

A_21998 wird ersetzt durch A_21998-01:

A_21998-01 - Kommunikation mit NET_WANDA_Basic
Der Basis- und KTR-Consumer als Produkt oder dessen Anbieter über die Betriebsumgebung MUSS sicherstellen, dass IP-Pakete mit dem Ziel NET_WANDA_Basic weitergeleitet werden.**[<=]**

~~ProGu~~ fkt. Eig. Test, Betriebshandbuch

=> funktionale Anforderung

A_17417 wird ersetzt durch A_17417-01:

A_17417-01 - Einschränkung von nicht genehmigten Traffic
Der Basis- und KTR-Consumer als Produkt oder dessen Anbieter über die Betriebsumgebung MUSS nicht genehmigten Traffic blockierenund dabei folgendes umsetzen:

- "default deny"
- Einschränkung auf IP-Protokolle 1 (ICMP; eingeschränkt auf Typ 8 und Typ 0 und ausschließlich für, per Anforderung genehmigten, Traffic), 17 (UDP) und 6 (TCP)
- Einschränkung auf genau nur die Ports die für den Betrieb unerlässlich sind

- abgelehnten IP-Pakete verwerfen (DROP), ohne ein ICMP-Destination-Unreachable (Type 3) zu schicken
- Maßnahmen zur Erkennung und Behebung unberechtigter oder verdächtiger Netzwerkaktivitäten (bspw. über Korrelation und Auswertung von Log-Daten).

In beiden Sicherheitsnachweisen muss klar dargestellt werden, wo die Sicherheitsleistung umgesetzt ist.
[<=]

ProGu, SIGu(Anbieter)

Die Anforderung A_17418 wird entfernt:

~~**A_17418 - Drop statt Reject**~~
~~Der Basis- und KTR-Consumer MUSS alle abgelehnten IP-Pakete verwerfen (DROP), ohne ein ICMP-Destination-Unreachable (Type 3) zu schicken.~~
~~**ProGu <=**~~

=> A_17417

Die Anforderung A_17419 wird entfernt:

~~**A_17419 - Abwehr von IP-Spoofing, DoS/DDoS-Angriffe und Martian Packets**~~
~~Der Basis- und KTR-Consumer MUSS geeignete technische Funktionen zur Abwehr von IP-Spoofing und DoS/DDoS-Angriffen implementieren.~~
~~Der Basis- und KTR-Consumer MUSS Martian Packets (Absender- oder Empfängeradressen aus den von der IETF als Special-Purpose definierten Netzbereichen), mindestens jedoch aus folgenden Netzbereichen 0.0.0.0/8, 127.0.0.0/8, 169.254.0.0/16, 192.0.0.0/24, 192.0.2.0/24, 198.18.0.0/15, 198.51.100.0/24, 203.0.113.0/24, 224.0.0.0/4, 240.0.0.0/4, verwerfen. Die in [RFC1918] und [RFC 6598] definierten Netzbereiche sind hiervon ausgenommen.~~
~~**ProGu <=**~~

=> verallgemeinert in A_17417 (unberechtigte/verdächtige Netzaktivitäten)

Die Anforderung A_17420 wird entfernt:

~~**A_17420 - Eingeschränkte Nutzung von „Ping“**~~
~~Der Basis- und KTR-Consumer MUSS TCP-Port-7(Echo)-Pakete verwerfen.~~
~~Der Basis- und KTR-Consumer MUSS ICMP-Echo-Request (Typ 8) und ICMP-Echo-Response (Typ 0) ausschließlich für, per Anforderung genehmigten, Traffic weiterleiten.~~
~~**ProGu <=**~~

=> A_17417

Die Anforderung A_17421 wird entfernt:

~~**A_17421 - Einschränkungen der IP-Protokolle**~~
~~Der Basis- und KTR-Consumer MUSS alle IP-Protokolle außer 1 (ICMP), 17 (UDP) und 6 (TCP) für alle ein- oder ausgehenden Pakete an allen seinen Adaptern verwerfen.~~
~~**ProGu <=**~~

=> A_17417

Die Anforderung A_17423 wird entfernt:

~~**A_17423 - Firewall Restart**~~
~~Der Basis- und KTR-Consumer MUSS gewährleisten, dass unmittelbar nach einer Änderung der Parameter eines Adapters (LAN-Adapter, WAN-Adapter) die Firewall des Basis- und KTR-Consumer neu erstellt und geladen wird.~~
~~**ProGu** <=~~

~~Umsetzungshinweis für den Hersteller: Es können zwei getrennten Firewall-Regelsets für den LAN- bzw. für den WAN-Adapter verwendet werden.~~

=> entfällt ersatzlos, da kein Thema für moderne Firewall-Lösungen

A_17424 wird ersetzt durch A_17424-01:

A_17424-01 - Firewall-Protokollierung
Der Basis- und KTR-Consumer als Produkt oder dessen Anbieter über die Betriebsumgebung MUSS an der Firewall folgende Aktivitäten nachvollziehbar protokollieren:

- ~~bei~~ Konfigurationsänderungen der Firewall ~~einen Protokolleintrag mit der Schwere „Warning" und dem Typ „Operations" sowie mindestens folgenden Informationen generieren:~~
- Zeitstempel, Aktion (Add/Delete/Change), Details (Beschreibung der Änderung), Auslöser (Prozess/User).

~~Der Basis- und KTR-Consumer MUSS für alle vom Basis- und KTR-Consumer ausgehenden, nicht zugelassenen Kommunikationsversuche einen Protokolleintrag mit der Schwere „Warning" und dem Typ „Security" sowie mindestens folgenden Informationen generieren:~~

- ~~Zeitstempel, Aktion (Drop, Reject), Absender-IP-Adresse, Empfänger-IP-Adresse, Protokoll, Absender-Port und Empfänger-Port, Interface, über die das Paket empfangen wurde.~~

~~Der Basis- und KTR-Consumer MUSS für alle verworfenen IP-Spoofing- und Martian-Packets einen Protokolleintrag mit der Schwere „Warning" und dem Typ „Security" sowie mindestens folgenden Informationen generieren:~~

- ~~Zeitstempel, Aktion (Drop, Reject), Absender-IP-Adresse, Empfänger-IP-Adresse, Protokoll, Absender-Port und Empfänger-Port, Interface über das das Paket empfangen wurde.~~
- ~~Der Basis- und KTR-Consumer MUSS für alle weiteren~~ von der Firewall verworfenen IP-Paketen~~einen Protokolleintrag mit der Schwere „Info" und dem Typ „Security" sowie mindestens folgenden Informationen generieren~~, wobei Layer 3 Broadcasts von der Protokollierung ausgenommen werden können~~:~~
- ~~Zeitstempel, Aktion (Drop, Reject), Absender-IP-Adresse, Empfänger-IP-Adresse, Protokoll, Absender-Port und Empfänger-Port, Interface über das das Paket empfangen wurde~~.

In beiden Sicherheitsnachweisen muss klar dargestellt werden, wo die Sicherheitsleistung umgesetzt ist.

[<=]

ProGu, SiGu(Anbieter)

=> Vereinfachung, da bisher über-reguliert

2.2 Anforderungen zu KIM-CM-Schlüsseln

In der Spezifikation gibt es eine unnötige und nicht sinnvolle direkte Verknüpfung der Personalisierung des HSM und der Speicherung von KIM-CM-Schlüsseln im HSM. Auf die KIM-CM-Schlüssel hat der Betreiber keinen Einfluss, weshalb dies aus dem Thema Personalisierung gelöst werden soll. Eine Speicherung der KIM-CM-Schlüssel in einem HSM ist dennoch sinnvoll, sofern das HSM sowieso vorhanden ist, da im Consumer-Umfeld keine Karten verwendet werden.

Tabelle 7: Tab_Personalisierung_HSM – Personalisierung des HSM

Aspekt	Beschreibung
Schlüsselmaterial der SMC-B	Das Schlüsselmaterial wird sicher im HSM erzeugt. Das private Schlüsselmaterial verlässt das HSM nicht oder nur zum Zwecke eines Backups auf einem Backup-HSM, wobei die Übertragung hinsichtlich Vertraulichkeit geschützt sein muss.
Zertifikatsrequest	Die benötigten Zertifikatsrequests werden im HSM erzeugt und exportiert. Die Zertifikatsrequests werden unter Wahrung der Authentizität und Integrität dem TSP übermittelt.
Zertifikat	Das Zertifikat wird vom TSP zum Betreiber übermittelt.
~~TLS-Schlüsselmaterial des KOM-LE-Clientmoduls~~	~~Der KOM-LE-Anbieter erzeugt die Schlüsselpaare für die Zertifikate des KOM-LE-Clientmoduls und bezieht aus der Komponenten-PKI der TI die C.CM.TLS-CS-Zertifikate. Das Schlüsselpaar muss zur sicheren Speicherung ins HSM eingebracht werden.~~

Hinweis:

- Ein Basis-Consumer für Leistungserbringerorganisationen verwendet SMC-B-ORG Schlüsselmaterial gemäß [gemSpec_PKI#10.7].
- Ein Basis-Consumer für Kostenträger verwendet SMC-B-KTR Schlüsselmaterial gemäß [gemSpec_PKI#10.4].
- Ein KTR-Consumer verwendet SMC-B-KTR Schlüsselmaterial gemäß [gemSpec_PKI#10.4] mit der Profession „oid_epa_ktr".
- Ein KTR-Consumer benötigt das Schlüsselmaterial der Profession „oid_kostentraeger" nicht.

A_17599 - Personalisierung des HSM

Der Anbieter des Basis- oder KTR-Consumers MUSS einen sicheren Prozess zur Personalisierung des HSMs definieren und etablieren, der die in Tab_Personalisierung_HSM genannten Aspekte beinhaltet.
<=

Neue Anforderung A_24026

A_24026 - Der Anbieter des Basis- oder KTR-Consumers SOLL private Schlüssel für KIM-CM-TLS...
Der Anbieter des Basis- oder KTR-Consumers SOLL private Schlüssel für KIM-CM-TLS-Zertifikate vor unberechtigtem Zugriff geschützt im HSM (siehe A_17598*) speichern, nachdem er sie vom KIM-Anbieter erhalten hat.
[<=]

SiGu(Anbieter) <=

Darunter folgender Informationstext:

Eine Abweichung von Anforderung A_XNEUX* ist gestattet für den Fall, dass entsprechend A_18195* kein HSM eingesetzt wird.