1 Änderungsbedarf: RSA/ECC-Registrierung von Konnektoren am VPN-Zugangsdienst

Aktuell sind alle im Feld befindlichen Konnektoren mir RSA-Zertifikaten bei ihren jeweiligen VPN-Zugangsdiensten registriert.
Bei jedem Verbindungsaufbau des Konnektors mit einem VPN-Konzentrator wird das gSMC-K-Zertifikat C.NK.VPN als Bestandteil der Kundenidentifikation durch den Autorisierungsserver des VPN-Zugangsdienstes geprüft.
Seit November 2020 sind Konnektoren mit dual-personalisierten gSMC-Ks im Feld. Der Konnektor besitzt dann zwei NK-Entitäten, bzw. die zwei Zertifikate RSA-C.NK.VPN und ECC-C.NK.VPN. Somit kann der Konnektor zwei unterschiedliche Zertifikate für jede Interaktion mit dem VPN-Zugangsdienst (Registrierung, Autorisierung) nutzen.
Ein Verbindungsaufbau mittels ECC-Zertifikat zwischen Konnektor und VPN-Zugangsdienst kann nur erfolgen, wenn zuvor das ECC-NK-Zertifikat der gSMC-K auch beim VPN-ZugD registriert wurde.

Allerdings ist bisher nicht festgelegt, wie der Ablauf der Registrierung mit ECC-Zertifikaten beim Registrierungsserver des VPN-Zugangsdienstes konkret erfolgen soll. Das wird mit diesem Änderungseintrag nachgeholt.
Wichtig ist, dass eine automatisierte Migration von RSA- auf ECC-Verwendung sichergestellt wird. Zudem soll die Migration der Authentisierung auf der IPsec-Strecke möglichst unverzüglich erfolgen, sobald sowohl ein Konnektor als auch der verwendete VPN-Zugangsdienst technisch dafür gerüstet sind.

2 Änderung: IKE-Verbindungsaufbau als Sonde

Die Anforderungen aus dem [gemSpec_Krypt#5.5], die festlegen, dass die Konnektoren ab PTV5 immer einen Verbindungsaufbau mit ECC versuchen müssen und im Negativ-Fall auf RSA zurückfallen, werden modifiziert.
Statt dessen merkt sich der Konnektor, welche Zertifikate beim VPN-ZugD registriert wurden. Solange nur RSA registriert wurde, wird der Verbindungsaufbau mit RSA durchgeführt. Erst wenn ECC registriert wurde, wird ECC verwendet.

Dazu soll ein Konnektor, der ECC für IPsec unterstützt aber noch ausschließlich mit dem RSA-NK-Zertifikat registriert ist, zweiwöchentlich beim IKE-Verbindungsaufbau-Versuch sein ECC-Zertifikat präsentieren.
Es wird das in [gemSpec_Krypt#5.5] beschriebene Vorgehen vorausgesetzt: Eine INVALID_KE_PAYLOAD-Nachricht gilt dabei als Signal, dass der VPN-Zugangsdienst ECC noch nicht unterstützt.

Wenn der VPN-Zugangsdienst signalisiert, dass er ECC auf der IPsec-Strecke unterstützt, soll der Konnektor die Registrierung mit seinem ECC-NK-Zertifikat beim VPN-Zugangsdienst automatisiert vornehmen. Ab dem Zeitpunkt der erfolgreichen Registrierung mit dem ECC-Zertifikat muss dann ausschließlich das ECC-NK-Zertifikat für IPsec verwendet werden.

Wenn der VPN-Zugangsdienst signalisiert, dass ECC auf der Strecke nicht unterstützt wird, darf der Konnektor beim IKE-Verbindungsaufbau weiterhin RSA verwenden.

Option :
Alternativ kann ein Konnektor, sobald er ECC für IPSec unterstützt, eine zusätzliche Registrierung mit dem ECC-Zertifikat vornehmen (also ohne De-Registrierung des RSA-Zertifikats), wenn dies der zugehörige VPN-Zugangsdienst unterstützt.

Offen:
Wechsel des VPN-Zugangsdienstanbieters nach ECC-Migration zu einem noch nicht ECC-vorbereiteten VPN-Zugangsdienst.

2.1 Änderung in gemSpec_Krypt

Das Kapitel 5.5 "ECC-Unterstützung bei IPsec" wird angepasst:

..... ~~Da davon auszugehen ist, dass alle VPN-Zugangsdienste rein technisch die mit ☐*ML-92705 - Missing cross-reference*~~ ~~geforderten Algorithmen schon beherrschen, wird es wahrscheinlich in der Praxis selten ein "Zurückfallen" geben.~~

A_22342 - Konnektor, IKE-Schlüsselaushandlung – Erleichterung Migrationsphase 1 (ECC-Migration)
Solange ein Konnektor nur mit einem RSA-Zertifikat am VPN-Zugangsdienst registriert ist, KANN der Konnektor den IKE-Verbindungsaufbau gemäß der Vorgaben aus GS-A_4382 durchführen. **[<=]**

A_22343 - Konnektor, IKE-Schlüsselaushandlung – Erleichterung Migrationsphase 2 (ECC-Migration)
Solange ein Konnektor nur mit einem RSA-Zertifikat am VPN-Zugangsdienst registriert ist, MUSS der Konnektor mindestens zweiwöchentlich den IKE-Verbindungsaufbau gemäß der Vorgaben aus A_17125 durchführen.
[<=]

2.2 Änderung in gemSpec_Kon

Das Kapitel 4.3.8 " Re-Registrierung des Konnektors mit neuem NK-Zertifikat" wird erweitert:

Am Anfang des Kapitel wird eingefügt:

Eine Re-Registrierung eines Konnektors am VPN-Zugangsdienst mit einem neuen NK-Zertifikat wird im Rahmen von Laufzeitverlängerung von gSMC-K-Zertifikaten mit einem erneuerten, verlängerten Zertifikat oder im Kontext der ECC-Migration der IPsec-Kommunikation zum VPN-Zugangsdienst mit einem ECC-Zertifikat notwendig.

A_22332 - Re-Registrierung mit ECC-NK-Zertifikat automatisch durchführen (ECC-Migration)
Sobald der Konnektor im Rahmen eines Verbindungsaufbau-Versuchs entsprechend A_22343 feststellt, dass der VPN-Zugangsdienst ECC-fähig ist, MUSS der Konnektor eine Re-Registrierung mit dem ECC-Zertifikat beim Registrierungsdienst des VPN-Zugangsdienstes durchführen. **[<=]**

A_21758-02 - TUC_KON_411 „Konnektor mit neuem NK-Zertifikat registrieren“
Der Konnektor MUSS den technischen Use Case TUC_KON_411 "Konnektor mit neuem NK-Zertifikat registrieren" umsetzen.

Tabelle 1: TAB_KON_932 – TUC_KON_411 „Konnektor mit neuem NK-Zertifikat registrieren“

Element	Beschreibung
Name	TUC_KON_411 "Konnektor mit neuem NK-Zertifikat registrieren"
Beschreibung	Dieser TUC führt eine Deregistrierung mit dem alten und eine Neuregistrierung mit dem neuen NK-Zertifikat durch.
Auslöser	A_21745, A_22332, Administrator
Vorbedingungen	Keine
Eingangsdaten	Keine

Komponenten	Konnektor, VPN-ZugD
Ausgangsdaten	Keine

Standardablauf	1. Der Konnektor ermittelt die URI des Registrierungsservers (MGM_ZGDP_REGSERVER) durch eine DNS-Anfrage nach dem SRV und TXT Resource Record „_regserver._tcp.<DNS_DOMAIN_VPN_ZUGD_INT>".
	2. Der Konnektor MUSS eine deRegisterKonnektorRequest-Struktur gemäß [gemSpec_VPN_ZugD] erstellen und mit den entsprechenden Parametern befüllen (aktuelles Datum/Uhrzeit, bei der letzten erfolgreichen Registrierung verwendetes C.NK.VPN-Zertifikat, MGM_ ZGDP_CONTRACTID).
	Der Konnektor MUSS die Request-Nachricht mittels einer verfügbaren SM-B (ID.HCI.OSIG) im Element deRegisterKonnektorRequest/Signature signieren. (MGM_ ZGDP_SMCB ist zu bevorzugen, es kann aber auch eine andere SM-B verwendet werden).
	3. Der Konnektor ruft unter Verwendung der erzeugten Request-Nachricht die in [gemSpec_VPN_ZugD#Tab_ZD_deregisterKonnektor] definierte Operation I_Registration_Service::deRegisterKonnektor mit der Zieladresse MGM_ZGDP_REGSERVER auf.
	Der Response der Operation wird verarbeitet:
	a. Setze MGM_TI_ACCESS_GRANTED auf
	- Enabled, wenn /RegistrationStatus = „Registriert"
	- Disabled, wenn /RegistrationStatus = „Nicht registriert"
	b. Persistiere diese Zustandsinformation zusammen mit dem Zeitpunkt
	c. Verteile das folgende Ereignis über TUC_KON_256: {
	topic = "MGM/TI_ACCESS_GRANTED";
	eventType = Op;
	severity = Info;
	parameters = „Active=$MGM_TI_ACCESS_GRANTED";
	doLog = true;
	doDisp=true }
	4. Der Konnektor MUSS eine registerKonnektorRequest-Struktur gemäß ProvisioningService.xsd [gemSpec_VPN_ZugD] erstellen und mit den entsprechenden Parametern befüllen (aktuelles Datum/Uhrzeit, ~~erneuertes~~ neues C.NK.VPN-Zertifikat, MGM_ ZGDP_CONTRACTID). Der Konnektor MUSS die

	Request-Nachricht mittels der ausgewählten SM-B (ID.HCI.OSIG) im Element registerKonnektorRequest/Signature signieren und das SM-B-Zertifikat im Element X509Data ablegen.
	5. Der Konnektor ruft unter Verwendung der erzeugten Request-Nachricht die in [gemSpec_VPN_ZugD#Tab_ZD_registerKonnektor] definierte Operation I_Registration_Service::registerKonnektor mit der Zieladresse MGM_ZGDP_REGSERVER auf.
	Der Response der Operation wird verarbeitet:
	a. Setze MGM_TI_ACCESS_GRANTED auf
	- Enabled, wenn /RegistrationStatus = „Registriert"
	- Disabled, wenn /RegistrationStatus = „Nicht registriert"
	b. Persistiere diese Zustandsinformation zusammen mit dem VPN:ContractStatus
	c. Verteile das folgende Ereignis über TUC_KON_256
	{
	topic = "MGM/TI_ACCESS_GRANTED";
	eventType = Op;
	severity = Info;
	parameters = „Active=$MGM_TI_ACCESS_GRANTED";
	doLog = true;
	doDisp = true }

Varianten/Alternativen	Automatische Registrierung: (->5) Wenn der Konnektor nicht mit dem neuen C.NK.VPN-Zertifikat registriert werden konnte, dann muss sich der Konnektor, beginnend mit Schritt 4, erneut mit dem alten C.NK.VPN-Zertifikat registrieren. Manuelle Registrierung: (->2) Der Administrator soll die zu verwendende SM-B auswählen können.

Fehlerfälle	(→ 2,4) Es konnte keine freigeschaltete SM-B ausgewählt werden:
	Fail=No_Smcb
	(->4,5) Im Fehlerfall
	TUC_KON_256 {
	topic = „SMC_K/REGISTER/ERROR";
	eventType = Op;
	severity = Error;
	parameters = „$Parameters";
	doLog = true;
	doDisp = true }
	Die Registrierung soll herstellerspezifisch erneut mehrmals versucht werden.
	Bei allen Fehlerfällen, die zum Abbruch führen:
	TUC_KON_256 {
	topic = „SMC_K/REGISTER/ERROR";
	eventType = Op;
	severity = Error;
	parameters = „$Parameters";
	doLog = true;
	doDisp = true }

Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 2: Tab_Kon_933 Fehlercodes TUC_KON_411 „Zertifikate aktualisieren"

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
herstellerspezifisch			

[<=]

Änderungen in gemProdT_Kon_PTV5

Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)

A_22332	Re-Registrierung mit ECC-NK-Zertifikat automatisch durchführen (ECC-Migration)	gemSpec_Kon
A_22342	Konnektor, IKE-Schlüsselaushandlung – Erleichterung Migrationsphase 1 (ECC-Migration	gemSpec_Krypt
A_22343	Konnektor, IKE-Schlüsselaushandlung – Erleichterung Migrationsphase 2 (ECC-Migration)	gemSpec_Krypt
A_21758-02	TUC_KON_411 „Konnektor mit neuem NK-Zertifikat registrieren“	gemSpec_Kon
A_21758-01	TUC_KON_411 „Konnektor mit neuem NK-Zertifikat registrieren“	gemSpec_Kon