

1.1.1 Änderungen in gemSpec_Krypt

1.1.1.1 5.5 ECC-Unterstützung bei IPsec

Abgelöst

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.

[<=]

Neu

A_22343-01 - Verwendung von ECC beim Verbindungsaufbau nach RE-Registrierung mit ECC-NK-Zertifikat (ECC-Migration)

Sobald der Konnektor mit einem ECC-Zertifikat am VPN-Zugangsdienst registriert ist, MUSS er den nächsten regulären Verbindungsaufbau zum VPN-Konzentrator gemäß der Vorgaben aus A_17125 durchführen.

[<=]

1.1.2 Änderungen in gemSpec_Kon

1.1.2.1 4.3.7 Online-Anbindung verwalten

Abgelöst

TIP1-A_4826 - Status Konnektorfreischaltung einsehen

Der Administrator MUSS über die Managementschnittstelle den aktuellen Freischaltstatus einsehen können (MGM_TI_ACCESS_GRANTED). Ist der Konnektor aktuell freigeschaltet, so MUSS ihm dies zusammen mit dem VPN:ContractStatus angezeigt werden.

[<=]

Neu

TIP1-A_4826-01 - Status Konnektorfreischaltung einsehen

Der Administrator MUSS über die Managementschnittstelle den aktuellen Freischaltstatus einsehen können (MGM_TI_ACCESS_GRANTED). Ist der Konnektor aktuell freigeschaltet, so MÜSSEN der VPN:ContractStatus, die für die Freischaltung verwendete(n) SMC-B und die verwendeten C.NK.VPN-Zertifikate angezeigt werden (RSA und/oder ECC).

[<=]

Abgelöst

A_22332 - Re-Registrierung mit ECC-NK-Zertifikat automatisch durchführen (ECC-Migration)

Sobald der VPN-Zugangsdienst beim Verbindungsaufbau mit dem Konnektor entsprechend A_22343 die Verwendung von ECC-Algorithmen akzeptiert, MUSS der Konnektor die Re-Registrierung mit seinem ECC-NK-Zertifikat beim Registrierungsdienst des VPN-Zugangsdienstes durchführen.[<=]

Neu

A_22332-01 - Re-Registrierung mit ECC-NK-Zertifikat automatisch durchführen (ECC-Migration)

Solange der Konnektor nur mit einem RSA-Zertifikat am VPN-Zugangsdienst registriert ist, MUSS er mindestens einmal wöchentlich die Re-Registrierung mit seinem ECC-NK-Zertifikat beim Registrierungsdienst durchführen. [<=]

Neu

A_23120 - Beschränkung der Anfragen zur Re-Registrierung (ECC-Migration)

Der Konnektor DARF die automatische Re-Registrierung mit seinem ECC-NK-Zertifikat NICHT öfter als einmal am Tag versuchen. [<=]

Neu

A_23150 - Konnektor (wiederholt) manuell registrieren

Der Konnektor MUSS dem Administrator über den Mechanismus in TUC_KON_411 ermöglichen, den Konnektor zu registrieren bzw. eine vorhandene Registrierung zu aktualisieren. Dabei MUSS der Administrator das für die Registrierung zu verwendende NK-Zertifikat (RSA oder ECC) und die zu verwendende SMC-B auswählen können. [<=]

Neu

A_23122 - Konfigurationsschalter für automatische Re-Registrierung (ECC-Migration)

Der Konnektor MUSS dem Administrator ermöglichen, die automatische Re-Registrierung mit dem ECC-NK-Zertifikat ein- und auszuschalten. Im Auslieferungszustand muss die automatische Re-Registrierung eingeschaltet sein. [<=]

Neu

A_23121 - Konfigurationsschalter für Verwendung von ECC bei IPsec/IKE (ECC-Migration)

Der Konnektor MUSS dem Administrator ermöglichen, die Verwendung von ECC bei IPsec/IKE-Verbindungen ein- und auszuschalten. Die Verwendung von ECC darf nur eingeschaltet werden, wenn der Konnektor mit seinem ECC-NK-Zertifikat beim VPN-Zugangsdienst registriert ist. Die Verwendung von ECC darf nur ausgeschaltet werden, wenn der Konnektor mit seinem RSA-NK-Zertifikat beim VPN-Zugangsdienst registriert ist.

Im eingeschalteten Zustand MUSS der Konnektor die Vorgaben in A_17125 umsetzen. Im ausgeschalteten Zustand MUSS der Konnektor die Vorgaben in GS-A_4382 umsetzen. [<=]

Neu

A_23149 - Konfigurationsschalter für Verwendung von ECC bei TLS (ECC-Migration)

Der Konnektor MUSS dem Administrator ermöglichen, die Verwendung von ECDSA-basierten Ciphersuiten bei TLS-Verbindungen ein- und auszuschalten. Im ausgeschalteten Zustand DARF der Konnektor ECDSA-basierte Ciphersuiten NICHT anbieten (Rolle TLS-Client) und NICHT auswählen (Rolle TLS-Server). Ebenfalls DARF der Konnektor dann NICHT während des TLS-Verbindungsaufbaus (genauer bei der Signatur der ephemeren (EC)DH-Schlüssel) mit ECDSA-basierten Zertifikaten bzw. deren privaten ECC-Schlüsselmateriale Daten authentisieren. [<=]

Informativ

Es können separate Konfigurationsschalter für einzelne TLS-Strecken umgesetzt werden.

Es gelten darüber hinaus:

- A_22457 und A_22458 für die Auswahl der Ciphersuiten und Authentisierungsalgorithmen für die TLS-Verbindung zum eHealth-Kartenterminal
- A_21760-01 für die Auswahl der Zertifikate für die TLS-Server-Authentisierung (SOAP) und TLS-Client-Authentisierung (CETP) des Konnektors an der Clientsystemschnittstelle

Update Auslöser, Vorbedingungen in TUC_KON_411:

A_21758-05 - 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 Neuregistrierung mit einem neuen (ECC) NK-Zertifikat durch.
Auslöser	A_22332-01, A_23150
Vorbedingungen	Die gSMC-K ist gemäß A_18928 dual-personalisiert.
Eingangsdaten	Keine
Komponenten	Konnektor, VPN-ZugD
Ausgangsdaten	Keine

Standardablauf	<ol style="list-style-type: none"> 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 registerKonnektorRequest-Struktur gemäß ProvisioningService.xsd [gemSpec_VPN_ZugD] erstellen und mit den entsprechenden Parametern befüllen (aktuelles Datum/Uhrzeit, neues C.NK.VPN-Zertifikat, MGM_ZGDP_CONTRACTID). Der Konnektor MUSS die Request-Nachricht mittels einer verfügbaren SM-B (ID.HCI.OSIG) im Element registerKonnektorRequest/Signature signieren und das SM-B-Zertifikat im Element X509Data ablegen. (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_registerKonnektor] definierte Operation I_Registration_Service::registerKonnektor mit der Zieladresse MGM_ZGDP_REGSERVER auf. Der Response der Operation wird verarbeitet: <ol style="list-style-type: none"> a. Setze MGM_TI_ACCESS_GRANTED auf <ul style="list-style-type: none"> - 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 <pre> { topic = "MGM/TI_ACCESS_GRANTED"; eventType = Op; severity = Info; parameters = „Active=\$MGM_TI_ACCESS_GRANTED“; doLog = true; doDisp = true } </pre>
Varianten/Alternativen	<p>Manuelle Registrierung: (->2) Der Administrator soll die zu verwendende SM-B auswählen können.</p>

Fehlerfälle	<p>(→ 2) Es konnte keine freigeschaltete SM-B ausgewählt werden: Fail=No_Smcb (->2,3) 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 }</p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 2: Tab_Kon_933 Fehlercodes TUC_KON_411 "Konnektor mit neuem NK-Zertifikat registrieren"

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

[<=]