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.

Änderungen in gemSpec_Kon

3.3 Betriebszustand

Tabelle 5: TAB_KON_504 Ausführungserlaubnis für Dienste in kritischen Fehlerzuständen

		EC_Software_Integrity_Check_Failed	EC_Random_Generator_Not_Reliable	EC_Security_Log_Not_Writable	EC_Time_Sync_Pending_Critical	EC_Time_Difference_Intolerable	EC_CRL_Out_Of_Date	EC_TSL_Out_Of_Date_Beyond_Grace_Period	EC_TSL_Trust_Anchor_Out_Of_Date	EC_Firewall_Not_Reliable	EC_Secure_Key Store_Not_Available	EC_FW_Not_Valid_Status_Blocked
Technische Use Cases (TUCs) der Basisdienste relevant für Fachanwendung und die Kommunikation mit Weitere Anwendungen und SIS												
Zugriffsberechtigungsdienst												
TUC_KON_000	PrüfeAufrufkontext	-	x	x	x	x	x	x	x	x	x	x
Dienstverzeichnisdienst												
TUC_KON_041	Einbringen der Endpunktinformationen während der Bootup-Phase	-	-	-	x	x	x	x	x	x	x	x
Kartenterminaldienst												
TUC_KON_051	Mit Anwender über Kartenterminal interagieren	-	-	-	-	-	x	x	x	-	-	x
Kartendienst												
TUC_KON_005	Card-to-Card authentisieren	-	-	-	-	-	x	x	x	-	-	x
TUC_KON_006	Datenzugriffsaudit eGK schreiben	-	-	-	-	-	x	x	x	-	-	x

	TUC_KON_018	eGK-Sperrung prüfen	-	-	-	-	-	x	x	x	-	-	x
	TUC_KON_024	Karte zurücksetzen	-	-	-	-	-	x	x	x	-	-	x
	TUC_KON_026	Liefere CardSession	-	-	-	-	-	x	-	x	-	-	-
	TUC_KON_200	SendeAPDU	-	-	-	-	-	x	x	x	-	-	x
	TUC_KON_202	LeseDatei	-	-	-	-	-	x	x	x	-	-	x
	TUC_KON_203	SchreibeDatei	-	-	-	-	-	x	x	x	-	-	x
	TUC_KON_209	LeseRecord	-	-	-	-	-	x	x	x	-	-	x
Systeminformationsdienst													
	TUC_KON_256	System ereignis absetzen	-	x	x	x	x	x	x	x	x	x	x
Verschlüsselungsdienst													
	TUC_KON_072	Daten symmetrisch verschlüsseln	-	-	-	x	x	x	x	x	-	-	x
	TUC_KON_073	Daten symmetrisch entschlüsseln	-	-	-	x	x	x	x	x	-	-	x
Zertifikatsdienst													
	TUC_KON_034	Zertifikats informationen extrahieren	-	-	-	x	x	x	x	x	-	-	x
Protokollierungsdienst													
	TUC_KON_271	Schreibe Protokoll eintrag	-	x	x	x	x	x	x	x	x	x	x
TLS-Dienst													
	TUC_KON_110	Kartenbasierte TLS-Verbindung aufbauen	-	-	-	-	-	-	-	-	-	-	-
Verbindung zum VPN-Konzentrator													
	~~TUC_KON_321 Verbindung zu dem VPN-Konzentrator der TI aufbauen~~		-	-	-	-	-	-	-	-	-	-	-
	TUC_VPN-ZD_0001 „IPsec Tunnel TI aufbauen”		-	-	-	-	-	-	-	-	-	-	-
	~~TUC_KON_322 Verbindung zu dem VPN-Konzentrator des SIS aufbauen~~		-	-	-	-	-	-	-	-	-	-	-
	TUC_VPN-ZD_0002 „IPsec Tunnel SIS aufbauen”		-	-	-	-	-	-	-	-	-	-	-
Operationen der Basisdienste													
Kartendienst													
	VerifyPin		-	-	-	-	-	x	x	x	-	-	x
	UnblockPin		-	-	-	-	-	x	x	x	-	-	x

	ChangePin	-	-	-	-	-	x	x	x	-	-	x
	GetPinStatus	-	-	-	-	-	x	x	x	-	-	x
Systeminformationsdienst												
	Schnittstelle der Ereignissenke	-	x	x	x	x	x	x	x	x	x	x
	GetCardTerminals	-	x	x	x	x	x	x	x	x	x	x
	GetCards	-	x	x	x	x	x	x	x	x	x	x
	GetResourceInformation	-	x	x	x	x	x	x	x	x	x	x
	Subscribe	-	x	x	x	x	x	x	x	x	x	x
	RenewSubscription	-	x	x	x	x	x	x	x	x	x	x
	Unsubscribe	-	x	x	x	x	x	x	x	x	x	x
	GetSubscription	-	x	x	x	x	x	x	x	x	x	x
Verschlüsselungsdienst												
	EncryptDocument	-	-	-	-	-	x	x	x	-	-	x
	DecryptDocument	-	-	-	-	-	x	x	x	-	-	x
Signaturdienst												
	SignDocument	-	-	-	-	-	x	x	x	-	-	x
	VerifyDocument	-	-	-	-	-	x	x	x	-	-	x
	GetJobNumber	-	-	-	-	-	x	x	x	-	-	x
	StopSignature	-	-	-	-	-	x	x	x	-	-	x
Authentifizierungsdienst												
	ExternalAuthenticate	-	-	-	-	-	x	x	x	-	-	x
Zertifikatsdienst												
	ReadCardCertificate	-	-	-	-	-	x	x	x	x	x	x
	CheckCertificateExpiration	-	-	-	-	-	x	x	x	x	x	x
	VerifyCertificate	-	-	-	-	-	x	-	x	x	x	x
Zeitdienst												
	I_NTP_Time_Information	-	-	-	-	-	x	x	x	-	x	-
Konnektormanagement												
	Softwareaktualisierung	x	x	x	x	x	x	x	x	x	x	x
	Protokolleinsicht	x	x	x	x	x	x	x	x	x	x	x
	Werksreset	x	x	x	x	x	x	x	x	x	x	x
	Sonstiges	-	x	x	x	x	x	x	x	x	x	x

4.2.4.3.1 TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“

TIP1-A_4783 - TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“
Der Konnektor MUSS den technischen Use Case TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“ umsetzen.

Tabelle 304: TAB_KON_635 – TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“

Element	Beschreibung
Name	TUC_KON_321 Verbindung zu dem VPN-Konzentrator der TI aufbauen
Beschreibung	Es wird ein IPsec-Tunnel zum VPN-Konzentrator der TI aufgebaut werden. Über den erfolgreichen Aufbau wird per Event informiert.
Auslöser	Bootup-Phase TUC_KON_305 „LAN-Adapter initialisieren“ TUC_KON_306 „WAN-Adapter initialisieren“ Event MGM/LU_CHANGED/LU_ONLINE Event NETWORK/VPN/CONFIG_CHANGED Manueller Aufruf über Managementschnittstelle
Vorbedingungen	Der TUC_KON_304 „Netzwerk-Routen einrichten“ MUSS fehlerfrei durchgelaufen sein.
Eingangsdaten	
Komponenten	Konnektor
Ausgangsdaten	Der virtuelle Adapter VPN_TI mit der IP-Adresse VPN_TUNNEL_TI_INNER_IP des Konnektors wurde zur Verfügung gestellt. • Innere Tunnel IP-Adresse des VPN-Konzentrators TI • DNS_SERVERS_TI • VPN_KONZENTRATOR_TI_IP_ADDRESS • DOMAIN_SRVZONE_TI
Standardablauf	1) Wenn der Auslöser = Event NETWORK/VPN/CONFIG_CHANGED ist, muss der VPN-Tunnel TI abgebaut werden. 2) Wenn der VPN-Tunnel TI noch aktiv ist, ist der Ablauf abgeschlossen. Anderenfalls ist mit Ablaufschritt 3) fortzufahren. 3) Prüfen, MGM_LU_ONLINE = Enabled, falls nicht ist der TUC ohne Ausgabe einer Fehlermeldung zu beenden. 4) Prüfen, ob die im Konnektor hinterlegte CRL noch gültig ist. Falls nicht, muss der TUC_KON_040 „CRL aktualisieren“ aufgerufen werden. Anschließend erneut prüfen, ob die im Konnektor hinterlegte CRL nun gültig ist. ~~Wenn Fehler 4173 nicht zutrifft, ist ein herstellerspezifischer Fehler zu verwenden.~~ Falls die CRL ~~noch~~ nicht gültig ist, ist der TUC mit Fehler zu beenden. 5) Aufrufen von TUC_VPN-ZD_0001 „IPsec Tunnel TI aufbauen” Die folgenden Rückgabewerte des TUC_VPN-ZD_0001 „IPsec Tunnel TI aufbauen” sind in die laufende Konfiguration des Konnektors zu übernehmen: • VPN_TUNNEL_TI_INNER_IP

	• DNS_SERVERS_TI 6) Aufrufen von TUC_KON_304 „Netzwerk-Routen einrichten“ Sobald der Tunnel erfolgreich aufgebaut wurde, ist der folgende Event zu generieren: TUC_KON_256 {"NETWORK/VPN_TI/UP"; Op; Info;IP= $VPN_TUNNEL_TI_INNER_IP}
Varianten/Alternativen	Keine
Fehlerfälle	(→4) CRL ist abgelaufen (outdated) Herstellerspezifisch kann entweder (4a) oder (4b) umgesetzt werden: (4a) Kritischer Fehlerzustand EC_CRL_Out_Of_Date wurde noch nicht festgestellt: 4173 (4b) kritischer Fehlerzustand EC_CRL_Out_Of_Date wurde bereits festgestellt: 4002 (→4) Wenn Fehler 4173 bzw. 4002 nicht zutreffen, ist ein herstellerspezifischer Fehler zu verwenden. (→5) VPN-Tunnel konnte nicht aufgebaut werden; Fehlercode: 4174
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 305: TAB_KON_636 Fehlercodes TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4002	Security	Fatal	Der Konnektor befindet sich in einem kritischen Betriebszustand
4172	Technical	Fatal	Es ist keine Online-Verbindung zulässig.
4173	Technical	Fatal	Die CRL ist nicht mehr gültig (outdated).
4174	Technical	Fatal	TI-VPN-Tunnel: Verbindung konnte nicht aufgebaut werden

[<=]

4.2.4.3.2 TUC_KON_322 „Verbindung zu dem VPN-Konzentrator des SIS aufbauen“

TIP1-A_4784 - TUC_KON_322 „Verbindung zu dem VPN-Konzentrator des SIS aufbauen“
Der Konnektor MUSS den technischen Use Case TUC_KON_322 „Verbindung zu dem VPN-Konzentrator der SIS aufbauen“ umsetzen.

Tabelle 306: TAB_KON_637 – TUC_KON_322 „Verbindung zu dem VPN-Konzentrator der SIS aufbauen“

Element	Beschreibung
Name	TUC_KON_322 Verbindung zu dem VPN-Konzentrator der SIS aufbauen
Beschreibung	Es muss ein IPsec-Tunnel zum VPN-Konzentrator der SIS aufgebaut werden
Auslöser	Bootup-Phase TUC_KON_305 „LAN-Adapter initialisieren TUC_KON_306 „WAN-Adapter initialisieren Event NETWORK/VPN/CONFIG_CHANGED Optional: Event MGM/LU_CHANGED/LU_ONLINE Manueller Aufruf über Managementschnittstelle
Vorbedingungen	ANLW_INTERNET_MODUS = SIS Die Verbindung VPN-Konzentrator TI ist aufgebaut. Der TUC_KON_304 „Netzwerk-Routen einrichten“ muss erfolgreich durchgeführt worden sein.
Eingangsdaten	Keine
Komponenten	Konnektor
Ausgangsdaten	Der virtuelle Adapter VPN_SIS mit der IP-Adresse VPN_TUNNEL_SIS_INNER_IP wurde zur Verfügung gestellt. 1. Innere Tunnel-IP-Adresse des VPN-Konzentrators SIS 2. VPN_KONZENTRATOR_SIS_IP_ADDRESS 3. DNS_SERVER_SIS
Standardablauf	1) Wenn der Auslöser Event NETWORK/VPN/CONFIG_CHANGED ist, muss der VPN-Tunnel SIS abgebaut werden. 2) Wenn der VPN-Tunnel SIS noch aktiv ist, ist der Ablauf abgeschlossen. Anderenfalls ist mit Ablaufschritt 3) fortzufahren. 3) Prüfen, ob (MGM_LU_ONLINE=Enabled). falls nicht ist der TUC ohne Ausgabe einer Fehlermeldung zu beenden. 4) entfällt 5) Prüfen, ob die im Konnektor hinterlegte CRL noch gültig ist. falls nicht, MUSS der TUC_KON_040 „CRL aktualisieren“ aufgerufen werden, Anschließend erneut prüfen, ob die im Konnektor hinterlegte CRL nun gültig ist. ~~Wenn Fehler 4173 nicht zutrifft, ist ein herstellerspezifischer Fehler zu verwenden.~~ Falls die CRL ~~noch~~ nicht gültig ist, ist der TUC mit Fehler zu beenden. 6) Aufrufen von TUC_VPN-ZD_0002 „IPsec Tunnel SIS aufbauen” 7) Aufrufen von TUC_KON_304 „Netzwerk-Routen einrichten“ Sobald der Tunnel erfolgreich aufgebaut wurde, ist der folgende Event zu generieren: TUC_KON_256 {"NETWORK/VPN_SIS/UP"; Op; Info;IP= $VPN_TUNNEL_SIS_INNER_IP}

Varianten/Alternativen	Keine
Fehlerfälle	(→3) Keine Online-Verbindung zulässig; 4172 (→5) CRL ist abgelaufen (outdated); Herstellerspezifisch kann entweder (5a) oder (5b) umgesetzt werden: (5a) Kritischer Fehlerzustand EC_CRL_Out_Of_Date wurde noch nicht festgestellt: 4173 (5b) kritischer Fehlerzustand EC_CRL_Out_Of_Date wurde bereits festgestellt: 4002 (→5) Wenn Fehler 4173 bzw. 4002 nicht zutreffen, ist ein herstellerspezifischer Fehler zu verwenden. (→6) VPN Tunnel konnte nicht aufgebaut werden; Fehlercode: 4176
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 307: TAB_KON_638 Fehlercodes TUC_KON_322 „Verbindung zu dem VPN-Konzentrator der SIS aufbauen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4002	Security	Fatal	Der Konnektor befindet sich in einem kritischen Betriebszustand
4172	Technical	Fatal	Es ist keine Online-Verbindung zulässig.
4173	Technical	Fatal	Die CRL ist nicht mehr gültig (outdated).
4176	Technical	Fatal	SIS-VPN-Tunnel: Verbindung konnte nicht aufgebaut werden

[<=]

Auszug aus gemSpec_VPN_ZugD

5.1 Schnittstelle I_Secure_Channel_Tunnel

TIP1-A_4373 - Konnektor, TUC_VPN-ZD_0001 “IPsec-Tunnel TI aufbauen”
Der Konnektor MUSS den technischen Use Case TUC_VPN-ZD_0001 “IPsec-Tunnel TI aufbauen” gemäß Tabelle Tab_ZD_TUC_IPsec_Tunnel_TI_aufbauen umsetzen.

Tabelle 5: Tab_ZD_TUC_IPsec_Tunnel_TI_aufbauen

Name	TUC_VPN-ZD_0001 “IPsec-Tunnel TI aufbauen”
Beschreibung	Dieser TUC stellt eine IPsec-gesicherte Verbindung zwischen dem Konnektor und einem VPN-Konzentrator TI des VPN-Zugangsdienstes her.

Vorbedingungen	• Eine gültige TSL ist im Konnektor geladen. • Eine gültige CRL ist im Konnektor geladen. • Es besteht eine IP-Netzwerkverbindung vom Konnektor zum Internet • Der gültige Internet DNS Root Trust Anchor der IANA ist in der DNS-Forwarder Konfiguration des Konnektors enthalten. • Der DNS-Resolver des Konnektors kann auf die vom Anbieter des VPN-Zugangsdienstes bereitgestellten Nameserver im Internet (Bezeichner DNS_SERVERS_INT) zugreifen.	
Eingangsdaten	• CRL (die im Konnektor verfügbare CRL) • TUNNEL_MTU (optional, Maximum Transfer Unit für den IPsec Tunnel) • TOP_LEVEL_DOMAIN_TI (Top-Level-Domain der TI) • DNS_DOMAIN_VPN_ZUGD_INT (DNS-Domainname für die Service Discovery der VPN-Konzentratoren) • DNS_SERVERS_INT (DNS Server im Internet) • HASH_AND_URL	
Komponenten	Konnektor, VPN-Zugangsdienst	
Ausgangsdaten	• VPN_TUNNEL_TI_INNER_IP (innere IP-Adresse des IPsec-Tunnels TI) • DNS_SERVERS_TI (Nameserver TI des VPN-Zugangsdienstes) • DOMAIN _SRVZONE_TI • VPN_KONZENTRATOR_TI_IP_ADDRESS (IP-Adresse des VPN-Konzentrators TI im Transportnetz zu dem der IPsec-Tunnel VPN aufgebaut wird)	
Standardablauf	Aktion	Beschreibung
	FQDN und IP-Adressen der VPN-Konzentratoren TI ermitteln	Durch eine DNS-Anfrage zur Auflösung eines SRV-RR mit dem Bezeichner "_isakmp._udp.ti-extern.<DNS_DOMAIN_VPN_ZUGD_INT>“ erhält der Konnektor eine Liste von priorisierten und gewichteten FQDN der VPN-Konzentratoren TI. Alle FQDN mit der höchsten Priorität (kleinere Zahlen entsprechen einer höheren Priorität) werden ihrem Gewicht entsprechend nach einem Zufallsverfahren neu sortiert. Dahinter folgen die ebenfalls zufällig sortierten FQDN der nächst niedrigeren Priorität. Dieser Vorgang wird wiederholt, bis alle FQDN in der neuen Liste enthalten sind. Der erste FQDN aus der Liste wird daraufhin in eine IP-Adresse aufgelöst (TUC-interner Bezeichner VPN_KONZENTRATOR_TI_FQDN). Es wird eine Firewall-Regel erzeugt, die einen IPsec-Verbindungsaufbau zu dieser IP-Adresse ermöglicht. Sollte sich im Folgenden herausstellen, dass es nicht möglich ist mit diesem VPN-Konzentrator eine Verbindung aufzubauen, wird der nächste FQDN aus der Liste verwendet. Dieses Verfahren wird wiederholt, bis der Verbindungsaufbau erfolgreich war oder alle Adressen erfolglos probiert wurden.

	Nameserver TI und Domainnamen der Service-Zone des VPN-Zugangsdienstes ermitteln	Durch eine DNS-Anfrage zur Auflösung eines TXT-RR mit dem Bezeichner VPN_KONZENTRATOR_TI_FQDN an den DNS-Forwarder erhält der Konnektor die IP-Adressen der Nameserver TI (DNS_SERVERS_TI) sowie die Domainnamen der Service Zone TI (DOMAIN_SRVZONE_TI) des VPN-Zugangsdienstes. Die key/value Paare der TXT-Records haben folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes): "txtvers=1" "NameserverTI=<IP-Adresse1>,<IP-Adresse2>[,<weitere IP-Adressen>]" "DomainSrvTI=<Domainname der Servicezone TI des VPN-Zugangsdienstes>" Beispiel für einen Zonendateieintrag: `vpnk1.ham.ti-vpn-zugd.anbieter.de. 3600 IN TXT "txtvers=1" "NameserverTI=100.97.20.13,100.97.20.14" "DomainSrvTI=ti-sz.ham.anbieter.vpn-zugd.telematik"`
	DNS-Forwarder für Namensraum TI konfigurieren	Die IP-Adressen aus DNS_SERVERS_TI werden in der Nameserver Konfiguration des DNS-Forwarders als Zieladressen für den Forward-Eintrag des Namensraumes TI eingetragen
	Verbindung aufbauen	• Der Verbindungsaufbau erfolgt gemäß oder [RFC7296] mit der ersten IP-Adresse aus der erzeugten IP-Adressliste der VPN-Konzentratoren. • Es muss das Encapsulating Security Payload Protocol (ESP) mit Verschlüsselung (siehe [RFC4303#3.2.1]) und Integritätsschutz (siehe [RFC4303#3.2.2]) verwendet werden. Die zu nutzenden kryptographischen Algorithmen sind in [gemSpec_Krypt#3.3.1] beschrieben. Der Aufbau der Security Association (SA) erfolgt nach dem Internet Key Exchange Protocol Version 2 gemäß [RFC 7296] oder [RFC7427.] • Der Konnektor empfängt vom VPN-Konzentrator das Zertifikat C.VPNK.VPN. Falls HASH_AND_URL = Enabled muss das Hash & URL Verfahren gemäß [RFC7296] zum Austausch der Zertifikate zwischen Konnektor und VPN-Konzentrator verwendet werden. • Das Zertifikat C.VPNK.VPN wird gemäß [gemSpec_PKI#TUC_PKI_018] mit Prüfmodus CRL geprüft. Wenn das Zertifikat C.VPNK.VPN nicht gültig oder das Zertifikat gesperrt ist, wird der Verbindungsaufbau mit einer Fehlermeldung gemäß [RFC7296] abgebrochen und es wird die nächste IP-Adresse aus der Liste der VPN-Konzentratoren angesprochen.

		• Der Konnektor authentisiert sich beim VPN-Konzentrator mit seinem Zertifikat C.NK.VPN • Die Autorisierungsprüfung erfolgt durch den VPN-Zugangsdienst. Bei einem negativen Prüfergebnis wird an den Konnektor die Fehlermeldung "AUTHENTICATION_FAILED" gemäß [[RFC7296] gesendet. Der IPsec-Tunnelaufbau ist damit beendet. • Bei erfolgreicher gegenseitiger Authentifizierung und Autorisierung durch den VPN-Zugangsdienst wird die Verbindung gemäß [RFC7296] weiter aufgebaut. Das IKE-Protokoll weist dem Konzentrator die innere IP-Adresse des IPsec-Tunnels aus dem Adressraum TI_Dezentral zu. Bei jedem Verbindungsaufbau wird eine andere IP-Adresse verwendet. • Die MTU wird automatisch mittels Path MT+R765U Discovery ermittelt und entsprechend eingestellt. Wenn der optionale Parameter TUNNEL_MTU angegeben ist, wird die MTU auf maximal diesen Wert eingestellt.
Varianten/Alternativen	Keine	
Zustand nach erfolgreichem Ablauf	Der Konnektor ist mit dem VPN-Konzentrator TI verbunden.	
Fehlerfälle	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC 7296] verwendet.	

[<=]

5.2 Schnittstelle I_Secure_Internet_Tunnel

TIP1-A_4397 - Konnektor, TUC_VPN-ZD_0002 “IPsec Tunnel SIS aufbauen”
Der Konnektor MUSS den technischen Use Case TUC_VPN-ZD_0002 “IPsec-Tunnel SIS aufbauen” gemäß Tabelle Tab_ZD_TUC_IPsec_Tunnel_SIS_aufbauen umsetzen.

Tabelle 7: Tab_ZD_TUC_IPsec_Tunnel_SIS_aufbauen

Name	TUC_VPN-ZD_0002 “IPsec-Tunnel SIS aufbauen”
Beschreibung	Dieser TUC stellt eine IPsec-gesicherte Verbindung zwischen dem Konnektor und dem VPN-Konzentrator SIS des VPN-Zugangsdienstes her.
Vorbedingungen	• Eine gültige TSL ist im Konnektor geladen. • Eine gültige CRL ist im Konnektor geladen. • Es besteht eine IP-Netzwerkverbindung vom Konnektor zum Internet • Der gültige Internet DNS Root Trust Anchor der IANA ist in der DNS-Forwarder Konfiguration des Konnektors enthalten. • Der Konnektor ist beim Anbieter des VPN-Zugangsdienstes registriert und zur Verbindung mit dem Sicheren Internet Service

	berechtigt. • Der DNS-Resolver des Konnektors kann auf die vom Anbieter des VPN-Zugangsdienstes bereitgestellten Nameserver im Internet (Bezeichner DNS_SERVERS_INT) zugreifen.	
Eingangsdaten	• CRL (die im Konnektor verfügbare CRL) • TUNNEL_MTU (optional, Maximum Transfer Unit für den IPsec Tunnel) • DNS_DOMAIN_VPN_ZUGD_INT (DNS-Domainname für die Service Discovery der VPN-Konzentratoren) • DNS_SERVERS_INT (DNS Server im Internet) • HASH_AND_URL	
Komponenten	Konnektor, VPN-Zugangsdienst	
Ausgangsdaten	• VPN_TUNNEL_SIS_INNER_IP (innere IP-Adresse des IPsec-Tunnels SIS) • DNS_SERVERS_SIS (Nameserver SIS des VPN-Zugangsdienstes) • VPN_KONZENTRATOR_SIS_IP_ADDRESS (IP-Adresse des VPN-Konzentrators SIS im Transportnetz zu dem der IPsec-Tunnel VPN_SIS aufgebaut wird)	
Standardablauf	Aktion	Beschreibung
	FQDN und IP-Adressen der VPN-Konzentratoren SIS ermitteln	Durch eine DNS-Anfrage zur Auflösung eines SRV-RR mit dem Bezeichner "_isakmp._udp.sis-extern.<DNS_DOMAIN_VPN_ZUGD_INT>“ erhält der Konnektor eine Liste von priorisierten und gewichteten FQDN der VPN-Konzentratoren SIS. Alle FQDN mit der höchsten Priorität (kleinere Zahlen entsprechen einer höheren Priorität) werden ihrem Gewicht entsprechend nach einem Zufallsverfahren neu sortiert. Dahinter folgen die ebenfalls zufällig sortierten FQDN der nächst niedrigeren Priorität. Dieser Vorgang wird wiederholt, bis alle FQDN in der neuen Liste enthalten sind. Der erste FQDN aus der Liste wird daraufhin in eine IP-Adresse aufgelöst (TUC-interner Bezeichner VPN_KONZENTRATOR_SIS_FQDN). Es wird eine Firewall-Regel erzeugt, die einen IPsec-Verbindungsaufbau zu dieser IP-Adresse ermöglicht. Sollte sich im Folgenden herausstellen, dass es nicht möglich ist mit diesem VPN-Konzentrator eine Verbindung aufzubauen, wird der nächste FQDN aus der Liste verwendet. Dieses Verfahren wird wiederholt, bis der Verbindungsaufbau erfolgreich war oder alle Adressen erfolglos probiert wurden.
	Nameserver SIS und Domainnamen der Service-Zone des VPN-Zugangsdienstes	Durch eine DNS-Anfrage zur Auflösung eines TXT-RR mit dem Bezeichner VPN_KONZENTRATOR_SIS_FQDN an den DNS-Forwarder erhält der Konnektor die IP-Adressen der Nameserver SIS (DNS_SERVERS_SIS) sowie die Domainnamen der Service Zone SIS

	ermitteln	(DOMAIN_SRVZONE_SIS) des VPN-Zugangsdienstes. Die key/value Paare der TXT-Records haben folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes): "txtvers=1" "NameserverSIS=<IP-Adresse1>,<IP-Adresse2>[,<weitere IP-Adressen>]" "DomainSrvSIS=<Domainname der Servicezone SIS des VPN-Zugangsdienstes>" Beispiel für einen Zonendateieintrag: `vpnk1.ham.sis-vpn-zugd.anbieter.de. 3600 IN TXT "txtvers=1" "NameserverSIS=100.97.21.13,100.97.21.14" "DomainSrvSIS=sis-sz.ham.anbieter.vpn-zugd.telematik"`
	DNS-Forwarder für Namensraum SIS konfigurieren	Die IP-Adressen aus DNS_SERVERS_SIS werden in der Nameserver Konfiguration des DNS-Forwarders als Zieladressen für den Forward-Eintrag des Namensraumes Internet eingetragen. Dabei werden die bestehenden Ziel-Nameservern DNS_SERVERS_INT mit den DNS_SERVERS_SIS überschrieben. Wenn die Verbindung zum VPN-Konzentrator SIS abgebaut wurde, müssen die Ziel-Nameservern wieder DNS_SERVERS_INT sein.
	Verbindung aufbauen	• Der Verbindungsaufbau erfolgt gemäß [RFC7296] mit der ersten IP-Adresse aus der erzeugten IP-Adressliste der VPN-Konzentratoren. • Es muss das Encapsulating Security Payload Protocol (ESP) mit Verschlüsselung (siehe [RFC4303#3.2.1]) und Integritätsschutz (siehe [RFC4303#3.2.2]) verwendet werden. Die zu nutzenden kryptographischen Algorithmen sind in [gemSpec_Krypt#3.3.1] beschrieben. Der Aufbau der Security Association (SA) erfolgt nach dem Internet Key Exchange Protocol Version 2 gemäß 7296 oder [RFC7427]. • Der Konnektor empfängt vom VPN-Konzentrator das Zertifikat C.VPNK.VPN-SIS. Falls HASH_AND_URL = Enabled muss das Hash & URL Verfahren gemäß [RFC7296] zum Austausch der Zertifikate zwischen Konnektor und VPN-Konzentrator verwendet werden. • Das Zertifikat C.VPNK.VPN-SIS wird gemäß [gemSpec_PKI#TUC_PKI_018] mit Prüfmodus CRL geprüft. Wenn das Zertifikat C.VPNK.VPN-SIS nicht gültig oder das Zertifikat gesperrt ist, wird der Verbindungsaufbau mit einer Fehlermeldung gemäß [RFC 7296] abgebrochen und es wird

		die nächste IP-Adresse aus der Liste der VPN-Konzentratoren angesprochen. • Der Konnektor authentisiert sich beim VPN-Konzentrator mit seinem Zertifikat C.NK.VPN • Die Autorisierungsprüfung erfolgt durch den VPN-Zugangsdienst. Bei einem negativen Prüfergebnis wird an den Konnektor die Fehlermeldung "AUTHENTICATION_FAILED" gemäß [RFC7296] gesendet. Der IPsec-Tunnelaufbau ist damit beendet. • Bei erfolgreicher gegenseitiger Authentifizierung und Autorisierung durch den VPN-Zugangsdienst wird die Verbindung gemäß [RFC7296] weiter aufgebaut. Das IKE-Protokoll weist dem Konzentrator die innere IP-Adresse des IPsec-Tunnels aus dem Adressraum TI_Dezentral zu. Bei jedem Verbindungsaufbau wird eine andere IP-Adresse verwendet. • Die MTU wird automatisch mittels Path MTU Discovery ermittelt und entsprechend eingestellt. Wenn der optionale Parameter TUNNEL_MTU angegeben ist, wird die MTU auf maximal diesen Wert eingestellt.
Varianten/Alternativen	Keine	
Zustand nach erfolgreichem Ablauf	Der Konnektor ist mit dem VPN-Konzentrator SIS verbunden.	
Fehlerfälle	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC7296] verwendet.	

[<=]