Änderungen in gemSpec_Kon

Im Folgenden werden die Änderungen in Kapitel 4.3.9 dargestellt.

4.3.9 Software- und Konfigurationsaktualisierung (KSR-Client)

Die Umsetzung des KSR-Clients bezüglich des Mechanismus zur Durchführung der Aktualisierungen, sowie die Art der Darstellung an der Managementschnittstelle sind herstellerspezifisch.

Innerhalb der Software- und Konfigurationsaktualisierung (KSR-Client) werden folgende Präfixe für Bezeichner verwendet:

- Events (Topic Ebene 1): „KSR“
- Konfigurationsparameter: „MGM_“

4.3.9.1 Funktionsmerkmalweite Aspekte

Der Konnektor muss einen KSR-Client bereitstellen, über den der Administrator sowohl den Konnektor selbst als auch die vom Konnektor verwalteten Kartenterminals (CT-Objects in CTM_CT_LIST mit CT.CORRELATION>=„gepairt“ und CT.VALID_VERSION=True und CT.IS_PHYSICAL = Ja) softwareseitig aktualisieren kann.

Weiterhin muss über den KSR-Client eine Aktualisierung von ausgewählten Konfigurationsdaten möglich sein.

TIP1-A_4829 - Vollständige Aktualisierbarkeit des Konnektors
Die Software-Aktualisierung des Konnektor SOLL sicherstellen, dass alle Software-Bestandteile des Konnektors aktualisiert werden können, damit eine ungehinderte Nachnutzung der Hardware-Basis im Feld mit neuen Funktionalitäten nicht durch nichtaktualisierbare Software-Bestandteile gefährdet wird. Weicht ein Hersteller für sein Konnektormodell von dieser Forderung in Teilen ab, so MUSS er im Rahmen der Zulassung nachweisen, dass dies auf Grund von Sicherheitsaspekten für sein eingereichtes Konnektormodell zwingend erforderlich ist.
[<=]

TIP1-A_5657 - Freischaltung von Softwareupdates
Der Konnektor MUSS ~~sicherstellen~~ die Möglichkeit bieten, dass Softwareupdates durch den Nutzer bzw. einen von ihm beauftragten Administrator einzeln freigeschaltet werden. ~~Der Konnektor DARF ein Softwareupdate NICHT ohne vorher erfolgte Freischaltung aktivieren.~~
[<=]

A_18387 – Automatische Softwareupdates

Der Konnektor SOLL die Möglichkeit bieten, die automatische Installation von Softwareupdates ein- und auszuschalten. Das Ein- und Ausschalten SOLL nur dann zur Verfügung stehen, wenn MGM_KSR_AUTODOWNLOAD=Enabled ist.

~~**TIP1-A_5659 - Bewusste Entscheidung bei Freischaltung von Softwareupdates**~~
~~Der Hersteller des Konnektors MUSS in seinem Handbuch den Nutzer (bzw. den von ihm beauftragten Administrator) darauf hinweisen, dass der Anwender ein Softwareupdate nur dann aktivieren soll, wenn er ausreichend Informationen über den Inhalt des Softwareupdates erhalten hat, die ihm eine bewusste Entscheidung bei der Freischaltung ermöglichen.~~
~~**[<=]**~~

A_18389 – Nur Nutzung von zugelassenen Versionen

Der Hersteller des Konnektors MUSS in seinem Handbuch den Nutzer darauf hinweisen, dass er sich bei der Arbeit mit dem Konnektor vergewissern muss dass er mit einer zugelassenen Version arbeitet und beschreiben, wie der Nutzer diese Information mittels seines Primärsystems erhalten kann.

TIP1-A_6476 - Lieferung von Softwareupdates
Der Hersteller des Konnektors MUSS jede zugelassene Firmware-Version umgehend als Update-Paket über die in [gemSpec_KSR] definierte Schnittstelle P_KSRS_Upload im Konfigurationsdienst (KSR) ablegen.
Der Hersteller des Konnektors MUSS in den jeweiligen UpdateInformation/Firmware/FirmwareReleaseNotes eine Internet-URL zum Download des FW-Updates bereitstellen.

[<=]

TIP1-A_6026 - Anzeige URL zum Download des FW-Updates an der Managementschnittstelle
Das Managementinterface des Konnektors MUSS einem authentisierten Administrator die Internet-URL zum Download des FW-Updates anzeigen.
[<=]

4.3.9.2 Durch Ereignisse ausgelöste Reaktionen

TIP1-A_4831 - KT-Update nach Wiedererreichbarkeit erneut anstoßen
Wenn aus (TIP1-A_4840 Auslösen der durchzuführenden Updates) heraus für ein Kartenterminal noch ein ausstehendes Updates vorhanden ist, dessen Ausführungszeitpunkt nicht gesetzt oder überschritten ist, und für dieses Kartenterminal das Ereignis „CT/CONNECTED“ eintritt, so MUSS TUC_KON_281 „Kartenterminalaktualisierung anstoßen“ für dieses KT gerufen werden.
[<=]

4.3.9.3 Interne TUCs, nicht durch Fachmodule nutzbar

4.3.9.3.1 TUC_KON_280 „Konnektoraktualisierung durchführen“

TIP1-A_4832 - TUC_KON_280 „Konnektoraktualisierung durchführen“
Der Konnektor MUSS den technischen Use Case TUC_KON_280 „Konnektoraktualisierung durchführen“ umsetzen.

Tabelle 346: TAB_KON_664 – TUC_KON_280 „Konnektoraktualisierung durchführen“

Element	Beschreibung
Name	TUC_KON_280 „Konnektoraktualisierung durchführen“
Beschreibung	Dieser TUC aktualisiert den Konnektor mit einem Update, dessen Update-Dateien entweder direkt übergeben oder per UpdateInformation (vom KSRS bezogen) referenziert werden
Auslöser	Der Administrator hat UpdateInformation zur Anwendung ausgewählt und bestätigt bzw. ein lokales Updatepaket bezogen und zur Anwendung übergeben. Ein automatisches Softwareupdate soll durchgeführt werden.
Vorbedingungen	~~Der Administrator hat bewusst das übergebene Paket für eine Installation ausgewählt~~
Eingangsdaten	• UpdateInformation (gemäß [gemSpec_KSR#5.2]) oder • Updatepaket (herstellerspezifisch, von lokaler Datenquelle, mit enthaltenen FirmwareFiles)
Komponenten	Konnektor, Konfigurationsdienst
Ausgangsdaten	Keine
Nachbedingungen	Der Konnektor arbeitet basierend auf der übergebenen, im Updatepaket enthaltenen neuen Version.
Standardablauf	Der Konnektor MUSS die zur Anwendung übergebene UpdateInformation wie folgt anwenden: 1. Integrität und Authentizität der UpdateInformation prüfen (Mechanismus ist herstellerspezifisch) 2. Download aller in UpdateInformation.FirmwareFiles gelisteten Dateien. Dabei wird die Komprimierung des File Transfers vom Konfigurationsdienst über http „Content Coding“ [RFC2616] „gzip“ genutzt. 3. Integrität und Authentizität jeder der via UpdateInformation/FirmwareFiles heruntergeladenen Dateien prüfen (Mechanismus ist herstellerspezifisch) 4. Prüfen auf Zulässigkeit des Updates basierend auf der Firmware-Gruppe (siehe [gemSpec_OM#2.5] 5. Anwenden der zur Verfügung stehenden FirmwareFiles a. TUC_KON_256{ topic = „KSR/UPDATE/START“; eventType = Sec; severity = Info; parameters = („Target=Konnektor, Name=$MGM_KONN_HOSTNAME“)} (betroffene Fachmodule und Basisdienste reagieren und stoppen sich) b. Herstellerspezifischer Mechanismus zur Aktualisierung der internen Konnektorsoftware durch die FirmwareFiles inklusive anschließender Prüfung auf Erfolg. c. Bestehende Konfigurationsdaten des Konnektors MÜSSEN erhalten bleiben und sofern erforderlich und möglich automatisch auf die Definitionen der neuen

	Firmware angepasst werden.
	d. Ist ein händischer Anpassungs- oder Ergänzungsbedarf der Konfigurationsdaten erforderlich, so MUSS der Administrator hierüber geeignet informiert werden
	e. TUC_KON_256 {
	topic = „KSR/UPDATE/SUCCESS";
	eventType = Sec;
	severity = Info;
	parameters = („Target=Konnektor,
	Name= $MGM_KONN_HOSTNAME,
	NewFirmwareversion =
	UpdateInformation.FirmwareVersion,
	ConfigurationChanged=<Ja/Nein>,
	ManualInputNeeded=<Ja/Nein>„) }
	Der TUC endet in jedem Fall mit:
	TUC_KON_256 {
	topic = „KSR/UPDATE/END";
	eventType = Sec;
	severity = Info;
	parameters = („Target=Konnektor,
	Name=$MGM_KONN_HOSTNAME") }
	(betroffene Fachmodule und Basisdienste reagieren und starten sich)

Varianten/Alternativen	Sofern direkt ein Updatepaket (mit enthaltenen FirmwareFiles) übergeben wurde beginnt der Ablauf ab Nummer 4 mit der Integritätsprüfung des Updatepakets

Fehlerfälle	Fehler in den folgenden Schritten des Ablaufs führen zu:
	a) Aufruf von TUC_KON_256 {
	topic = „KSR/ERROR";
	eventType = $ErrorType;
	severity = $Severity;
	parameters = („Target=Konnektor,
	Name= $MGM_KONN_HOSTNAME,
	Error=$Fehlercode,
	Bedeutung=$Fehlertext") }
	
	b) Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes
	
	(→1) Integritätsprüfung UpdateInformation fehlgeschlagen, Fehlercode: 4181
	(→2) Fehler bei der Downloaddurchführung, Fehlercode: 4182
	(→3) Integritätsprüfung eines FirmwareFiles fehlgeschlagen, Fehlercode: 4183
	(→ 4) Firmwaregruppenprüfung fehlgeschlagen, Fehlercode: 4185
	(→5b) Interne Aktualisierung fehlgeschlagen, dann:
	1. Rollback auf vorherige Version
	2. Abbruch mit Fehlercode: 4184

Nichtfunktionale Anforderungen	Der laufende Updatevorgang MUSS in der Managementschnittstelle ausgewiesen und der Fortschritt mindestens für die Schritte 1-5b dargestellt werden.
Zugehörige Diagramme	Abbildung 21: PIC_KON_105 Aktivitätsdiagramm Konnektoraktualisierung durchführen

Tabelle 347: TAB_KON_665 Fehlercodes TUC_KON_280 „Konnektoraktualisierung durchführen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4181	Security	Error	Integritätsprüfung UpdateInformation fehlgeschlagen.
4182	Security	Error	Download nicht aller UpdateFiles möglich.
4183	Security	Error	Integritätsprüfung UpdateFiles fehlgeschlagen.
4184	Security	Error	Anwendung der UpdateFiles fehlgeschlagen (<Details>).
4185	Security	Error	Firmware-Version liegt außerhalb der gültigen Firmware-Gruppe

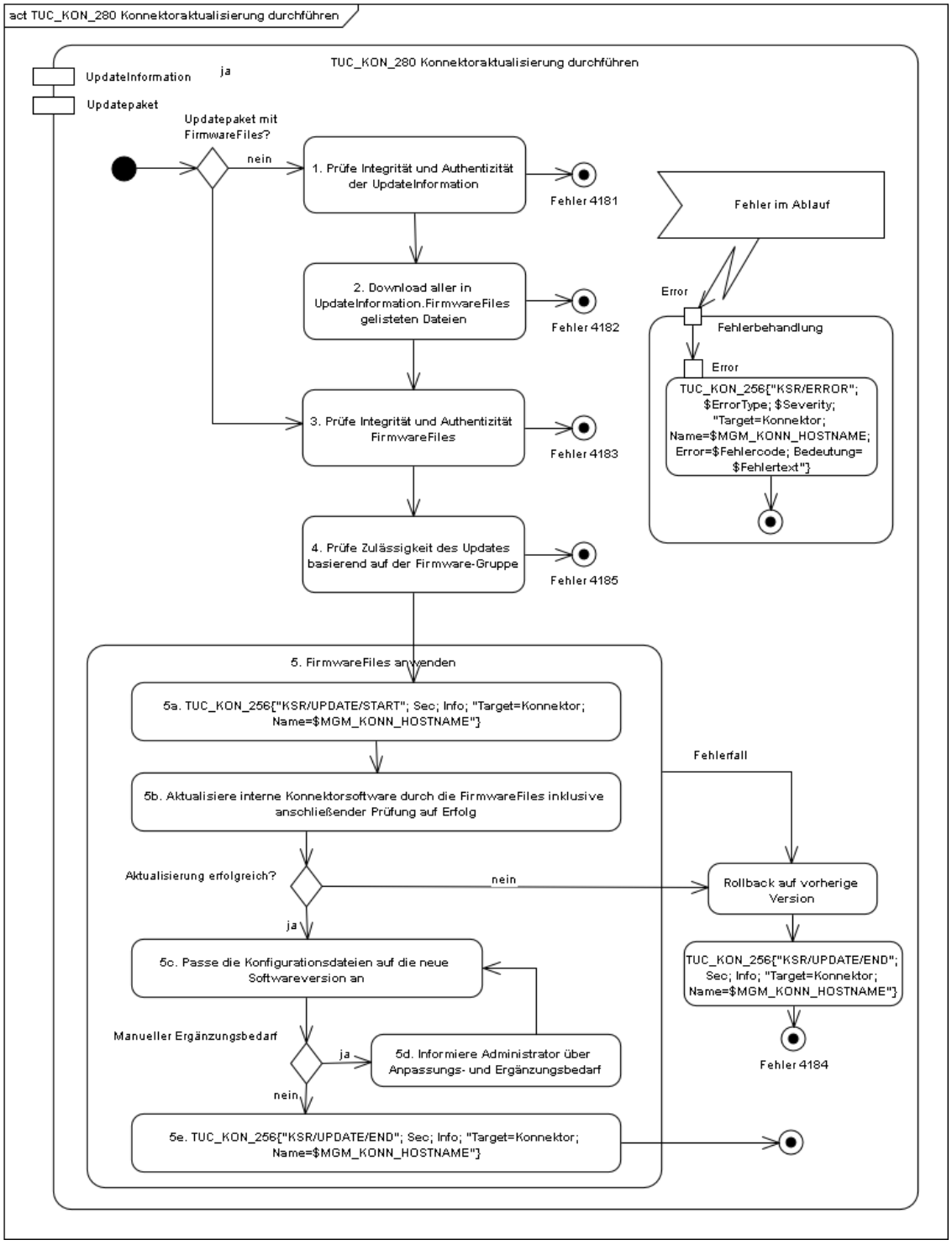

Abbildung 21: PIC_KON_105 Aktivitätsdiagramm Konnektoraktualisierung durchführen

[<=]

4.3.9.3.2 TUC_KON_281 „Kartenterminalaktualisierung anstoßen“

Im Vergleich zur Durchführung des Konnektor-Update (TUC_KON_280), werden die Updates der Kartenterminals nur durch den Konnektor initiiert. Der Konnektor liefert dem

Kartenterminal das Updatefile, der eigentliche Updatevorgang (inklusive der Prüfung des Updatepakets auf Integrität und Authentizität) erfolgt ausschließlich und eigenverantwortlich auf Seiten des Kartenterminals.

TIP1-A_4833 - TUC_KON_281 „Kartenterminalaktualisierung anstoßen“
Der Konnektor MUSS den technischen Use Case TUC_KON_281 „Kartenterminalaktualisierung anstoßen“ umsetzen.

Tabelle 348: TAB_KON_666 – TUC_KON_281 „Kartenterminalaktualisierung anstoßen“

Element	Beschreibung
Name	TUC_KON_281 „Kartenterminalaktualisierung anstoßen“
Beschreibung	Dieser TUC fordert ein Kartenterminal auf einen Update durchzuführen, dessen Update-Dateien entweder direkt übergeben oder per UpdateInformation (vom KSRS bezogen) referenziert werden
Auslöser	Der Administrator hat UpdateInformation für ein Kartenterminal zur Anwendung ausgewählt und bestätigt bzw. ein lokales Updatepaket für ein Kartenterminal bezogen und zur Anwendung übergeben. Ein automatisches Softwareupdate soll durchgeführt werden.
Vorbedingungen	• ~~Der Administrator hat bewusst das übergebene Paket für eine Installation ausgewählt~~ • CT(ctId).IS_PHYSICAL=Ja • CT(ctId).CORRELATION>=”gepairt”
Eingangsdaten	• ctId (ID des Ziel-KTs) • UpdateInformation (gemäß [gemSpec_KSR]) oder • Updatepaket (herstellerspezifisch, von lokaler Datenquelle, mit enthaltenen FirmwareFiles)
Komponenten	Konnektor, Kartenterminal
Ausgangsdaten	Keine
Nachbedingungen	Das Kartenterminal arbeitet basierend auf der übergebenen, im Updatepaket enthaltenen neuen Version.
Standardablauf	Der Konnektor MUSS die zur Anwendung übergebene UpdateInformation wie folgt anwenden: 1. Download der in UpdateInformation/FirmwareFiles gelisteten Datei (für KT-Updates darf nur genau ein FirmwareFile angegeben werden) 2. TUC_KON_256{ topic = „KSR/UPDATE/START”; eventType = Sec; severity = Info; parameters = („Target=KT, CtID=$ctId“) } 3. Durchführen des KT-Updates durch: a) Wechsel in eine Admin-Session durch TUC_KON_050 „Beginne Kartenterminalsitzung“{role=„Admin“; ctId} b) Senden der SICCT Kommandos: SICCT CT Download INIT, SICCT CT Download DATA (Übermittlung des UpdateFiles) und SICCT CT Download FINISH an ctId c) TUC_KON_256{ topic = „KSR/UPDATE/SUCCESS”;

	eventType = Sec;
	severity = Info;
	parameters = („Target=KT,
	Name= $CT.HOSTNAME, CtID =$ctId,
	NewFirmwareversion =
	<UpdateInformation.FirmwareVersion>„}
	
	Der TUC endet in jedem Fall mit:
	• TUC_KON_256 {
	topic = „KSR/UPDATE/END";
	eventType = Sec;
	severity = Info;
	parameters = („Target=KT, CtID =$ctId") }

Varianten/Alternativen	Sofern direkt ein Updatepaket (mit enthaltenem FirmwareFile) übergeben wurde beginnt der Ablauf ab Nummer 2 mit Signalisierung des Beginns des KT-Updates

Fehlerfälle	Fehler in den folgenden Schritten des Ablaufs führen zu:
	a) Aufruf von TUC_KON_256 {
	topic = „KSR/ERROR";
	eventType = $ErrorType;
	severity = $Severity;
	parameters = („Target=KT, Name=$CT.HOSTNAME,
	CtID =$ctId, Error=$Fehlercode,
	Bedeutung=$Fehlertext") }
	b) Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes
	(→1) Download fehlgeschlagen, Fehlercode: 4186
	(→3b) SICCT-Download fehlgeschlagen, Fehlercode: 4187

Nichtfunktionale Anforderungen	Die Durchführung eines KT-Updates DARF die weitere Operation des Konnektors NICHT behindern (weder auf Schnittstellenebene noch in der Managementschnittstelle). Der laufende Updatevorgang eines KT MUSS in der Managementschnittstelle ausgewiesen und der Fortschritt dargestellt werden. Der Konnektor MUSS mindestens 5 Kartenterminal-Updates parallel durchführen können.
Zugehörige Diagramme	keine

Tabelle 349: TAB_KON_667 Fehlercodes TUC_KON_281 „Kartenterminalaktualisierung anstoßen"

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4186	Security	Error	Download nicht aller UpdateFiles möglich.
4187	Security	Error	KT-Update fehlgeschlagen (<Fehlerinfo gemäß SICCT>)

[<=]

Es ist spezifikationskonform und intendiert, dass der Konnektor ein optimiertes Verhalten hinsichtlich des im Schritt 2b) des Standardablaufs von TIP1-A_4833 vom Kartenterminal erhaltenen Download Termination Data Object implementiert. In diesem Download

Termination Data Object liefert das Kartenterminal als Antwort auf SICCT CT Download FINISH Kommando die voraussichtliche Zeit, die es braucht, um das Firmware-Update zu verarbeiten.
Eine optimierte Konnektor-Implementierung kann z.B. berücksichtigen, dass anhand der vom Kartenterminal geschickten Serviceannouncement-Nachrichten erkannt wird, ob vor dem Ablauf der angegeben Zeit das Kartenterminal bereits zu benutzen ist. Es muss dabei berücksichtigt werden, dass Service-Announcement-Nachrichten optional sind.
Eine weitere optimierte Konnektor-Implementierung wäre auch, vor dem Ablauf der angegeben Zeit Service-Discovery-Nachrichten an das Kartenterminal zu schicken, um durch ihre Beantwortung zu überprüfen, ob es bereits ansprechbar ist.

4.3.9.3.3 TUC_KON_282 „UpdateInformationen beziehen“

TIP1-A_4834 - TUC_KON_282 „UpdateInformationen beziehen“
Der Konnektor MUSS den technischen Use Case TUC_KON_282 „UpdateInformationen beziehen“ umsetzen.

Tabelle 350: TAB_KON_668 – TUC_KON_282 „UpdateInformationen beziehen“

Element	Beschreibung
Name	TUC_KON_282 „UpdateInformationen beziehen“
Beschreibung	Dieser TUC ermittelt vom zentralen Konfigurationsdienst sowohl für den Konnektor als auch für alle durch ihn verwalteten Kartenterminals die verfügbaren UpdateInformationen
Auslöser	• Manuell durch den Administrator • Automatisch
Vorbedingungen	Keine
Eingangsdaten	Keine
Komponenten	Konnektor, Konfigurationsdienst
Ausgangsdaten	Keine
Nachbedingungen	Der Konnektor verfügt über alle aktuellen UpdateInformationen

Standardablauf	Der Konnektor MUSS folgende Schritte durchlaufen:
	1. Der Konnektor MUSS die TLS-Verbindungen zum Konfigurationsdienst anhand des in MGM_KSR_FIRMWARE_URL angegebenen Wertes aufbauen. Dabei MUSS er das durch den Server präsentierte Zertifikat mittels
	TUC_KON_037 „Zertifikat prüfen“ {
	certificate = C.ZD.TSL-S;
	qualifiedCheck = not_required;
	offlineAllowNoCheck = true;
	policyList = oid_zd_tls_s;
	intendedKeyUsage= intendedKeyUsage(C.ZD.TSL-S);
	intendedExtendedKeyUsage = id-kp-serverAuth;
	validationMode = OCSP}
	auf Gültigkeit prüfen.
	Das Server-Zertifikat C.ZD.TLS-S MUSS für den Konfigurationsdienst ausgestellt sein.
	2. Der Konnektor MUSS sowohl für sich wie auch für jedes Kartenterminal (CT) aus CTM_CT_LIST mit

	CT.IS_PHYSICAL=Ja und CT.CORRELATION>=„gepairt“ folgende Schritte durchlaufen: a. Belegen von listUpdatesRequest mit den korrekten Werten für ProductVendorID, ProductCode, HardwareVersion und FirmwareVersion b. Aufruf von I_KSRS_Download::list_Updates Liefert der Aufruf mindestens eine UpdateInformation mit einer UpdateInformation/Firmware/FWVersion > aktuelle Version der Konnektorsoftware, deren UpdateInformation/Firmware/FWPriority = „Kritisch“, dann geht der Konnektor über in den Betriebszustand EC_Connector_Software_Out_Of_Date. Liefert der Aufruf mindestens eine UpdateInformation mit einer UpdateInformation/Firmware/FWVersion > aktuelle Version der Kartenterminalsoftware, deren UpdateInformation/Firmware/FWPriority = „Kritisch“, dann geht der Konnektor über in den Betriebszustand EC_CardTerminal_Software_Out_Of_Date. 3. Beenden der TLS-Verbindung
Varianten/Alternativen	Keine

Fehlerfälle	Fehler in den folgenden Schritten des Ablaufs führen zu:
	a) Aufruf von TUC_KON_256 {
	topic = „KSR/ERROR“;
	eventType = $ErrorType;
	severity = $Severity;
	parameters = („Error=$Fehlercode; Bedeutung=$Fehlertext“)}
	
	b) Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes
	(→1) Konfigurationsdienst nicht erreichbar, Fehlercode: 4188
	(→1) Serverzertifikat ist nicht C.ZD.TLS_S, Fehlercode: 4189
	(→2b) Fehler beim Beziehen der Updatelisten, Fehlercode: 4190

Nichtfunktionale Anforderungen	Der Konnektor muss die Vorgaben aus [gemSpec_Krypt#3.3.2] für TLS-Verbindungen und hinsichtlich ECC-Migration die Vorgaben aus [gemSpec_Krypt#5] befolgen.
Zugehörige Diagramme	keine

Tabelle 351: TAB_KON_669 Fehlercodes TUC_KON_282 „UpdateInformationen beziehen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases, sowie der Fehlercodes von „I_KSRS_Download::listUpdates Response“ können folgende weitere Fehlercodes auftreten:			
4188	Technical	Error	Konfigurationsdienst nicht erreichbar, konfigurierte Adresse kontrollieren.
4189	Security	Fatal	Konfigurationsdienst liefert falsches Zertifikat
4190	Technical	Error	Fehler beim Beziehen der Updatelisten

[<=]

4.3.9.3.4 TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“

TIP1-A_5153 - TUC_Kon_283 „Infrastruktur Konfiguration aktualisieren“
Der Konnektor MUSS den technischen Use Case TUC_Kon_283 „Infrastruktur Konfiguration aktualisieren“ umsetzen.

Tabelle 352: TAB_KON_799 – TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“

Element	Beschreibung
Name	TUC_KON_283 Infrastruktur Konfiguration aktualisieren
Beschreibung	Dieser TUC liest die Infrastrukturdaten vom KSR ein.
Auslöser	Automatisch einmal täglich; BOOTUP, Administrator
Vorbedingungen	Der TUC_KON_304 „Netzwerk-Routen einrichten“ MUSS fehlerfrei durchgelaufen sein. Der TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“ MUSS fehlerfrei durchgelaufen sein.
Eingangsdaten	Keine
Komponenten	Konnektor, Konfigurationsdienst
Ausgangsdaten	Keine

Standardablauf	Der Konnektor MUSS folgende Schritte durchlaufen:
	1. „Einlesen des Konfigurations-XML“:
	a. Der Konnektor MUSS eine TLS-Verbindung zum Konfigurationsdienst anhand des in MGM_KSR_KONFIG_URL angegebenen Parameters aufbauen. Dabei MUSS er das durch den Server präsentierte Zertifikat mittels TUC_KON_037 „Zertifikat prüfen“ {
	certificate = C.ZD.TSL-S;
	qualifiedCheck = not_required;
	offlineAllowNoCheck = true;
	policyList = oid_zd_tls_s;
	intendedKeyUsage = intendedKeyUsage(C.ZD.TSL-S);
	intendedExtendedKeyUsage = id-kp-serverAuth;
	validationMode = OCSP}
	auf Gültigkeit prüfen.
	Das Server-Zertifikat C.ZD.TLS-S MUSS für den Konfigurationsdienst ausgestellt sein.
	b. Herunterladen der Konfigurationsdaten mittels I_KSRS_Download::get_Ext_Net_Config (MGM_KSR_KONFIG_URL, „Bestandsnetze.xml“)
	2. Beenden der TLS-Verbindung
	„Prüfen der Versionskennung auf Änderungen“:
	Wenn das Element /Infrastructure/Version der heruntergeladenen Datei keine höhere Versionsnummer als die aktuell im Konnektor hinterlegte Version trägt, muss der TUC ohne Fehler beendet und ein Protokolleintrag geschrieben werden:
	TUC_KON_271 „Schreibe Protokolleintrag“ {
	topic = „KSR/UPDATE_KONFIG“;
	eventType = Op;
	severity = Info;
	parameters = („AlteVersion=$aktuelleVersion, NeueVersion=/Infrastructure/Version“)}
	3. Aktualisieren der Gesamtnetzliste
	Alle in der Datei enthaltenen Netzsegmente sind nach ANLW_BESTANDSNETZE zu übernehmen. In Abhängigkeit von ANLW_IA_BESTANDSNETZE sind neue angeschlossene Netze des Gesundheitswesens mit aAdG-NetG nach ANLW_AKTIVE_BESTANDSNETZE zu übernehmen. Identifiziert wird ein Bestandsnetz hierbei an dessen ID in der Bestandsnetze.xml (<ID>). War der Aktivierungsstatus eines dieser Netze bereits durch den Administrator manuell konfiguriert, so muss dieser Status erhalten bleiben.
	4. „Aktualisieren von Konfigurationsinformationen“
	Haben sich Konfigurationsdaten zu einem in ANLW_AKTIVE_BESTANDSNETZE gelisteten Netz verändert, so
	a. sind die Änderungen entsprechend zu übernehmen und zu aktivieren (Anpassung ANLW_AKTIVE_BESTANDSNETZE, DHCP_AKTIVE_BESTANDSNETZE_ROUTES,

	DNS_SERVERS_BESTANDSNETZE).
	b. alle Statusänderungen an ANLW_AKTIVE_BESTANDSNETZE sind zu protokollieren. Der Protokolleintrag je Änderung enthält den Status, <ID>, <Name> und <NetworkAddress/NetworkPrefix> als topic=KSR/UPDATE_KONFIG,protocolType=OP und protocolSeverity=INFO.
	c. ist anschließend TUC_KON_304 „Netzwerk-Routen einrichten“ aufzurufen
	5. „Entfernen von nicht mehr gültigen angeschlossenen Netzen des Gesundheitswesens mit aAdG-NetG“
	Ist ein Netz in der neuen Datei gegenüber der alten Datei nicht mehr vorhanden, so:
	a. a) sind alle diesbezüglichen Daten zu entfernen und die Änderungen direkt aktiv zu schalten (Anpassung ANLW_AKTIVE_BESTANDSNETZE, DHCP_AKTIVE_BESTANDSNETZE_ROUTES, DNS_SERVERS_BESTANDSNETZE).
	b. b) ist anschließend TUC_KON_304 „Netzwerk-Routen einrichten“ aufzurufen.
	6. Protokollierung der heruntergeladenen Version von Bestandsnetze.xml durch Aufruf von TUC_KON_271 „Schreibe Protokolleintrag“ {
	topic = „KSR/UPDATE_KONFIG“;
	eventType = Op;
	severity = Info;
	parameters = („AlteVersion=$aktuelleVersion, NeueVersion=/Infrastructure/Version“)}

Varianten/Alternativen	Keine
Fehlerfälle	(→ 1-5) Es ist ein unerwarteter Fehler aufgetreten; Fehlercode: 4198
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 353: Tab_Kon_726 Fehlercodes TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4198	Technical	Error	Beim Übernehmen der angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG ist ein Fehler aufgetreten.

[<=]

4.3.9.4 Interne TUCs, auch durch Fachmodule nutzbar

4.3.9.4.1 TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“

TIP1-A_6018 - TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“
Der Konnektor MUSS den technischen Use Case TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“ umsetzen.

Tabelle 354: TAB_KON_833 – TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“

Element	Beschreibung
Name	TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“
Beschreibung	Dieser TUC ermittelt vom zentralen Konfigurationsdienst für ein Fachmodul die verfügbaren UpdateInformationen eines angegebenen SW-Pakets.
Auslöser	• Aufruf durch Fachmodul
Vorbedingungen	• Verbindung zum VPN-Konzentrator der TI wurde erfolgreich aufgebaut
Eingangsdaten	• productVendorID [String] - (Identifiziert den Hersteller des Produkts, für welches auf Updates geprüft werden soll.) • productCode [String] – (Identifiziert das Produkt zusammen mit ProductVendorID, für welches auf Updates geprüft werden soll.) • hwVersion [String] (Identifiziert die Hardware zusammen mit ProductCode und ProductVendorID, für welches auf Updates geprüft werden soll. [gemSpec_OM] beschreibt dieses Element ausführlich.) • fwVersion [String] aktuell im Produkt verwendete Firmwareversion Hinweis: Definition von productVendorID, productCode, hwVersion, fwVersion (entspricht FWVersion) siehe [gemSpec_KSR#TIP1-A_3331]
Komponenten	Konnektor, Konfigurationsdienst
Ausgangsdaten	• listOfUpdates [listUpdatesResponse] Liste von Update Informationen der verfügbaren Pakete für das angegebene Produkt; Datentyp listUpdatesResponse definiert in Konfigurationsdienst.xsd siehe [gemSpec_KSR]
Nachbedingungen	keine

Standardablauf	Der Konnektor MUSS folgende Schritte durchlaufen:
	1. Der Konnektor MUSS die TLS-Verbindung zum Konfigurationsdienst anhand des in MGM_KSR_FIRMWARE_URL angegebenen Wertes aufbauen. Dabei MUSS er das durch den Server präsentierte Zertifikat mittels
	TUC_KON_037 „Zertifikat prüfen“ {
	certificate = C.ZD.TSL-S;
	qualifiedCheck = not_required;

	offlineAllowNoCheck = true;
	policyList = oid_zd_tls_s;
	intendedKeyUsage = intendedKeyUsage(C.ZD.TSL-S);
	intendedExtendedKeyUsage = id-kp-serverAuth;
	validationMode = OCSP}
	auf Gültigkeit prüfen.
	Das Server-Zertifikat C.ZD.TLS-S MUSS für den Konfigurationsdienst ausgestellt sein.
	2. Belegen von listUpdatesRequest mit den korrekten Werten für ProductVendorID, ProductCode, HardwareVersion und FirmwareVersion = fwVersion
	3. Aufruf von I_KSRS_Download::list_Updates gemäß [gemSpec_KSR#TIP1-A_3331]
	4. Beenden der TLS-Verbindung

Varianten/Alternativen	Keine
Fehlerfälle	Fehler in den folgenden Schritten des Ablaufs führen zu: (→1) Konfigurationsdienst nicht erreichbar, Fehlercode: 4188 (→1) Serverzertifikat ist nicht C.ZD.TLS_S, Fehlercode: 4189 (→3) Fehler beim Beziehen der Updatelisten, Fehlercode: 4190
Nichtfunktionale Anforderungen	Der Konnektor muss die Vorgaben aus [gemSpec_Krypt#3.3.2] für TLS-Verbindungen und hinsichtlich ECC-Migration die Vorgaben aus [gemSpec_Krypt#5] befolgen.
Zugehörige Diagramme	keine

Tabelle 355: TAB_KON_834 Fehlercodes TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases, sowie der Fehlercodes von „I_KSRS_Download::listUpdates Response“ können folgende weitere Fehlercodes auftreten:			
4188	Technical	Error	Konfigurationsdienst nicht erreichbar, konfigurierte Adresse kontrollieren.
4189	Security	Fatal	Konfigurationsdienst liefert falsches Zertifikat
4190	Technical	Error	Fehler beim Beziehen der Updatelisten

[<=]

4.3.9.4.2 TUC_KON_286 „Paket für Fachmodul laden“

TIP1-A_6019 - TUC_KON_286 „Paket für Fachmodul laden“
Der Konnektor MUSS den technischen Use Case TUC_KON_286 „Paket für Fachmodul laden“ umsetzen.

Tabelle 356: TAB_KON_835 – TUC_KON_286 „Paket für Fachmodul laden“

Element	Beschreibung

Name	TUC_KON_286 „Paket für Fachmodul laden“
Beschreibung	Dieser TUC lädt ein bestimmtes SW-Paket für ein Fachmodul vom zentralen Konfigurationsdienst.
Auslöser	Aufruf durch Fachmodul
Vorbedingungen	• Verbindung zum VPN-Konzentrator der TI wurde erfolgreich aufgebaut
Eingangsdaten	• filename (Filename des SW-Pakets, welches vom KSR geladen werden soll)
Komponenten	Konnektor, Konfigurationsdienst
Ausgangsdaten	• swPackage (das durch filename am KSR identifizierte SW-Paket wurde heruntergeladen)
Nachbedingungen	keine

Standardablauf	1. Der Konnektor MUSS die TLS-Verbindung zum Konfigurationsdienst anhand des in MGM_KSR_FIRMWARE_URL angegebenen Wertes aufbauen. Dabei MUSS er das durch den Server präsentierte Zertifikat mittels
	TUC_KON_037 „Zertifikat prüfen“ {
	certificate = C.ZD.TSL-S;
	qualifiedCheck = not_required;
	offlineAllowNoCheck = true;
	policyList = oid_zd_tls_s;
	intendedKeyUsage = intendedKeyUsage(C.ZD.TSL-S);
	intendedExtendedKeyUsage = id-kp-serverAuth;
	validationMode = OCSP}
	auf Gültigkeit prüfen.
	Das Server-Zertifikat C.ZD.TLS-S MUSS für den Konfigurationsdienst ausgestellt sein.
	2. Herunterladen der Softwarepakets swPackage mittels I_KSRS_Download::get_File (MGM_KSR_FIRMWARE_URL /$filename)
	3. Beenden der TLS-Verbindung
	4. swPackage an Aufrufer zurückgeben

Varianten/Alternativen	keine
Fehlerfälle	(→ 1) Verbindung zum KSR konnte nicht aufgebaut werden; Fehlercode: 4188 (→ 1) Serverzertifikat ist nicht C.ZD.TLS_S, Fehlercode: 4189 (→ 2) Wenn Größe des Pakets größer als 25MB, Fehlercode: 4242 (→ 2) Sonstige Fehler beim Download: Das Paket konnte nicht geladen werden, Fehlercode: 4238
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 357: TAB_KON_836 Fehlercodes TUC_KON_286 „Paket für Fachmodul laden“

Fehlercode	ErrorType	Severity	Fehlertext

Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4188	Technical	Error	Konfigurationsdienst nicht erreichbar, konfigurierte Adresse kontrollieren.
4189	Security	Fatal	Konfigurationsdienst liefert falsches Zertifikat
4238	Technical	Error	Der Download des Pakets vom KSR ist fehlgeschlagen.
4242	Technical	Error	Der Download des Pakets vom KSR ist fehlgeschlagen. Das Paket ist größer als 25MB.

[<=]

4.3.9.5 Operationen an der Außenschnittstelle

Keine.

4.3.9.6 Betriebsaspekte

4.3.9.6.1 TUC_KON_284 KSR-Client initialisieren

TIP1-A_5938 - TUC_KON_284 „KSR-Client initialisieren“
Der Konnektor MUSS in der Bootup-Phase TUC_KON_284 „KSR-Client initialisieren“ durchlaufen.

Tabelle 358: TAB_KON_864~~TAB_KON_644~~ – TUC_KON_284 „KSR-Client initialisieren“

Element	Beschreibung
Name	TUC_KON_284 ”KSR-Client initialisieren”
Beschreibung	Der Konnektor muss während des Bootups die Downloadpunkte für Konfigurationsdaten und Firmware ermitteln.
Eingangsanforderung	Keine
Auslöser und Vorbedingungen	Bootup Verbindung zum VPN-Konzentrator TI muss aufgebaut sein
Eingangsdaten	Keine
Komponenten	Konnektor
Ausgangsdaten	• MGM_KSR_KONFIG_URL • MGM_KSR_FIRMWARE_URL
Standardablauf	- Falls MGM_LU_ONLINE=Enabled: - Durch DNS-Anfragen an den DNS-Forwarder zur Auflösung der SRV-RR und TXT-RR mit den Bezeichnern „_ksrkonfig._tcp.ksr.<TOP_LEVEL_DOMAIN_TI>„ und „_ksrfirmware._tcp.ksr.<TOP_LEVEL_DOMAIN_TI>„ erhält der Konnektor URLs der Downloadpunkte des KSR für Konfigurationsdaten (MGM_KSR_KONFIG_URL) und für Firmware (MGM_KSR_FIRMWARE_URL).

Varianten/Alternativen	Keine
Fehlerfälle	Keine
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 359: TAB_KON_822 Fehlercodes TUC_KON_284 „KSR-Client initialisieren“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.			

[<=]

TIP1-A_4835 - Konfigurationswerte des KSR-Client
Der Administrator MUSS die in TAB_KON_670 aufgelisteten Parameter über die Managementschnittstelle konfigurieren und die in TAB_KON_820 aufgelisteten Parameter ausschließlich einsehen können.

Tabelle 360: TAB_KON_670 Konfigurationsparameter der Software-Aktualisierung

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_KSR_ AUTODOWNLOAD	Enabled/ Disabled	Der Administrator MUSS den automatischen Download verfügbarer Update-Pakete über den Konfigurationsparameter MGM_KSR_AUTODOWNLOAD an- und abschalten können. Default-Wert: Enabled
MGM_KSR_SHOW_ TRIAL_UPDATES	Enabled / Disabled	Der Administrator MUSS einschalten können, dass zusätzlich zur Anzeige von Update-Paketen für den Online-Produktivbetrieb auch die Anzeige von Erprobungs-Update-Paketen erfolgt. Wenn MGM_KSR_SHOW_TRIAL_UPDATES von Disabled auf Enabled gesetzt wird, muss ein Warnhinweis angezeigt werden, dass die Installation von Erprobungs-Update-Paketen nur für Teilnehmer der Erprobungen vorgesehen ist. Default-Wert: Disabled
MGM_KSR_AUTO_UPDATE	Enabled / Disabled	Der Administrator MUSS pro Gerät (Konnektor und Kartenterminals) das automatische Softwareupdate ein- und ausschalten können. Default-Wert: Disabled

MGM_KSR_AUTO_UPDATE_TIME	Wochentag / Uhrzeit Oder täglich / Uhrzeit	Der Administrator MUSS den Wochentag und die Uhrzeit einstellen können, wann automatische Softwareupdates durchgeführt werden. Als Wochentag MUSS es neben den einzelnen Wochentagen auch einen Wert für eine tägliche Prüfung auf Aktualität und gegebenenfalls Durchführung von Softwareupdates geben. Default-Wert: Montag / 1:00 Uhr

Tabelle 361: TAB_KON_820 Einsehbare Konfigurationsparameter der Software-Aktualisierung

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_KSR_KONFIG_URL	URL	SOAP-Endpunkt des Konfigurationsdienstes zum Download von Konfigurationsdaten
MGM_KSR_FIRMWARE_URL	URL	SOAP-Endpunkt des Konfigurationsdienstes zum Download der Firmware

[<=]

Hinweis: Die Adressen des Konfigurationsdienstes werden im Rahmen des VPN-Verbindungsaufbaus ermittelt (siehe [gemSpec_VPN_ZugD#5.1.1.2 TUC_VPN-ZD_0001])

TIP1-A_6025 - Zugang zur TI sperren, wenn Deadline für kritische FW-Updates erreicht

Der Konnektor MUSS täglich überprüfen, ob unter den auf die aktuelle Konnektor-Firmware anwendbaren Updates ein Update mit FWPriority = „Kritisch“ ist, dessen Deadline (entspricht `UpdateInformation/DeploymentInformation/Deadline`) abgelaufen ist, d.h. Deadline <= Systemzeit. In diesem Fall MUSS der Konnektor den Verbindungsaufbau zur TI Plattform verhindern, bestehende Verbindungen in die TI abbauen und den kritischen Betriebszustand EC_FW_Not_Valid_Status_Blocked annehmen.

[<=]

TIP1-A_4836 - Automatische Prüfung und Download von Update-Paketen

Der Konnektor MUSS täglich die folgenden Schritte durchführen:

1. TUC_KON_282 „UpdateInformationen beziehen“ aufrufen.
2. pro zurück geliefertem Listeneintrag prüfen, ob eine neuere Version enthalten ist, als auf dem zugehörigen Gerät (Konnektor selbst oder Kartenterminal) vorhanden
3. Ist für wenigstens ein Gerät eine neuere Version vorhanden, MUSS der Konnektor darüber via
   TUC_KON_256 „Systemereignis absetzen“ {
   topic = „KSR/UPDATES_AVAILABLE“;
   eventType = Op;
   severity = Info;
   parameters = (<Param>);
   doLog=false }
   informieren. Je gefundenem Update MUSS <Param> mit folgenden Werten belegt

sein:
<Param> = „ProductVendorID= $UpdateInformation/ProductVendorID;
ProductCode= $UpdateInformation/ProductCode;
ProductName=$UpdateInformation/ProductName;
FirmwareVersion=$UpdateInformation/FirmwareVersion;
Deadline=$UpdateInformation/DeploymentInformation/Deadline;
FWPriority=$UpdateInformation/Firmware/FWPriority;
FirmwareReleaseNotes=
$UpdateInformation/Firmware/FirmwareReleaseNotes“

4. Die listUpdateResponse mit neueren Firmwareversionen MÜSSEN für eine spätere Einsichtnahme durch den Administrator bereitgehalten werden (via (TIP1-A_4837) „Übersichtsseite des KSR-Client). Ein neuerlicher Abruf dieser Informationen DARF NICHT erforderlich sein.
5. Sofern ein Update-Paket für den Konnektor vorliegt, MUSS der Konnektor die mit diesem Paket gelieferten Parameter `Priority` (entspricht `UpdateInformation/Firmware/FWPriority)` und `Deadline` (entspricht `UpdateInformation/DeploymentInformation/Deadline)` auswerten und bei `KSR:Priority=Kritisch` persistent ablegen.
6. Sofern `MGM_KSR_AUTODOWNLOAD` = Enabled, MUSS der Konnektor bei Update-Paketen, die den Konnektor selbst betreffen, das Update-Paket mit der höchsten FirmwareVersion über I_KSRS_Download::get_Updates herunterladen.
7. Ist der Download von Update-Paketen für den Konnektor abgeschlossen, MUSS der Konnektor darüber via
   TUC_KON_256 „Systemereignis absetzen“ {
   topic = „KSR/UPDATE/KONNEKTOR_DOWNLOAD_END“;
   eventType = Op;
   severity = Info;
   parameters = (<Param>)}
   informieren. Je heruntergeladenem FW-Paket MUSS <Param> mit folgenden Werten belegt sein:
   <Param> = „ProductVendorID= $UpdateInformation/ProductVendorID;
   ProductCode= $UpdateInformation/ProductCode;
   ProductName=$UpdateInformation/ProductName;
   FirmwareVersion=$UpdateInformation/Firmware/FWVersion;
   Deadline=$UpdateInformation/DeploymentInformation/Deadline;
   FWPriority=$UpdateInformation/Firmware/FWPriority;
   FirmwareReleaseNotes
   =$UpdateInformation/Firmware/FirmwareReleaseNotes“
8. Sofern `MGM_KSR_AUTODOWNLOAD` = Enabled, SOLL der Konnektor bei Update-Paketen, die Kartenterminals betreffen, pro KT-Modell das Update-Paket mit der höchsten FirmwareVersion über I_KSRS_Download::get_Updates herunterladen.

Der Konnektor MUSS immer nur die neusten Update-Pakete für eine Nutzung vorhalten. Eventuell vorhandene ältere, nicht genutzte Update-Pakete KÖNNEN überschrieben werden.**[<=]**

TIP1-A_4836-02 - ab PTV4: Automatische Prüfung und Download von Update-Paketen
Der Konnektor MUSS täglich die folgenden Schritte durchführen:

TUC_KON_282 „UpdateInformationen beziehen“ aufrufen.

pro zurück geliefertem Listeneintrag prüfen, ob eine neuere Version enthalten ist, als auf dem zugehörigen Gerät (Konnektor selbst oder Kartenterminal) vorhanden

Ist für wenigstens ein Gerät eine neuere Version vorhanden, MUSS der Konnektor darüber via
TUC_KON_256 „Systemereignis absetzen“ {
topic = „KSR/UPDATES_AVAILABLE“;
eventType = Op;
severity = Info;
parameters = (<Param>);
doLog=false }
informieren. Je gefundenem Update MUSS <Param> mit folgenden Werten belegt sein:
<Param> = „ProductVendorID= $UpdateInformation/ProductVendorID;
ProductCode= $UpdateInformation/ProductCode;
ProductName=$UpdateInformation/ProductName;
FirmwareVersion=$UpdateInformation/FirmwareVersion;
Deadline=$UpdateInformation/DeploymentInformation/Deadline;
FWPriority=$UpdateInformation/Firmware/FWPriority;
FirmwareReleaseNotes=
$UpdateInformation/Firmware/FirmwareReleaseNotes“

Ist für wenigstens ein Gerät eine neuere Version vorhanden, MUSS der Konnektor in den Betriebszustand EC_FW_Update_Available übergehen.

Die listUpdateResponse mit neueren Firmwareversionen MÜSSEN für eine spätere Einsichtnahme durch den Administrator bereitgehalten werden (via (TIP1-A_4837) „Übersichtsseite des KSR-Client). Ein neuerlicher Abruf dieser Informationen DARF NICHT erforderlich sein.

Sofern ein Update-Paket für den Konnektor selbst vorliegt, MUSS der Konnektor die mit diesem Paket gelieferten Parameter `Priority` (entspricht `UpdateInformation/Firmware/FWPriority)` und `Deadline` (entspricht `UpdateInformation/DeploymentInformation/Deadline)` auswerten und bei `KSR:Priority=Kritisch` persistent ablegen.

Sofern `MGM_KSR_AUTODOWNLOAD` = Enabled, MUSS der Konnektor bei Update-Paketen, die den Konnektor selbst betreffen, das Updatepaket mit der höchsten FirmwareVersion über I_KSRS_Download::get_Updates herunterladen, falls das Update-Paket nicht bereits von einem vorherigen Download auf dem Konnektor vorhanden ist.

Sofern I_KSRS_Download::get_Updates den http Status Code 503 Server Unavailable zurückgibt, MUSS der Konnektor die Informationen aus dem zurückgegebenen Retry-After Header nutzen, um den Zeitpunkt des Retry zu bestimmen.

Ist der Download von Update-Paketen für den Konnektor abgeschlossen, MUSS der Konnektor darüber via
TUC_KON_256 „Systemereignis absetzen“ {
topic = „KSR/UPDATE/KONNEKTOR_DOWNLOAD_END“;
eventType = Op;
severity = Info;
parameters = (<Param>)}
informieren. Je heruntergeladenem FW-Paket MUSS <Param> mit folgenden Werten belegt sein:
<Param> = „ProductVendorID= $UpdateInformation/ProductVendorID;
ProductCode= $UpdateInformation/ProductCode;
ProductName=$UpdateInformation/ProductName;

FirmwareVersion=$UpdateInformation/Firmware/FWVersion;
Deadline=$UpdateInformation/DeploymentInformation/Deadline;

FWPriority=$UpdateInformation/Firmware/FWPriority;

FirmwareReleaseNotes
=$UpdateInformation/Firmware/FirmwareReleaseNotes“

Sofern `MGM_KSR_AUTODOWNLOAD` = Enabled, SOLL der Konnektor bei Update-Paketen, die Kartenterminals betreffen, pro KT-Modell das Updatepaket mit der höchsten FirmwareVersion über I_KSRS_Download::get_Updates herunterladen, falls das Update-Paket nicht bereits von einem vorherigen Download auf dem Konnektor vorhanden ist.

Sofern I_KSRS_Download::get_Updates den http Status Code 503 Server Unavailable zurückgibt, MUSS der Konnektor die Informationen aus dem zurückgegebenen Retry-After Header nutzen, um den Zeitpunkt des Retry zu bestimmen.

Der Konnektor MUSS immer nur die neusten Update-Pakete für eine Nutzung vorhalten. Eventuell vorhandene ältere, nicht genutzte Update-Pakete KÖNNEN überschrieben werden.
Nach einem erfolgreichen Download DÜRFEN die Namen der Dateien eines Update-Paketes beim Abspeichern NICHT verändert werden.**[<=]**

TIP1-A_7220 - Konnektoraktualisierung File Transfer Ranges
Der Konnektor KANN für den Download von Update-Paketen über I_KSRS_Download::get_Updates die Option Range Requests [RFC7233#3.1] zur Fortsetzung von unterbrochenen Transfers nutzen.**[<=]**

TIP1-A_4837 - Übersichtsseite des KSR-Client
Die Administrationsoberfläche des KSR-Clients MUSS dem Administrator eine Übersichtseite anbieten, die einen Geräteeintrag für den Konnektor selbst, sowie eine Liste von Geräteeinträgen für jedes Kartenterminal (CT) aus CTM_CT_LIST mit CT.IS_PHYSICAL=Ja und CT.CORRELATION>=„gepairt“ enthält.
Der Administrator MUSS die Liste der Kartenterminals nach Kartenterminalmodellen gruppieren können (gleiche Werte für ProductVendorID, ProductCode, HardwareVersion und FirmwareVersion).
Je Geräteeintrag MÜSSEN die über „Automatische Prüfung und Download von Update-Paketen“ ermittelten listUpdatesResponse bereitstehen.
Je Geräteeintrag MUSS die Version der aktuell installierten Software dargestellt werden. Sind Bestandteile der installierten Software unabhängig aktualisierbar, so MUSS für jedes der Bestandteile die Version angezeigt werden.
Der Administrator MUSS eine Aktualisierung aller listUpdatesResponse über TUC_KON_282 „UpdateInformationen beziehen“ auslösen können.
Geräteeinträge, die über listUpdatesResponse mit neuerer Firmwareversion als das zugehörige Gerät verfügen, MÜSSEN hervorgehoben werden.
Je Geräteeintrag MUSS die Zugehörigkeit der installierten Software und der Software-Updates zum Online-Produktivbetrieb oder zu einer Erprobung (inklusive Name der Erprobung) dargestellt werden.
[<=]

TIP1-A_4838 - Einsichtnahme in Update-Informationen
Für alle Geräteeinträge MUSS der Administrator zu den listUpdatesResponse sowohl die FirmwareGroupReleaseNotes als auch jedes enthaltene UpdateInformation-Element einsehen können. Dazu MUSS der Konnektor

alle Felder der Struktur verständlich umsetzen und strukturiert anzeigen (inkl. der Notes für jedes Firmwarefiles- und Documentationsfiles-Element)

jedes über das Documentationfiles-Element erreichbare Dokument auf Anforderung des Administrator herunterladen und anzeigen. Es MÜSSEN dabei mindestens die folgenden Dokumentenformate zur Anzeige gebracht werden können: Text, PDF, JPEG, TIFF

[<=]

TIP1-A_4839 - Festlegung der durchzuführenden Updates

Der Administrator MUSS in der Übersichtsliste einzelne Geräteeinträge bzw. Gruppen mit der jeweils anzuwendenden UpdateInformation für die Durchführung eines Updates markieren können.
Alternativ MUSS der Administrator neben der Markierung je Geräteeintrag bzw. Gruppe Update-Pakete lokal einspielen können (etwa durch ein Upload- bzw. Download-Interface in der Administrationsoberfläche).
Je Geräteeintrag MUSS der Administrator einen individuellen Ausführungszeitpunkt für die Durchführung des Updates einstellen können.
Der Administrator MUSS für den Geräteeintrag Konnektor festlegen können, ob dieses Update erst gestartet werden darf, wenn zuvor alle festgelegten KT-Updates erfolgreich durchlaufen wurden.
Der Administrator MUSS zu jeder Zeit die gerätebezogene Festlegung für ein Update ändern bzw. löschen können, sofern dieses konkrete Update noch nicht begonnen wurde.
Je Geräteeintrag MUSS der Administrator automatische Softwareupdates aktivieren und deaktivieren können.

[<=]

TIP1-A_4840 – Manuelles Auslösen der durchzuführenden Updates
Der Administrator MUSS für die Liste der markierten Geräteeinträge ein gesammeltes Update auslösen können. Dieses MUSS nach folgendem Muster ablaufen:

Alle Kartenterminaleinträge abarbeiten. Pro markiertem Kartenterminal:

Wenn Ausführungszeitpunkt nicht gesetzt:
Anwenden des definierten Updates mittels TUC_KON_281 „Kartenterminalaktualisierung anstoßen“

Wenn Ausführungszeitpunkt gesetzt:
Anwenden des definierten Updates mittels TUC_KON_281 sobald der Ausführungszeitpunkt erreicht ist oder, sofern der Konnektor zum Ausführungszeitpunkt nicht in Betrieb war, überschritten wurde. Konnte das Kartenterminal nicht erreicht werden, so MUSS das gesetzte Update im KSR-Client für eine spätere Anwendung erhalten bleiben (wird ereignisgesteuert neu ausgelöst).

Sofern die KonnektorUpdate-Abhängigkeit von KT-Updates nicht gesetzt wurde oder wenn alle vorgesehenen Kartenterminal-Updates durchgeführt wurden, MUSS das Konnektor-Updates mittels TUC_KON_280 „Konnektoraktualisierung durchführen“ wie folgt begonnen werden:

wenn Ausführungszeitpunkt nicht gesetzt: TUC-Aufruf direkt

wenn Ausführungszeitpunkt gesetzt: TUC-Aufruf direkt sobald der Ausführungszeitpunkt erreicht ist oder, sofern der Konnektor zum Ausführungszeitpunkt nicht in Betrieb war, überschritten wurde

~~Der Konnektor DARF NICHT automatisch ein Update für sich oder einem seiner verwalteten Kartenterminals ausführen, wenn der Administrator diesem Update zuvor nicht explizit zugestimmt hat.~~
Wenn der Administrator ein Erprobungs-Update zur Installation auswählt, MUSS er über einen Warnhinweis darüber informiert werden,

dass es sich um ein Erprobungs-Update handelt,

für welche Erprobung es vorgesehen ist,

dass das Update-Paket nur installiert werden sollte, wenn die Institution oder Organisation des Gesundheitswesens an der Erprobung teilnimmt,

dass, falls die Institution oder Organisation des Gesundheitswesens nicht an der Erprobung teilnimmt und dennoch das Update installiert wird, es zu funktionalen Einschränkungen des Konnektors kommen kann.**[<=]**

Wurde die ECC-Migration durchgeführt, so muss sichergestellt werden, dass der Konnektor auch wieder in den ursprünglichen Zustand, d.h. den Zustand vor der ECC-Migration (TI-Vertrauensanker für RSA und Firmware vor der ECC-Migration), zurückgesetzt werden kann.

A_18390 - Automatisches Auslösen der durchzuführenden Updates

Wenn für mindestens ein Gerät das automatische Softwareupdate aktiviert ist, MUSS der Konnektor zur MGM_KSR_AUTO_UPDATE_TIME die Updates nach folgendem Muster durchführen:

- Alle Geräte (Kartenterminals und Konnektor), für die `MGM_KSR_AUTO_UPDATE`=Enabled ist, werden markiert.
- Alle Kartenterminaleinträge abarbeiten.
  - Pro markiertem Kartenterminal: Anwenden des automatischen Updates mittels TUC_KON_281 „Kartenterminalaktualisierung anstoßen“

Sofern die Konnektorupdate-Abhängigkeit von KT-Updates nicht gesetzt wurde oder wenn alle vorgesehenen Kartenterminal-Updates durchgeführt wurden, MUSS für einen markierten Konnektor das Konnektor-Update mittels TUC_KON_280 „Konnektoraktualisierung durchführen“ begonnen werden.

A_18391 - Automatisches Updates nicht nachholen

Sofern der Konnektor zu MGM_KSR_AUTO_UPDATE_TIME nicht in Betrieb war, DÜRFEN die automatischen Updates später NICHT nachgeholt werden.

[<=]

A_17804 - Fallback auf Firmwareversion vor der ECC-Migration (ECC-Migration)
Nach durchgeführter ECC-Migration MUSS der Konnektor die Möglichkeit bieten, einen Downgrade auf eine Firmwareversion vor der ECC-Migration durchzuführen.
[<=]

Änderungen in gemProdT_Kon_PTV4

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_Kon]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 1: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_18387	Automatische Softwareupdates	gemSpec_Kon
A_18389	Nur Nutzung von zugelassenen Versionen	gemSpec_Kon
A_18390	Automatisches Auslösen der durchzuführenden Updates	gemSpec_Kon
A_18391	Automatisches Updates nicht nachholen	gemSpec_Kon