gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Konfigurationsdienst

Version:	2.4.0
Revision:	167278
Stand:	02.10.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_KSR

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
2.0.0	02.08.17		Initialversion Online-Rollout (Stufe 2.1)	gematik
2.1.0	14.05.18		Einarbeitung lt. Änderungsliste	gematik
2.2.0	26.10.19		Einarbeitung lt. Änderungsliste P15.9	gematik
2.3.0	15.05.19		Einarbeitung lt. Änderungsliste P18.1	gematik
			Einarbeitung lt. Änderungsliste P20.1 und 16.1/2	gematik
2.4.0	02.10.19		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes 5
1.1 Zielsetzung 5
1.2 Zielgruppe 5
1.3 Geltungsbereich 5
1.4 Abgrenzungen 5
1.5 Methodik 6
2 Systemüberblick 7
3 Systemkontext 8
3.1 Akteure und Rollen 8
3.2 Nachbarsysteme 10
4 Zerlegung des Produkttyps 12
4.1 KSR-Upload 14
4.2 KSR-Download 14
4.3 KSR-Management 15
4.4 Schnittstellen 15
5 Übergreifende Festlegungen 18
5.1 Inhalt von Firmware-Update-Paketen 18
5.2 Hersteller-Update-Informationen 20
5.3 Behandlung von Firmware-Gruppen im Konfigurationsdienst 28
5.3.1 Signatur der Datei „FirmwareGroupInfo.xml“ 35
5.4 Behandlung von Konfigurationsdatenfiles 36
5.5 Kommunikation 36
5.5.1 TLS Transport Layer Security (TLS) 36
5.5.2 IP Version 37
5.5.3 DNS Resource Record 37
5.6 Logging 38
5.7 Statistische Daten 41
5.8 Lokalisierung von Firmware 43
5.9 Kryptographische Festlegungen 45
5.9.1 Basisfunktionalität 45
5.9.2 Algorithmenwechsel 45

6 Funktionsmerkmale 47

6.1 Basisdienste 47

6.1.1 Schnittstelle I_KSRS_Download (Provided) 47

6.1.1.1 I_KSRS_Download::listUpdates 47

6.1.1.1.1 I_KSRS_Download::listUpdates Request 48

6.1.1.1.2 I_KSRS_Download::listUpdates Response 50

6.1.1.2 I_KSRS_Download::getUpdates 52

6.1.1.3 I_KSRS_Download::get_Ext_Net_Config 54

6.1.1.4 TUC_KSR_001 „Get File“ 55

6.1.1.5 KSR Download Cache 57

6.2 Organisatorische Schnittstellen 58

6.2.1 Registrierung berechtigter Nutzer 58

6.2.2 Berechtigungs- und Rollenkonzept 59

6.2.3 Uploadschnittstelle P_KSRS_Upload 60

6.2.3.1 Schnittstellendefinition 60

6.2.3.2 Eingangsprüfung durch den Konfigurationsdienst 62

6.2.3.3 Pfadreferenzen 67

6.2.3.4 Verfahren zum Erstellen eines signierten Update-Paketes 67

6.2.3.5 Signier-Tool für Update-Pakete 68

6.2.4 Managementdienste P_KSRS_Operations 69

6.2.4.1 Schnittstellendefinition 69

7 Anhang A – Verzeichnisse 76

7.1 Abkürzungen 76

7.2 Glossar 76

7.3 Abbildungsverzeichnis 76

7.4 Tabellenverzeichnis 77

7.5 Referenzierte Dokumente 79

7.5.1 Dokumente der gematik 79

7.5.2 Weitere Dokumente 80

8 Anhang B – Nutzungsbeispiel I_KSRS_Download 81

9 Anhang C – Konfigurationsdatenfile zur Anbindung von Bestandsnetzen (Netzkonfiguration aAdG-NetG) 83

1 Einordnung des Dokumentes

1.1 Zielsetzung

Das Dokument definiert die Anforderungen an den Konfigurationsdienst, inkl. der durch diesen Dienst bereitgestellten Schnittstellen.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter eines Konfigurationsdienstes der TI sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des Deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Spezifiziert werden in diesem Dokument die vom Produkttyp Konfigurationsdienst bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttyps beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang Kap. 7.5).

Die vollständige Anforderungslage für den Produkttyp Konfigurationsdienst ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps Konfigurationsdienst verzeichnet.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche innerhalb der Afo-ID und der Textmarke angeführten Inhalte.

2 Systemüberblick

Der Konfigurationsdienst der TI ist ein betriebsunterstützendes System und speichert Update-Pakete für dezentrale Produkte der TI (z. B. Konnektoren und eHealth-Kartenterminals). Unabhängig vom Konfigurationsdienst können Updates der dezentralen Komponenten auch über lokale Mechanismen geladen werden.

Der Konfigurationsdienst stellt zugelassene Update-Pakete zum Download bereit.

Darüber hinaus stellt der Konfigurationsdienst zentrale Konfigurationsdatenfiles für Konnektoren bereit.

Das Dokument spezifiziert neben den Anforderungen Interfaces hinsichtlich:

- der Bereitstellung der für den Wirkbetrieb zugelassenen Firmware-Versionen für dezentrale Produkte auf dem Konfigurationsdienst,
- der Bereitstellung der Firmware-Versionen der dezentralen Produkte für die Referenzumgebung und die Testumgebung auf dem Konfigurationsdienst,
- dem Download von Update-Paketen für dezentrale Produkte ,
- Update-Informationen, welche die Hersteller dezentraler Komponenten den Firmware-Versionen beilegen müssen,
- Statistiken über Firmware-Downloads für die Hersteller dezentraler Komponenten für ihre Produkte,
- Statistiken und Loginformationen über Firmware-Down- und Uploads, welche dem Gesamtverantwortlichen der TI (GTI) zu Verfügung gestellt werden,
- dem Download von zentralen Konfigurationsdaten-Files für Konnektoren.

Die Aktivierung der Firmware-Versionen erfolgt mittels der Gerätefunktionen der dezentralen Produkte.

Aktuell wird der Konfigurationsdienst zur Verteilung von Update-Paketen für folgende dezentrale Komponenten genutzt:

- Konnektor
- eHealth-Kartenterminals (der Konnektor ruft für seine eHealth-Kartenterminals die Update-Pakete vom Konfigurationsdienst ab)

3 Systemkontext

3.1 Akteure und Rollen

Die Abbildungen Abb_KSR_001 und Abb_KSR_011 geben einen Überblick über die externen Akteure und Use Cases des Konfigurationsdienstes.

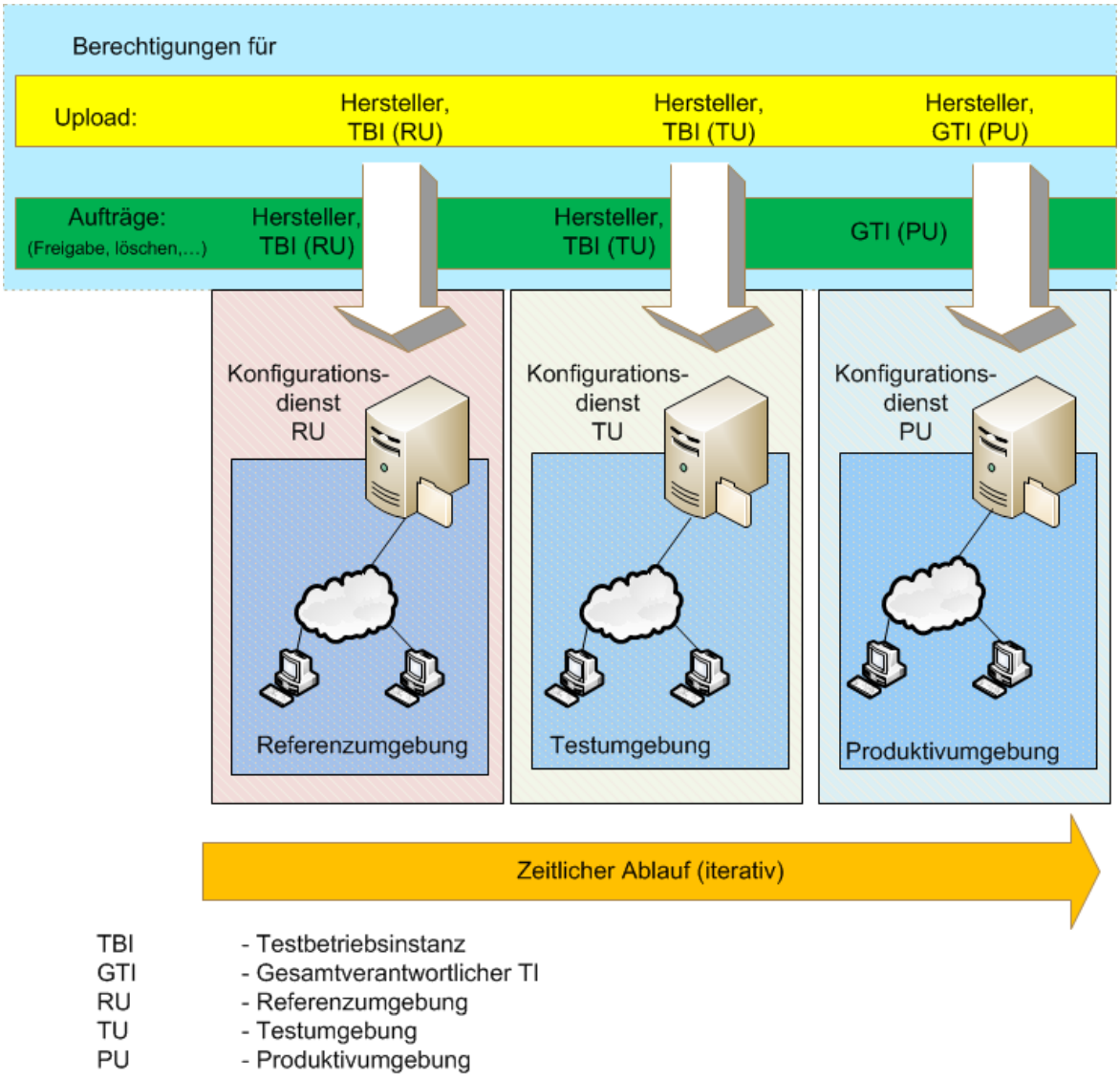


Abbildung 1: Abb_KSR_001 Überblick externe Akteure Konfigurationsdienst

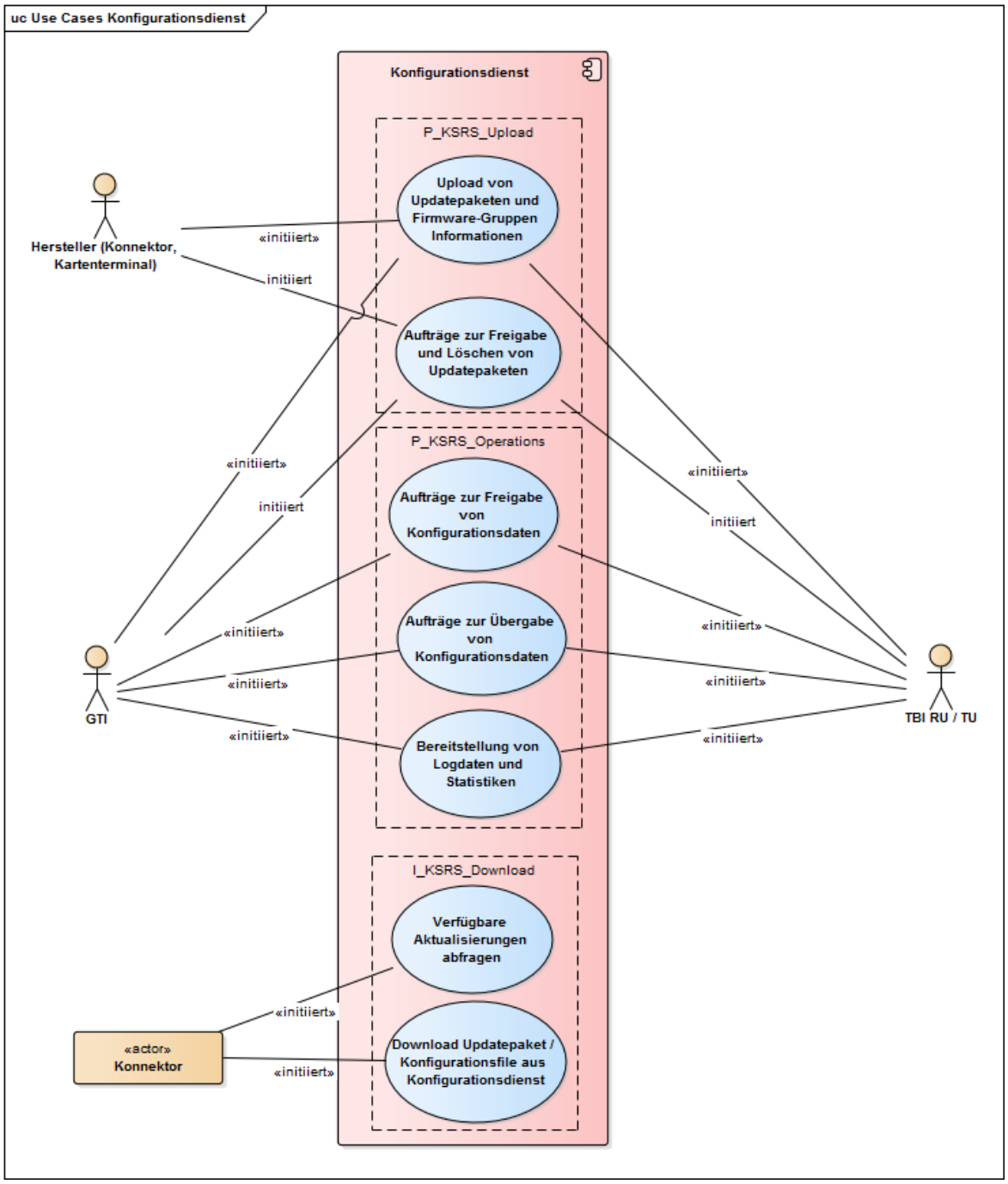


Abbildung 2: Abb_KSR_011 Überblick Use Cases Konfigurationsdienst

Der Konfigurationsdienst wird für jede Umgebung (Referenzumgebung, Testumgebung, Produktivumgebung) bereitgestellt. Für die Skalierung des Konfigurationsdienstes für die jeweilige Umgebung ist der Anbieter des Konfigurationsdienstes verantwortlich.

Die Akteure zur Erteilung von Aufträgen zum Freigeben und Löschen von Update-Paketen etc. sind abhängig von der Umgebung und werden wie folgt festgelegt:

- Referenzumgebung (RU): die ~~Testbetriebsverantwortliche~~ Testbetriebsinstanz (TBI) der RU
- Testumgebung (TU): die ~~Testbetriebsverantwortliche~~ Testbetriebsinstanz (TBI) der TU
- Produktivumgebung (PU): der ~~Servicebetriebsverantwortliche~~ Gesamtverantwortlicher ~~der~~ TI~~-Plattform (SBV-TIP~~ GTI)

Die Bereitstellung der Update-Pakete auf dem Konfigurationsdienst kann durch den Hersteller der jeweiligen dezentralen Komponente oder die oben aufgezählten Akteure der Umgebungen erfolgen. Mit der Bereitstellung der Update-Pakete werden diese noch nicht automatisch in die TI (bzw. RU/TU/PU) geladen. Dies erfolgt erst nach Freigabe durch die jeweils verantwortliche Instanz.

Aufträge zum Bereitstellen von zentralen Konfigurationsdaten im Konfigurationsdienst werden durch die verantwortliche Instanz der jeweiligen Umgebung erteilt und durch den Anbieter des Konfigurationsdienstes ausgeführt. Für diese Konfigurationsdaten erfolgt ebenfalls eine Freigabe durch die jeweils verantwortliche Instanz.

Die Anlässe, auf Grund derer berechtigte Akteure Aufträge zur Aufnahme oder Löschung von Update-Paketen an den Anbieter des Konfigurationsdienstes stellen, sind unterschiedlicher Natur und ergeben sich aus vorgelagerten Prozessen, wie beispielsweise Zulassung, Test, Release- und Changemanagement.

Die einzige Ausprägung eines zentralen Konfigurationsdatenfiles ist zu diesem Zeitpunkt das Konfigurationsdatenfile zur Netzkonfiguration aAdG-NetG (siehe Anhang C).

3.2 Nachbarsysteme

Die Abbildung Abb_KSR_002 zeigt die Nachbarsysteme und Akteure des Konfigurationsdienstes.

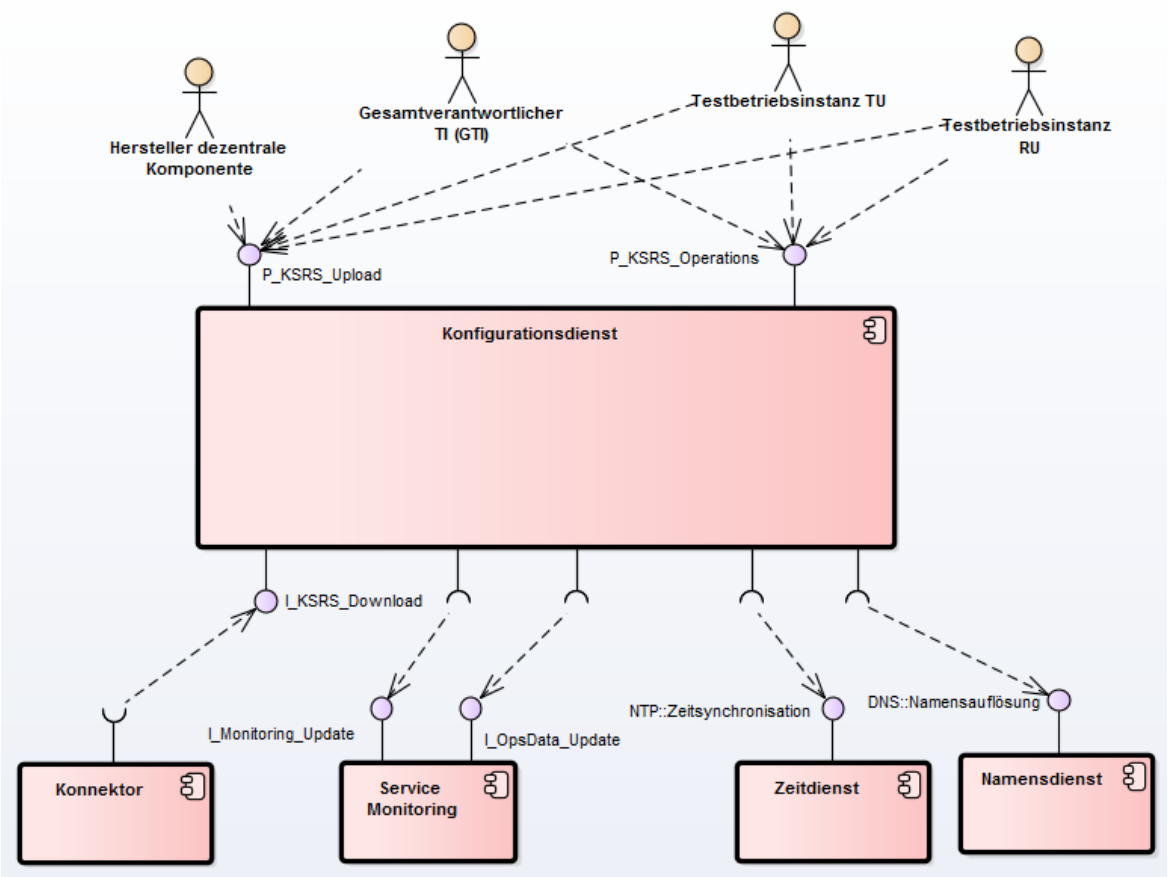


Abbildung 3: Abb_KSR_002 Kontextdiagramm Konfigurationsdienst

4 Zerlegung des Produkttyps

Im Folgenden wird die Zerlegung des Konfigurationsdienstes dargestellt, welche für die Übersicht der funktionalen Leistungsmerkmale in vorliegender Spezifikation nötig ist.

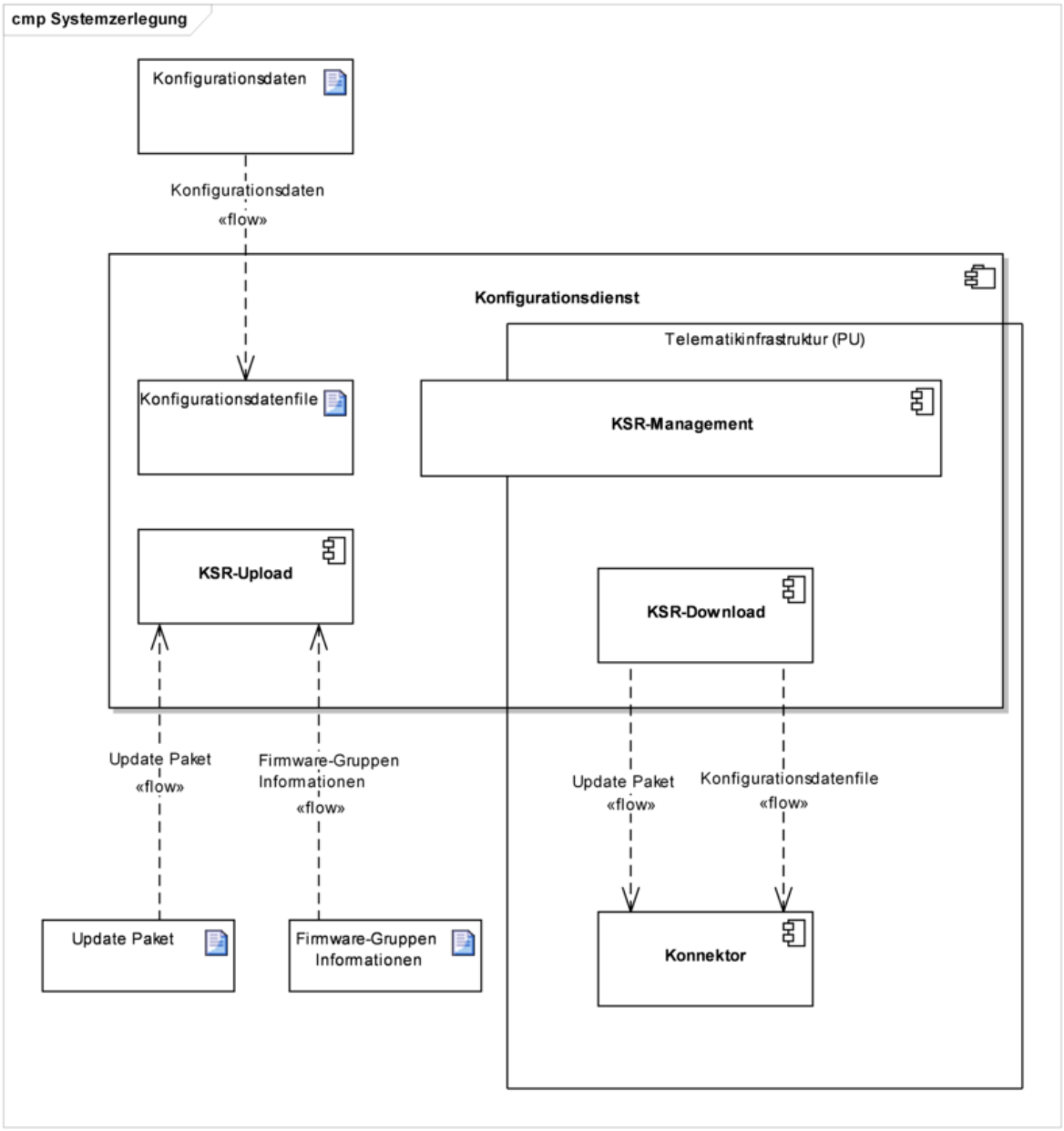


Abbildung 4: Abb_KSR_003 Zerlegung Konfigurationsdienst

Die Abbildung Abb_KSR_003 zeigt die Einbettung des Konfigurationsdienstes in die Produktivumgebung (PU).

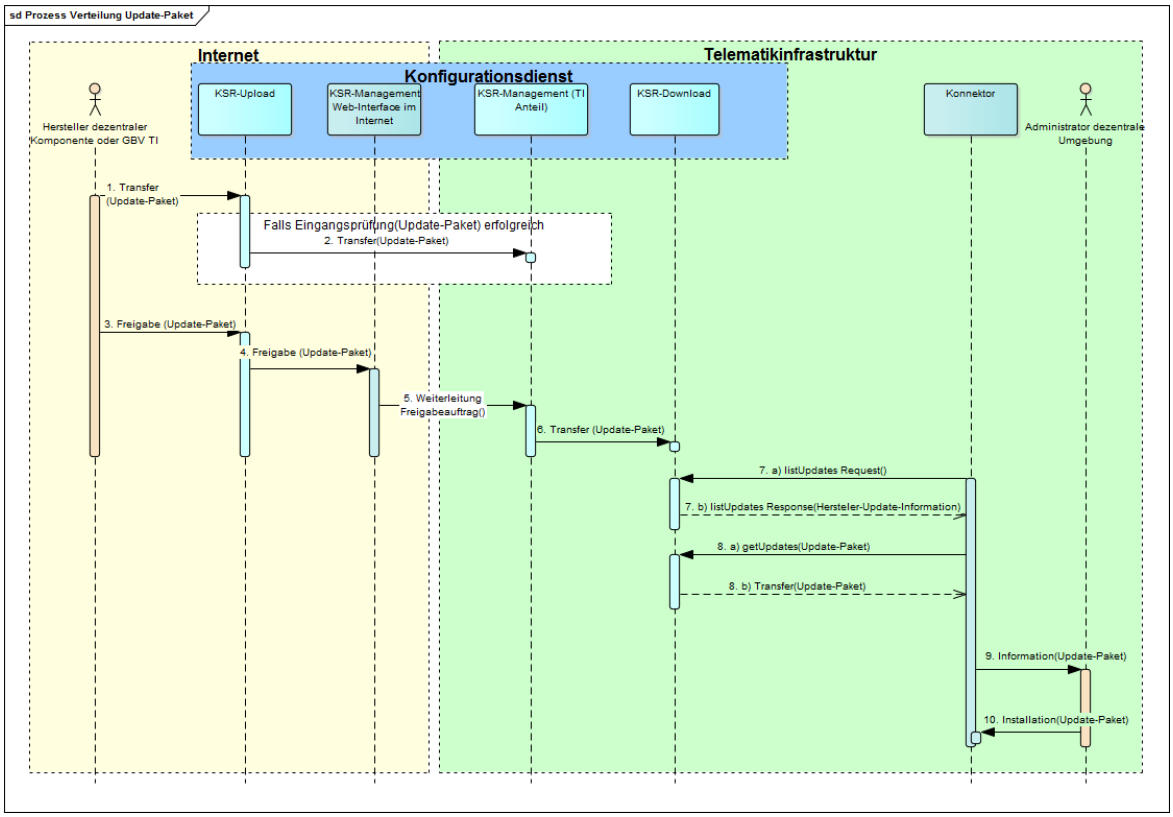


Abbildung 5: Abb_KSR_012 Verteilungsprozess Update-Paket ~~(PU)~~

Abbildung Abb_KSR_012 gibt einen Überblick über die Verteilung eines Update-Pakets in der Produktivumgebung (PU):

1. Der Hersteller der jeweiligen dezentralen Komponente transferiert das Update-Paket in den Upload-Bereich des Konfigurationsdienstes (siehe Kapitel 4.1 und 6.1.1).

~~Die Prozesse bis zur Freigabe des Update-Pakets durch den SBV-TIP werden in dieser Spezifikation nicht betrachtet.~~

2. Falls die Eingangsprüfung des Update-Paketes erfolgreich war, erfolgt der Transfer in den Managementbereich der jeweiligen Umgebung (siehe Kapitel 4.3 und 6.2.4).

Vor dem Transfer in die jeweilige Umgebung muss die Eingangsprüfung erfolgreich durchgeführt werden und das Update-Paket darf nach dieser Prüfung nicht manipulierbar sein.

3. Der ~~SBV-TIP~~GTI oder Hersteller erteilt ~~nach entsprechender Prüfung~~ die Freigabe für die jeweilige Umgebung ~~PU~~ mit einem Auftrag an den Konfigurationsdienst (siehe Kapitel 4.3 und 6.2.4).

4. Der Freigabeauftrag wird von KSR-Upload an KSR-Management weitergegeben.

5. Der Freigabeauftrag wird von KSR-Management (Internetanteil) an KSR-Management in der jeweiligen TI-Umgebung weitergegeben.

~~5. Der Freigabeauftrag wird im Konfigurationsdienst geprüft (siehe Kapitel 4.3 und 6.2.4).~~

~~Falls auch die Eingangsprüfung des Update-Paketes erfolgreich war, erfolgt der Transfer in den Downloadbereich der PU (siehe Kapitel 4.3 und 6.2.4).~~

~~Vor dem Transfer in die jeweilige Umgebung muss die Eingangsprüfung erfolgreich durchgeführt werden und das Update-Paket darf nach dieser Prüfung nicht manipulierbar sein.~~

6. Das Update-Paket wird vom Managementbereich an den Downloadbereich der jeweiligen Umgebung übergeben.

7. Der Konnektor fragt bei dem Konfigurationsdienst nach verfügbaren Updates und erhält eine Liste der aktuell verfügbaren Update-Pakete (siehe Kapitel 4.2 und 6.1.1).

8. Der Konnektor selektiert (entweder automatisch die höchste Version oder manuell durch den Administrator) ein Update-Paket und lädt es vom Konfigurationsdienst (siehe Kapitel 4.2 und 6.1.1.2).

9. Der Administrator des Konnektors wird informiert, wenn ein neues Update-Paket auf dem Konnektor vorliegt (siehe [gemSpec_Kon]).

10. Der Administrator des Konnektors installiert das Update-Paket (siehe [gemSpec_Kon]).

Für die Referenzumgebung (RU) und die Testumgebung (TU) gelten vom Prinzip her die gleichen Abläufe, jedoch erfolgt die Freigabe durch die jeweils verantwortende Instanz der Umgebung. Die Installation eines Update-Pakets auf einem Kartenterminal wird in diesem Beispiel nicht gezeigt (wäre eine Variante von Schritt 8).

4.1 KSR-Upload

Die Komponente KSR-Upload stellt folgende Funktionalitäten bereit:

- Schnittstelle zur Annahme der Update-Pakete
- Übermittlung der freigegebenen Update-Pakete an die Komponente KSR-Download
- Logging von Upload-Aktivitäten

4.2 KSR-Download

Während KSR-Upload einen direkten Zugang für die Hersteller – außerhalb der TI – bereitstellt, wird KSR-Download innerhalb der zentralen TI-Plattform der jeweiligen Betriebsumgebung angeboten. Da der Konfigurationsdienst einen Informationsfluss zwischen KSR-Upload und KSR-Download realisiert, müssen die Übergänge zwischen diesen Komponenten so geschützt werden, dass keine zusätzlichen Bedrohungen für die Betriebsumgebungen der TI entstehen (siehe [TIP1-A_3312] und [TIP1-A_3313]). Der Schutz dieser Übergänge wird auf Basis der in [gemProdT_KSR] verzeichneten Anforderungen (z.B. Anforderungen aus [gemSpec_Net]) realisiert.

TIP1-A_3312 - Nur zugelassene Update-Pakete im Downloadbereich der PU
Der Konfigurationsdienst MUSS sicherstellen, dass nur Update-Pakete in den Downloadbereich der Produktivumgebung der TI (PU) gelangen

- deren Bereitstellung im Downloadbereich der PU durch den ~~SBV-TIP~~ GTI beauftragt wurde und
- die eine Zulassung durch die gematik besitzen.

[<=]

TIP1-A_5157 - Nur freigegebene Konfigurationsdatenfiles im Downloadbereich der PU
Der Konfigurationsdienst MUSS sicherstellen, dass nur Konfigurationsdatenfiles in den Downloadbereich der Produktivumgebung der TI (PU) gelangen

- deren Bereitstellung im Downloadbereich der PU durch den ~~SBV-TIP~~ GTI beauftragt wurde.

[<=]

TIP1-A_3313 - Anzahl Update-Pakete pro dezentralem Produkt
Der Konfigurationsdienst MUSS für alle dezentralen Produkte mindestens die Update-Pakete speichern können, die der Hersteller in der aktuellen Firmware-Gruppen-Informationen referenziert. Der Speicherplatz für die Update-Pakete muss skalierbar sein.
[<=]

TIP1-A_6129 - Bereitzustellende Dateien pro Update-Paket
Der Konfigurationsdienst MUSS für jedes freigegebene Update-Paket die folgenden Dateien im KSR Downloadbereich zur Übertragung mit Operation I_KSRS_Download::getUpdates für den KSR Client bereitstellen:

- Die in UpdateInfo.xml referenzierten Dateien
- Die optionale detached Signatur „UpdateInfo.sig

[<=]

4.3 KSR-Management

KSR-Management stellt die Funktionalitäten für das Management der Update-Pakete bereit. Dazu gehören die Schnittstelle zum ~~Servicebetriebsverantwortliche~~ Gesamtverantwortlichen ~~der~~ TI ~~-Plattform~~ (~~SBV-TIP~~ GTI) sowie zu der ~~Testbetriebsverantwortlichen~~ Testbetriebsinstanz (TBI) der RU und TU.

Die ausführliche Beschreibung von KSR-Management inklusive Anforderungen enthält Kapitel 6.2.4.

4.4 Schnittstellen

Die Tabelle Tab_KSR_001 erläutert die Schnittstellen des Konfigurationsdienstes.

Tabelle 1: Tab_KSR_001 Schnittstellen des Konfigurationsdienstes

Bereitgestellte Schnittstellen		
Schnittstelle	**Nutzer**	**Spezifikation**
I_KSRS_Download	Konnektor	[gemSpec_KSR]
	Der KSR-Client im Konnektor nutzt den Konfigurationsdienst zur Aktualisierung der Firmware von dezentralen Komponenten.	
P_KSRS_Upload	Hersteller, ~~SBV-TIP~~ GTI, ~~Testbetriebsverantwortlicher~~ TBI RU/TU	[gemSpec_KSR]
	Für die dezentralen Komponenten werden Update-Pakete auf dem Konfigurationsdienst bereitgestellt.	
P_KSRS_Operations	Hersteller, ~~SBV-TIP~~ GTI, TBI ~~Testbetriebsverantwortlicher~~ RU/TU	[gemSpec_KSR]
	Der ~~Servicebetriebsverantwortliche der TI-Plattform~~ Gesamtverantwortliche TI (GTI) [gemKPT_Betr#3.1] überwacht und steuert den Betrieb der TI~~-Komponenten und gibt Update-Pakete für den Download in der PU frei~~. Für die RU und TU übernimmt diese Aufgabe die jeweilige TBI ~~Testbetriebsverantwortliche~~ und/oder der Hersteller.	
Benötigte Schnittstellen		
Schnittstelle	**Anbieter**	**Spezifikation**
I_NTP_Time_Information	Zeitdienst	[gemSpec_Net]
	Über den Zeitdienst wird innerhalb der TI die Zeit aller Komponenten synchronisiert.	
I_DNS_Name_Resolution	Namensdienst	[gemSpec_Net]
	Der Namensdienst löst Hostnamen zu IP-Adressen auf.	
I_IP Transport	Zentrales Netz TI	[gemSpec_Net]
	Das Zentrale Netz TI stellt die Transportmechanismen in der zentralen TI bereit.	
I_Monitoring_Update	Service Monitoring	[gemSpec_ServiceMon]

	Über diese Schnittstelle werden Verfügbarkeits- und Performancedaten an das Service Monitoring gesendet.	
I_OpsData_Update	Service Monitoring	[gemSpec_ServiceMon]
	Über diese Schnittstelle werden Log- und Statistikdaten an das Service Monitoring gesendet.	

Die Tabelle Tab_KSR_002 zeigt die Abbildung der – in vorliegender Spezifikation definierten – Spezifikationsschnittstellen des Konfigurationsdienstes auf die konzeptionellen Schnittstellen aus [gemKPT_Arch_TIP].

Tabelle 1: Tab_KSR_002 Schnittstellenabbildung Konfigurationsdienst

Spezifikationsschnittstelle [gemSpec_KSR]	**Konzeptionelle Schnittstelle [gemKPT_Arch_TIP]**
I_KSRS_Download	I_KSRS_Download I_KSRS_Net_Config
P_KSRS_Upload	P_KSRS_Maintenance
P_KSRS_Operations	P_KSRS_Maintenance

5 Übergreifende Festlegungen

Durch den Konfigurationsdienst werden Firmware-Update-Pakete für die dezentralen Komponenten bereitgestellt.

In den folgenden Kapiteln werden die notwendigen übergreifenden Festlegungen zur Verteilung dieser Daten beschrieben.

5.1 Inhalt von Firmware-Update-Paketen

Hersteller dezentraler Komponenten stellen Firmware-Update-Pakete bereit. Neben der Möglichkeit lokale Firmware-Updates durchzuführen werden durch den Konfigurationsdienst den dezentralen Komponenten zugelassene und geeignete Firmware-Update-Pakete zum Download bereitgestellt. Zur Verwaltung und Auswahl der geeigneten Pakete im Konfigurationsdienst sind Festlegungen zum Inhalt von Update-Paketen nötig. Dieser Inhalt muss vom Hersteller der Komponenten geliefert werden, deren Update-Pakete über den Konfigurationsdienst verteilt werden.

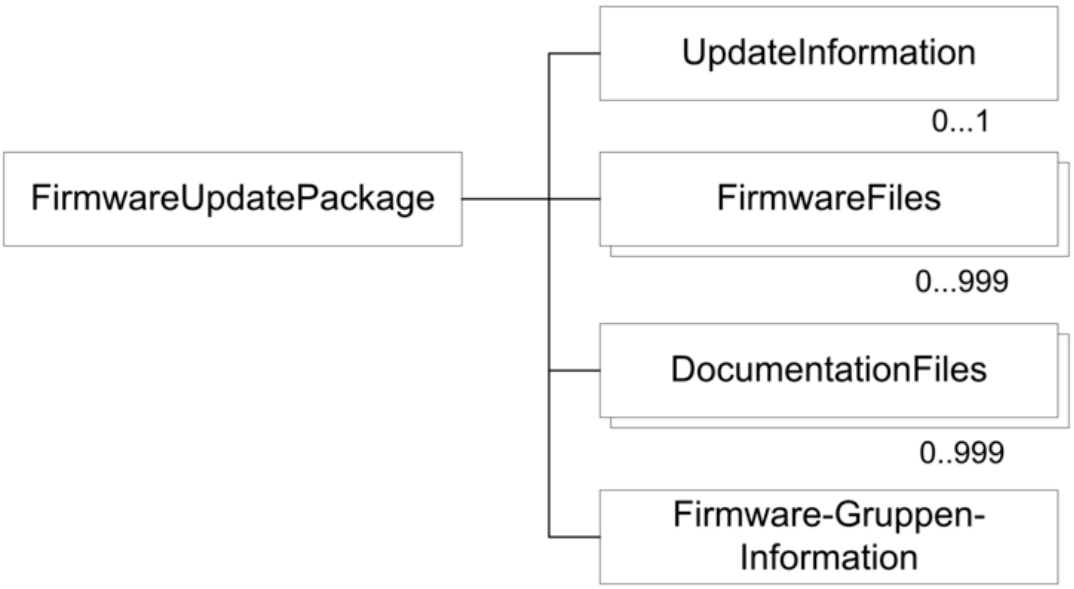


Abbildung 6: Abb_KSR_004 Inhalt von Firmware-Update-Paketen

Die Tabelle Tab_KSR_003 zeigt den Schutz der Update-Pakete und der enthaltenen Informationen. Dabei stellt der Konfigurationsdienst zusammen mit dem Hersteller einer dezentralen Komponente, die den KSR nutzt, die Integrität und Authentizität des gesamten Update-Pakets sicher. Der Schutz von enthaltenen Teilinformationen ist für den Konfigurationsdienst transparent und wird von ihm nicht geprüft.

Tabelle 2: Tab_KSR_003 Schutz der Firmware-Update-Pakete

Informationsobjekt	Schutzanforderungen	Prüfung durch	KSR Anforderungen
Updatepaket	Integritäts- und Authentizitätsschutz Gesamtpaket durch Hersteller	Konfigurationsdienst	TIP1-A_3347
UpdateInformation	Integritäts- und Authentizitätsschutz durch Hersteller	Konnektor	TIP-A_3896 TIP-A_3897
Firmwarefiles	Integritäts- und Authentizitätsschutz durch Hersteller	dezentrale Komponenten, die den KSR nutzen	siehe [gemSpec_Kon], [gemSpec_KT]
DocumentationFiles	Keine	-	Keine
Firmware-Gruppen Information	Integritäts- und Authentizitätsschutz durch Hersteller	Konfigurationsdienst	TIP1-A_3322
Konfigurationsdatenfile	Keine	-	-

TIP1-A_3314 - Inhalt Update-Paket – Hersteller-Update-Informationen
Hersteller von Komponenten, die den KSR nutzen, MÜSSEN in jedem Firmware-Update-Paket ein File mit Namen UpdateInfo.xml mit Hersteller-Update-Informationen gemäß Element UpdateInformation aus Konfigurationsdienst.xsd (siehe auch Abbildung Abb_KSR_005 und Tabellen Tab_KSR_004-009, Tab_KSR_012-020) liefern.
[<=]

TIP1-A_3895 - Inhalt Update-Paket – Konnektor FirmwareFiles
Hersteller von Konnektoren MÜSSEN in jedem Firmware-Update-Paket 0 bis maximal 999 Firmwarefile(s) liefern.
[<=]

TIP1-A_5158 - Inhalt Update-Paket – Kartenterminal FirmwareFiles
Hersteller von Kartenterminals MÜSSEN in jedem Firmware-Update-Paket genau ein Firmware File liefern.
[<=]

TIP1-A_3315 - Inhalt Update-Paket – DokumentationFiles
Hersteller von Komponenten, die den KSR nutzen, MÜSSEN in jedem Firmware-Update-Paket bis zu maximal 999 Files mit Dokumentationen für das Update liefern.

[<=]

TIP1-A_5159 - Inhalt Update-Paket – Firmware-Gruppen-Information
Hersteller von Komponenten, die den KSR nutzen, MÜSSEN in jedem Firmware-Update-Paket ein File mit der aktuell gültigen Firmware-Gruppen-Information gemäß „Abb_KSR_007 Firmware-Gruppen-Informationen“ liefern. Diese Firmware-Gruppen-Information muss der im Firmwarefile enthaltenen Information entsprechen.
[<=]

TIP1-A_3347 - Integrität und Authentizität
Der Konfigurationsdienst MUSS die Integrität und Authentizität der durch den Hersteller von Komponenten, die den KSR nutzen, übermittelten Update-Pakete (Gesamtpaket) bis zur Übertragung an den KSR-Client durch die Prüfung der Update-Paket – Signatur (TIP1-A_6123) gewährleisten.
[<=]

TIP1-A_6777 - KSR, Hersteller von Konnektoren, Deadline und alternative URL
Hersteller von Konnektoren MÜSSEN im Update-Paket in der Datei UpdateInfo.xml im Element KSR:FirmwareReleaseNotes eine URL für einen separaten Downloadpunkt des Update-Pakets im Internet angeben und, wenn das Element KSR:Priority den Wert „Kritisch“ hat, im Element UpdateInformation das Element KSR:Deadline mit einem gültigen Wert befüllen.
[<=]

TIP1-A_6778 - KSR, GTI, Deadline und alternative URL
Der ~~SBV-TIP~~ GTI MUSS im Rahmen der Freigabe eines Konnektor-Update-Pakets für die PU prüfen, dass das Update-Paket in der Datei UpdateInfo.xml im Element KSR:FirmwareReleaseNotes eine URL für einen separaten Downloadpunkt des Update-Pakets im Internet enthalten ist und, wenn das Element KSR:Priority den Wert „Kritisch“ hat, im Element UpdateInformation das Element KSR:Deadline mit einem gültigen Wert enthalten ist.
Wenn die Deadline (bei KSR:Priority = „Kritisch“) oder die URL nicht enthalten sind, muss die Freigabe abgelehnt werden.
[<=]

5.2 Hersteller-Update-Informationen

In diesem Kapitel werden die enthaltenen Hersteller-Update-Informationen erläutert. Die Befüllung und Prüfung der Hersteller-Update-Informationen (UpdateInfo.xml) erfolgt

- initial durch den Hersteller von Komponenten, die den KSR nutzen,
- durch den Anbieter des Konfigurationsdienstes erfolgt eine Eingangsprüfung und
- durch den Test in der Referenz- und Testumgebung.

TIP1-A_3896 - Signatur der Update-Informationen durch Konnektorhersteller
Konnektorhersteller MÜSSEN die Update-Informationen (UpdateInfo.xml) signieren. Dazu kann er das Element UpdateInformationSignature in den Update-Informationen oder eine detached Signatur nutzen.
[<=]

Die Update-Informationen (UpdateInfo.xml) werden durch den Konnektorhersteller signiert und gemäß Anforderung [TIP1-A_3314] und Kapitel 5.2 an den Konfigurationsdienst geliefert. Der Konfigurationsdienst liefert die Update-Informationen wiederum in Operation I_KSRS_Download::listUpdates Response als Liste von Update-Informationen an den Konnektor.

~~Der Konfigurationsdienst gewährleistet, dass die UpdateInformation-Elemente in der I_KSRS_Download::listUpdates Response an den Konnektor bis auf kanonische Transformationen gleich denen der zugehörigen Dateien in den Firmware-Update-Paketen sind.~~

~~Die Prüfung der Signatur durch den Konnektor kann durch folgende Schritte erfolgen:~~

~~1. XML-Element UpdateInformation aus der I_KSRS_Download::listUpdates Response ausschneiden und als root-Element in extra Datei ablegen, die eine XML-Deklaration zum Encoding wie die I_KSRS_Download::listUpdates Response erhält.~~

~~2. Die so erzeugte Datei wie folgt kanonisieren:~~

- ~~Inhalt des Elements KSR:UpdateInformationSignature wird entfernt.~~
- ~~Default-Namespace Deklaration wird im root-Element gesetzt.~~
- ~~XML Kanonisierung wird gemäß https://www.w3.org/TR/xml-c14n11/ durchgeführt.~~

~~Für die so erhaltene Datei kann die Signatur durch den Konnektor geprüft werden. Bei der Signaturerstellung sind diese Regeln ebenfalls zu berücksichtigen.~~

A_14538 - KSR – Richtlinien zum Erhalt der Update-Informationen Signatur
Der Konfigurationsdienst MUSS gewährleisten, dass die UpdateInformation-Elemente in der I_KSRS_Download::listUpdates Response an den Konnektor bis auf kanonische Transformationen gleich denen der zugehörigen Dateien in den Firmware-Update-Paketen sind.
Die Prüfung der Gleichheit MUSS durch folgende Schritte möglich sein:

1. XML-Element UpdateInformation aus der I_KSRS_Download::listUpdates Response ausschneiden und als root-Element in extra Datei ablegen, die eine XML-Deklaration zum Encoding wie die I_KSRS_Download::listUpdates Response erhält.
2. Die so erzeugte Datei und ursprüngliche Paketdatei wie folgt kanonisieren:
   - Inhalt des Elements KSR:UpdateInformationSignature wird entfernt.
   - Default-Namespace Deklaration wird im root-Element gesetzt.
   - XML Kanonisierung wird gemäß https://www.w3.org/TR/xml-c14n11/durchgeführt.
3. Wenn die so erhaltenen Dateien bitweise identisch sind, besteht Gleichheit, andernfalls keine Gleichheit.

[<=]

TIP1-A_3897 - Keine Signatur der Update-Informationen durch Kartenterminalhersteller
Kartenterminalhersteller SOLLEN die Update-Informationen (UpdateInfo.xml) NICHT signieren.
[<=]

Kartenterminals erhalten die Update-Informationen nicht und der Konnektor kann diese Kartenterminalherstellersignatur nicht prüfen.

Die UpdateInformation der Hersteller setzen sich aus folgenden Daten zusammen:

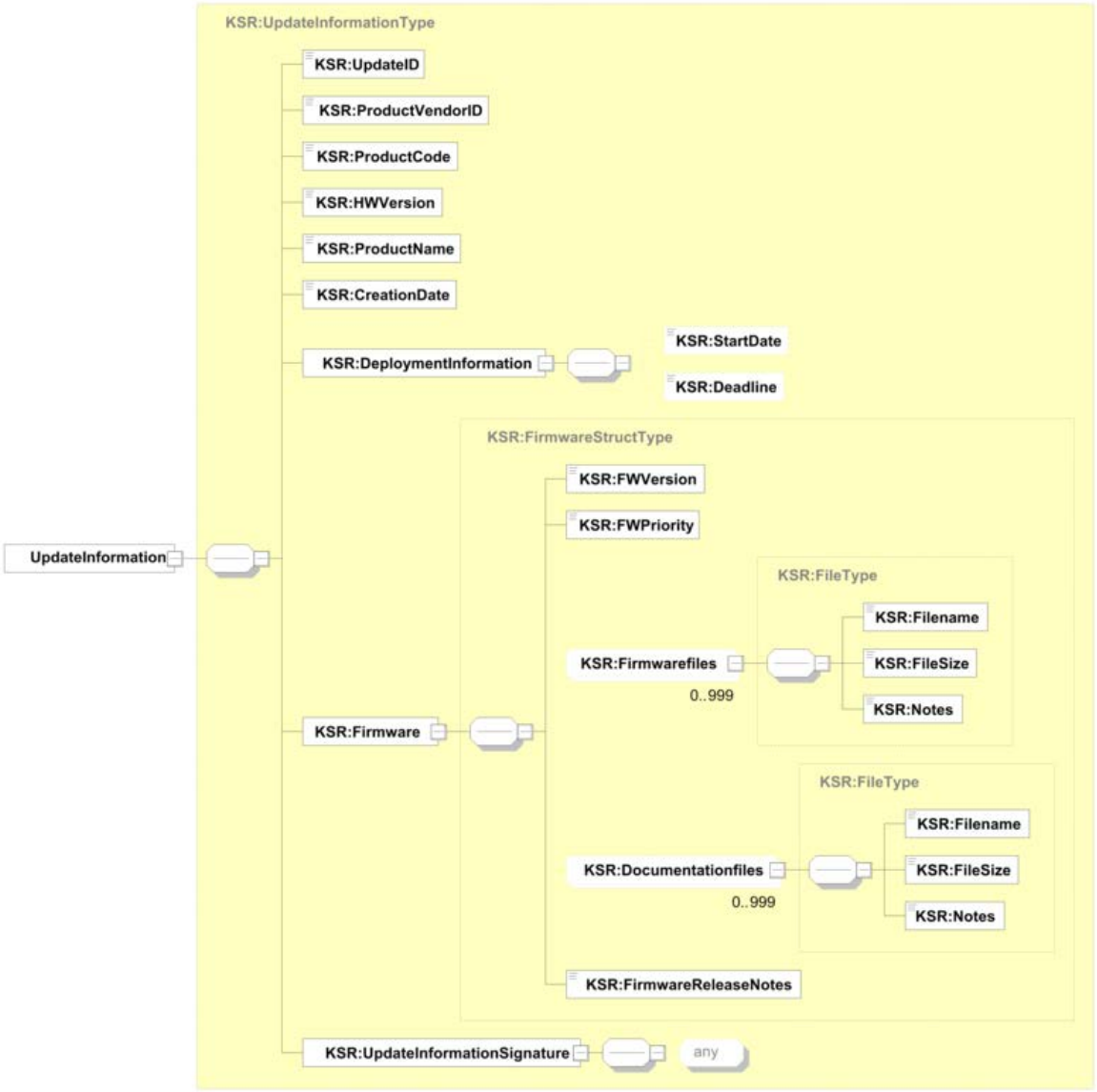


Abbildung 7: Abb_KSR_005 Hersteller-Update-Informationen (UpdateInfo.xml)

Tabelle 3: Tab_KSR_004 Hersteller-UpdateInformation – Element UpdateID

Bezeichnung	UpdateID
Beschreibung	Identifiziert das Update eindeutig.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit Pattern "[a-zA-Z0-9]{1,24}_[a-zA-Z0-9]{1,7}". Maximale Länge: 32 Zeichen Syntax: <eindeutiger Teil, max. 24 Zeichen>_<OPB oder Name der Erprobung, max. 7 Zeichen> Die UpdateID ist vom Hersteller von Komponenten, die den KSR nutzen, so

	zu generieren, dass sie für diesen Hersteller eindeutig ist und in eine URL eingebunden werden kann, d.h. die Pfadangabe zusammen mit der Hostadresse des Download-Bereiches muss eine gültige URL ergeben. Der Suffix OPB gibt an, dass es sich um ein Update-Paket für den Online-Produktivbetrieb handelt. Andere Suffixe geben an, dass es sich um ein Update-Paket für eine Erprobung handelt. Der Hersteller muss die zulässigen Erprobungs-Suffixe vor der Verwendung mit dem Gesamtverantwortlichen der TI (GTI) abstimmen. Eine einmal benutzte ID für einen Upload kann auch im Falle einer nicht bestandenen Eingangsprüfung mit anschliessender Löschung des Paketes nicht ein weiteres Mal genutzt werden.

Tabelle 4: Tab_KSR_005 Hersteller-UpdateInformation – Element ProductVendorID

Bezeichnung	ProductVendorID
Beschreibung	Identifiziert den Hersteller des Produkts, für welches das Update geeignet ist. [gemSpec_OM] beschreibt dieses Element unter der Bezeichnung „Hersteller-/Anbieter-ID“ ausführlich.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML Datentyp „string“ mit Pattern "[a-zA-Z0-9_]*". Maximale Länge 5 Zeichen.

Tabelle 5: Tab_KSR_006 Hersteller-UpdateInformation – Element ProductCode

Bezeichnung	ProductCode
Beschreibung	Identifiziert das Produkt zusammen mit dem ProductVendorID, für welches das Update geeignet ist. [gemSpec_OM] beschreibt dieses Element unter der Bezeichnung „Produktkürzel“ ausführlich.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML Datentyp „string“ mit Pattern "[a-zA-Z0-9_]*". Maximale Länge 8 Zeichen.

Tabelle 6: Tab_KSR_007 Hersteller-UpdateInformation – Element HWVersion

Bezeichnung	HWVersion
Beschreibung	Identifiziert zusammen mit ProductCode und ProductVendorID die Hardware, für welche das Update geeignet ist. [gemSpec_OM] beschreibt dieses Element ausführlich.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	nein
Wertebereich	Entspricht genau einem Eintrag mit dem Wertebereich vom XML-Datentyp

	„string“ mit Pattern „[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}“

Tabelle 7: Tab_KSR_008 Hersteller-UpdateInformation – Element ProductName

Bezeichnung	ProductName
Beschreibung	Name des Produkts, für welches das Update geeignet ist. Dies ist der ausgeschriebene Produktname. Dieses Element kann vom Client zur Auswahl des Updates genutzt werden, wenn ein sprechender Name benötigt wird. [gemSpec_OM] beschreibt dieses Element ausführlich.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 256 Zeichen.

Tabelle 8: Tab_KSR_009 Hersteller-UpdateInformation – Element CreationDate

Bezeichnung	CreationDate
Beschreibung	Datum der Firmware. Es dient der Information des Clients zur Auswahl des Updates.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „date“.

Mit den Unterelementen von DeploymentInformation kann der Hersteller Hinweise zum Aktivierungszeitraum geben:

Tabelle 9: Tab_KSR_012 Hersteller-UpdateInformation – Element DeploymentInformation.StartDate

Bezeichnung	DeploymentInformation.StartDate
Beschreibung	Frühestes Aktivierungsdatum. Falls nicht vorhanden, kann sofort aktiviert werden. Diese Information ist zur Information der dezentralen Komponente gedacht. Durch den Konfigurationsdienst wird dieser Wert nicht ausgewertet.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	ja
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „date“.

Tabelle 10: Tab_KSR_013 Hersteller-UpdateInformation – Element DeploymentInformation.Deadline

Bezeichnung	DeploymentInformation.Deadline

Beschreibung	Zeigt an, bis wann das Update aktiviert werden sollte. Falls nicht vorhanden, gibt es keine derartige Empfehlung. Diese Information ist zur Information der dezentralen Komponente gedacht. Im Element UpdateInformation muss dieses Element enthalten und mit einem Wert ausgefüllt sein, wenn das Element FWPriority den Wert „Kritisch“ hat.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	ja
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „date“.

Die Unterelemente von Firmware enthalten die Informationen zum Firmware-Update selbst:

Tabelle 11: Tab_KSR_014 Hersteller-UpdateInformation – Element Firmware.FWVersion

Bezeichnung	FWVersion
Beschreibung	Die Firmware-Version des vorliegenden Updates. [gemSpec_OM] beschreibt dieses Element ausführlich.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit Pattern "[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}"

In den „Files“-Unterelementen können mehrere FirmwareFiles und DocumentationFiles angegeben werden.

Tabelle 12: Tab_KSR_040 Hersteller-UpdateInformation – Element Firmware.FWPriority

Bezeichnung	FWPriority
Beschreibung	Mit diesem Element definiert der Hersteller der dezentralen Komponente die Kritikalität des Firmware Updates. Auf kritische Updates wird der Administrator des Konnektors besonders hingewiesen.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	nein
Wertebereich	„Normal“, „Kritisch“

In den „Files“-Unterelementen können mehrere FirmwareFiles und DocumentationFiles angegeben werden.

Tabelle 13: Tab_KSR_015 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.Filename

Bezeichnung	Files.Firmwarefiles.Filename
Beschreibung	Filename inklusive absolutem Pfad. Dieser Wert wird in der Operation getUpdates HTTP Request als Parameter <filename> genutzt.
Befüllung	Hersteller von Komponenten, die den KSR nutzen

	(z.B. „/ProductVendorID/ProductCode/UpdateID/KonFW123.fw“) Der Pfad muss der Definition in TIP1-A_6122 Pfadreferenz genügen und am Ende einen Filename enthalten, der im Update-Paket eindeutig zu finden ist.
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“.

Tabelle 14: Tab_KSR_041 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.FileSize

Bezeichnung	Files.Firmwarefiles.FileSize
Beschreibung	Größe des Files in Byte.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit Pattern "[0-9]{1,10}".

Tabelle 15: Tab_KSR_016 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.Notes

Bezeichnung	Files.Firmwarefiles.Notes
Beschreibung	Kurze Erläuterung zum Inhalt/Zweck des zugehörigen Files. Diese Information dient der Information der dezentralen Komponente.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 256 Zeichen.

Tabelle 16: Tab_KSR_017 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.Filename

Bezeichnung	Files.Documentationfiles.Filename
Beschreibung	Filename inklusive absolutem Pfad. Dieser Wert wird in der Operation getUpdates HTTP Request als Parameter <filename> genutzt.
Befüllung	Hersteller von Komponenten, die den KSR nutzen . (z.B. „/ProductVendorID/ProductCode/UpdateID/KonFW123.pdf“)
Optional	Ja
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“.

Tabelle 17: Tab_KSR_042 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.FileSize

Bezeichnung	Files.Documentationfiles.FileSize

Beschreibung	Größe des Files in Byte.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit Pattern "[0-9]{1,10}".

Tabelle 18: Tab_KSR_018 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.Notes

Bezeichnung	Files.Documentationfiles.Notes
Beschreibung	Kurze Erläuterung des zugehörigen Files. Diese Information dient der Information der dezentralen Komponente.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	Nein, falls zugehörigen File vorhanden.
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 256 Zeichen.

Tabelle 19: Tab_KSR_019 Hersteller-UpdateInformation – Element Firmware.FirmwareReleaseNotes

Bezeichnung	FirmwareReleaseNotes
Beschreibung	Durch den Hersteller erstellte Beschreibung des Updates. Hersteller von Konnektoren müssen innerhalb dieses Elements eine URL mit einem alternativen Downloadpunkt im Internet für das Update-Paket angeben.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 2048 Zeichen.

Tabelle 20: Tab_KSR_020 Hersteller-UpdateInformation – Element UpdateInformationSignature

Bezeichnung	UpdateInformationSignature
Beschreibung	Dieses Element kann ein Hersteller von Komponenten, die den KSR nutzen, zur Signatur der UpdateInformation nutzen. Die Signatur kann auch als „Detached-Signature“ in einer eigenen Datei übermittelt werden. Das Signaturverfahrenen liegt in Verantwortung des Herstellers, der Konfigurationsdienst wertet dieses Feld nicht aus.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	Ja.

Wertebereich	Any (vom Hersteller festzulegen)

Das nachfolgende Beispiel zeigt eine ausgefüllte UpdateInfo.xml. Die Datei definiert eine Firmware-Datei und eine Dokumentations-Datei. Eine Signatur ist nicht eingefügt.

```
<UpdateInformation
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://ws.gematik.de/ksr/v1.1">
  <UpdateID>Update_00000123</UpdateID>
  <ProductVendorID>Vendor1</ProductVendorID>
  <ProductCode>Kon123</ProductCode>
  <HWVersion>1.0.0</HWVersion>
  <ProductName>Konnektor123</ProductName>
  <CreationDate>2017-02-01</CreationDate>
  <DeploymentInformation>
    <StartDate>2017-04-01</StartDate>
    <Deadline>2017-06-30</Deadline>
  </DeploymentInformation>
  <Firmware>
    <FWVersion>1.0.1</FWVersion>
    <FWPriority>Normal</FWPriority>
    <Firmwarefiles>
      <Filename>/Vendor1/Kon123/Update_00000123/FW0_0_0_0.bin</Filename>
      <FileSize>12501</FileSize>
      <Notes>Firmwarefile</Notes>
    </Firmwarefiles>
    <Documentationfiles>
      <Filename>/Vendor1/Kon123/Update_00000123/FW0_0_0_0.pdf</Filename>
      <FileSize>3201</FileSize>
      <Notes>Installationsanleitung</Notes>
    </Documentationfiles>
    <FirmwareReleaseNotes>
        Release Notes der Version 1.0.1
        Informationen zu den behobenen Fehlern finden sich auf der Webseite.
        Alternativer Bezugspunkt für die Firmware:
        http://www.Vendor1.de/service/Kon123/Konektor123/
    </FirmwareReleaseNotes>
  </Firmware>
  <UpdateInformationSignature></UpdateInformationSignature>
</UpdateInformation>
```

Abbildung 8: Abb_KSR_006 Beispiel UpdateInfo.xml

5.3 Behandlung von Firmware-Gruppen im Konfigurationsdienst

Über das Firmware-Gruppenkonzept für dezentrale Komponenten wird gesteuert, welche Firmware lokal auf der Komponente installiert werden darf. Das Firmware-

Gruppenkonzept für dezentrale Komponenten wird in der Übergreifenden Spezifikation Operations und Maintenance [gemSpec_OM#2.5] beschrieben.

Die nötigen Daten für das Firmware-Gruppenkonzept sind in der Firmware der jeweiligen dezentralen Komponenten enthalten und können durch den Konfigurationsdienst nicht ausgewertet werden. Deshalb liefern die Hersteller von diesen dezentralen Komponenten in einer separaten Datei die aktuellen Firmware-Gruppen-Informationen in einem vom Konfigurationsdienst vorgegebenen Format (siehe unten). Die vom Hersteller gelieferten Firmware-Gruppen-Informationen müssen immer den Informationen, die auch in der aktuellsten Firmware selbst enthalten sind, entsprechen. Der Hersteller kann die Firmware-Gruppen-Informationen auch unabhängig von einem Firmware-Update liefern, um z. B. eine fehlerhafte Firmware-Version von der Verteilung über den Konfigurationsdienst zu entfernen. (In diesem Fall erhält zunächst nur der Konfigurationsdienst die neuen Firmware-Gruppen-Information. Zur Aktualisierung der Firmware-Gruppe in der dezentralen Komponente muss die neue Firmware-Gruppen-Information in das nächste Firmware-Update einfließen.)

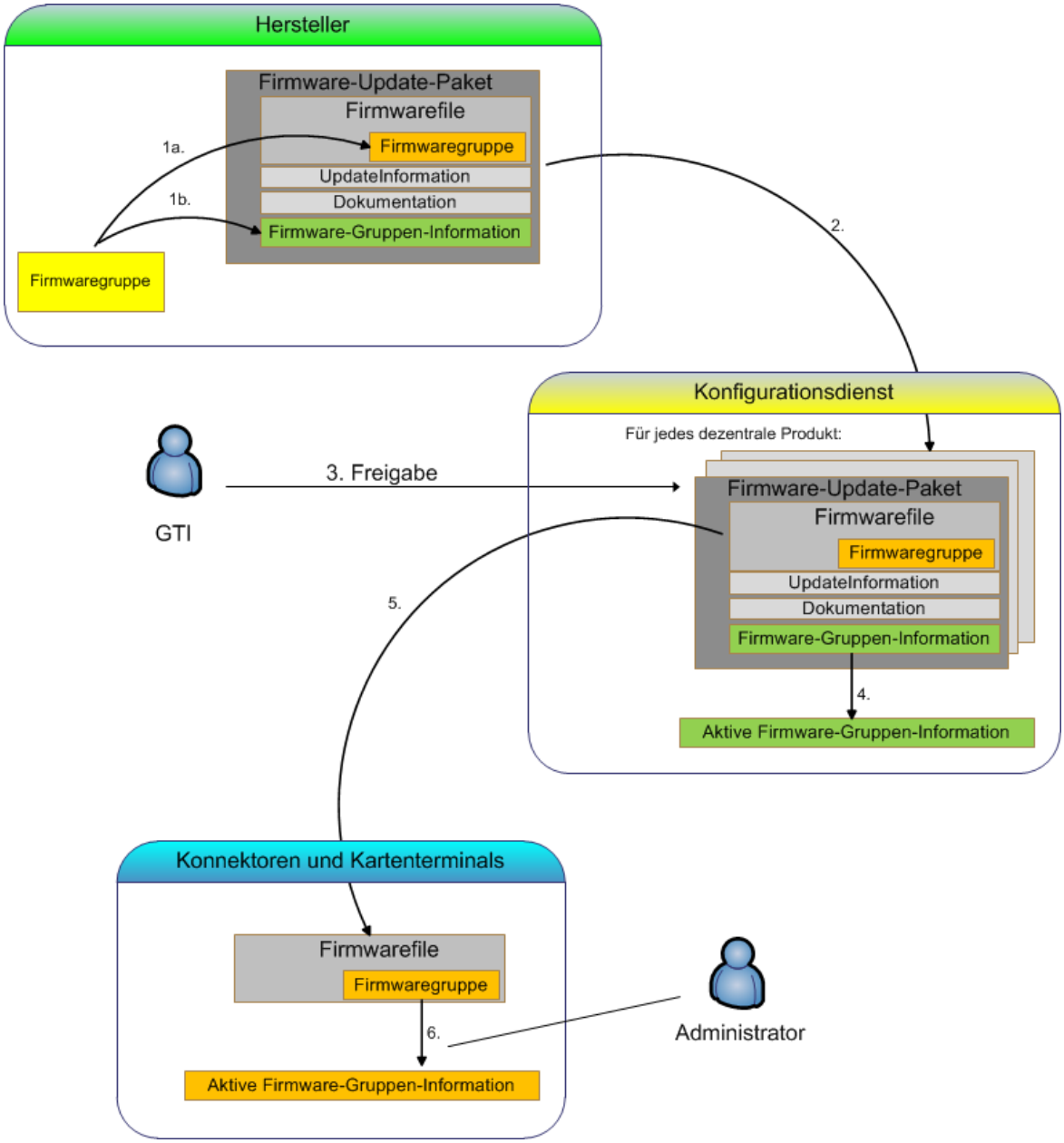


Abbildung 9: Abb_KSR_013 Verteilungsprozess Firmware-Gruppen-Informationen

Abbildung Abb_KSR_013 gibt einen Überblick über die Verteilung von Firmware-Gruppen-Informationen in der Produktivumgebung (PU) am Beispiel für einen Konnektor:

1. Der Hersteller integriert die aktuell gültige Firmware-Gruppe in das Firmwarefile und die gleichen Informationen in die Firmware-Gruppen-Information für den Konfigurationsdienst.
2. Der Hersteller transferiert das Firmware-Update-Paket zum Konfigurationsdienst.
3. Der ~~SBV-TIP~~ GTI erteilt eine Freigabe für das Firmware-Update-Paket (inklusive Firmware-Gruppe).

4. Der Konfigurationsdienst übernimmt die Firmware-Gruppen-Information falls sie eine höhere Versionsnummer hat als die aktuell gültige Firmware-Gruppen-Information und die Prüfung der Integrität und Authentizität erfolgreich war.
5. Der Konnektor lädt das Firmware File.
6. Der Administrator des Konnektors startet das Firmware Update. Der Konnektor prüft Integrität und Authentizität des Firmware Files und übernimmt die Firmware-Gruppe falls sie eine höhere Versionsnummer hat als die aktuell gültige Firmware-Gruppe.

Der Hersteller kann die Firmware-Gruppen-Information auch ohne Firmware Update liefern. Dann gilt der Ablauf bis zum Schritt 4 mit folgenden Abweichungen:

- Es wird nur die Firmware-Gruppen-Information erstellt und zum Konfigurationsdienst übertragen.
- Der ~~SBV-TIP~~ GTI erteilt die Freigabe für die Firmware-Gruppen-Information.

TIP1-A_3316 - Firmware-Gruppenkonzept Informationen für den Konfigurationsdienst
Der Hersteller einer dezentralen Komponente, welche das Firmware-Gruppenkonzept unterstützt und Firmware an den Konfigurationsdienst liefert, MUSS dem Konfigurationsdienst Informationen über die aktuelle Firmware-Gruppe bereitstellen. Der Hersteller MUSS für die aktuelle Firmware-Gruppe folgende Informationen bereitstellen:

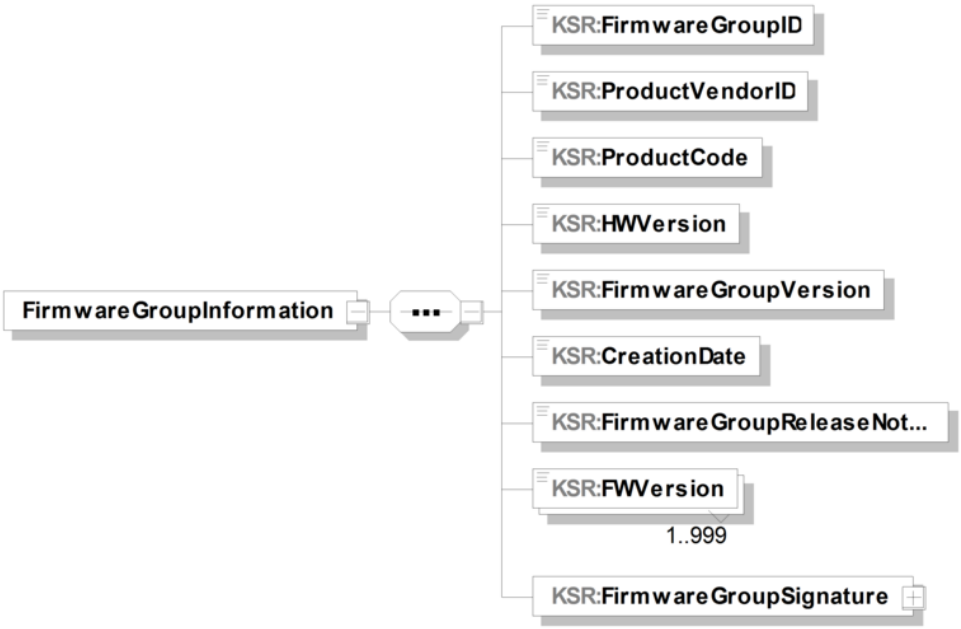


Abbildung 10: Abb_KSR_007 Firmware-Gruppen-Informationen

Tabelle 21: Tab_KSR_021 Firmware-Gruppen-Information – Element FirmwareGroupID

Bezeichnung	FirmwareGroupID
Beschreibung	Identifiziert die Firmware-Gruppe eindeutig.
Befüllung	Hersteller von Komponenten, die den KSR nutzen

Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit dem Pattern „[a-zA-Z0-9_]*“. Maximale Länge: 32 Zeichen

Tabelle 22: Tab_KSR_022 Firmware-Gruppen-Information – Element FirmwareGroupVersion

Bezeichnung	FirmwareGroupVersion
Beschreibung	Die Versionsnummer der aktuellen Firmware-Gruppe. Laut GS-A_4868 [gemSpec_OM] muss die Firmware-Gruppe mit aufsteigenden ganzzahligen Nummern versioniert werden. Der Inhalt wird als nummerisches Feld interpretiert.
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit dem Pattern „[0-9]*“ (ganzzahlige Zahlen). Maximale Länge 5 Zeichen.

Tabelle 23: Tab_KSR_023 Firmware-Gruppen-Information – Element FirmwareGroupReleaseNotes

Bezeichnung	FirmwareGroupReleaseNotes
Beschreibung	Durch den Hersteller von Komponenten, die den KSR nutzen, erstellte Beschreibung der Firmware-Gruppe. Falls es Abhängigkeiten zwischen den referenzierten Produktversionen (Update-Paketen) gibt, MUSS der Hersteller sie hier beschreiben.
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 2048 Zeichen.

Tabelle 24: Tab_KSR_024 Firmware-Gruppen-Information – Element FirmwareGroupSignature

Bezeichnung	FirmwareGroupSignature
Beschreibung	Dieses Element kann der Hersteller von Komponenten, die den KSR nutzen, zur Signatur der Firmware-Gruppen-Information nutzen. Die Signatur wird in TIP1-A_6133 definiert. Der Hersteller kann die Signatur auch als „Detached“-Signature nach dem in 5.3.1 definierten Verfahren im Update-Paket speichern. Sofern dieses Feld durch den Hersteller verwendet wird, entspricht der Inhalt des Feldes einer Detached-Signature in einem Base64-Codierten String.
Befüllung	Hersteller von Komponenten, die den KSR nutzen
Optional	Ja.
Wertebereich	Any (vom Hersteller festzulegen)

Die Parameter ProductVendorID, ProductCode, HWVersion, CreationDate und

FWVersion entsprechen den Definitionen in Tabellen Tab_KSR_005, Tab_KSR_006, Tab_KSR_007, Tab_KSR_009 und Tab_KSR_014.
Die Parameter ProductVendorID, ProductCode, HWVersion identifizieren zusammen die Hardware, für welche die Firmware-Gruppen-Information gilt.
Das Element FWVersion enthält die Liste der aktuell durch den Hersteller von Komponenten, die den KSR nutzen, unterstützten und zugelassenen Firmwareversionen. Es können bis zu 999 FWVersionen in der Liste enthalten sein.
[<=]

TIP1-A_6131 - FirmwareGroupInfo.xml und UpdateInfo.xml - Format
Der Konfigurationsdienst und Hersteller von Komponenten, die den KSR nutzen, MÜSSEN die Datei FirmwareGroupInfo.xml und UpdateInfo.xml nach folgenden Vorgaben prüfen bzw. bereitstellen:

- Die Datei verwendet das charset-encoding „UTF-8“
- Die Datei definiert den Namespace http://ws.gematik.de/ksr/v1.1 als Default-Namespace.
- Es ist keine „schemaLocation“ enthalten. Die Validierung erfolgt ausschließlich mit lokalen Schemadateien im jeweiligen System.
- Die Datei kann erfolgreich gegen das XSD-Schema „Konfigurationsdienst.xsd“ validiert werden.

[<=]

TIP1-A_3317 - Firmware-Gruppenkonzept – Lieferung mit Firmware
Hersteller von Komponenten, die den KSR nutzen, MÜSSEN die Firmware-Gruppen-Information zusammen mit dem Firmware-Update, welches die neue Firmware-Gruppe enthält an den Konfigurationsdienst übergeben.
[<=]

Mit der Eingangsprüfung der Updatepakete (siehe Anforderung TIP1-A_3346) wird die korrekte Lieferung von Firmware-Gruppen-Informationen sichergestellt.

TIP1-A_3908 - Firmware-Gruppenkonzept – Streichung Firmware
Hersteller von Komponenten, die den KSR nutzen, MÜSSEN eine aktualisierte Firmware-Gruppen-Information an den Konfigurationsdienst übergeben, wenn eine bisher enthaltene Firmwareversion ungültig (z.B. Sicherheitsproblem, fehlerhafte Firmware, nicht mehr unterstützte Firmware,…) wird.
[<=]

TIP1-A_3318 - Firmware-Gruppenkonzept – Lieferung ohne Firmware
Hersteller von Komponenten, die den KSR nutzen, KÖNNEN die Firmware-Gruppen-Information ohne Zusammenhang zu einem Firmware-Update an den Konfigurationsdienst übergeben, falls zu dieser Firmware-Gruppen-Information kein Firmware-Update gehört.
[<=]

Dies kann z.B. der Fall sein, wenn eine fehlerhafte Firmware von der Download-Liste gestrichen werden soll.

TIP1-A_3319 - Firmware-Gruppenkonzept – Aktive Firmware-Gruppen-Information
Der Konfigurationsdienst MUSS für jedes Produkt vom Produkttyp Konnektor und eHealth-Kartenterminal genau eine „aktive“ Firmware-Gruppen-Information verwalten. Ein Produkt ist eindeutig identifiziert über die Attribute

- Hersteller-/Anbieter-ID
- Produktkürzel
- Hardwareversion.

[<=]

TIP1-A_3320 - Firmware-Gruppenkonzept - Übernahme Firmware-Gruppe
Der Konfigurationsdienst MUSS die in einem Update enthaltene bzw. einzeln gelieferte Firmware-Gruppen-Information übernehmen, wenn

- eine Freigabe für das Update-Paket, welches die Firmware-Gruppen-Information enthält, bzw. die einzeln gelieferte Firmware-Gruppen-Information vorliegt und
- die Firmware-Gruppen-Information eine höhere Versionsnummer hat als die der aktuell vorliegenden Firmware-Gruppen-Information und
- Integrität und Authentizität der Firmware-Gruppen-Information erfolgreich geprüft wurde.

[<=]

TIP1-A_3321 - Firmware-Gruppenkonzept – Unterstützte Firmware Versionen
Der Konfigurationsdienst MUSS für jedes Produkt ausschließlich die Firmware-Versionen der „aktiven“ Firmware-Gruppen-Information zum Download anbieten.
[<=]

TIP1-A_3322 - Firmware-Gruppenkonzept – Integritäts- und Authentizitätsschutz
Der Konfigurationsdienst MUSS – zusammen mit dem Hersteller von Komponenten, die den KSR nutzen, – die Integrität und Authentizität der Firmware-Gruppen-Information für die gesamte Lebenszeit dieser Informationen gewährleisten.
[<=]

Das nachfolgende Beispiel zeigt den Inhalt einer ausgefüllten FirmwareGroupInfo.xml.

```
<FirmwareGroupInformation
    xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
    xmlns='http://ws.gematik.de/ksr/v1.0'>
    <FirmwareGroupID>FWG1</FirmwareGroupID>
    <ProductVendorID>CXX01</ProductVendorID>
    <ProductCode>KT25</ProductCode>
    <HWVersion>1.0.1</HWVersion>
    <FirmwareGroupVersion>23</FirmwareGroupVersion>
    <CreationDate>2014-01-14</CreationDate>
    <FirmwareGroupReleaseNotes>
        Release Notes der Version 2.10.0.
    </FirmwareGroupReleaseNotes>
    <FWVersion>2.10.0</FWVersion>
    <FWVersion>2.10.1</FWVersion>
    <FWVersion>2.10.2</FWVersion>
    <FirmwareGroupSignature>
    </FirmwareGroupSignature>

</FirmwareGroupInformation>
```

Abbildung 11: Abb_KSR_016 Beispiel aus FirmwareGroupInfo.xml

5.3.1 Signatur der Datei „FirmwareGroupInfo.xml“

Das Element „FirmwareGroupSignature“ kann der Hersteller von Komponenten, die den KSR nutzen, zur Signatur der Firmware-Gruppen-Information nutzen.

Für die Signatur der Datei „FirmwareGroupInfo.xml“ sind die in [gemSpec_Krypt#3.1] definierten Standards bindend. Dazu gehört u.a. der Signatur-Standard [ETSI-XAdES].

TIP1-A_6108 - FirmwareGroupInfo.xml Signatur
Der Konfigurationsdienst und Hersteller von Komponenten, die den KSR nutzen, MÜSSEN die Detached-Signature der FirmwareGroupInfo.xml und das in TIP1-A_6133 definierte FirmwareGroupInfo.xml - Element „FirmwareGroupSignature“ unterstützen bzw. prüfen.
[<=]

TIP1-A_6132 - Detached-Signature der FirmwareGroupInfo.xml
Bei Verwendung einer Detached-Signatur MÜSSEN Hersteller von Komponenten, die den KSR nutzen, und der Konfigurationsdienst eine Detached-Signature (UTF-8-kodierte XML-Datei) zur Datei „FirmwareGroupInfo.xml“ mit folgenden Eigenschaften bereitstellen bzw. prüfen:

- Die Signatur hat die XAdES-Form. Optionale XAdES-Attribute sind erlaubt, werden aber bei der Signaturprüfung ignoriert.
- Die Signatur erfolgt über das gesamte XML-Dokument nach Kanonisierung. Ein etwaig angegebenes URI-Attribut des zugehörigen Reference-Elements wird bei der Signaturprüfung akzeptiert, aber nicht geprüft.
- Es werden alle Kanonisierungsverfahren gemäß [XML-DSIG] unterstützt.
- Eine Transformationsvorschrift im Reference-Element über das Dokument

  <ds:Transform Algorithm=""http://www.w3.org/2000/09/xmldsig#enveloped-signature""></ds:Transform>

  wird akzeptiert, aber nicht verlangt und bei der Prüfung ignoriert.
- Die Signatur enthält das Signer-Zertifikat im XML-Block des XML-Elementes KeyInfo.
- Die Signatur ist konform mit der Anforderung [gemSpec_Krypt# GS-A_4370] und [gemSpec_Krypt#A_17360].
- Für die Signatur ist das gleiche Zertifikat zu verwenden mit dem auch das Update-Paket signiert ist.

[<=]

Hinweis zur Möglichkeit zum Erzeugen der Detached-Signature:

Erstellung einer enveloped-signature als letzter Kind-Knoten des Wurzel-XML-Elementes im Eingabe-XML-Text nach [XMLDSig] und anschließend Verschieben (Kopie und Löschen) des XML-Blockes des resultierenden XML-Elementes signature in eine neue UTF-8-kodierte XML-Datei der Detached-Signature.

TIP1-A_6133 - FirmwareGroupInfo.xml - Element „FirmwareGroupSignature“
Bei Verwendung des Elements „FirmwareGroupSignature“ in der Datei „FirmwareGroupInfo.xml“ MÜSSEN Hersteller von Komponenten, die den KSR nutzen, und der Konfigurationsdienst den Inhalt nach folgender Vorgabe bereitstellen bzw. prüfen:

- Die Signatur wurde als Detached-Signature [TIP1-A_6132] erstellt.
- Die erstellte Signatur wurde in einer UTF-8 kodierte XML-Datei gespeichert und diese als Base64-Codierter String in das Feld „FirmwareGroupSignature“ geschrieben.

[<=]

5.4 Behandlung von Konfigurationsdatenfiles

Die einzige Ausprägung eines zentralen Konfigurationsdatenfiles ist das Konfigurationsdatenfile zur Anbindung von Bestandsnetzen.

TIP1-A_5154 - Konfigurationsdatenfiles zur Anbindung von Bestandsnetzen
Der Anbieter des Konfigurationsdienstes MUSS für die über Aufträge bereitgestellten Konfigurationsdaten zur Anbindung von Bestandsnetzen Konfigurationsdatenfiles erstellen. Die Konfigurationsdatenfiles MÜSSEN auf dem XML-Schema [InfrastrukturKonfig.xsd] entsprechend Abb_KSR_014 basieren und den Vorgaben aus Tabelle Tab_KSR_045 genügen.
[<=]

Hinweis: Abb_KSR_014 und Tab_KSR_045 befinden sich im Anhang C.

TIP1-A_6134 - Konfigurationsdatenfile - Format
Der Konfigurationsdienst DARF NICHT von folgenden Vorgaben abweichende Formate akzeptieren:

- Die Datei verwendet das charset-encoding „UTF-8“
- Es ist keine „schemaLocation“ enthalten. Die Validierung erfolgt ausschließlich mit lokalen Schemadateien im jeweiligen System.
- Die Datei kann erfolgreich gegen das XSD-Schema „InfrastrukturKonfig.xsd“ validiert werden.

[<=]

5.5 Kommunikation

5.5.1 TLS Transport Layer Security (TLS)

Wie in [gemKPT_Arch_TIP] dargestellt, wird die Verbindung zwischen Konnektor und Konfigurationsdienst durch TLS abgesichert, um dem Schutzbedarf der übertragenen Informationen (Operationen listUpdates und getUpdates) zu entsprechen.

TIP1-A_3323 - Konfigurationsdienst TLS-Authentisierung
Der Konfigurationsdienst MUSS bei der Absicherung der Verbindung zum Konnektor durch TLS die einseitige Serverauthentisierung unter Nutzung des X.509-Komponentenzertifikats mit der TLS-Server-Identität ID.ZD.TLS_S zur Serverauthentisierung umsetzen.
[<=]

TIP1-A_3324 - Konfigurationsdienst TLS-Zertifikatserstellung
Der Anbieter des Konfigurationsdienstes MUSS beim zuständigen PKI-Registrierungsdienst über die Schnittstelle I_Cert_Provisioning [gemKPT_Arch_TIP] das X.509-Komponentenzertifikat mit der TLS-Server-Identität ID.ZD.TLS_S zur TLS Serverauthentisierung beantragen.

[<=]

TIP1-A_3325 - Konfigurationsdienst Keine Verbindungen ohne TLS
Der Konfigurationsdienst MUSS an der Schnittstelle zum Konnektor ausschließlich Verbindungen mit TLS akzeptieren.
[<=]

5.5.2 IP Version

TIP1-A_3326 - IPv4 und Ipv6 Unterstützung
Der Konfigurationsdienst MUSS IPv4 und IPv6 parallel unterstützen (Dual-Stack-Modus).
[<=]

5.5.3 DNS Resource Record

Die Schnittstelle I_KSRS_Download stellt Funktionen bereit, die über URLs aufgerufen werden können.

TIP1-A_6130 - Bereitstellung DNS Resource Records
Der Anbieter des KSR MUSS SRV und optional TXT Resource Records im DNS bereitstellen. Wenn die TXT Resource Records nicht existieren MÜSSEN die <PFAD1> und <PFAD2> Anteile der URL leere Strings sein.
Im DNS sind dazu folgende Einträge durch den KSR Anbieter einzutragen:

Owner	TTL	Class	Type	Data
_ksrfirmware._tcp.ksr.<TOP_LEVEL_DOMAIN_TI>	<TTL1>	<IN>	<SRV>	<Priorität1> <Gewicht1> <Port1> <FQDN1>
_ksrfirmware._tcp.ksr.<TOP_LEVEL_DOMAIN_TI>	<TTL2>	<IN>	<TXT>	"txtvers=<VERSION1>" "path=<PFAD1>"
_ksrkonfig._tcp.ksr.<TOP_LEVEL_DOMAIN_TI>	<TTL3>	<IN>	<SRV>	<Priorität2> <Gewicht2> <Port2> <FQDN2>
_ksrkonfig._tcp.ksr.<TOP_LEVEL_DOMAIN_TI>	<TTL4>	<IN>	<TXT>	"txtvers=<VERSION2>" "path=<PFAD2>"

TOP_LEVEL_DOMAIN_TI: in der PU = telematik.; in der RU/TU = telematik-test.
[<=]

Die URLs werden vom Konnektor automatisch durch Abfrage der DNS SRV und TXT Resource Records ermittelt. Vom Konnektor werden immer die SRV und TXT Resource Records abgefragt. Wenn die TXT Resource Records nicht existieren sind die <PFAD1>

und <PFAD2> Anteile der URL leere Strings.

Die URLs werden wie folgt gebildet:

URL für I_KSRS_Download::listUpdates: https://<FQDN1>:<PORT1><PFAD1>/

URL für I_KSRS_Download „Get File“:
https://<FQDN1>:<PORT1><PFAD1>/<relativer_Pfad_und_Dateiname_der_Firmware>

URL für I_KSRS_Download::get_Ext_Net_Config:
https://<FQDN2>:<PORT2><PFAD1>/Bestandsnetze.xml

Beispiele

DNS-Abfragen in der TU

[root@srv02 ~]# dig _ksrfirmware._tcp.ksr.telematik-test. SRV +noall +answer

; <<>> DiG 9.10.2-RedHat-9.10.2-0.el6 <<>> _ksrfirmware._tcp.ksr.telematik-test. SRV +noall +answer

_ksrfirmware._tcp.ksr.telematik-test. 86400 IN SRV 10 10 443 download-test.ksr.telematik-test.

[root@srv02 ~]# dig _ksrfirmware._tcp.ksr.telematik-test. TXT +noall +answer

; <<>> DiG 9.10.2-RedHat-9.10.2-0.el6 <<>> _ksrfirmware._tcp.ksr.telematik-test. TXT +noall +answer

_ksrfirmware._tcp.ksr.telematik-test. 86400 IN TXT "txtvers=1" "path=/"

[root@srv02 ~]# dig _ksrkonfig._tcp.ksr.telematik-test. SRV +noall +answer

; <<>> DiG 9.10.2-RedHat-9.10.2-0.el6 <<>> _ksrkonfig._tcp.ksr.telematik-test. SRV +noall +answer

_ksrkonfig._tcp.ksr.telematik-test. 86400 IN SRV 10 10 443 download-test.ksr.telematik-test.

[root@srv02 ~]# dig _ksrkonfig._tcp.ksr.telematik-test. TXT +noall +answer

; <<>> DiG 9.10.2-RedHat-9.10.2-0.el6 <<>> _ksrkonfig._tcp.ksr.telematik-test. TXT +noall +answer

_ksrkonfig._tcp.ksr.telematik-test. 86400 IN TXT "txtvers=1" "path=/"

5.6 Logging

Die Spezifikation [gemSpec_OM] beschreibt die allgemeinen Anforderungen an das Logging und Tracing. Im Folgenden werden die spezifischen Anforderungen an das Logging des Konfigurationsdienstes beschrieben.

TIP1-A_3328 - Logging Datenänderungen im Konfigurationsdienst
Der Konfigurationsdienst MUSS für alle Aktionen (sowohl intern wie auch an den Außenschnittstellen) mit Update-Paketen und Firmware-Gruppen-Informationen und

Konfigurationsdatenfiles Log-Informationen erfassen. Dabei MUSS mindestens folgende Information gespeichert/bereitgestellt werden:

- Wer hat etwas getan
- Was hat er getan
- Mit welchem Informationsobjekt
- Zeitpunkt der Aktion

[<=]

TIP1-A_6135 - Löschen der Logging-Daten
Der Konfigurationsdienst MUSS die gesammelten Logging-Daten nach einer konfigurierten Zeitspanne, spätestens aber nach 90 Tagen aus dem Konfigurationsdienst entfernen.

[<=]

TIP1-A_6136 - Umfang der gespeicherten Logdaten
Der Konfigurationsdienst MUSS die in Tabelle 26 „Logdatenformat“ enthaltenen Felder entsprechend ihrer Definition füllen und persistent speichern.

Tabelle 25: Tab_KSR_048 Logdatenformat

Position	Feld	Beschreibung	Typ
1	Timestamp	Zeitpunkt, zu dem die Aktion gestartet wurde.	String, Timestamp-Format „YYYY-MM-DD HH:mm:SS,SSS”, Beispiel: „2014-01-08 09:46:18,780“. Die Zeitzone ist UTC
2	UserID	Eindeutiger Identifikator des eingeloggten Users, bzw. des ausführenden Herstellers (z.B. beim Upload oder Download einer Datei). Sofern das System selbst die Aktion gestartet hat (z.B. durch einen Timer), wird das Feld mit der ID „SYSTEM_KSR“ belegt.	String, max. 32 Zeichen
3	InfoID	Identifiziert das Informationsobjekt, mit dem die Aktion ausgeführt wurde. Z.B. UpdateID, FirmwareGroupId	String, max. 255 Zeichen
4	Action	Bezeichner der durchgeführten Aktion, z.B. „FREIGABE“, „UPLOAD“,	String, max. 32 Zeichen
5	State	Status-Ergebnis der durchgeführten Aktion.	String, entweder „ERFOLG“, „FEHLER“ oder „REMOTE-FEHLER“

6	Description	Textuelle Beschreibung des Ergebnisses der ausgeführten Aktion. Kann leer sein, wenn die Aktion korrekt ausgeführt wurde, enthält in einem Fehlerfall, die Fehlerbeschreibung.	String, max. 2048 Zeichen

Der Inhalt im Feld InfoID ist abhängig von dem Wert im Feld Action nach den Angaben der folgenden Tabelle. Das Operator-Zeichen „|“ im Feld InfoID steht für ENTWEDER ODER der Parameter des Feldes. Ein Feld hat den Wert des linken Operands, wenn dieser nicht leer ist und damit gültig ist und hat andernfalls den Wert des rechten Operands.

Tabelle 26: Tab_KSR_049 Werte im Feld InfoID zu Action

Action	InfoID
FILE_UPLOAD	FILE-IDENTIFIER
INSERT_CONFIG	FILE-IDENTIFIER
PROZESS_FREIGABE_UPDATE_PAKET_AKZEPTIERT	UPDATE-ID | FIRMWAREGROUP-ID
PROZESS_FREIGABE_UPDATE_PAKET_FREIGEGEBEN	UPDATE-ID | FIRMWAREGROUP-ID
PROZESS_FREIGABE_UPDATE_PAKET_AKTIVIERT	UPDATE-ID | FIRMWAREGROUPID
PROZESS_FREIGABE_UPDATE_PAKET_ABGELEHNT	FILE-IDENTIFIER
PROZESS_FREIGABE_UPDATE_PAKET_DEAKTIVIERT	UPDATE-ID | FIRMWAREGROUP-ID
get_Updates	UPDATE-ID | Bestandsnetze.xml
list_Updates	FIRMWAREGROUP-ID
BESTANDSNETZE_UPLOAD	Bestandsnetze.xml
BESTANDSNETZE_CONFIRM	Bestandsnetze.xml
BESTANDSNETZE_REJECT	Bestandsnetze.xml

[<=]

A_17455 - KSR Logging-Daten – Bereitstellung
Der Konfigurationsdienst MUSS täglich zu einem konfigurierbaren Zeitpunkt - die im Konfigurationsdienst angefallenen - Logging-Daten entsprechend Tab_KSR_048 an die Schnittstelle I_OpsData_Update [gemSpec_SST_LD_BD] liefern. Dazu MUSS die Schnittstelle I_OpsData_Update::fileUpload benutzt werden.
Die Logging-Daten MÜSSEN für jeden vollständigen Berichtszeitraum in einer Datei mit folgenden Namenskonventionen gesendet werden:

KSR_Logging_<Start>_<Ende>.csv

<Start> und <Ende> entspricht den Festlegungen in A_17453**.**

Der Konfigurationsdienst MUSS in jedem Sendevorgang alle seit dem letzten Senden angefallenen Dateien senden.
[<=]

TIP1-A_6102 - Datei-Format Logging- und Statistik-Daten
Der Konfigurationsdienst MUSS die Logging- und Statistik-Daten im CSV-Format bereitstellen.

- Die Datei verwendet UTF-8 Codierung
- Die Zeilenenden schließen mit dem LF-Zeichen (0x10) ab.
- Das Trennzeichen zwischen den Werten ist „;“

[<=]

TIP1-A_5038 - FehlerLog
Der Konfigurationsdienst MUSS lokal erkannte Fehler und Remote-Fehler im lokalen Protokollspeicher (FehlerLog) protokollieren.
[<=]

TIP1-A_5039 - Remote-Fehlerbehandlung
Der Konfigurationsdienst MUSS für empfangene Fehlermeldungen von anderen Komponenten folgende allgemeine Vorgaben berücksichtigen:

- Empfangene Fehlermeldungen sind als Remote-Fehler zu protokollieren.
- Durch empfangene Fehlermeldungen resultierende Folgefehler KÖNNEN an die Fehlermeldung angefügt werden.

[<=]

5.7 Statistische Daten

TIP1-A_3353 - Inhalt der statistischen Daten
Der Anbieter des Konfigurationsdienstes MUSS in den statistischen Daten des Konfigurationsdienstes, die pro Produkt im Downloadbereich angefragten Updates (Operation I_KSRS_Download::listUpdates inklusive aller Parameter des Requests) und bereitgestellten Updates (Operation I_KSRS_Download::getUpdates inklusive UpdateID und Filename) inklusive aller Anfragen bei KSR Download Cache Servern, aufgeschlüsselt nach Produkt und Update-Paket (Element „UpdateID“) im zeitlichen Verlauf entsprechend Tab_KSR_046 auflisten.

Tabelle 27: Tab_KSR_046 Statistikdatenformat

Position	Feld	Beschreibung	Typ
1	Timestamp	Zeitpunkt, zu dem der Download gestartet wurde.	String, Timestamp-Format „YYYY-MM-DD HH:mm:SS,SSS”, Beispiel: „2014-01-08 09:46:18,780“. Die Zeitzone ist UTC
2	ProductVendorID	Identifiziert den Hersteller des Produkts.	String, max. 5 Zeichen Wenn „listUpdates“ aufgerufen

		[gemSpec_OM] beschreibt dieses Element unter der Bezeichnung „Hersteller-/Anbieter-ID“ ausführlich.	wurde, enthält dieses Feld den entsprechenden Parameter des Requests, beim Aufruf von „getUpdates“ die ProductVendorID der gesendeten Datei.
3	ProductCode	Identifiziert das Produkt zusammen mit der ProductVendorID. [gemSpec_OM] beschreibt dieses Element unter der Bezeichnung „Produktkürzel“ ausführlich.	String, max. 8 Zeichen Wenn „listUpdates“ aufgerufen wurde, enthält dieses Feld den entsprechenden Parameter des Requests, beim Aufruf von „getUpdates“ den ProductCode der gesendeten Datei.
4	HWVersion	Identifiziert zusammen mit ProductCode und ProductVendorID die Hardware. [gemSpec_OM] beschreibt dieses Element ausführlich.	String „[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}“) Wenn „listUpdates“ aufgerufen wurde, enthält dieses Feld den entsprechenden Parameter des Requests, beim Aufruf von „getUpdates“ die Hardware-Version der gesendeten Datei.
5	FWVersion	Firmware Version des heruntergeladenen Updates. [gemSpec_OM] beschreibt dieses Element ausführlich.	String „[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}“) Wenn „listUpdates“ aufgerufen wurde, enthält dieses Feld den entsprechenden Parameter des Requests, beim Aufruf von „getUpdates“ die Firmware-Version der gesendeten Datei.
6	Action	Ausgeführte Aktion	String, “listUpdates” für einen Aufruf der Operation “listUpdates”. “getUpdates“, wenn die Operation „getUpdates“ aufgerufen wurde.
7	UpdateID	Eindeutige Bezeichnung des Updates.	String, wenn „listUpdates“ aufgerufen wurde, ist dieses Feld leer, ansonsten enthält es die UpdateID des Paketes.
8	Filename	Dateiname des heruntergeladenen Paketes.	String, wenn „listUpdates“ aufgerufen wurde, ist dieses Feld leer, ansonsten enthält es den Filename der aufgerufenen Datei ohne den Pfad.

[<=]

TIP1-A_3354 - KSR-Statistiken – Format
Der Anbieter des Konfigurationsdienstes MUSS alle Download-Berichte und Berichte über die listUpdates Abfragen im CSV-Format bereitstellen. Die CSV-Datei MUSS im durch TIP1-A_3353 definierten Format vorliegen.
[<=]

A_17453 - KSR-Statistiken – Bereitstellung
Der Konfigurationsdienst MUSS täglich zu einem konfigurierbaren Zeitpunkt KSR-Statistiken im CSV-Format an die Schnittstelle I_OpsData_Update [gemSpec_SST_LD_BD] liefern. Dazu MUSS die Schnittstelle I_OpsData_Update::fileUpload benutzt werden.
Die Statistik-Daten MÜSSEN für jeden vollständigen Berichtszeitraum in einer Datei mit folgenden Namenskonventionen gesendet werden:

KSR_Statistik_<Start>_<Ende>.csv

- <Start> = Startzeitpunkt des Berichtsintervalls als Unixzeit-Zeitstempel in Millisekunden
  (immer volle Minuten, erster Zeitraum des Tages beginnt um 00:00 Uhr UTC)
- <Ende> = Endezeitpunkt des Berichtsintervalls als Unixzeit-Zeitstempel in Millisekunden
  (offenes Intervallende, d.h. erster Zeitpunkt, der gerade nicht mehr zum Intervall gehört, immer volle Minuten)

Der Konfigurationsdienst MUSS in jedem Sendevorgang alle seit dem letzten Senden angefallenen Dateien senden.

[<=]

5.8 Lokalisierung von Firmware

Aus besonderen Anlässen kann eine Lokalisierung von dezentralen Komponenten nötig sein. Ein Beispiel dafür ist das Finden von Geräten mit nicht zugelassener Firmware.

A_18383 - KSR, Lokalisierung von Firmware
Der Konfigurationsdienst MUSS eine tagesaktuelle Log-Datei bereitstellen, die für alle Aufrufe der Operation-I_KSRS_Download::listUpdates die Parameter entsprechend Tab_KSR_051 enthält.

Tabelle 28: Tab_KSR_051 Lokalisierungsdaten

Position	Feld	Beschreibung	Typ
1	Timestamp	Zeitpunkt, zu dem die Operation aufgerufen wurde.	String, Timestamp-Format „YYYY-MM-DD HH:mm:SS,SSS", Beispiel: „2014-01-08 09:46:18,780". Die Zeitzone ist UTC
2	ProductVendorID	Identifiziert den Hersteller des Produkts. [gemSpec_OM] beschreibt dieses Element unter der Bezeichnung „Hersteller-/Anbieter-ID" ausführlich.	String, max. 5 Zeichen Wenn „listUpdates" aufgerufen wurde, enthält dieses Feld den entsprechenden Parameter des Requests, beim Aufruf von „getUpdates" die ProductVendorID der gesendeten Datei.

3	ProductCode	Identifiziert das Produkt zusammen mit der ProductVendorID. [gemSpec_OM] beschreibt dieses Element unter der Bezeichnung „Produktkürzel“ ausführlich.	String, max. 8 Zeichen Wenn „listUpdates“ aufgerufen wurde, enthält dieses Feld den entsprechenden Parameter des Requests, beim Aufruf von „getUpdates“ den ProductCode der gesendeten Datei.
4	HWVersion	Identifiziert zusammen mit ProductCode und ProductVendorID die Hardware. [gemSpec_OM] beschreibt dieses Element ausführlich.	String „[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}“) Wenn „listUpdates“ aufgerufen wurde, enthält dieses Feld den entsprechenden Parameter des Requests, beim Aufruf von „getUpdates“ die Hardware-Version der gesendeten Datei.
5	FWVersion	Firmware-Version des heruntergeladenen Updates. [gemSpec_OM] beschreibt dieses Element ausführlich.	String „[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}“) Wenn „listUpdates“ aufgerufen wurde, enthält dieses Feld den entsprechenden Parameter des Requests, beim Aufruf von „getUpdates“ die Firmware-Version der gesendeten Datei.
6	Client Adresse	IP Adresse des Clients.	String. Darstellung entsprechend RFC791.

[<=]

A_18384 - KSR, Lokalisierungsdaten – Format
Der Konfigurationsdienst MUSS die Lokalisierungsdaten im CSV-Format bereitstellen. Die CSV-Datei MUSS im durch TIP1-A_6102 definierten Format und entsprechend A_18383 vorliegen. **[<=]**

A_18385 - KSR, Lokalisierungsdaten – Bereitstellung
Der Konfigurationsdienst MUSS die tagesaktuellen KSR-Lokalisierungsdaten im CSV-Format, reduziert um die zugelassenen bzw. genehmigten dezentralen Produkte gemäß dem gematik Fachportal, über eine organisatorische Schnittstelle zum Download bereitstellen. **[<=]**

A_18386 - KSR, Lokalisierungsdaten – Löschen
Der Konfigurationsdienst MUSS KSR-Lokalisierungsdaten automatisch nach einer konfigurierbaren Anzahl von Tagen löschen. **[<=]**

A_18495 - KSR, Lokalisierungsdaten – Abruf nur durch dedizierten VPN-Zugangsdienst
Der Anbieter des Konfigurationsdienstes MUSS sicherstellen, dass die tagesaktuellen KSR-Lokalisierungsdaten nur dem jeweiligen netzsegment-entsprechenden VPN-Zugangsdienst über einen Service-Abruf, der vorher von der gematik zu genehmigen ist, bereitgestellt werden. **[<=]**

5.9 Kryptographische Festlegungen

5.9.1 Basisfunktionalität

TIP1-A_5040 - Schlüssel sicher speichern
Der Konfigurationsdienst MUSS Schlüssel sicher speichern und ihr Auslesen verhindern.
[<=]

5.9.2 Algorithmenwechsel

Kryptographische Algorithmen haben eine zeitlich begrenzte Zulässigkeit. Der Konfigurationsdienst muss den Wechsel auf neue kryptographische Algorithmen unterstützen. Im KSR sind folgende Themenbereiche betroffen:

- Signaturerstellung und Prüfung der Update-Pakete (TIP1-A_6123)
- Signaturerstellung und Prüfung der Datei FirmwareGroupInfo.xml (TIP1-A_6132)
- TLS (übergreifend durch gemSpec_Krypt geregelt)

Der Konfigurationsdienst muss für die Migration zu neuen kryptographischen Algorithmen folgende Funktionalitäten unterstützen:

- Der Betreiber des Konfigurationsdiensts muss das "Signier-Tool" (TIP1-A_6066) mit Unterstützug der neuen kryptographischen Algorithmen bereitstellen (A_17344).
- Der Konfigurationsdienst muss die Signaturprüfung für die neuen kryptographischen Algorithmen unterstützen (TIP1-A_6132, TIP1-A_6123).
- Information der Nutzer des Konfigurationsdienstes über die zeitliche Planung der Migrationsschritte (A_17344).
- Der Konfigurationsdienst muss die Signaturprüfung für die alten kryptographischen Algorithmen abschalten. Ab diesen Zeitpunkt werden nur noch die neuen kryptographischen Algorithmen bei der Signaturprüfung akzeptiert.
- Auf dem Konfigurationsdienst abgelegte – beim Upload erfolgreich geprüfte – Firmware-Pakete bleiben gültig und werden weiterhin zum Download angeboten (A_17374).
- Die Hersteller sind für die Migration der UpdateInformation Signatur (TIP1-A_3896, TIP1-A_3897) bzw. des Integritäts- und Authentizitätsschutzes der Firmware zuständig.

Die Signaturen der Update-Pakete (TIP1-A_6123) und der Datei FirmwareGroupInfo.xml (TIP1-A_6132) werden durch den Hersteller der dezentralen Komponente erstellt (z.B. mit dem "Signier-Tool" (TIP1-A_6066)) und durch den Konfigurationsdienst geprüft. Diese Signaturen werden nicht an die Konnektoren weitergeleitet. Deshalb ist der Konnektor nicht von Änderungen dieser Signaturen betroffen.

Die Signatur der Update-Informationen (TIP1-A_3896) wird durch den Konnektor Hersteller erstellt und durch den Konfigurationsdienst mit dem I_KSRS_Download::listUpdates Response an den Konnektor weitergeleitet. Der Konfigurationsdienst prüft diese Signatur nicht. Diese Signatur wird nicht in

vorliegendem Dokument beschrieben. Der Konnektor Hersteller ist für die Kompatibilität dieser Signatur mit den Konnektoren an welche sie weitergeleitet wird zuständig.

6 Funktionsmerkmale

6.1 Basisdienste

6.1.1 Schnittstelle I_KSRS_Download (Provided)

Das vorliegende Kapitel spezifiziert das technische Interface I_KSRS_Download.

Über diese Schnittstelle können die zur Verfügung stehenden Update-Pakete vom Konfigurationsdienst abgefragt und heruntergeladen werden.

Im vorliegenden Kapitel werden die Operationen der Schnittstellen detailliert beschrieben. Zu jeder Operation gibt es ein Request- und ein Response-Element.

TIP1-A_3909 - Bereitstellung I_KSRS_Download
Der Konfigurationsdienst MUSS für Clients den Dienst I_KSRS_Download entsprechend der Tabelle Tab_KSR_025 bereitstellen.

Tabelle 29: Tab_KSR_025 Konfigurationsdienst

Name	`I_KSRS_Download`	
Version (KDV)	gemäß Produkttypversion	
Namensraum	http://ws.gematik.de/ksr/v1.1	
Namensraum-Kürzel	KSR	
Operationen	**Name**	**Kurzbeschreibung**
	`listUpdates`	Auflisten verfügbarer Updates
WSDL	`Konfigurationsdienst.wsdl`	
Schema	`Konfigurationsdienst.xsd`	

[<=]

TIP1-A_6103 - SOAP-Version
Der Konfigurationsdienst und der Konnektor (KSR-Client) MÜSSEN ausschließlich „SOAP über http“, Version 1.1 für ihre Kommunikation verwenden.
[<=]

6.1.1.1 I_KSRS_Download::listUpdates

Über diese Operation können zur Verfügung stehende Update-Pakete vom Konfigurationsdienst abgefragt werden.

Als Technologie wird für diese Operation SOAP genutzt.

TIP1-A_3330 - I_KSRS_Download::listUpdates
Der Konfigurationsdienst MUSS die logische Operation listUpdates entsprechend der Tabelle Tab_KSR_026 implementieren.

Tabelle 30: Tab_KSR_026 Operation I_KSRS_Download::listUpdates

Element	Beschreibung
Name	I_KSRS_Download::listUpdates
Beschreibung	Die Operation listet die auf dem Konfigurationsdienst verfügbaren Update-Pakete für eine dezentrale Komponente der TI-Plattform auf.
Initiierender Akteur	Konnektor
Weitere Akteure	Keine
Auslöser	Konnektor
Berechtigungen	Konnektor
Vorbedingungen	Aufgebaute TLS-Verbindung vom Konnektor zum Konfigurationsdienst entsprechend Kapitel 5.5.1.
Nachbedingungen	Konfigurationsdienst hat Log-Daten der Abfrage gespeichert und KSR-Client hat UpdateInfos vorliegen sowie gespeichert.
Aufruf	Der Aufrufer (Konnektor) ruft über die hier definierte Schnittstelle den Konfigurationsdienst mit den in Kapitel 6.1.1.1.1 definierten Parametern auf. Aufruf der Operation listUpdates mit der URL https://<host>:<port><path> (<host>:<port> wird durch Abfrage des DNS SRV Resource Record „_ksrfirmware._tcp.ksr.telematik“ ermittelt. <path> wird durch Abfrage des DNS TXT Resource Record „_ksrfirmware._tcp.ksr.telematik“ ermittelt.)
Antwort	Die Liste der auf dem Konfigurationsdienst verfügbaren Update-Pakete für die dezentrale Komponente entsprechend Beschreibung in Kapitel 6.1.1.1.2.
Standardablauf	Der Konfigurationsdienst MUSS die Liste der verfügbaren Updates für die dezentrale Komponente der TI-Plattform zusammenstellen. Diese Liste entspricht dem Element Firmware-Version der „aktiven“ Firmware-Gruppe (siehe Kapitel 5.3) für die Komponente. Der Konfigurationsdienst MUSS im Response die Liste der verfügbaren Updates (Parameter UpdateInformation) sowie die FirmwareGroupReleaseNotes (entspricht Element FirmwareGroupReleaseNotes der „aktiven“ Firmware-Gruppe) an den Client senden. Der Konfigurationsdienst MUSS – entsprechend Festlegungen in Kapitel 5.6 – Log-Daten von dieser Operation speichern.
Fehlerfälle	Tritt während der Verarbeitung ein Fehler auf, so MUSS der Konfigurationsdienst die Webservice-Anfrage mit einem SOAP-Fault entsprechend [gemSpec_OM] beantworteten. Die Fehlercodes sind entsprechend Tabelle Tab_Gen_Fehler aus [gemSpec_OM] zu nutzen.

[<=]

6.1.1.1.1 I_KSRS_Download::listUpdates Request

TIP1-A_3331 - I_KSRS_Download::listUpdates Request
Für den Konfigurationsdienst MUSS die Operation I_KSRS_Download::listUpdates Request mit folgenden Parametern bereitstellen:

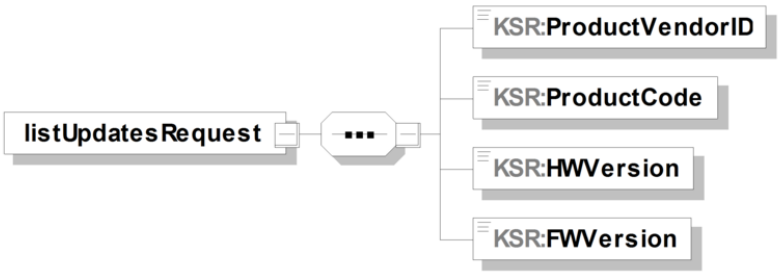


Abbildung 12: Abb_KSR_008 Operation I_KSRS_Download::listUpdates Request

Tabelle 31: Tab_KSR_027 I_KSRS_Download::listUpdates Request

Bezeichnung	I_KSRS_Download::listUpdates Request
Beschreibung	Operations-Element des Request der Operation I_KSRS_Download::listUpdates

Tabelle 32: Tab_KSR_028 Hersteller-Update-Informationen – Element ProductVendorID

Bezeichnung	ProductVendorID
Beschreibung	Identifiziert den Hersteller des Produkts, für welches auf Updates geprüft werden soll.
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string““ mit Pattern „[a-zA-Z0-9_]*“. Maximale Länge 5 Zeichen.

Tabelle 33: Tab_KSR_029 Hersteller-Update-Informationen – Element ProductCode

Bezeichnung	ProductCode
Beschreibung	Identifiziert das Produkt zusammen mit dem ProductVendorID, für welches auf Updates geprüft werden soll.
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string““ mit Pattern „[a-zA-Z0-9_]*“. Maximale Länge 8 Zeichen.

Tabelle 34: Tab_KSR_030 Hersteller-Update-Informationen – Element HWVersion

Bezeichnung	HWVersion
Beschreibung	Identifiziert die Hardware zusammen mit ProductCode und ProductVendorID, für welches auf Updates geprüft werden soll. [gemSpec_OM] beschreibt dieses Element ausführlich.

Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML Datentyp „string“ mit Pattern „[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}“.

Tabelle 35: Tab_KSR_031 Hersteller-Update-Informationen – Element FWVersion

Bezeichnung	FWVersion
Beschreibung	Die FirmwareVersion des Produkts, für welches auf Updates geprüft werden soll.
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit Pattern „[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}“.

[<=]

6.1.1.1.2 I_KSRS_Download::listUpdates Response

TIP1-A_3332 - I_KSRS_Download::listUpdates Response
Der Konfigurationsdienst MUSS die Operation I_KSRS_Download::listUpdates Response mit folgenden Parametern (siehe Abb_KSR_009, Tab_KSR_032, Tab_KSR_033, Tab_KSR_034) bereitstellen:

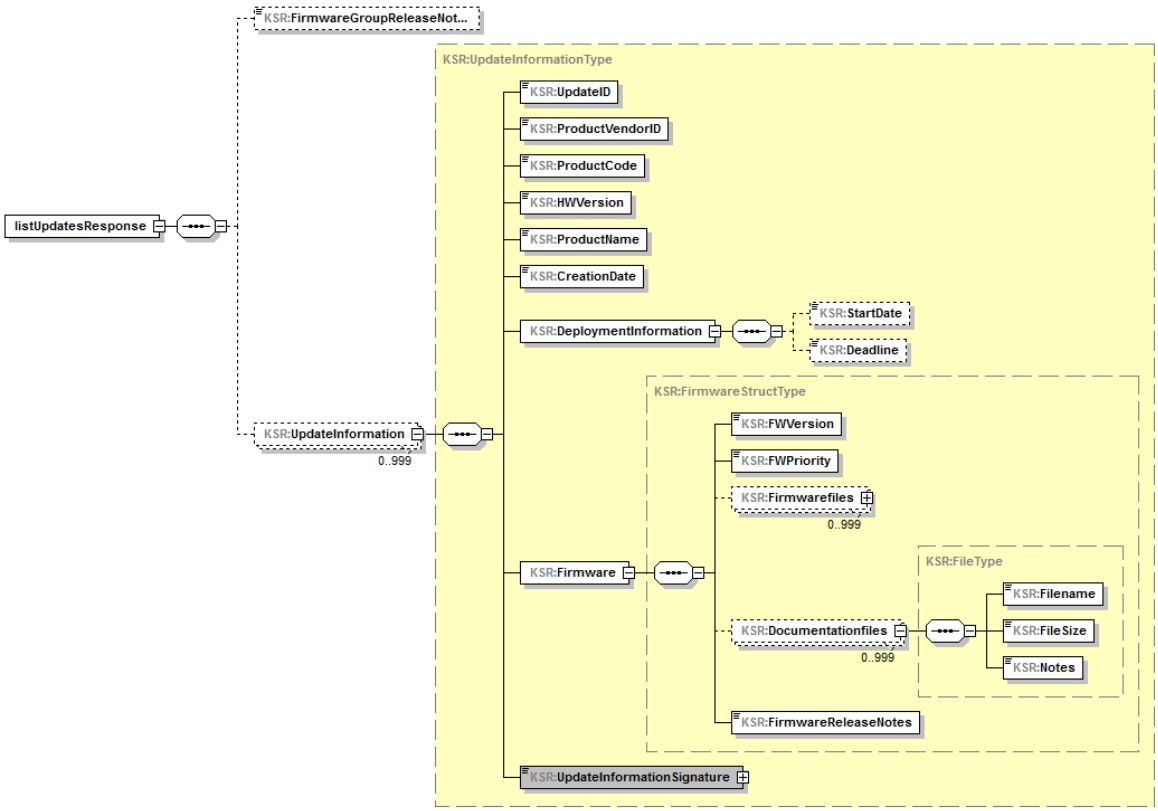


Abbildung 13: Abb_KSR_009 Operation I_KSRS_Download::listUpdates Response

Tabelle 36: Tab_KSR_032 I_KSRS_Download::listUpdates – Response

Bezeichnung	I_KSRS_Download::listUpdates Response
Beschreibung	Operations-Element des Response der Operation I_KSRS_Download::listUpdates

Tabelle 37: Tab_KSR_033 I_KSRS_Download::listUpdates – Element FirmwareGroupReleaseNotes

Bezeichnung	FirmwareGroupReleaseNotes
Beschreibung	Dieses Element enthält die Release Notes der Firmware-Gruppen-Information. Es beschreibt die Update-Pakete bzw. Firmware der Firmware-Gruppe.
Optional	Ja (falls keine Update-Pakete auf dem Konfigurationsdienst vorhanden sind)

Tabelle 38: Tab_KSR_034 I_KSRS_Download::listUpdates – Element UpdateInformation

Bezeichnung	UpdateInformation
Beschreibung	Dieses Element liefert eine Liste mit bis zu 999 verfügbaren Updates für den im Request spezifizierten Client. Jedes Element der Liste beschreibt ein Update mit allen Elementen der Hersteller-Update-Informationen (siehe Kapitel 5.2).
Optional	Ja (falls keine Update-Pakete auf dem Konfigurationsdienst vorhanden sind)

[<=]

TIP1-A_3333 - Konfigurationsdienst SOAP-Fehlercodes
Der Konfigurationsdienst MUSS für seine SOAP-Schnittstelle die generischen Fehlercodes

- Code 2: Verbindung zurückgewiesen
- Code 3: Nachrichtenschema fehlerhaft
- Code 4: Version Nachrichtenschema fehlerhaft
- Code 6: Protokollfehler

aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM] im SOAP-Fault verwenden. Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM]) abgebildet werden.
[<=]

Tabelle 39: Tab_KSR_047 I_KSRS_Download::listUpdates Fehlercodes

Code	ErrorType	Severity	ErrorText	Auslösende Bedingung
2	Technical	Fatal	Verbindung zurückgewiesen	Die Verbindung wurde vom angefragten System zurückgewiesen
3	Technical	Fatal	Nachrichtenschema fehlerhaft	Das Nachrichtenschema

				war inkorrekt
4	Technical	Fatal	Version Nachrichtenschema fehlerhaft	Die Version des Nachrichtenschemas stimmt nicht mit der geforderten Version überein
6	Technical	Fatal	Protokollfehler	Genauere Aufschlüsselung des Protokollfehlers werden in den Details erfasst

6.1.1.2 I_KSRS_Download::getUpdates

TIP1-A_3334 - I_KSRS_Download::getUpdates

Der Konfigurationsdienst MUSS die Operation I_KSRS_Download::getUpdates für die Übertragung von Aktualisierungspaketen an dezentrale Komponente der TI-Plattform durch den Konfigurationsdienst entsprechend Tabelle Tab_KSR_035 bereitstellen.

Tabelle 40: Tab_KSR_035 Operation I_KSRS_Download::getUpdates

Element	Beschreibung
Name	I_KSRS_Download::getUpdates
Beschreibung	Mit dieser Operation ruft der Konnektor verfügbare Updates für eine dezentrale Komponente der TI-Plattform vom Konfigurationsdienst ab. Die Auswahl der Files zum Download erfolgt auf Grundlage der zurückgegebenen Werte in Operation listUpdates Response. Die optionale detached Signatur „UpdateInfo.sig“ kann ebenfalls mit dieser Operation übertragen werden. Mit jedem Aufruf dieser Operation wird ein File übertragen.
Initiierender Akteur	Konnektor
Weitere Akteure	keine
Auslöser	Konnektor
Vorbedingungen	Aufgebaute TLS-Verbindung vom Konnektor zum Konfigurationsdienst entsprechend Kapitel 5.5.1.
Nachbedingungen	Konfigurationsdienst hat Log-Daten gespeichert und der Konnektor hat die Update-Datei vorliegen und gespeichert.
Aufruf	Aufruf von TUC_KSR_001 „Get File“ mit der URL https://<host>:<port><path>/<filename> (<host>:<port> wird durch Abfrage des DNS SRV Resource Record „_ksrfirmware._tcp.ksr.telematik“ ermittelt. <path> wird durch Abfrage des DNS TXT Resource Record „_ksrfirmware._tcp.ksr.telematik“ ermittelt. <filename> entspricht dem Filename der Firmwaredatei inklusive absoluten Pfad (siehe z.B. Tab_KSR_015).)
Standardablauf	Der KSR sendet die angeforderte Datei an den aufrufenden Konnektor.

Fehlerfälle	Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.

[<=]

Der Konnektor kann das Vorhandensein von Updatepaketen mit folgendem Beispielablauf prüfen:

1 Der Konnektor ruft vom KSR mit Operation I_KSRS_Download::listUpdates die Liste der vorliegenden Updatepakete ab (TIP1-A_3331, TIP1-A_3332) ab.

2 Der Konnektor prüft für jedes im listUpdates Response vorhandene Konnektor Updatepaket die Signatur ([gemSpec_Kon#TAB_KON_664] Punkt 1, Tab_KSR_003).

2.1 Falls das Konnektor Updatepaket die Signatur im XML Element UpdateInformationSignature enthält wird UpdateInformation mit dieser Signatur validiert (TIP1-A_3896, Tab_KSR_020).

2.2 Falls das Konnektor Updatepaket die Signatur nicht im XML Element UpdateInformationSignature enthält wird es mit seiner detached Signatur validiert (TIP1-A_3896, TIP1-A_6120).

2.2.1 Mit Operation I_KSRS_Download::getUpdates wird die detached Signatur vom KSR geladen (TIP1-A_3334):

2.2.1.1 Zum Aufruf der Operation werden die - noch nicht vorhandenen - Elemente zur Bildung der URL ermittelt:

2.2.1.1.1 Dem Konnektor Updatepaket werden aus UpdateInformation die Werte der XML-Elemente <ProductVendorId>, <ProductCode> und <UpdateID> entnommen (TIP1-A_3332, Tab_KSR_004 , Tab_KSR_005, Tab_KSR_006).

2.2.1.1.2 Für die detached Signatur des Elementes „UpdateInformation“ ist der Dateiname „UpdateInfo.sig“ festgelegt (TIP1-A_6120).

2.2.1.1.3 <host>:<port> wird durch Abfrage des DNS SRV Resource Record „_ksrfirmware._tcp.ksr.telematik“ ermittelt (TIP1-A_3334).

2.2.1.1.4 <path> wird durch Abfrage des DNS TXT Resource Record „_ksrfirmware._tcp.ksr.telematik“ ermittelt (TIP1-A_3334).

2.2.1.2 Aus diesen Werten wird für Operation I_KSRS_Download::getUpdates die URL nach folgendem Schema gebildet: https://<host>:<port><path>/<ProductVendorId>/<ProductCode>/<UpdateID>/UpdateInfo.sig (TIP1-A_3334, Tab_KSR_015)

2.2.1.3 Mit der über diese URL aufgerufenen Operation I_KSRS_Download::getUpdates wird die detached Signaturdatei UpdateInfo.sig auf den Konnektor geladen.

2.2.2 Der Konnektor validiert die UpdateInformation des Konnektor Updatepaketes mit dieser detached Signatur ([gemSpec_Kon#TAB_KON_664] Punkt 1, Tab_KSR_003).

2.3 Falls das Konnektor Updatepaket (UpdateInformation) nicht validiert werden kann wird es nicht weiter verarbeitet ([gemSpec_Kon#TAB_KON_664], TIP1-A_3896).

6.1.1.3 I_KSRS_Download::get_Ext_Net_Config

Für den Download von Konnektor-Konfigurationsdatenfiles wird der technische Use Case TUC_KSR_001 „Get File“ (Kapitel 6.1.1.4) genutzt. Die Konnektor-Konfigurationsdatenfiles erhalten im Gegensatz zu Firmware-Update-Paketen feste URLs. Deshalb können die Konnektor Clients zum Download diese URL direkt – ohne Aufruf von I_KSRS_Download::listUpdates (Kapitel 6.1.1.1) – zum Download nutzen. Die Konnektor-Konfigurationsdatenfiles enthalten immer die aktuellen Konfigurationsdaten, d.h. es gibt jeweils nur eine Version des Konfigurationsdatenfiles im Konfigurationsdienst. Die Aktualisierung der Konnektor-Konfigurationsdaten erfolgt über die organisatorischen Schnittstellen (Kapitel 6.2).

TIP1-A_5160 - I_KSRS_Download::get_Ext_Net_Config

Der Konfigurationsdienst MUSS die Operation I_KSRS_Download::get_Ext_Net_Config für die Übertragung von Konfigurationsdatenfiles an dezentrale Komponenten der TI-Plattform durch den Konfigurationsdienst entsprechend Tabelle Tab_KSR_044 bereitstellen.

Tabelle 41: Tab_KSR_044 Operation I_KSRS_Download::get_Ext_Net_Config

Element	Beschreibung
Name	I_KSRS_Download::get_Ext_Net_Config
Beschreibung	Mit dieser Operation ruft der Konnektor verfügbare Konfigurationsdatenfiles vom Konfigurationsdienst ab. Die Auswahl der Konfigurationsdatenfiles zum Download erfolgt auf Grundlage ihrer fest vorgegebenen Filenamen. Mit jedem Aufruf dieser Operation wird ein File übertragen.
Initiierender Akteur	Konnektor
Weitere Akteure	keine
Auslöser	Konnektor
Vorbedingungen	Aufgebaute TLS-Verbindung vom Konnektor zum Konfigurationsdienst entsprechend Kapitel 5.5.1.
Nachbedingungen	Konfigurationsdienst hat Log-Daten gespeichert und der Konnektor hat das Konfigurationsdatenfile vorliegen und gespeichert.
Aufruf	Aufruf von TUC_KSR_001 „Get File“ mit der URL https://<host>:<port><path>/<filename> (<host> und <port> werden durch Abfrage des DNS SRV Resource Record „_ksrkonfig._tcp.ksr.telematik“ ermittelt.

	<path> wird durch Abfrage des DNS TXT Resource Record „_ksrkonfig._tcp.ksr.telematik“ ermittelt und enthält den Pfad des Konfigurationsdatenfiles.)
Standardablauf	Der KSR sendet das angeforderte Konfigurationsdatenfile an den aufrufenden Konnektor.
Fehlerfälle	Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.

[<=]

TIP1-A_5375 - Filename des Konfigurationsdatenfiles zur Anbindung von Bestandsnetzen
Der Konfigurationsdienst MUSS das Konfigurationsdatenfile zur Anbindung von Bestandsnetzen unter dem Filenamen „Bestandsnetze.xml“ zum Download bereitstellen.
[<=]

6.1.1.4 TUC_KSR_001 „Get File“

TIP1-A_5161 - TUC_KSR_001 „Get File“
Der Konfigurationsdienst MUSS den technischen Use Case für die Übertragung von Files an dezentrale Komponente der TI-Plattform durch den Konfigurationsdienst entsprechend Tabelle Tab_KSR_043 TUC_KSR_001 „Get File“ bereitstellen.

Tabelle 42: Tab_KSR_043 TUC_KSR_001 „Get File“

Element	Beschreibung
Name	TUC_KSR_001 „Get File“
Beschreibung	Dieser technische Use Case wird von den Operationen zum Abruf von Files durch den Konnektor vom Konfigurationsdienst genutzt. Mit jedem Aufruf dieser Operation wird ein File übertragen.
Initiierender Akteur	Konnektor (bzw. I_KSRS_Download::getUpdates, I_KSRS_Download::get_Ext_Net_Config)
Weitere Akteure	keine
Auslöser	Konnektor (bzw. I_KSRS_Download::getUpdates, I_KSRS_Download::get_Ext_Net_Config)
Vorbedingungen	Aufgebaute TLS-Verbindung vom Konnektor zum Konfigurationsdienst entsprechend Kapitel 5.5.1.
Eingangsdaten	filename (Filename welches vom KSR geladen werden soll)
Nachbedingungen	Konfigurationsdienst hat Log-Daten gespeichert und der Konnektor hat die Update-Datei vorliegen und gespeichert.
Aufruf	http GET entsprechend TIP1-A_3335.
Standardablauf	Der Konfigurationsdienst MUSS dem Client das angegebene File mit dem Bezeichner filename entsprechend http 1.1 [RFC2616] übertragen. Der Konfigurationsdienst MUSS Log-Daten von dieser Operation speichern (siehe Kapitel 5.6).

Fehlerfälle	Tritt während der Verarbeitung ein Fehler auf, so MUSS der Konfigurationsdienst im http-Response einen entsprechenden http Status Code senden (siehe TIP1-A_4120).

[<=]

TIP1-A_3335 - Konfigurationsdienst File Transfer HTTP Request
Der Konfigurationsdienst MUSS den Download eines Files mit einem http GET unterstützen. Dafür MUSS ein http URL-Schema entsprechend [RFC1738] sowie Tabellen Tab_KSR_036 und Tab_KSR_037 unterstützt werden:

https://<host>/<path>

Tabelle 43: Tab_KSR_036 File Transfer HTTP Request – Element host

Bezeichnung	host
Beschreibung	Der FQDN (fully qualified domain name) des Konfigurationsdienstes und optional eine Portnummer.
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom Datentyp „string“.

Tabelle 44: Tab_KSR_037 File Transfer HTTP Request – Element path

Bezeichnung	path
Beschreibung	Absoluter Pfad (siehe z.B. Tab_KSR_015, Tab_KSR_017.
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom Datentyp „string“.

[<=]

TIP1-A_3336 - File Transfer HTTP Response
Der Konfigurationsdienst MUSS in das http-Response die notwendigen http-Header-Datenfelder gemäß [RFC2616] aufnehmen. Im http-Body MUSS der Konfigurationsdienst das angeforderte File zurückgeben.
[<=]

TIP1-A_4120 - File Transfer HTTP Status Codes
Der Konfigurationsdienst MUSS die http Status Codes entsprechend [RFC2616] unterstützen.
[<=]

TIP1-A_5162 - http Status Code „Retry After“
Wenn der Konfigurationsdienst den getUpdates Request wegen temporärer Überlast oder Maintenance nicht verarbeiten kann, MUSS er den http Status Code 503 Server Unavailable an den Client zurückgeben. Falls dem Konfigurationsdienst der Zeitraum der Nichtverfügbarkeit bekannt ist, SOLL er den Retry-After Header zur Information des Clients nutzen. Der Retry-After Header MUSS ebenfalls bei Überlast zur zeitlichen Lastverteilung genutzt werden.**[<=]**

TIP1-A_3910 - Konfigurationsdienst File Transfer http Komprimierung
Der Konfigurationsdienst MUSS die Komprimierung des File Transfers über http unterstützen. Dazu muss er das „Content Coding“ [RFC2616] „gzip“ implementieren.
[<=]

TIP1-A_7221 - Konfigurationsdienst File Transfer Range Requests
Der Konfigurationsdienst MUSS für den File Transfers über http die Option Range Requests [RFC7233#3.1] zur Fortsetzung von unterbrochenen Transfers unterstützen.**[<=]**

6.1.1.5 KSR Download Cache

Zur Entlastung des zentralen Netzes von häufigen Update-Paket-Übertragungen wird im SZZP (Sicherer Zentraler Zugangspunkt) der VPN-Zugangsdienste ein KSR Download Cache Server vorgesehen.

TIP1-A_6104 - KSR Download Cache Server
Der Konfigurationsdienst MUSS für jeden SZZP der VPN-Zugangsdienste einen KSR Download Cache Server vorsehen. Jeder einzelne dieser KSR Download Cache Server MUSS dabei autark laufen und sich eigenständig synchronisieren. Für die zentralen Komponenten des Konfigurationsdienstes MUSS das Vorhandensein und die Anzahl von KSR Download Cache Servern transparent sein.
Die KSR Download Cache Server MÜSSEN folgende Eigenschaften haben:

- Jede Instanz MUSS separat in den Umgebungen deploybar sein.
- Jede Instanz MUSS eine eigene lokale Datenhaltung besitzen.
- Jede Instanz MUSS die Anfragen dezentraler Komponenten ohne die Kommunikation mit anderen Instanzen beantworten können.

[<=]

TIP1-A_6105 - KSR Download Cache Server Transparenz
Der Konfigurationsdienst MUSS für die dezentralen Komponenten die Transparenz der KSR Cache Server sicherstellen. Mit den KSR Download Cache Servern MUSS die gleiche Schnittstelle I_KSRS_Download bereitgestellt werden wie sie der KSR selbst unterstützt. Der Konfigurationsdienst MUSS sicherstellen, dass Hinzufügen, Entfernen und Ausfall (Redundanzfall) eines KSR Download Cache Servers keinerlei Anpassungen in dezentralen Komponenten erfordert.
[<=]

TIP1-A_6106 - KSR Download Cache Server Redundanz
Der Konfigurationsdienst MUSS für die KSR Download Cache Server eine redundante Lösung vorsehen. Der Konfigurationsdienst MUSS sicherstellen, dass Aktivieren und Deaktivieren der Redundanzlösung keinerlei Anpassungen in dezentralen Komponenten erfordert.
[<=]

TIP1-A_6125 - KSR Störungsampel Monitoringdaten
Der Konfigurationsdienst MUSS für alle seine Komponenten inklusive der KSR Download Cache Server Monitoringdaten an die Störungsampel senden [gemSpec_St_Ampel] (Schnittstelle I_Monitoring_Update).
[<=]

TIP1-A_6109 - KSR Nutzung des zentralen Netzes während Redundanz
Der Konfigurationsdienst KANN während des Ausfalls eines KSR Download Cache Servers für die Übertragung der Update-Pakete zu den dezentralen Komponenten das zentrale Netz verwenden.
[<=]

6.2 Organisatorische Schnittstellen

Das vorliegende Kapitel spezifiziert die organisatorischen Interfaces P_KSRS_Upload und P_KSRS_Operations auf Basis der konzeptionellen Schnittstelle P_KSRS_Maintenance (siehe [gemKPT_Arch_TIP#TIP1-A_2394]). Dieses Interface kann vom Anbieter des Konfigurationsdienstes durch technische Schnittstellen und/oder organisatorische Prozesse umgesetzt werden.

Die organisatorischen Schnittstellen ermöglichen es berechtigten Akteuren, Update-Pakete und Konfigurationsdaten in den Download-Bereichen der unterschiedlichen Umgebungen (RU, TU, PU) verfügbar zu machen beziehungsweise~~zu löschen~~ und sich über den Status der Update-Pakete im KSR zu informieren. Dies wird durch Aufträge der berechtigten Akteure an den Anbieter des Konfigurationsdienstes realisiert.

6.2.1 Registrierung berechtigter Nutzer

Hersteller ~~(~~und TBI ~~TBV~~/~~SBV-TIP~~GTI~~)~~ müssen sich für den Zugang zu den organisatorischen KSR-Schnittstellen registrieren. Nach der erfolgreichen Einrichtung werden die Zugangsdaten dem Anwender mitgeteilt und für den Konfigurationsdienst freigeschaltet. Erst nach Freischaltung kann der Anwender sich beim Konfigurationsdienst anmelden und z.B. Update-Pakete einspielen. Hersteller von Komponenten, die den KSR nutzen, bekommen ~~nur~~ die Berechtigung sich im Upload-Bereich anzumelden, Update-Pakete hochzuladen und Statistikdaten herunterzuladen. Die TBI ~~TBV~~/~~SBV-TIP~~GTI der jeweiligen Umgebung erhalten Berechtigung für den Upload- und dem Konfigurationsbereich. Die TBI ~~TBV~~/~~SBV-TIP~~GTI können damit Update-Pakete im Upload-Bereich einspielen und die hoch geladenen Pakete im Konfigurationsbereich bearbeiten, d.h. Aufträge zum Deaktivieren ~~Löschen~~ oder zur Freigabe des Update-Paketes erteilen. Hersteller von Komponenten, die den KSR nutzen, können – nach Prüfung durch die gematik - Berechtigungen für den Konfigurationsbereich der Testumgebungen erhalten. Die jeweilige Berechtigung wird bei Nutzung der organisatorischen KSR-Schnittstellen durch den Konfigurationsdienst durch die Zugehörigkeit eines Anwenders zu einer Berechtigungsgruppe des Konfigurationsdienstes ermittelt.

TIP1-A_6107 - Bereitstellung Registrierungsinterface
Der Anbieter des Konfigurationsdienstes MUSS berechtigten Akteuren die Registrierung für die Nutzung der organisatorischen KSR-Schnittstellen ermöglichen und ihnen die nötigen Zugangsdaten bereitstellen.
[<=]

TIP1-A_6110 - Authentisierung und Autorisierung
Der Konfigurationsdienst MUSS Akteure der organisatorischen KSR-Schnittstellen authentisieren und autorisieren.
[<=]

6.2.2 Berechtigungs- und Rollenkonzept

Im vorliegenden Dokument werden Hersteller von Komponenten, die den KSR nutzen, TBI ~~TBV~~, ~~SBV-TIP~~GTI oder allgemein Akteure (außer Konnektoren) aus technischer Sicht als Anwender mit einer oder mehreren Rollen betrachtet. Jede Rolle besitzt unterschiedliche Berechtigungen innerhalb des Konfigurationsdienstes.

TIP1-A_6111 - Gruppen und Berechtigungen
Der Konfigurationsdienst MUSS den Akteuren der organisatorischen KSR-Schnittstellen jeweils Rollen gemäß ihrer Gruppenzugehörigkeit und Umgebung entsprechend Tab_KSR_011 zuweisen.

Tabelle 45: Tab_KSR_011 Gruppen und Berechtigungen

Rolle/Gruppe	Berechtigung
Hersteller_RU	Die Rolle kann sich an der Web-Applikation des Upload-Bereichs in RU anmelden, Pakete hochladen, den Status einsehen und Statistikdaten herunterladen.
Hersteller_RU_RO	Die Rolle kann sich an der Web-Applikation des Upload-Bereichs in RU anmelden, den Status einsehen und Statistikdaten herunterladen. Es sind keine Änderungen von Daten im Konfigurationsdienst erlaubt.
Hersteller_TU	Die Rolle kann sich an der Web-Applikation des Upload-Bereichs in TU anmelden, Pakete hochladen, den Status einsehen und Statistikdaten herunterladen.
Hersteller_TU_RO	Die Rolle kann sich an der Web-Applikation des Upload-Bereichs in TU anmelden, den Status einsehen und Statistikdaten herunterladen. Es sind keine Änderungen von Daten im Konfigurationsdienst erlaubt.
Hersteller_RU_Konfig	Die Rolle kann sich an der Web-Applikation des Konfigurationsbereichs in RU anmelden, die Auftragsliste einsehen, Pakete ablehnen, freigeben oder deaktivieren, Statistikdaten herunterladen. Akteure mit dieser Rolle dürfen nur auf eigene Pakete (Pakete mit dem ProductVendorID des Akteurs) und Daten über eigene Pakete zugreifen.
Hersteller_TU_Konfig	Die Rolle kann sich an der Web-Applikation des Konfigurationsbereichs in TU anmelden, die Auftragsliste einsehen, Pakete ablehnen, freigeben oder deaktivieren, Statistikdaten herunterladen. Akteure mit dieser Rolle dürfen nur auf eigene Pakete (Pakete mit dem ProductVendorID des Akteurs) und Daten über eigene Pakete zugreifen.
Hersteller_PU	Die Rolle kann sich an der Web-Applikation des Upload-Bereichs in PU anmelden, Pakete hochladen, den Status einsehen und Statistikdaten herunterladen. Diese Rolle erlaubt in der PU nicht die Funktionalitäten Pakete ablehnen, freigeben oder deaktivieren.

Hersteller_PU_RO	Die Rolle kann sich an der Web-Applikation des Upload-Bereichs in PU anmelden, den Status einsehen und Statistikdaten herunterladen. Es sind keine Änderungen von Daten im Konfigurationsdienst erlaubt.
TBI ~~TBV~~_RU	Die Rolle kann sich an der Web-Applikation des Konfigurationsbereichs in RU anmelden, die Auftragsliste einsehen, Pakete ablehnen, freigeben oder deaktivieren, Statistik- und Logdaten herunterladen sowie Konfigurationsdatenfiles für RU hochladen, freigeben oder ablehnen.
TBI ~~TBV~~_TU	Die Rolle kann sich an der Web-Applikation des Konfigurationsbereichs in TU anmelden, die Auftragsliste einsehen, Pakete ablehnen, freigeben oder deaktivieren, Statistik- und Logdaten herunterladen sowie Konfigurationsdatenfiles für TU hochladen, freigeben oder ablehnen.
GTI~~SBV~~_PU	Die Rolle kann sich an der Web-Applikation des Konfigurationsbereichs in PU anmelden, die Auftragsliste einsehen, Pakete ablehnen, freigeben oder deaktivieren, Statistik- und Logdaten herunterladen sowie Konfigurationsdatenfiles für PU hochladen, freigeben oder ablehnen.

[<=]

Im vorliegenden Dokument wird von folgenden Rollenzugehörigkeiten ausgegangen. Die Zuordnung dient ausschließlich als Beispiel für dieses Dokument.

Tabelle 46: Tab_KSR_038 Beispiel Gruppenzuordnung

Akteur	Mitgliedschaft in Gruppe
Hersteller	Hersteller_PU, Hersteller_TU und Hersteller_RU Optional und nach gematik-Bestätigung: Hersteller_RU_Konfig
Hersteller_RO	Hersteller_PU_RO, Hersteller_TU_RO und Hersteller_RU_RO
TBI ~~TBV~~	Hersteller_TU, Hersteller_RU, TBI ~~TBV~~_RU, TBI ~~TBV~~_TU Optional und nach gematik-Bestätigung: Hersteller_TU_Konfig
~~SBV-TIP~~GTI	Hersteller_PU, ~~SBV_PU~~ GTI

6.2.3 Uploadschnittstelle P_KSRS_Upload

Diese Kapitel beschreibt die organisatorische Schnittstelle des Konfigurationsdienstes zum „Befüllen“ des Konfigurationsdienstes (Upload-Bereich) durch die Hersteller dezentraler Komponenten.

6.2.3.1 Schnittstellendefinition

Über KSR-Upload können Hersteller dezentraler Komponenten Update-Pakete für die Verteilung über den Konfigurationsdienst bereitstellen.

KSR-Upload stellt folgende Funktionalitäten bereit:

- Schnittstelle zur Annahme der Update-Pakete
- Kontrollierte Übermittlung der Update-Pakete zur Eingangsprüfung
- Protokollierung von Upload-Aktivitäten

TIP1-A_3342 - Bereitstellung P_KSRS_Upload
Der Anbieter des Konfigurationsdienstes MUSS berechtigten Herstellern dezentraler Komponenten der TI, dem ~~Servicebetriebsverantwortlichen TI-Plattform~~ Gesamtverantwortlichen TI (PU) und der ~~Testbetriebsverantwortlichen~~ Testbetriebsinstanz TU/RU eine Möglichkeit zum Übermitteln von Update-Paketen und zugehörigen Firmware-Gruppen-Informationen entsprechend Tabelle Tab_KSR_039 zur Verfügung stellen (P_KSRS_Upload).

Tabelle 47: Tab_KSR_039 P_KSRS_Upload Schema

Name	`P_KSRS_Upload`	
Version (KDV)	gemäß Produkttypversion	
Namensraum	http://ws.gematik.de/ksr/v1.1	
Namensraum-Kürzel	KSR	
Informationsobjekte	**Name**	**Kurzbeschreibung**
	`UpdateInformation`	Metainformationen zum Update-Paket
	`FirmwareGroupInformation`	Liste der aktuell freigegebenen Firmware-Versionen eines Produkts.
Schema	`Konfigurationsdienst.xsd`	

[<=]

TIP1-A_3343 - Berechtigung P_KSRS_Upload
Der Anbieter des Konfigurationsdienstes MUSS sicherstellen, dass nur berechtigte Akteure (berechtigte Hersteller von Komponenten, die den KSR nutzen, ~~Servicebetriebsverantwortlicher TI-Plattform~~ Gesamtverantwortlicher TI (PU), ~~Testbetriebsverantwortlicher~~ Testbetriebsinstanz TU und ~~Testbetriebsverantwortlicher~~ Testbetriebsinstanz (RU) auf P_KSRS_Upload der jeweiligen Umgebung zugreifen können.
[<=]

TIP1-A_3348 - Form und Inhalt Upload-Interface
Der Anbieter des Konfigurationsdienstes MUSS die Form des Upload-Interfaces definieren und mit den berechtigten Akteuren abstimmen.
[<=]

TIP1-A_5042 - P_KSRS_Upload parallel nutzbar
Der Konfigurationsdienst SOLL die Kommunikationsschnittstelle von KSR-Upload so implementieren, dass sie parallel durch mehrere Aufrufer nutzbar ist.
[<=]

TIP1-A_3345 - KSR Logging – Upload-Interface
Der Konfigurationsdienst MUSS mindestens für folgende Vorgänge Logging-Daten erfassen:

- Upload von Update-Paketen und Firmware-Gruppen-Informationen
- Ergebnis der Eingangsprüfung

Ein Log-Eintrag MUSS mindestens folgende Informationen erfassen:

- Wer hat etwas getan
- Was wurde getan
- Zeitpunkt
- Updatepaket.UpdateInformation.UpdateID bzw. FirmwareGroupInformation.FirmwareGroupID

[<=]

TIP1-A_6065 - KSR Fortschrittsinformation im Interface P_KSRS_Upload
Der Konfigurationsdienst MUSS während des Übermittelns von Update-Paketen den Nutzer über den Fortschritt des Filetransfers informieren.
[<=]

A_14540 - P_KSRS_Upload & P_KSRS_Operations, Optionen zur Anzeige von Listen
Der Anbieter des Konfigurationsdienstes MUSS in den Schnittstellen P_KSRS_Upload und P_KSRS_Operations Nutzern folgende Optionen bei der Anzeige von Update-Paketen – zur Erleichterung der Arbeit mit langen Listen – bereitstellen:

- Die Listen müssen – entsprechend der vom Nutzer gewählten Spalte – auf und absteigend sortierbar sein.
- Die Listen müssen – entsprechend der vom Nutzer gewählten Spalte – nach einem Zeitpunkt (mindestens Tag bzw. Monat in Spalte Timestamp) und Strings in den restlichen Anzeigespalten - filterbar sein.
- Die Listen müssen maximierbar (Ausnutzung eines großen Bereichs des Fensters für die Liste der Update-Pakete) sein.

[<=]

A_15171 - P_KSRS_Upload & P_KSRS_Operations, Gesicherter Zugang
Der Anbieter des Konfigurationsdienstes MUSS in den Schnittstellen P_KSRS_Upload und P_KSRS_Operations den Zugriff der Anwender auf diese Schnittstellen ausschließlich über eine TLS-Verbindung mit serverseitiger Authentifizierung ermöglichen. **[<=]**

6.2.3.2 Eingangsprüfung durch den Konfigurationsdienst

TIP1-A_3346 - Eingangsprüfung
Der Konfigurationsdienst MUSS die übermittelten Update-Pakete und Firmware-Gruppen-Informationen einer Eingangsprüfung unterziehen.
Die Eingangsprüfung MUSS folgende Prüfungen enthalten:

- Prüfung der Integrität und Authentizität
  - Die Signatur des Update-Paketes muss beim Übergang zwischen Upload-Bereich und Konfigurationsbereich geprüft werden. Die Prüfung muss mindestens die folgende Schritte umfassen:
    - Prüfung der Gültigkeit des Zertifikats über den zuständigen OCSP-Responder,

    - Prüfung der Zertifikatstyp-OID auf Zulässigkeit,
    - Prüfung der mathematischen Korrektheit des Zertifikats.
  - Die Integrität des ZIP-Containers
  - Der Konfigurationsdienst MUSS – im Sinne Integrität und Authentizität - fehlerhafte Update-Pakete ohne weitere Prüfung ihrer Inhalte ablehnen.
- Prüfung auf syntaktische Korrektheit (Update-Informationen und Firmware-Gruppen-Informationen)
  - Sofern die Datei UpdateInfo.xml im Container enthalten ist, wird die XML-Struktur validiert. Die in dem Element „Files“ angegebenen Dateien müssen im Container enthalten sein, die Pfadangaben müssen dem in Anforderung „TIP1-A_6122 Pfadreferenz“ definiertem Format entsprechen. Alle Pflichtfelder müssen mit korrekten Werten belegt sein, die angegebene ProductVendorID muss mit der ID des übertragenden Herstellers identisch sein, außer es handelt sich um ein Update-Paket, das durch den ~~TBV~~TBI/~~SBV-TIP~~GTI eingestellt wurde.
  - Die Datei „FirmwareGroupInfo.xml“ wird mit dem XSD-Schema validiert und sichergestellt, dass die Version aktueller ist, als die bereits vorhandene.
- Prüfung auf Vollständigkeit (Vorhandensein aller aus den Update-Informationen referenzierten Files)
  - Das Update-Paket wird geöffnet und festgestellt, dass alle notwendigen Dateien im ZIP-Container enthalten sind. (FirmwareGroupInfo.xml, optional UpdateInfo.xml)
  - Es dürfen nicht mehr Dateien im Container enthalten sein, als die in 6.2.3.1 definierten Elemente. Die Firmware- und Dokumentationsdateien müssen alle durch UpdateInfo.xml referenziert werden. Update-Pakete mit Dateien ohne Referenz werden abgelehnt. Die optionalen detached Signaturen „UpdateInfo.sig“ und „FirmwareGroupInfo.sig“ können – ohne Referenz - im Update-Paket enthalten sein.
- Prüfung ob der eingeloggte Nutzer die Berechtigung hat das Update-Paket zu übermitteln. Der Nutzer muss zu der Organisation gehören welche das Update-Paket signiert hat oder die ~~TBV~~ TBI bzw. ~~SBV~~ GTI Rolle für die jeweilige Umgebung besitzen.

[<=]

Der Hersteller von Komponenten, die den KSR nutzen, erstellt das entsprechende Update-Paket für seine Komponente. Das Update-Paket für eine Komponente entspricht genau einer Datei. Zur Übertragung des Update-Paketes an den Konfigurationsdienst wird ein ZIP-Container verwendet. Der ZIP-Container ist nach dem Standard [ZIP-APP] formatiert und ist nicht mit einem Passwort geschützt.

Der Konfigurationsdienst soll das Update-Paket in der Eingangsprüfung möglichst vollständig prüfen. Nur bei fehlgeschlagener Prüfung von Integrität und Authentizität muss die Prüfung sofort abgebrochen werden.

TIP1-A_6112 - Name des Update-Paketes
Hersteller von Komponenten, die den KSR nutzen, MÜSSEN den Dateinamen so wählen, das er dem Pattern „[A-Za-z0-9_-.]*“ entspricht und nicht länger als 32 Zeichen ist und

der Konfigurationsdienst MUSS die Einhaltung dieser Definition prüfen.
[<=]

TIP1-A_6113 - Definition Update-Paket-Struktur
Hersteller von Komponenten, die den KSR nutzen, MÜSSEN Update-Pakete mit den in Tab_KSR_010 (Struktur Update-Paket) definierten Elementen in Form eines ZIP-Containers nach dem Standard [ZIP-APP] erzeugen und der Konfigurationsdienst MUSS die Einhaltung dieser Definition prüfen.
[<=]

TIP1-A_6114 - Passwort des Update-Paketes
Hersteller von Komponenten, die den KSR nutzen, DÜRFEN NICHT den ZIP-Container mit einem Passwort schützen und der Konfigurationsdienst DARF NICHT passwortgeschützte ZIP-Container akzeptieren.
[<=]

TIP1-A_6115 - Größe des Update-Paketes
Hersteller von Komponenten, die den KSR nutzen, DÜRFEN NICHT Update-Pakete hochladen, deren entkomprimierte Paketgröße den abgestimmten Maximalwert übersteigt und der Konfigurationsdienst DARF NICHT Update-Pakete akzeptieren welche diesen Maximalwert übersteigen.
[<=]

TIP1-A_7253 - KSR – Konfigurierbare Maximalgröße von Update-Paketen
Der Konfigurationsdienst MUSS die Konfiguration der maximalen Größe von Update-Paketen erlauben. Der initiale Wert für diesen Konfigurationsparameter MUSS 1500 Mbyte betragen. Die Änderung des Wertes dieses Konfigurationsparameters durch die gematik MUSS ermöglicht werden.**[<=]**

TIP1-A_7346 - KSR – Löschen von deaktivierten Update-Paketen
Der Konfigurationsdienst SOLL bei Deaktivierung von Update-Paketen die – vom Hersteller gelieferten – Daten des Update-Paketes im Konfigurationsdienst löschen und die im Konfigurationsdienst vorhandenen Metadaten (Daten über das Update-Paket, welche im GUI angezeigt oder in Logfiles und Reports enthalten sind) entsprechend der vorgegebenen Speicherdauer für diese Daten weiterhin zur Verfügung stellen.**[<=]**

TIP1-A_7347 - KSR – Anzahl Update-Pakete
Der Konfigurationsdienst MUSS pro Hersteller von dezentralen Produkttypen mindestens 10 Update-Pakete speichern und zum Download anbieten können.
Diese Anzahl muss erweiterbar sein.**[<=]**

Das Update-Paket enthält folgende Elemente im Wurzel-Verzeichnis des Containers:

Tabelle 48: Tab_KSR_010 Struktur Update-Paket

Element	Beschreibung	Anzahl
UpdateInformation	XML- Datei mit den Metadaten des Update-Paketes. Der Dateiname des Elementes „UpdateInformation“ ist festgelegt auf „UpdateInfo.xml“. Der Typ „UpdateInformation“ wird in dem Schema „Konfigurationsdienst.xsd“ spezifiziert.	0..1

UpdateInfo_Signature	Optionale „Detached Signature“ für das Element „UpdateInformation“. Der Dateiname ist auf „UpdateInfo.sig“ festgelegt. Die Datei darf höchstens einmal im Paket vorhanden sein.	0..1
FirmwareFiles	Firmware Dateien zum späteren Download. Maximal dürfen 999 Firmware-Dateien enthalten sein. Sofern eine UpdateInformation im Paket enthalten ist, muss mindestens eine Firmware-Datei enthalten sein.	0..999
DocumentationFiles	Dokumentationsdateien zum späteren Download. Maximal dürfen 999 Dokumentationsdateien enthalten sein.	0...999
Firmware-Gruppen-Information	XML-Datei mit den Firmware-Gruppen-Informationen. Der Typ „FirmwareGroupInformation“ wird in dem Schema „Konfigurationsdienst.xsd“ spezifiziert. Der Dateiname des Elementes „Firmware-Gruppen-Information“ ist festgelegt auf „FirmwareGroupInfo.xml“. Das Element „Firmware-Gruppen-Information“ muss in jedem Update-Paket genau einmal vorhanden sein.	1
FirmwareGroupInfo_Signature	Optionale „Detached Signature“ für das Element „Firmware-Gruppen-Information“. Der Dateiname ist auf „FirmwareGroupInfo.sig“ festgelegt. Die Datei darf höchstens einmal im Paket vorhanden sein.	0..1

TIP1-A_6116 - Update-Paket - Dateinamen und Unterverzeichnisse
Der Konfigurationsdienst und Hersteller von Komponenten, die den KSR nutzen, MÜSSEN folgende Vorgaben im ZIP-Container gewährleisten und fehlerhafte Update-Pakete MÜSSEN abgelehnt werden:

- Die Dateinamen innerhalb des Paketes sind eindeutig.
- Es existieren keine Unterverzeichnisse innerhalb des ZIP-Containers.

[<=]

TIP1-A_6117 - Referenzierungen des Update-Paketes
Hersteller von Komponenten, die den KSR nutzen, MÜSSEN Update-Pakete erstellen, in denen alle Firmware- und Dokumentationsdateien in der Datei UpdateInfo.xml referenziert werden.
Der Konfigurationsdienst MUSS die Update-Pakete auf die Referenzierung aller Firmware- und Dokumentationsdateien in der Datei UpdateInfo.xml prüfen und fehlerhafte Update-Pakete ablehnen.
[<=]

TIP1-A_6118 - Zusätzliche Dateien im Update-Paket
Hersteller von Komponenten, die den KSR nutzen, MÜSSEN das Update-Paket so erstellen, das nur die in Tab_KSR_010 definierten Elemente in ihr enthalten sind.
Der Konfigurationsdienst MUSS prüfen, dass Update-Pakete nur die in Tab_KSR_010 definierten Elemente enthalten und fehlerhafte Update-Pakete ablehnen.
[<=]

TIP1-A_6119 - Update-Paket – Übertragung „Firmware-Gruppen-Information“
Hersteller von Komponenten, die den KSR nutzen, MÜSSEN, sofern es sich um ein Update einer Firmware-Gruppen-Information ohne neue Firmware handelt, das Update-Paket ausschließlich mit dem Element „Firmware-Gruppen-Information“ und dem optionalen Element „FirmwareGroupInfo-Signature“ füllen.
Der Konfigurationsdienst MUSS die Einhaltung dieser Definition prüfen und fehlerhafte Update-Pakete ablehnen.
[<=]

TIP1-A_6120 - Update-Paket – Dateinamen der UpdateInformation Detached-Signatur
Hersteller von Komponenten, die den KSR nutzen, und der Konfigurationsdienst MÜSSEN, sofern das Update-Paket eine Detached-Signatur der Datei UpdateInfo.xml enthält, die Signatur in der Datei mit dem Namen „UpdateInfo.sig“ erstellen bzw. prüfen und fehlerhafte Update-Pakete ablehnen.
[<=]

TIP1-A_6121 - Update-Paket – Dateinamen der FirmwareGroupInfo Detached-Signatur
Hersteller von Komponenten, die den KSR nutzen, und der Konfigurationsdienst MÜSSEN, sofern das Update-Paket eine Detached-Signatur der Datei FirmwareGroupInfo.xml enthält, die Signatur in der Datei mit dem Namen „FirmwareGroupInfo.sig“ erstellen bzw. prüfen und fehlerhafte Update-Pakete ablehnen.
[<=]

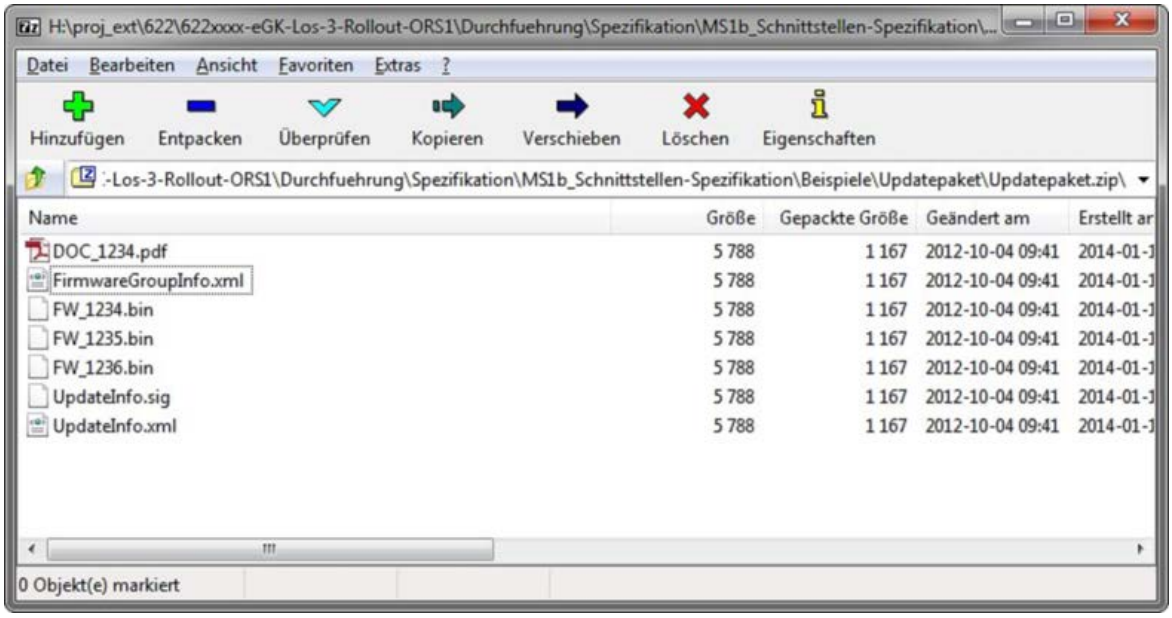


Abbildung 14: Abb_KSR_017 Beispiel Struktur Update-Paket

TIP1-A_6128 - Vollständige Update-Pakete
Der Konfigurationsdienst DARF unvollständige Update-Pakete NICHT verarbeiten.
[<=]

6.2.3.3 Pfadreferenzen

Für den Download der Dateien des Update-Paketes über die Schnittstelle I_KSRS_Download::getUpdates muss das Update-Paket mit der Pfadreferenz eindeutig bestimmt werden. In der Datenstruktur der Datei „UpdateInfo.xml“ müssen die Felder „Filename“ die Pfadangabe und den Dateinamen enthalten.

TIP1-A_6122 - Pfadreferenz
Hersteller von Komponenten, die den KSR nutzen, MÜSSEN alle Pfadangaben nach folgenden Vorgaben erstellen, der Konfigurationsdienst MUSS die Einhaltung dieser Definition prüfen und fehlerhafte Update-Pakete ablehnen:

- Schema: /<ProductVendorId>/<ProductCode>/<UpdateID>/<Filename>
- Als Trennzeichen muss das Zeichen „/“ verwendet werden.
- <Filename> entspricht dem Pattern „[A-Za-z0-9_-.]*“ und ist nicht länger als 32 Zeichen.

[<=]

Die Pfadangabe dient als Referenz auf das Update-Paket beim Download. Innerhalb des Paketes liegen die Dateien im Wurzel(root)-Verzeichnis (siehe Kapitel 6.2.3.1) und werden mit dem <Filename> am Pfadende eindeutig referenziert.

Damit wird es notwendig die UpdateID so zu generieren, dass sie für diesen Hersteller eindeutig und in eine URL eingebunden werden kann, d.h. die Pfadangabe zusammen mit der Hostadresse des Download-Bereiches muss eine gültige URL ergeben.

6.2.3.4 Verfahren zum Erstellen eines signierten Update-Paketes

Der Hersteller von Komponenten, die den KSR nutzen, hat ein - entsprechend den Vorgaben des Konfigurationsdienst-Anbieters beantragtes - X.509-Zertifikat mit einem Private-Key zum Signieren der Dateien erhalten. Mit dem privaten Schlüssel dieses Zertifikats kann der Hersteller mit Hilfe eines Tools die Update-Pakete signieren. Die Grundlage des Signaturverfahrens ist in [gemSpec_Krypt#3.7] definiert. Darin ist der Signaturstandard [ETSI-CAdES] vorgegeben.

Der Konfigurationsdienst verwendet die Signatur des Herstellers zum Verifizieren der Gültigkeit und des Zertifikates.

Folgendes Verfahren wird angewendet zur Verifikation der Signatur der Datei:

1. Der Hersteller erstellt ein Update-Paket.
2. Der Hersteller signiert das Update-Paket mit dem privaten Schlüssel seines X.509-Zertifikats und erstellt eine PKCS#7 Signatur-Datei des Update-Paketes.
3. Das Update-Paket und die Signatur-Datei werden über das Web-Frontend des Upload-Bereiches durch den Hersteller hochgeladen.
4. Der Konfigurationsdienst verifiziert die Signatur und gibt das Update-Paket zur weiteren Bearbeitung frei.

TIP1-A_6123 - Update-Paket – Signatur
Der Konfigurationsdienst und Hersteller von Komponenten, die den KSR nutzen, MÜSSEN die detached PKCS#7-Signatur zum Update-Paket mit Signatur-Vorgaben entsprechend [gemSpec_Krypt#A_17359] unterstützen. Das Feld certificates des Feldes signedData der Signatur MUSS das Zertifikat des Signers enthalten (Validation Policy zu [ETSI-CAdES#5.4]). Das Feld signedAttrs der Signatur MUSS die Attribute content-type (OID 1.2.840.113549.1.9.3), message-digest (OID 1.2.840.113549.1.9.4) und ESS signing-certificate-v2 (OID 1.2.840.113549.1.9.16.2.47) enthalten laut [ETSI-CAdES#5.7].**[<=]**

TIP1-A_6124 - Bereitstellung KSR Update-Paket Zertifikat
Der KSR-Anbieter MUSS für die Hersteller dezentraler Komponenten X.509-Zertifikate und zugehörige private Schlüssel zum Signieren der Update-Pakete bereitstellen und ihnen Vorgaben machen wie diese Zertifikate beantragt werden können. Hersteller von Komponenten, die den KSR nutzen, MÜSSEN den privaten Schlüssel des bereitgestellten X.509-Zertifikats zum Signieren ihrer Update-Pakete verwenden.
[<=]

TIP1-A_6127 - Fehlerhafte Signaturen
Der Konfigurationsdienst DARF Pakete mit einer fehlerhaften oder nicht verifizierten Signatur NICHT weiter verarbeiten.
[<=]

A_17344 - KSR Bereitstellung "Signier-Tool" für neue kryptographische Algorithmen (ECC-Migration)
Der Anbieter des Konfigurationsdienstes MUSS berechtigten Herstellern dezentraler Komponenten der TI, dem ~~Servicebetriebsverantwortlichen TI-Plattform~~ Gesamtverantwortlichen TI (PU) und der ~~Testbetriebsverantwortlichen~~ Testbetriebsinstanz TU/RU das Tool zur ECC-Signatur von Update-Paketen rechtzeitig vor Auslauf der bisherigen kryptographische Algorithmen bereitstellen.
[<=]

A_17759 - KSR Informationspflicht über neue kryptographische Algorithmen (ECC-Migration)
Der Anbieter des Konfigurationsdienstes MUSS die registrierten Nutzer von dem Upload-Interface – spätestens ab Bereitstellung des Tools – auf das geänderte Tool und den Zeitplan für den Wechsel der kryptographischen Algorithmen hinweisen. **[<=]**

A_17374 - KSR Gültigkeit der Update-Pakete bei Migration zu neuen kryptographischen Algorithmen (ECC-Migration)
Der Konfigurationsdienst MUSS Update-Pakete, welche erfolgreich die Eingangsprüfung bestanden haben, aber mit abgelösten kryptographischen Algorithmen signiert wurden, weiterhin für die dezentralen Produkte bereitstellen.
[<=]

6.2.3.5 Signier-Tool für Update-Pakete

Hersteller dezentraler Komponenten der TI - welche Update-Pakete über den KSR verteilen - müssen diese Update-Pakete signieren. Der Konfigurationsdienst prüft Signaturen dieser Update-Pakete.

Zur Vereinfachung der Signatur von Update-Paketen stellt der Anbieter des Konfigurationsdienstes ein Signatur-Tool bereit. Dieses Signatur-Tool können Hersteller dezentraler Komponenten zur Erstellung der - durch den KSR geprüften - Signaturen nutzen. Damit werden die Hersteller dezentraler Komponenten entlastet und die

Weiterentwicklung dieser Signaturen (z.B. Wechsel von Signaturalgorithmen) kann zentral erfolgen.

TIP1-A_6066 - KSR Bereitstellung "Signier-Tool"
Der Anbieter des Konfigurationsdienstes MUSS berechtigten Herstellern dezentraler Komponenten der TI, dem Gesamtverantwortlichen TI (PU) ~~Servicebetriebsverantwortlichen TI-Plattform (PU)~~ und der ~~Testbetriebsverantwortlichen~~ Testbetriebsinstanz TU/RU ein plattformunabhängiges Tool (z.B. auf Java Basis) zur Signatur von Update-Paketen - mit dem vom Anbieter des Konfigurationsdienstes gelieferten X.509-Zertifikat (TIP1-A_6124) - bereitstellen, welches alle durch den KSR geprüften Signaturen eines Update-Paketes erstellen kann. Das sind

- die Signatur der Datei FirmwareGroupInfo.xml (siehe Kap. 5.3.1) und
- die Signatur des Update-Pakets (siehe Kap. 6.2.3.4).

[<=]

6.2.4 Managementdienste P_KSRS_Operations

Dieses Kapitel beschreibt die organisatorische Schnittstelle des Konfigurationsdienstes zum ~~Servicebetriebsverantwortlichen der TI-Plattform~~ Gesamtverantwortlichen TI und zur ~~den Testbetriebsverantwortlichen~~ Testbetriebsinstanz der RU und TU.

~~Abbildung~~ 15~~: Abb_KSR_010 Beispiel Auftragsabarbeitung (P_KSRS_Operations)~~

Wird für diese Schnittstelle TLS zur Verschlüsselung der übertragenen Daten eingesetzt, dann gelten alle - im Produkttypsteckbrief aufgeführten - TLS Anforderungen.

6.2.4.1 Schnittstellendefinition

KSR-Management bietet für den ~~Servicebetriebsverantwortlichen der TI-Plattform~~ Gesamtverantwortlichen TI Funktionalität zur Steuerung und Kontrolle der Verteilung von Update-Paketen.

TIP1-A_3349 - Organisatorische Schnittstelle zur Erteilung von Aufträgen
Der Anbieter des Konfigurationsdienstes MUSS ~~eine Schnittstelle~~ ein Web-Interface für jede Umgebung (RU, TU, PU) im Internet bereitstellen, über die berechtigte Akteure Aufträge zur Aufnahme und Löschung von Update-Paketen und Konfigurationsdatenfiles in die Download-Bereiche der von ihnen verantworteten Umgebungen erteilen können.
[<=]

TIP1-A_3350 - Organisatorische Schnittstelle Form und Inhalt von Aufnahme-Aufträgen
Der Anbieter des Konfigurationsdienstes MUSS Form und Inhalt eines Auftrags zur Aufnahme eines Update-Pakets/Firmware-Gruppen-Informationen und Konfigurationsdatenfiles in den Download-Bereich definieren und mit den berechtigten Akteuren abstimmen. ~~Folgende Informationen MÜSSEN zwingend enthalten sein:~~

- ~~Auftraggeber~~
- ~~Umgebung, in der der Auftrag ausgeführt werden soll~~
- ~~Eindeutige Referenz auf das bereitzustellende Update-Paket „UpdateID“, Firmware-Gruppen-Informationen „FirmwareGroupID“ bzw. die Konfigurationsdaten.~~

[<=]

TIP1-A_6126 - Organisatorische Schnittstelle Form und Inhalt Ergebnisse von Aufnahme-Aufträgen
Der Anbieter des Konfigurationsdienstes MUSS Form und Inhalt des Ergebnisses eines Auftrags definieren und mit den berechtigten Akteuren abstimmen. Die Ergebnisse MÜSSEN permanent gespeichert und durch berechtigte Nutzer im Web-Interface abrufbar sein. Folgende Informationen MÜSSEN mindestens ~~zwingend~~ enthalten sein:

- Auftraggeber
- Eindeutige Referenz des verarbeiteten Update-Pakets „UpdateID“, Firmware-Gruppen-Information „FirmwareGroupID“ bzw. Konfigurationsdaten.
- Status des verarbeiteten Update-Pakets „UpdateID“, Firmware-Gruppen-Information „FirmwareGroupID“ bzw. Konfigurationsdaten nach Auftragsabarbeitung entsprechend Tab_KSR_050.
- Datum und Uhrzeit der Auftragsabarbeitung.
- Ergebnis der Auftragsabarbeitung.

[<=]

Tabelle 49: Tab_KSR_050 Status Definition

Status	Beschreibung
Neu	Das Paket wurde an den Konfigurationsbereich übergeben und wartet auf den Start der Eingangsprüfung. Der Start erfolgt automatisch.
Test	Die Eingangsprüfung wird gerade durchgeführt (für Update-Pakete).
Akzeptiert	Die Eingangsprüfung wurde erfolgreich durchgeführt. Das Paket wartet auf die Freigabe.
Abgelehnt	Die Eingangsprüfung meldete einen Fehler, das Update-Paket wird zurückgewiesen.
Freigegeben	Das Paket wurde zum Download freigegeben und wird an den Download-Bereich übertragen. Sobald die Übertragung abgeschlossen ist, wird das Paket automatisch aktiviert.
Aktiviert	Das Update-Paket ist in Download-Bereich übertragen und steht dort zum Download durch die Konnektoren bereit.
Deaktiviert	Das Update-Paket wurde deaktiviert und ist nicht mehr im Download-Bereich verfügbar.

TIP1-A_5163 - Organisatorische Schnittstelle zur Übergabe von Konfigurationsdaten
Der Anbieter des Konfigurationsdienstes MUSS Form und Inhalt eines Auftrags zur Übergabe von Konfigurationsdaten definieren und mit den berechtigten Akteuren abstimmen. Folgende Informationen MÜSSEN zwingend enthalten sein:

- Auftraggeber
- Umgebung, in der der Auftrag ausgeführt werden soll
- Name des Konfigurationsdatenfiles
- Format für die Übergabe der zugehörigen Konfigurationsdaten

Die übergebenen Konfigurationsdaten ersetzen (nach Freigabe durch die verantwortliche Instanz) die aktuellen Konfigurationsdaten.

[<=]

TIP1-A_3913 - Organisatorische Schnittstelle Form und Inhalt von Lösch-Aufträgen
Der Anbieter des Konfigurationsdienstes MUSS Form und Inhalt eines Auftrags zur Löschung eines Update-Pakets/Firmware-Gruppen-Informationen aus dem Download-Bereich definieren und mit den berechtigten Akteuren abstimmen. Folgende Informationen MÜSSEN zwingend enthalten sein:

- Auftraggeber
- Umgebung, in der der Auftrag ausgeführt werden soll
- Eindeutige Referenz auf das bereitzustellende Update-Paket „UpdateID“ bzw. Firmware-Gruppen-Informationen „FirmwareGroupID“

[<=]

TIP1-A_3355 - Schutz Managementschnittstelle
Der Anbieter des Konfigurationsdienstes MUSS die Kommunikationsschnittstelle P_KSRS_Operations gegen unberechtigte Nutzung schützen. Dazu muss der Anbieter des Konfigurationsdienstes den Auftraggeber identifizieren und authentisieren. Der Anbieter des Konfigurationsdienstes kann weitere Schutzmaßnahmen definieren.
[<=]

A_14541 - Status Update-Pakete P_KSRS_Operations
Der Anbieter des Konfigurationsdienstes MUSS sicherstellen, dass berechtigte Akteure (berechtigte Hersteller von Komponenten, die den KSR nutzen, GTI (PU), TBI (TU) und TBI (RU)) in Schnittstelle P_KSRS_Operations der jeweiligen Umgebung den Status der Update-Pakete einsehen können.
[<=]

TIP1-A_3914 - Berechtigungen für Aufträge PU-Download-Bereich
~~Der Anbieter des Konfigurationsdienstes DARF NICHT Aufträge für den Download-Bereich der PU von anderen Auftraggebern als dem Servicebetriebsverantwortlichen der TI-Plattform verarbeiten.~~
[<=]

TIP1-A_3915 - Berechtigungen für Aufträge TU-Downloadbereich
~~Der Anbieter des Konfigurationsdienstes DARF NICHT Aufträge für den Download-Bereich der TU von anderen Auftraggebern als dem Testbetriebsverantwortlichen der TU verarbeiten.~~
[<=]

TIP1-A_3916 - Berechtigungen für Aufträge RU-Downloadbereich
~~Der Anbieter des Konfigurationsdienstes DARF NICHT Aufträge für den Download-Bereich der RU von anderen Auftraggebern als dem Testbetriebsverantwortlichen der RU verarbeiten.~~
[<=]

TIP1-A_3917 - Keine Aufnahme von invaliden Update-Paket bzw. Firmware-Gruppen-Informationen
Ist ein zur Aufnahme beauftragtes Update-Paket bzw. Firmware-Gruppen-Informationen technisch nicht valide (siehe Eingangsprüfung), so DARF der Anbieter des Konfigurationsdienstes es NICHT in den entsprechenden Download-Bereich einstellen.
[<=]

TIP1-A_3918 - Aufnahme von validen Update-Paket bzw. Firmware-Gruppen-Informationen
Ist ein zur Aufnahme beauftragtes Update-Paket bzw. eine Firmware-Gruppen-Information technisch valide, so MUSS der Anbieter des Konfigurationsdienstes es nach erfolgreicher Prüfung des Auftrags in den entsprechenden Download-Bereich einstellen.
[<=]

TIP1-A_3919 - Durchführungsbestätigung eines Auftrags
Nach Ausführung eines Auftrags MUSS der Anbieter des Konfigurationsdienstes den Auftraggeber die erfolgreiche Durchführung des Auftrages bestätigen bzw. über aufgetretene Fehler informieren.
[<=]

TIP1-A_3920 - Form und Inhalt der Durchführungsbestätigung eines Auftrags
Der Anbieter des Konfigurationsdienstes MUSS Form und Inhalt der Durchführungsbestätigung eines Auftrags definieren und mit den berechtigten Akteuren abstimmen.
[<=]

TIP1-A_3921 - Logging der Auftragsbearbeitung
Der Anbieter des Konfigurationsdienstes MUSS die Durchführung des Prozesses einschließlich der Beauftragung und Bestätigung in Log-Dateien dokumentieren**.**
[<=]

TIP1-A_3351 - Organisatorische Schnittstelle zur Bereitstellung von PU-Log-Daten
Der Anbieter des Konfigurationsdienstes MUSS dem ~~Servicebetriebsverantwortlichen der TI-Plattform~~ Gesamtverantwortlichen TI auf Anforderung die Log-Dateien des Upload- und Download-Bereiches der Produktivumgebung (PU) übermitteln.
[<=]

TIP1-A_3922 - Organisatorische Schnittstelle zur Bereitstellung von RU-Log-Daten
Der Anbieter des Konfigurationsdienstes MUSS der ~~Testbetriebsverantwortlichen~~ Testbetriebsinstanz RU auf Anforderung die Log-Dateien des Upload- und Download-Bereiches der Referenzumgebung (RU) übermitteln.
[<=]

TIP1-A_3923 - Organisatorische Schnittstelle zur Bereitstellung von TU-Log-Daten
Der Anbieter des Konfigurationsdienstes MUSS der ~~Testbetriebsverantwortlichen~~ Testbetriebsinstanz TU auf Anforderung die Log-Dateien des Upload- und Download-Bereiches der Testumgebung (TU) übermitteln.
[<=]

TIP1-A_3352 - Organisatorische Schnittstelle zur Bereitstellung von statistischen Daten der PU
Der Anbieter des Konfigurationsdienstes MUSS dem ~~Servicebetriebsverantwortlichen der TI-Plattform~~ Gesamtverantwortlicher TI zyklisch jeden Monat und zusätzlich auf Anfrage adhoc einen Bericht mit den statistischen Daten der Produktivumgebung (PU)

übermitteln.
[<=]

TIP1-A_3924 - Organisatorische Schnittstelle zur Bereitstellung von statistischen Daten der RU
Der Anbieter des Konfigurationsdienstes MUSS demr ~~Testbetriebsverantwortlichen~~ Testbetriebsinstanz RU zyklisch jeden Monat und zusätzlich auf Anfrage adhoc einen Bericht mit den statistischen Daten der Referenzumgebung (RU) übermitteln.
[<=]

A_14542 - Berechtigung P_KSRS_Operations
Der Anbieter des Konfigurationsdienstes MUSS sicherstellen, dass

- nur berechtigte Akteure (berechtigte Hersteller von Komponenten, die den KSR nutzen, GTI (PU), TBI (TU) und TBI (RU)) auf P_KSRS_Operations der jeweiligen Umgebung zugreifen können.
- die Rollen Hersteller_RU und Hersteller_RU_Konfig sowie Hersteller_TU und Hersteller_TU_Konfig nicht dem gleichen Akteur zugeordnet werden.
- Akteure mit den Rollen Hersteller_* nur auf eigene Pakete (Pakete mit dem ProductVendorID des Akteurs) und Daten über eigene Pakete zugreifen können.

[<=]

A_14543 - P_KSRS_Operations parallel nutzbar
Der Konfigurationsdienst SOLL die Kommunikationsschnittstelle von P_KSRS_Operations so implementieren, dass sie parallel durch mehrere Aufrufer nutzbar ist.
[<=]

A_14544 - KSR Logging – P_KSRS_Operations
Der Konfigurationsdienst MUSS mindestens für alle Vorgänge welche Daten im Konfigurationsdienst ändern (z.B. Aufnahme-Aufträge und Lösch-Aufträge) Logging-Daten erfassen.
Ein Log-Eintrag MUSS mindestens folgende Informationen erfassen:

- Wer hat etwas getan
- Was wurde getan
- Zeitpunkt
- Updatepaket.UpdateInformation.UpdateID bzw. FirmwareGroupInformation.FirmwareGroupID

[<=]

TIP1-A_3925 - Organisatorische Schnittstelle zur Bereitstellung von statistischen Daten der TU
Der Anbieter des Konfigurationsdienstes MUSS der Testbetriebsinstanz ~~Testbetriebsverantwortlichen~~ TU zyklisch jeden Monat und zusätzlich auf Anfrage adhoc einen Bericht mit den statistischen Daten der Test~~Referenz~~umgebung (TU) übermitteln.
[<=]

TIP1-A_5043 - Organisatorische Schnittstellen parallel nutzbar
Der Konfigurationsdienst SOLL die organisatorischen Schnittstellen so realisieren, dass sie parallel durch mehrere Aufrufer nutzbar sind.
[<=]

TIP1-A_6067 - Organisatorische Schnittstelle zur Bereitstellung von KSR Statusberichten der PU
Der Anbieter des Konfigurationsdienstes MUSS dem ~~Servicebetriebsverantwortlichen der TI-Plattform~~ Gesamtverantwortlichen TI einen Statusbericht im XML-Format mit den Informationen aller auf dem KSR vorliegenden Firmware-Pakete der Produktivumgebung (PU) übermitteln. Dieser Statusbericht MUSS bei jeder Änderung der enthaltenen Daten übermittelt werden.
[<=]

TIP1-A_6074 - Organisatorische Schnittstelle zur Bereitstellung von KSR Statusberichten der PU – Inhalt
Der Anbieter des Konfigurationsdienstes MUSS in dem Statusbericht zu jedem Firmware-Paket mindestens folgende Informationen liefern:

- Timestamp (Zeitstempel des Hochladens auf den KSR)
- Kurzbeschreibung (beim Hochladen auf den KSR eingegebene Kurzbeschreibung)
- FirmwareGroupInformation
  - FirmwareGroupID
  - ProductVendorID
  - ProductCode
  - HWVersion
  - FirmwareGroupVersion
  - CreationDate
  - FirmwareGroupReleaseNotes
  - Liste von Firmwareversionen (FWVersion)
  - Aktive FG (Kennzeichen ob diese Firmwaregruppe aktiv ist)
- UpdateInformation
  - UpdateID
  - ProductVendorID
  - ProductCode
  - HWVersion
  - ProductName
  - CreationDate
  - DeploymentInformation
    - StartDate
    - Deadline
  - Firmware
    - FWVersion
    - FWPriority

    - FirmwareReleaseNotes
  - Status
  - Status-Beschreibung

[<=]

TIP1-A_6075 - Organisatorische Schnittstelle zur Bereitstellung von KSR-Statusberichten der PU – Anhänge
Der Anbieter des Konfigurationsdienstes MUSS mit dem Statusbericht als Anlage alle weiteren aktuell gültigen Konfigurationsdateien hinzufügen, welche die Auswahl von Update-Paketen beeinflussen.
[<=]

TIP1-A_6076 - Organisatorische Schnittstelle zur Bereitstellung von KSR-Statusberichten der PU – Excel-Import
Der Anbieter des Konfigurationsdienstes MUSS den Statusbericht in einem XML-Format liefern, welches den Excel-Import und die weitere Analyse des Reports in Excel ermöglicht.
[<=]

7 Anhang A – Verzeichnisse

7.1 Abkürzungen

Kürzel	Erläuterung
FQDN	Fully Qualified Domain Name
GTI	Gesamtverantwortlicher der TI
KSR	Konfigurations- und Software Repository
PU	Produktivumgebung
RU	Referenzumgebung
SOAP	Simple Object Access Protocol
TBI	Testbetriebsinstanz
TLS	Transport Layer Security
TU	Testumgebung

7.2 Glossar

Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung gestellt.

7.3 Abbildungsverzeichnis

Abbildung 1: Abb_KSR_001 Überblick externe Akteure Konfigurationsdienst....8
Abbildung 2: Abb_KSR_011 Überblick Use Cases Konfigurationsdienst....9
Abbildung 3: Abb_KSR_002 Kontextdiagramm Konfigurationsdienst....11
Abbildung 4: Abb_KSR_003 Zerlegung Konfigurationsdienst....12
Abbildung 5: Abb_KSR_012 Verteilungsprozess Update-Paket ~~(PU)~~....13
Abbildung 6: Abb_KSR_004 Inhalt von Firmware-Update-Paketen 18
Abbildung 7: Abb_KSR_005 Hersteller-Update-Informationen (UpdateInfo.xml)....22

Abbildung 8: Abb_KSR_006 Beispiel UpdateInfo.xml 28
Abbildung 9: Abb_KSR_013 Verteilungsprozess Firmware-Gruppen-Informationen 30
Abbildung 10: Abb_KSR_007 Firmware-Gruppen-Informationen 31
Abbildung 11: Abb_KSR_016 Beispiel aus FirmwareGroupInfo.xml.....34
Abbildung 12: Abb_KSR_008 Operation I_KSRS_Download::listUpdates Request 49
Abbildung 13: Abb_KSR_009 Operation I_KSRS_Download::listUpdates Response 50
Abbildung 14: Abb_KSR_017 Beispiel Struktur Update-Paket 66
~~Abbildung 15: Abb_KSR_010 Beispiel Auftragsabarbeitung (P_KSRS_Operations)~~.....69
Abbildung 16: Abb_KSR_015 Beispielablauf für ein Firmware Update.....82
Abbildung 17: Abb_KSR_014 Schema InfrastrukturKonfig.xsd 83

7.4 Tabellenverzeichnis

Tabelle 1: Tab_KSR_001 Schnittstellen des Konfigurationsdienstes 16
Tabelle 2: Tab_KSR_003 Schutz der Firmware-Update-Pakete 19
Tabelle 3: Tab_KSR_004 Hersteller-UpdateInformation – Element UpdateID.....22
Tabelle 4: Tab_KSR_005 Hersteller-UpdateInformation – Element ProductVendorID.....23
Tabelle 5: Tab_KSR_006 Hersteller-UpdateInformation – Element ProductCode 23
Tabelle 6: Tab_KSR_007 Hersteller-UpdateInformation – Element HWVersion.....23
Tabelle 7: Tab_KSR_008 Hersteller-UpdateInformation – Element ProductName 24
Tabelle 8: Tab_KSR_009 Hersteller-UpdateInformation – Element CreationDate.....24
Tabelle 9: Tab_KSR_012 Hersteller-UpdateInformation – Element DeploymentInformation.StartDate 24
Tabelle 10: Tab_KSR_013 Hersteller-UpdateInformation – Element DeploymentInformation.Deadline 24
Tabelle 11: Tab_KSR_014 Hersteller-UpdateInformation – Element Firmware.FWVersion 25
Tabelle 12: Tab_KSR_040 Hersteller-UpdateInformation – Element Firmware.FWPriority 25
Tabelle 13: Tab_KSR_015 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.Filename 25
Tabelle 14: Tab_KSR_041 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.FileSize 26
Tabelle 15: Tab_KSR_016 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.Notes 26
Tabelle 16: Tab_KSR_017 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.Filename 26

Tabelle 17: Tab_KSR_042 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.FileSize 26
Tabelle 18: Tab_KSR_018 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.Notes 27
Tabelle 19: Tab_KSR_019 Hersteller-UpdateInformation – Element Firmware.FirmwareReleaseNotes....27
Tabelle 20: Tab_KSR_020 Hersteller-UpdateInformation – Element UpdateInformationSignature 27
Tabelle 21: Tab_KSR_021 Firmware-Gruppen-Information – Element FirmwareGroupID 31
Tabelle 22: Tab_KSR_022 Firmware-Gruppen-Information – Element FirmwareGroupVersion....32
Tabelle 23: Tab_KSR_023 Firmware-Gruppen-Information – Element FirmwareGroupReleaseNotes....32
Tabelle 24: Tab_KSR_024 Firmware-Gruppen-Information – Element FirmwareGroupSignature....32
Tabelle 25: Tab_KSR_048 Logdatenformat 39
Tabelle 26: Tab_KSR_049 Werte im Feld InfoID zu Action 40
Tabelle 27: Tab_KSR_046 Statistikdatenformat....41
Tabelle 28: Tab_KSR_051 Lokalisierungsdaten 43
Tabelle 29: Tab_KSR_025 Konfigurationsdienst....47
Tabelle 30: Tab_KSR_026 Operation I_KSRS_Download::listUpdates....48
Tabelle 31: Tab_KSR_027 I_KSRS_Download::listUpdates Request 49
Tabelle 32: Tab_KSR_028 Hersteller-Update-Informationen – Element ProductVendorID 49
Tabelle 33: Tab_KSR_029 Hersteller-Update-Informationen – Element ProductCode 49
Tabelle 34: Tab_KSR_030 Hersteller-Update-Informationen – Element HWVersion....49
Tabelle 35: Tab_KSR_031 Hersteller-Update-Informationen – Element FWVersion 50
Tabelle 36: Tab_KSR_032 I_KSRS_Download::listUpdates – Response 51
Tabelle 37: Tab_KSR_033 I_KSRS_Download::listUpdates – Element FirmwareGroupReleaseNotes....51
Tabelle 38: Tab_KSR_034 I_KSRS_Download::listUpdates – Element UpdateInformation 51
Tabelle 39: Tab_KSR_047 I_KSRS_Download::listUpdates Fehlercodes....51
Tabelle 40: Tab_KSR_035 Operation I_KSRS_Download::getUpdates 52
Tabelle 41: Tab_KSR_044 Operation I_KSRS_Download::get_Ext_Net_Config....54
Tabelle 42: Tab_KSR_043 TUC_KSR_001 „Get File“....55
Tabelle 43: Tab_KSR_036 File Transfer HTTP Request – Element host 56

Tabelle 44: Tab_KSR_037 File Transfer HTTP Request – Element path 56
Tabelle 45: Tab_KSR_011 Gruppen und Berechtigungen 59
Tabelle 46: Tab_KSR_038 Beispiel Gruppenzuordnung 60
Tabelle 47: Tab_KSR_039 P_KSRS_Upload Schema 61
Tabelle 48: Tab_KSR_010 Struktur Update-Paket 64
Tabelle 49: Tab_KSR_050 Status Definition 70
Tabelle 50: Tab_KSR_045 Attribute des Konfigurationsdatenfiles zur Anbindung von Bestandsnetzen 83

7.5 Referenzierte Dokumente

7.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	**Herausgeber: Titel**
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemKPT_Betr]	gematik: Betriebskonzept
[gemSpec_Kon]	gematik: Konnektorspezifikation
[gemSpec_KT]	gematik: Spezifikation eHealth-Kartenterminal
[gemSpec_Net]	gematik: Spezifikation Netzwerk
[gemSpec_OM]	gematik: Spezifikation Operations und Maintenance
[gemProdT_KSR]	gematik: Produkttypsteckbrief Konfigurationsdienst
[gemSpec_Krypt]	gematik. Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur

[gemSpec_Perf]	gematik: Performance und Mengengerüst TI-Plattform
[gemSpec_SST_LD_BD]	gematik: Spezifikation Logdaten- und Betriebsdatenerfassung
[gemSpec_StAmpel]	gematik: Spezifikation Störungsampel

7.5.2 Weitere Dokumente

[Quelle]	**Herausgeber (Erscheinungsdatum): Titel**
[RFC1738]	Uniform Resource Locators (URL)
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109
[RFC2616]	Hypertext Transfer Protocol – http/1.1
[ZIP-APP]	http://www.pkware.com/documents/casestudies/APPNOTE.TXT
[XMLDSig]	XML Signature Syntax and Processing (Second Edition) W3C Recommendation 10 June 2008 http://www.w3.org/TR/2008/PER-xmldsig-core-20080326/
[ETSI-CAdES]	ETSI TS 101 733 V1.7.4 (2008-07), Electronic Signatures and Infrastructures (ESI); CMS AdvancedElectronic Signatures (CAdES)
[ETSI-XAdES]	ETSI TS 101 903 V1.4.2 (2010-12), Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)

8 Anhang B – Nutzungsbeispiel I_KSRS_Download

Im Folgenden wird ein Beispiel für die Aktualisierung einer dezentralen Komponente beschrieben.

Das Update-Paket besteht im Beispiel aus

- Hersteller UpdateInformation ‚AdminInfo.xml',
  - Firmwarefile ‚Firmware.fw' und
  - PDF Dokumentation ‚Documentation.PDF'.

Der Administrator / Konnektor befragt zuerst den Konfigurationsdienst nach verfügbaren Updates (Operation listUpdates). Der Konfigurationsdienst gibt eine Liste von verfügbaren Update-Paketen inklusive Release Notes für den angefragten Client zurück. Falls weitere Informationen benötigt werden, können die Dokumentation der Update-Pakete vom Konfigurationsdienst geladen werden.

Der Administrator wählt aus der Liste ein Update-Paket aus und startet das Update (Operation do_Update) für ein ausgewähltes Firmwarefile.

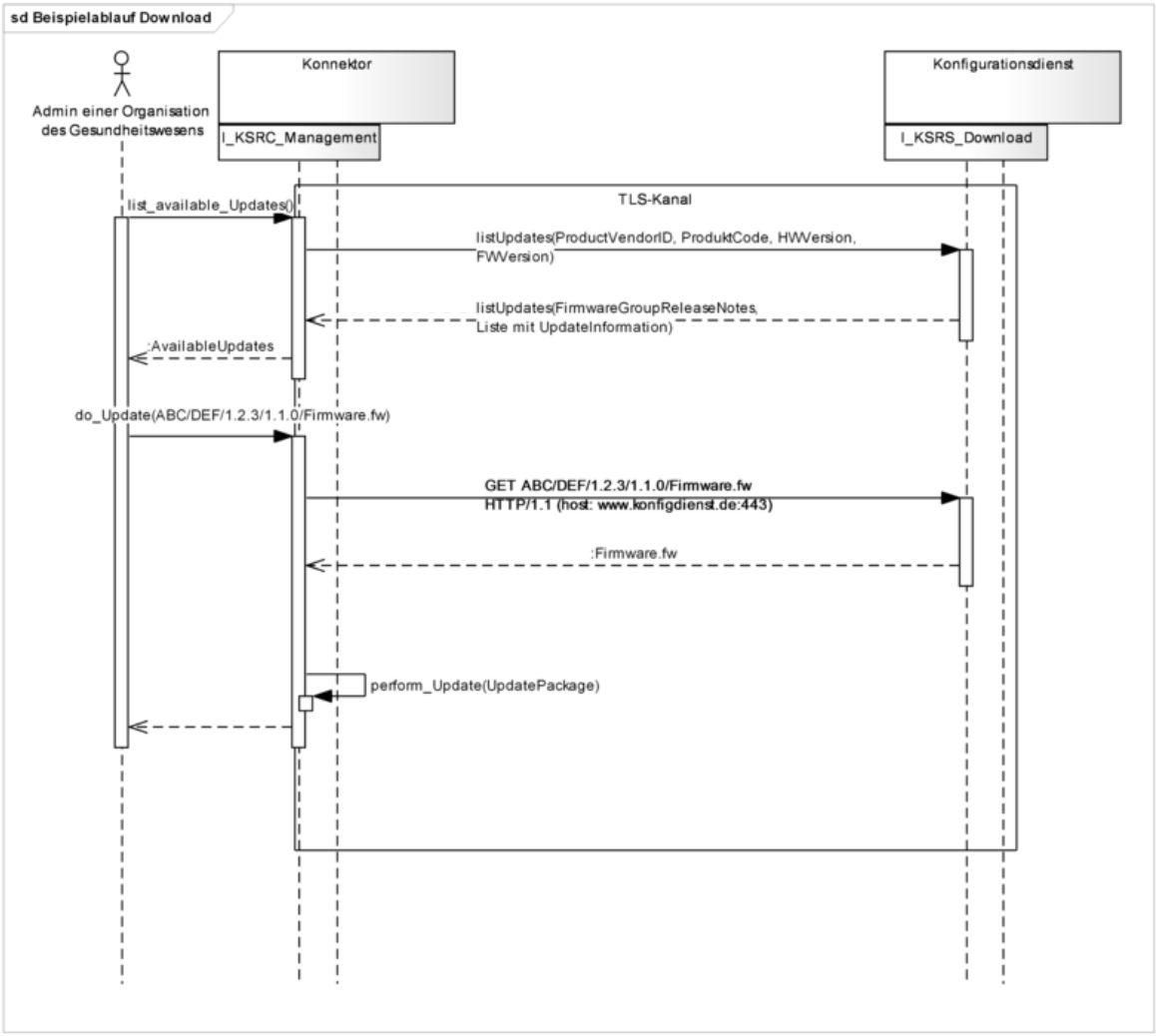


Abbildung 16: Abb_KSR_015 Beispielablauf für ein Firmware Update

Wahlweise kann sich der Administrator vor dem Download der Firmware die Dokumentation ansehen. Der Administrator kann dann den Download der Firmware ausführen oder den Ablauf ohne Firmware-Download beenden.

9 Anhang C – Konfigurationsdatenfile zur Anbindung von Bestandsnetzen (Netzkonfiguration aAdG-NetG)

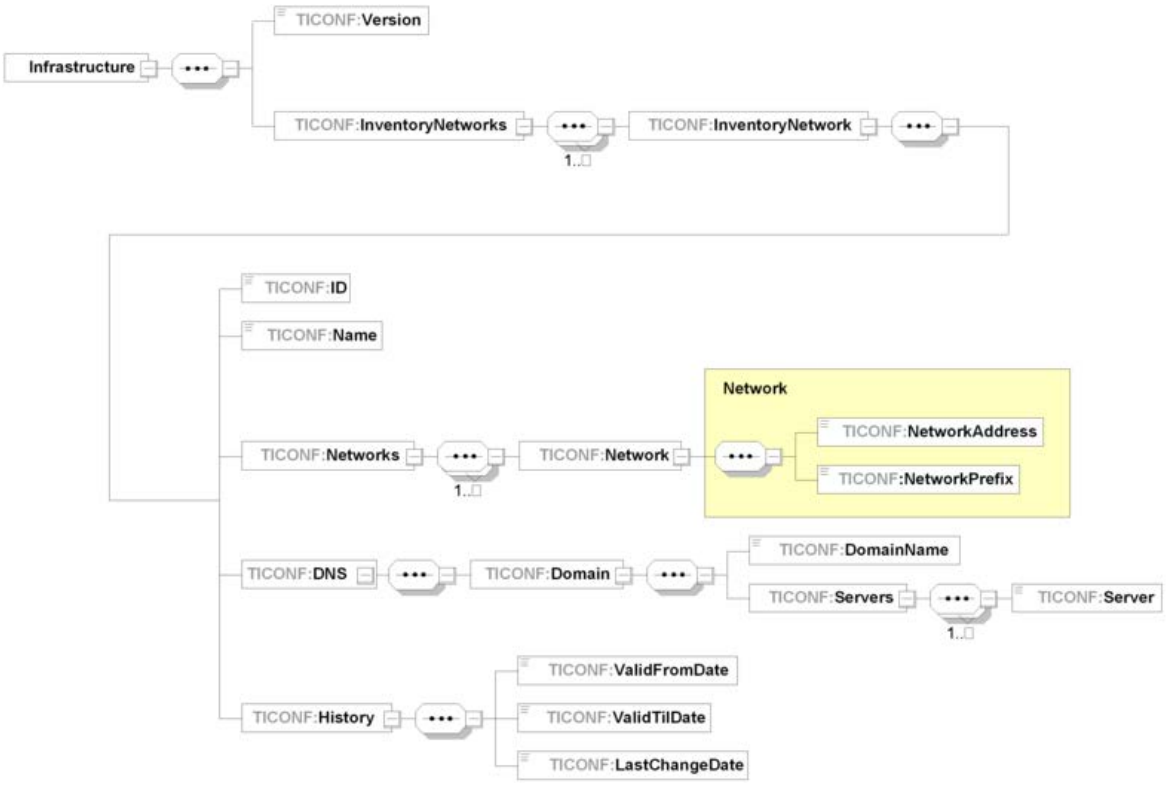


Abbildung 17: Abb_KSR_014 Schema InfrastrukturKonfig.xsd

Tabelle 50: Tab_KSR_045 Attribute des Konfigurationsdatenfiles zur Anbindung von Bestandsnetzen

Datenelement	Typ	Beschreibung	Wertebereich
Version	string	Version des Konfigurationsdatenfiles	entsprechend gemSpec_OM# GS-A_3695
InventoryNetworks	complex type	Netzwerkinformation zu einem oder mehreren Bestandsnetzen	
InventoryNetwork	complex type	Netzwerkinformation für ein Bestandsnetz	
ID	string	Identifier des Bestandsnetzes - Der Identifier muss innerhalb von Bestandsnetze.xml eindeutig sein. - Der Identifier darf für ein einmal propagiertes Bestandsnetz nicht geändert werden, da sonst dieses	

		Bestandsnetz als ein neues Bestandsnetz interpretiert wird.	
Name	string	Name des Bestandsnetzes	
Networks	complex type	Netzwerkinformation zu einem oder mehreren Netzwerken	
Network	complex type	Netzwerkwerkinformation zu einem Netzwerk	
NetworkAddress	string	Netzwerkadresse	Darstellung entsprechend RFC791
NetworkPrefix	string	Netzwerkpräfix	Entsprechend RFC 4632 (1-32)
DNS	complex type	DNS-Information zu einer	
Domain	complex type	Domaininformation zu einer Domain	
DomainName	string	Domain Name	Darstellung entsprechend RFC1035
Servers	complex type	Liste von einem oder mehreren DNS-Servern	
Server	string	Host-Adresse für einen DNS-Server	Darstellung entsprechend RFC791
History	complex type	Informationen zum Gültigkeitsdatum und Änderungsdatum	
ValidFromDate	string	Gültig ab	YYYY-MM-DD
ValidTilDate	string	Gültig bis	YYYY-MM-DD
LastChangeDate	string	Änderungsdatum	YYYY-MM-DD