Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation

Konfigurationsdienst

Version:	1.4.0
Revision:	\main\rel_online\rel_ors1\23
Stand:	17.06.2014
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_KSR

Dokumentinformationen

Änderungen zur Vorversion

In der Aufllistung der Schnittstellen des KSR wurde die benötigte Schnittstelle ergänzt, eine Referenz wurde gestrichen – gemäß P11-Änderungsliste.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	23.07.12		zur Abstimmung freigegeben	PL P77
			Überarbeitung nach Kommentierung und Workshop	P77
1.0.0	15.10.12		freigegeben	gematik
			Einarbeitung Kommentare	P77
1.0.9	22.04.13		zur Abstimmung freigegeben	PL P77
1.1.0 RC	30.05.13		zur Freigabe empfohlen	PL P77
1.1.0	06.06.13		freigegeben	gematik
			Einarbeitung lt. Änderungsliste vom 08.08.13	P77
1.2.0	15.08.13		freigegeben	gematik
	04.02.14		Losübergreifende Synchronisation	P77
1.3.0	21.02.14		freigegeben	gematik
	22.04.14		In der Aufllistung der Schnittstellen des KSR wurde die benötigte Schnittstelle ergänzt, eine Referenz wurde gestrichen – gemäß P11-Änderungsliste.	P77
1.4.0	17.06.14		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen 2
Inhaltsverzeichnis 3
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 11
4.1 KSR-Upload 13
4.2 KSR-Download 13
4.3 KSR-Management 14
4.4 Schnittstellen 14
5 Übergreifende Festlegungen 16
5.1 Inhalt von Firmware-Update-Paketen 16
5.2 Hersteller-Update-Informationen 18
5.3 Behandlung von Firmware-Gruppen im Konfigurationsdienst 24
5.4 Behandlung von Konfigurationsdatenfiles 29
5.5 Kommunikation 30
5.5.1 TLS Transport Layer Security (TLS) 30
5.5.2 IP Version 30
5.6 Logging 30
5.7 Statistische Daten 31
5.8 Kryptographische Festlegungen 31

6 Funktionsmerkmale 32
6.1 Basisdienste 32
6.1.1 Schnittstelle I_KSRS_Download (Provided) 32
6.1.1.1 I_KSRS_Download::listUpdates 32
6.1.1.1.1 I_KSRS_Download::listUpdates Request 34
6.1.1.1.2 I_KSRS_Download::listUpdates Response 35
6.1.1.2 I_KSRS_Download::getUpdates 37
6.1.1.3 I_KSRS_Download::get_Ext_Net_Config 38
6.1.1.4 TUC_KSR_001 „Get File“ 39
6.2 Organisatorische Schnittstellen 41
6.2.1 Uploadschnittstelle P_KSRS_Upload 42
6.2.1.1 Schnittstellendefinition 42
6.2.2 Managementdienste P_KSRS_Operations 44
6.2.2.1 Schnittstellendefinition 45
Anhang A – Verzeichnisse 49
A1 – Abkürzungen 49
A2 – Glossar 49
A3 – Abbildungsverzeichnis 49
A4 – Tabellenverzeichnis 50
A5 – Referenzierte Dokumente 51
A5.1 – Dokumente der gematik 51
A5.2 – Weitere Dokumente 52
Anhang B – Nutzungsbeispiel I_KSRS_Download 53
Anhang C – Konfigurationsdatenfile zur Anbindung von Bestandsnetzen 55

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 A5).

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:

⌦ **TIP1-A_xxxx <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Systemüberblick

Der Konfigurationsdienst der TI ist ein betriebsunterstützendes System und speichert Update-Pakete für dezentrale Produkte der TI (Konnektoren und eHealth-Kartenterminals). Unabhängig vom Konfigurationsdienst können Updates der dezentralen Komponenten Konnektor und Kartenterminal 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:

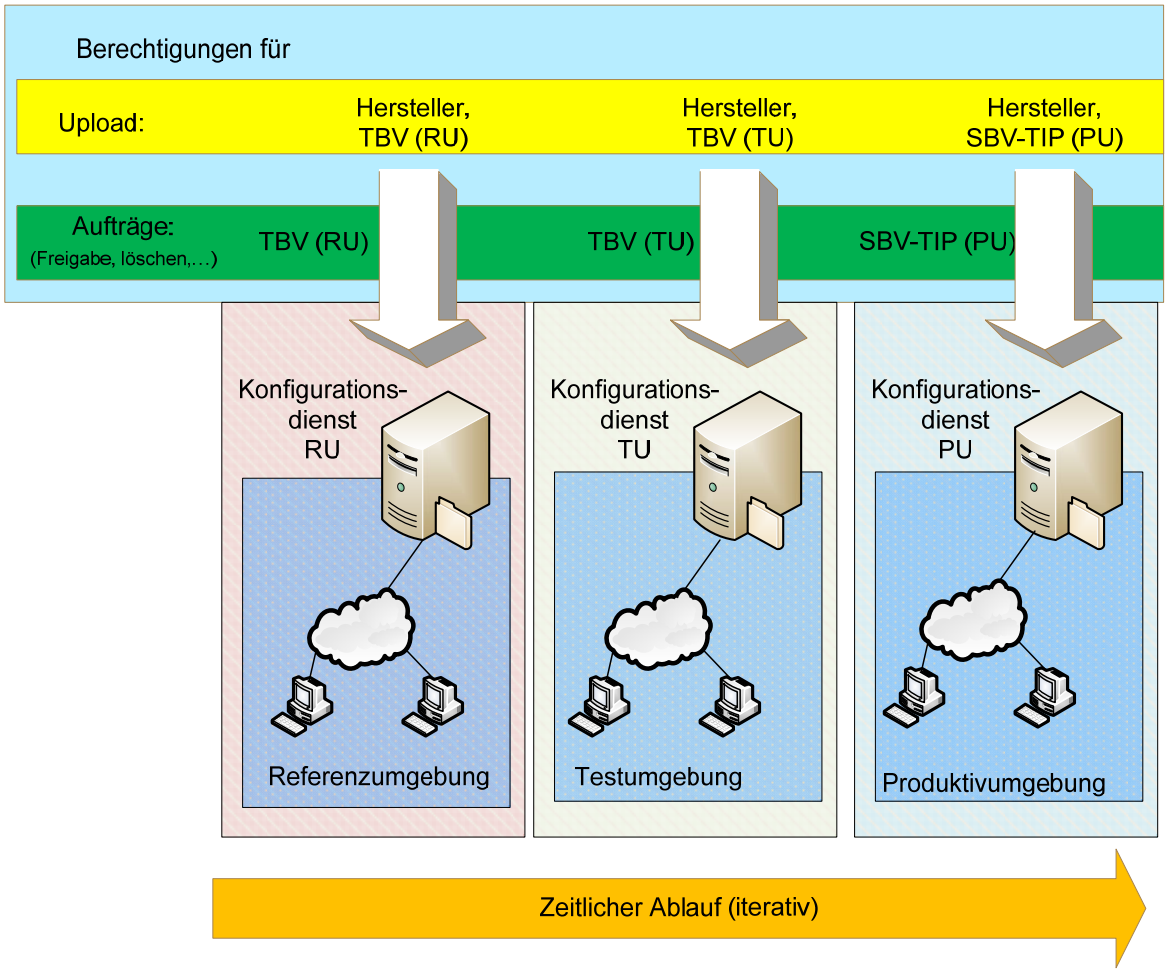
- der Bereitstellung der für den Wirkbetrieb zugelassenen Firmware-Versionen der dezentralen Produkte Konnektor und eHealth-Kartenterminal auf dem Konfigurationsdienst,
- der Bereitstellung der Firmware-Versionen der dezentralen Produkte für die Referenzumgebung und die Testumgebung auf dem Konfigurationsdienst,
- dem Download von Firmware-Versionen für die dezentralen Produkte Konnektor und eHealth-Kartenterminal,
- 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 Gesamtbetriebsverantwortlichen zu Verfügung gestellt werden,
- dem Download von zentralen Konfigurationsdaten-Files für Konnektoren.

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

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.



TBV - Testbetriebsverantwortlicher
SBV-TIP - Servicebetriebsverantwortlicher der TI-Platform
RU - Referenzumgebung
TU - Testumgebung
PU - Produktivumgebung

Abbildung 1: Abb_KSR_001 Überblick externe Akteure Konfigurationsdienst

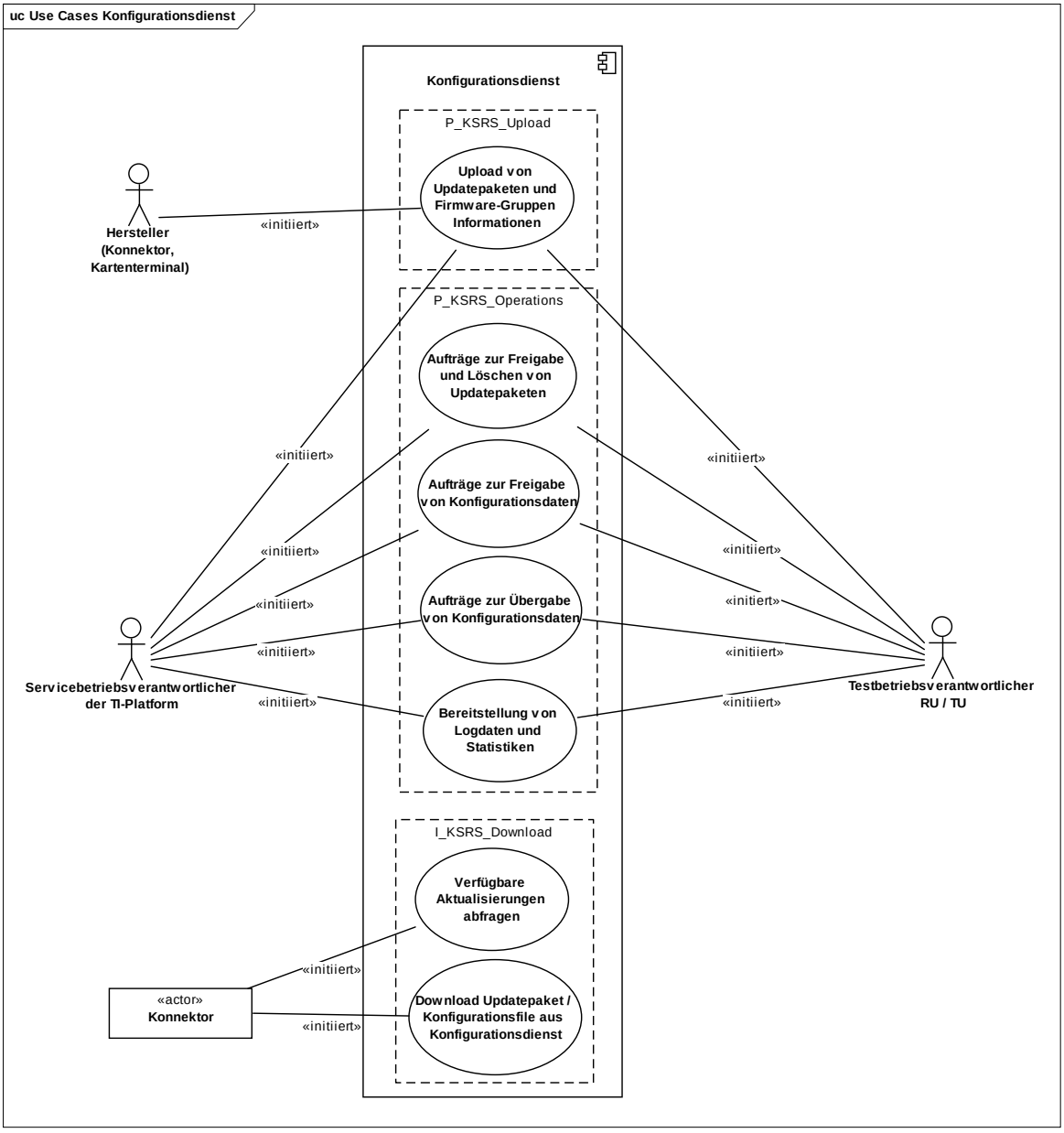


Abbildung 2: Abb_KSR_011 Überblick Use Cases Konfigurationsdienst

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): der Testbetriebsverantwortliche der RU
- Testumgebung (TU): der Testbetriebsverantwortliche der TU
- Produktivumgebung (PU): Der Servicebetriebsverantwortliche der TI-Plattform (SBV-TIP)

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 Anbindung von Bestandsnetzen (siehe Anhang C).

3.2 Nachbarsysteme

Die Abbildung Abb_KSR_002 zeigt die Nachbarsysteme und Akteure des Konfigurationsdienstes.

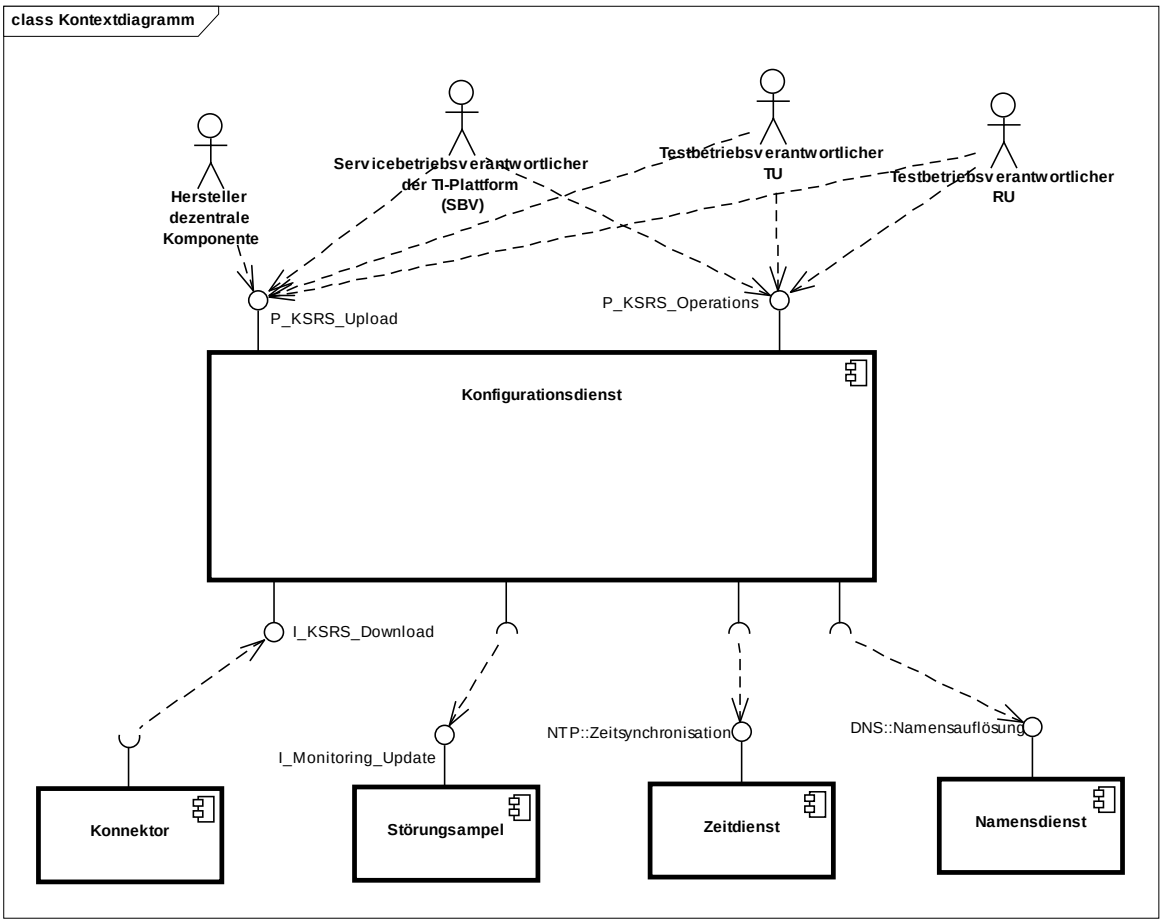


Abbildung 3: Abb_KSR_002 Kontextdiagramm Konfigurationsdienst

4 Zerlegung des Produkttyps

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

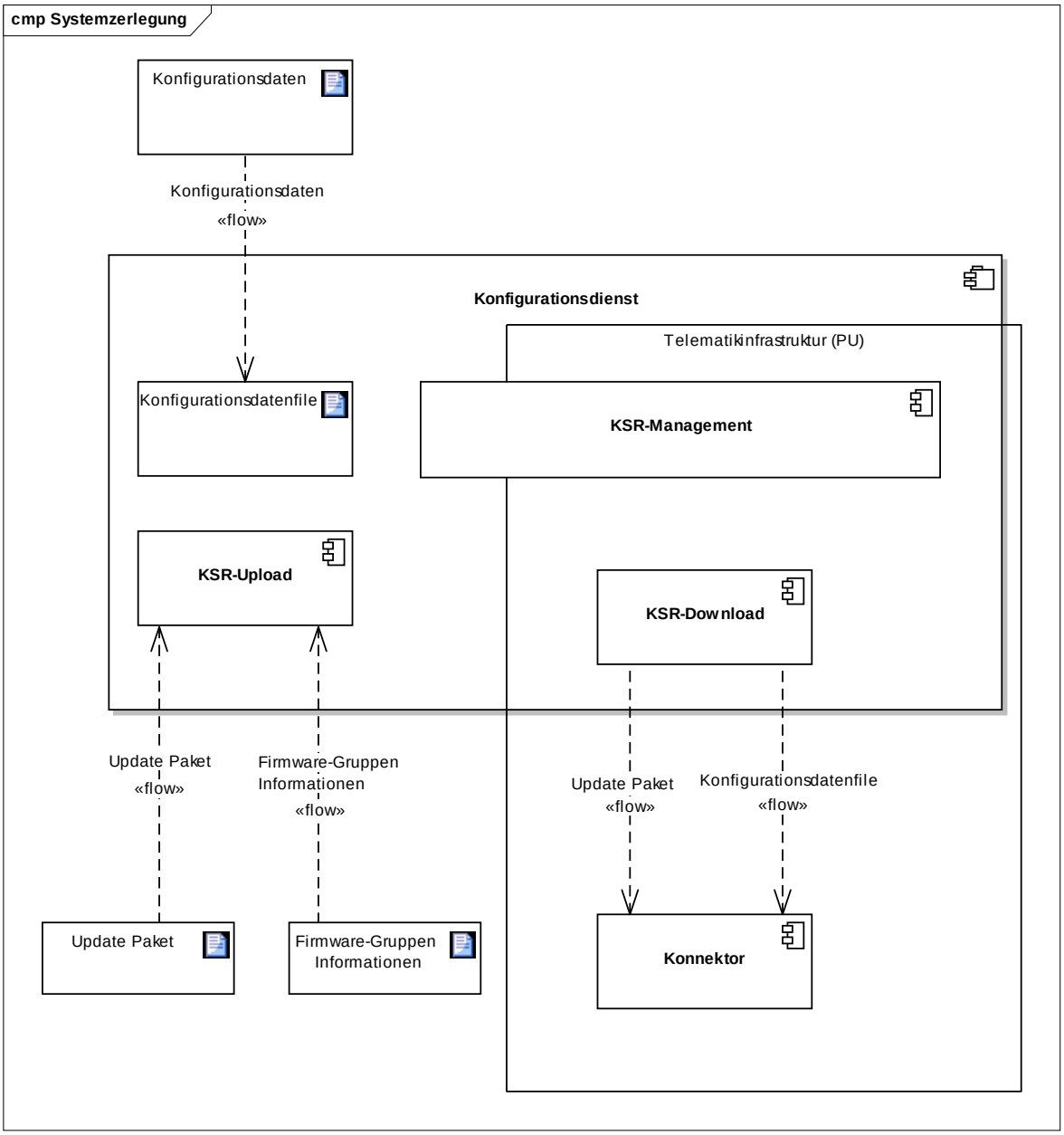


Abbildung 4: Abb_KSR_003 Zerlegung Konfigurationsdienst

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

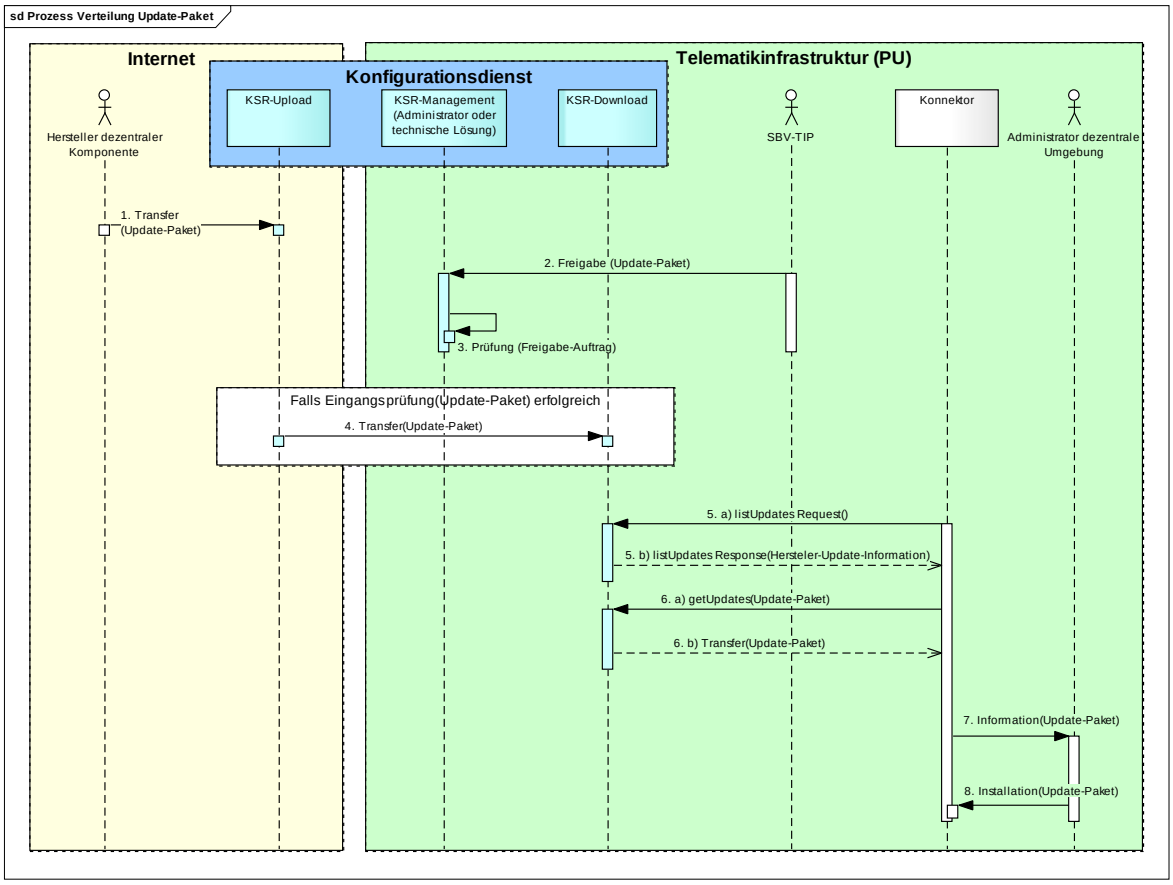


Abbildung 5: Abb_KSR_012 Verteilungsprozess Update-Paket (PU)

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. Der SBV-TIP erteilt nach entsprechender Prüfung die Freigabe für die PU mit einem Auftrag an den Konfigurationsdienst (siehe Kapitel 4.3 und 6.2.2).

3. Der Freigabeauftrag wird im Konfigurationsdienst geprüft (siehe Kapitel 4.3 und 6.2.2).

4. Falls auch die Eingangsprüfung des Update-Paketes erfolgreich war, erfolgt der Transfer in den Downloadbereich der PU (siehe Kapitel 4.3 und 6.2.2).

   Wann und wo die Eingangsprüfung erfolgt, wird in vorliegender Spezifikation nicht festgelegt. Vor dem Transfer in die jeweilige Umgebung muss sie auf jeden Fall erfolgreich durchgeführt werden und das Update-Paket darf nach dieser Prüfung nicht mehr manipulierbar sein.

5. 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).

6. 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).
7. Der Administrator des Konnektors wird informiert, wenn ein neues Update-Paket auf dem Konnektor vorliegt (siehe [gemSpec_Kon]).
8. 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_SiBetrUmg] und [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 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 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.⌫

4.3 KSR-Management

KSR-Management stellt die Funktionalitäten für das Management der Update-Pakete bereit. Dazu gehören die Schnittstelle zum Servicebetriebsverantwortlichen der TI-Plattform sowie zu den Testbetriebsverantwortlichen der RU und TU.

Die ausführliche Beschreibung von KSR-Management inklusive Anforderungen enthält Kapitel 6.2.2.

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 Konnektor- und Kartenterminal-Firmware.	
P_KSRS_Upload	Hersteller, SBV-TIP, Testbetriebsverantwortlicher RU/TU	[gemSpec_KSR]
	Für die dezentralen Komponenten (Konnektor und Kartenterminal) werden Update-Pakete auf dem Konfigurationsdienst bereitgestellt.	
P_KSRS_Operations	SBV-TIP, Testbetriebsverantwortlicher RU/TU	[gemSpec_KSR]
	Der Servicebetriebsverantwortliche der TI-Plattform [gemKPT_Betr_ORS1#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 der jeweilige Testbetriebsverantwortliche.	
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	Störungsampel	[gemSpec_St_Ampel]
	Über diese Schnittstelle werden Verfügbarkeits- und Performancedaten an die Störungsampel 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 2: Tab_KSR_002 Schnittstellen des Konfigurationsdienstes

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.

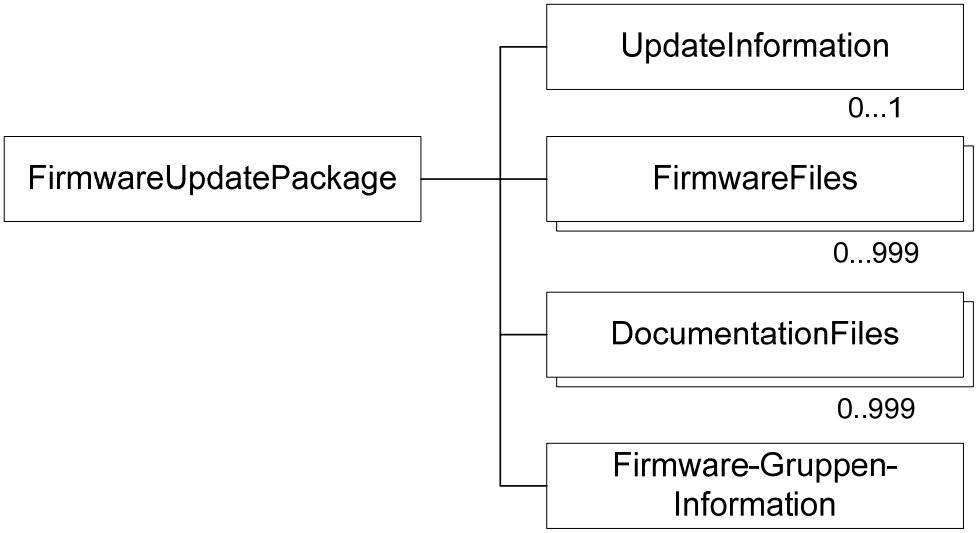


Abbildung 6: Abb_KSR_004 Inhalt von Firmware-Update-Paketen

Die Tabelle Tab_KSR_003 zeigt den Schutz der Update-Pakete und der enthaltenen Informationen. Dabei stellt der Konfigurationsdienst zusammen mit dem Hersteller von Konnektoren und Kartenterminals 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 3: 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	Konnektor, Kartenterminal	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 Konnektoren und Kartenterminals 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 ein 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 Konnektoren und Kartenterminals MÜSSEN in jedem Firmware-Update-Paket bis maximal 999 Files mit Dokumentationen für das Update liefern. ⌫

⌦ **TIP1-A_5159 Inhalt Update-Paket – Firmware-Gruppen-Information**

Hersteller von Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals übermittelten Update-Pakete (Gesamtpaket) bis zur Übertragung an den KSR-Client gewährleisten.⌫

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 Konnektoren und Kartenterminals,
- 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.⌫

⌦ **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:

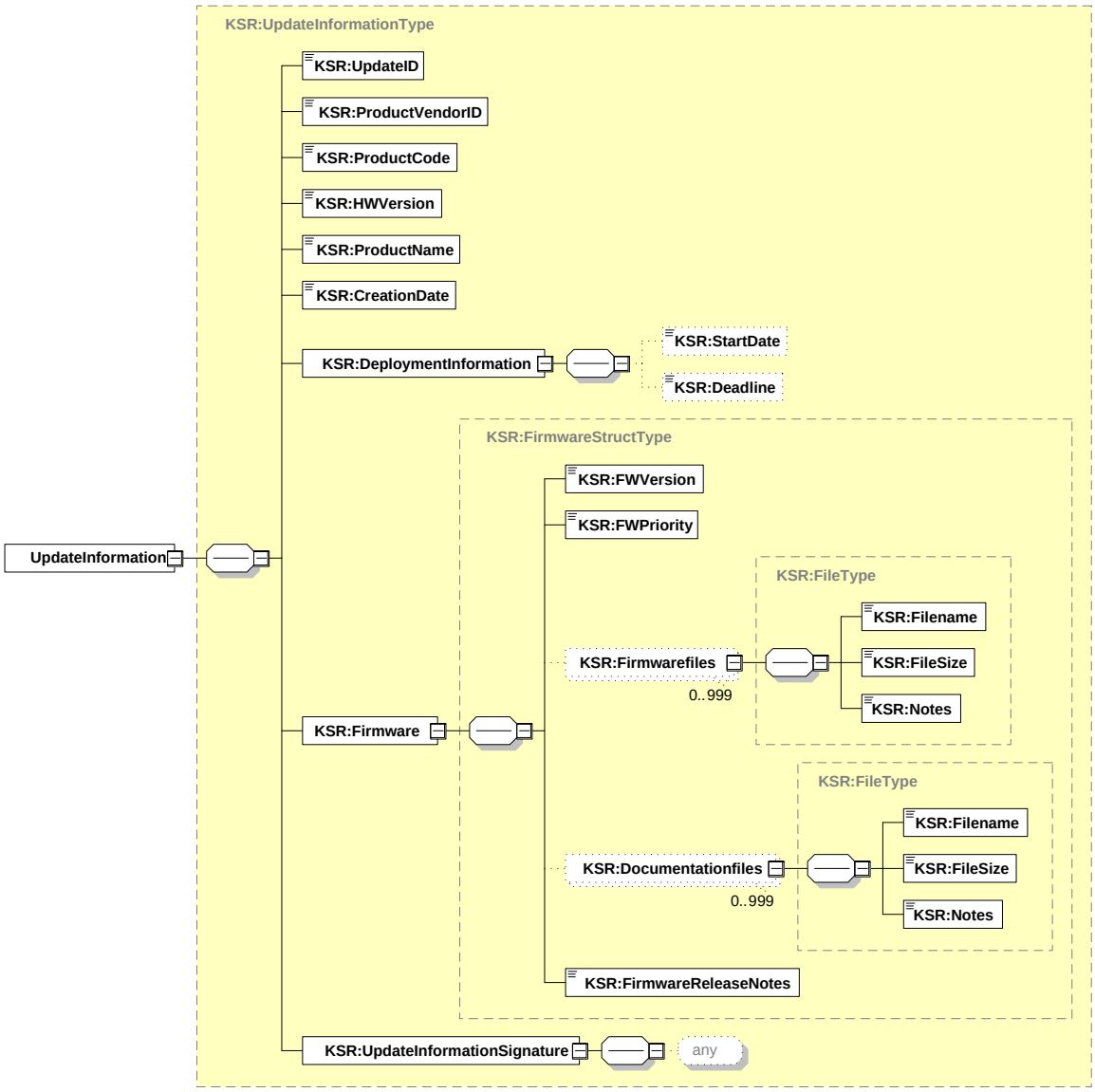


Abbildung 7: Abb_KSR_005 Hersteller-Update-Informationen (UpdateInfo.xml)

Tabelle 4: Tab_KSR_004 Hersteller-UpdateInformation – Element UpdateID

Bezeichnung	UpdateID
Beschreibung	Identifiziert das Update eindeutig.
Befüllung	Hersteller von Konnektoren und Kartenterminals
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit Pattern "[a-zA-Z0-9_]*".

Tabelle 5: 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 Konnektoren und Kartenterminals
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML Datentyp „string“ mit Pattern "[a-zA-Z0-9_]*". Maximale Länge 5 Zeichen.

Tabelle 6: 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 Konnektoren und Kartenterminals
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML Datentyp „string“ mit Pattern "[a-zA-Z0-9_]*". Maximale Länge 8 Zeichen.

Tabelle 7: 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 Konnektoren und Kartenterminals
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 8: 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 Konnektoren und Kartenterminals

Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 256 Zeichen.

Tabelle 9: 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 Konnektoren und Kartenterminals
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „date“.

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

Tabelle 10: 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 Konnektoren und Kartenterminals
Optional	ja
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „date“.

Tabelle 11: 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. Durch den Konfigurationsdienst wird dieser Wert nicht ausgewertet.
Befüllung	Hersteller von Konnektoren und Kartenterminals
Optional	ja
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „date“.

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

Tabelle 12: 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 Konnektoren und Kartenterminals
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 13: 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 Konnektoren und Kartenterminals
Optional	nein
Wertebereich	„Normal“, „Kritisch“

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

Tabelle 14: Tab_KSR_015 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.Filename

Bezeichnung	Files.Firmwarefiles.Filename
Beschreibung	Filename inklusive relativem Pfad. Dieser Wert wird in Operation getUpdates HTTP Request als Parameter <path> genutzt.
Befüllung	Durch Hersteller von Konnektoren und Kartenterminals in Absprache mit dem Anbieter des Konfigurationsdienstes bezüglich dem relativem Pfad (z.B. „/ManufacturerID/ProductShortName/HardwareVersion/FirmwareVersion/KonFW123.fw“)
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“.

Tabelle 15: Tab_KSR_041 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.FileSize

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

Tabelle 16: 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 Konnektoren und Kartenterminals
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 256 Zeichen.

Tabelle 17: Tab_KSR_017 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.Filename

Bezeichnung	Files.Documentationfiles.Filename
Beschreibung	Filename inklusive relativem Pfad. Dieser Wert wird in Operation getUpdates HTTP Request als Parameter <path> genutzt.
Befüllung	Durch Hersteller von Konnektoren und Kartenterminals in Absprache mit dem Anbieter des Konfigurationsdienstes bezüglich dem relativem Pfad. (z.B. „/ManufacturerID/ProductShortName/HardwareVersion/ FirmwareVersion/KonFW123.pdf“)
Optional	Ja
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“.

Tabelle 18: Tab_KSR_042 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.FileSize

Bezeichnung	Files.Documentationfiles.FileSize
Beschreibung	Größe des Files in Byte.
Befüllung	Hersteller von Konnektoren und Kartenterminals
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit Pattern "[0-9]{1,10}".

Tabelle 19: 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 Konnektoren und Kartenterminals
Optional	Nein, falls zugehörigen File vorhanden.
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 256 Zeichen.

Tabelle 20: Tab_KSR_019 Hersteller-UpdateInformation – Element Firmware.FirmwareReleaseNotes

Bezeichnung	FirmwareReleaseNotes
Beschreibung	Durch den Hersteller von Konnektoren und Kartenterminals erstellte Beschreibung des Updates.
Befüllung	Hersteller von Konnektoren und Kartenterminals
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 2048 Zeichen.

Tabelle 21: Tab_KSR_020 Hersteller-UpdateInformation – Element UpdateInformationSignature

Bezeichnung	UpdateInformationSignature
Beschreibung	Dieses Element kann der Konnektorhersteller zur Signatur der UpdateInformation nutzen. Hersteller von Kartenterminals sollen dieses Element nicht nutzen und die UpdateInformation nicht signieren.
Befüllung	Hersteller von Konnektoren
Optional	Ja.
Wertebereich	Any (vom Hersteller festzulegen)

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 Konnektoren und Kartenterminals

dieser dezentralen Komponenten in einer separaten Datei die aktuellen Firmware-Gruppen-Informationen in einem vom Konfigurationsdienst vorgegebenen Format (siehe unten). Die vom Hersteller der Konnektoren und Kartenterminals 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.)

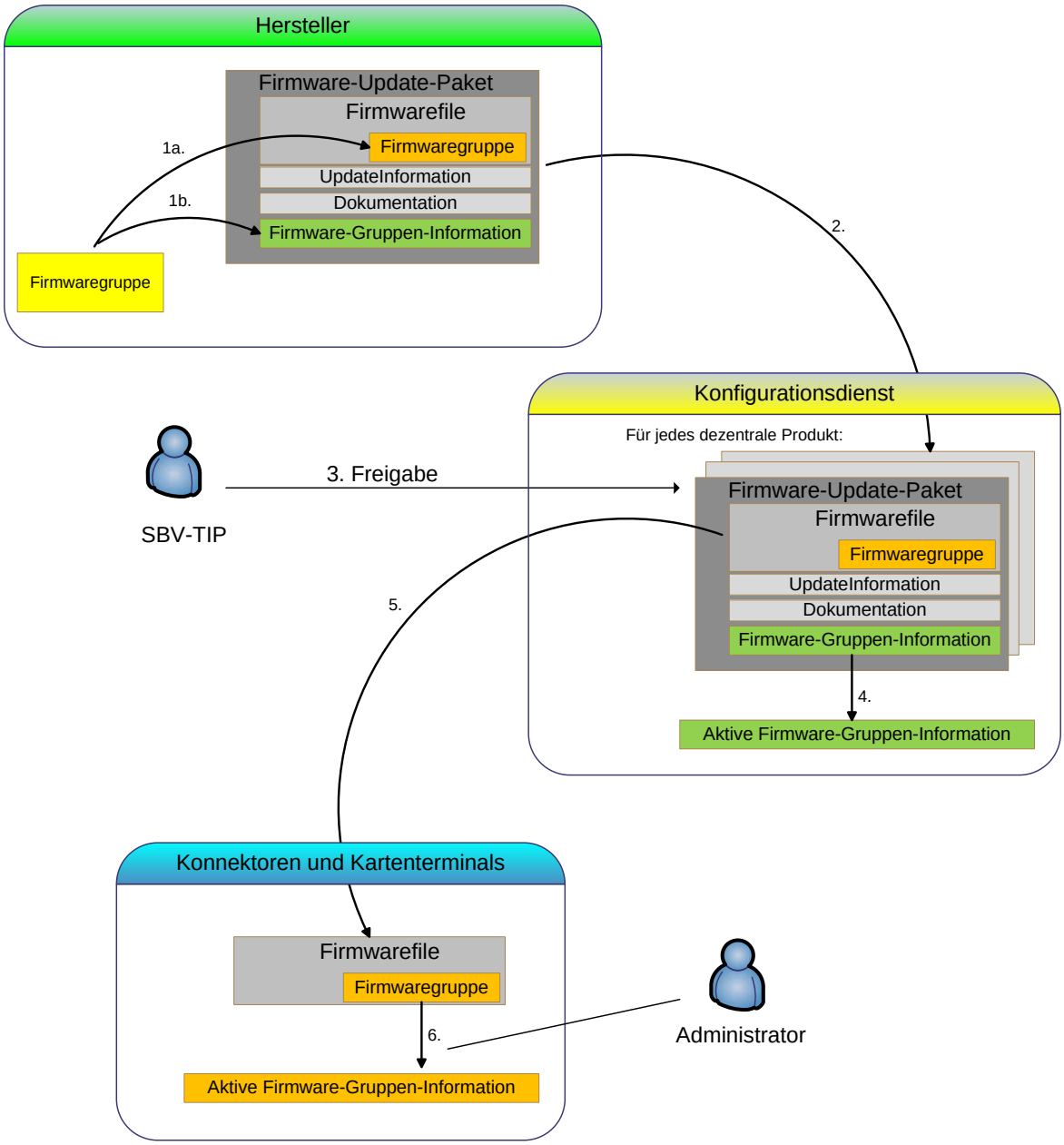


Abbildung 8: Abb_KSR_013 Verteilungsprozess Firmware-Gruppen-Informationen

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 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 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:

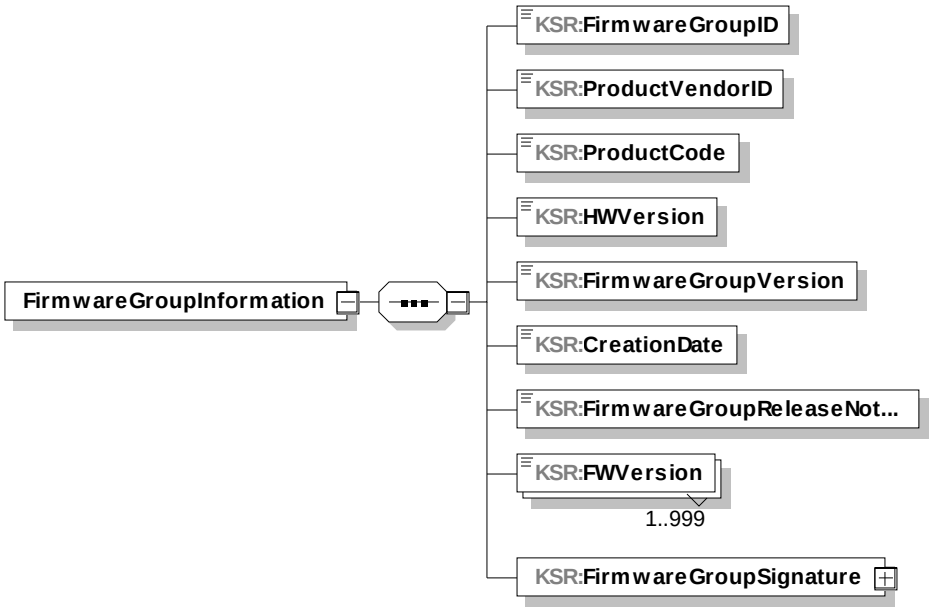


Abbildung 9: Abb_KSR_007 Firmware-Gruppen-Informationen

Tabelle 22: Tab_KSR_021 Firmware-Gruppen-Information – Element FirmwareGroupID

Bezeichnung	FirmwareGroupID
Beschreibung	Identifiziert die Firmware-Gruppe eindeutig.
Befüllung	Hersteller von Konnektoren und Kartenterminals
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“.

Tabelle 23: Tab_KSR_022 Firmware-Gruppen-Information – Element FirmwareGroupVersion

Bezeichnung	FirmwareGroupVersion
Beschreibung	Die Versionsnummer der aktuellen Firmware-Gruppe.
Optional	nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 5 Zeichen.

Tabelle 24: Tab_KSR_023 Firmware-Gruppen-Information – Element FirmwareGroupReleaseNotes

Bezeichnung	FirmwareGroupReleaseNotes
Beschreibung	Durch den Hersteller von Konnektoren und Kartenterminals 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 25: Tab_KSR_024 Firmware-Gruppen-Information – Element FirmwareGroupSignature

Bezeichnung	FirmwareGroupSignature
Beschreibung	Dieses Element kann der Hersteller von Konnektoren und Kartenterminals zur Signatur der Firmware-Gruppen-Information nutzen. Da die Prüfung durch den Konfigurationsdienst erfolgt, muss die Art der Signatur zwischen dem Anbieter des Konfigurationsdienstes und Hersteller abgestimmt werden.
Befüllung	Hersteller von Konnektoren und Kartenterminals
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 Konnektoren und Kartenterminals unterstützten und zugelassenen Firmwareversionen. Es können bis zu 999 FWVersion’en in der Liste enthalten sein. ⌫

⌦ **TIP1-A_3317 Firmware-Gruppenkonzept – Lieferung mit Firmware**

Hersteller von Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals – die Integrität und Authentizität der Firmware-Gruppen-Information für die gesamte Lebenszeit dieser Informationen gewährleisten. ⌫

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.

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).⌫

5.6 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_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 der PU angefragten Updates (Operation I_KSRS_Download::listUpdates inklusive aller Parameter des Requests) und bereitgestellten Updates (Operation I_KSRS_Download::getUpdates inklusive UpdateID und Filename), aufgeschlüsselt nach Produkt und Update-Paket (Element „UpdateID“) im zeitlichen Verlauf auflisten. ⌫

⌦ **TIP1-A_3354 KSR-Statistiken – Format**

Der Anbieter des Konfigurationsdienstes MUSS alle Download-Berichte und Berichte über die listUpdates Abfragen im CSV-Format bereitstellen. ⌫

5.8 Kryptographische Festlegungen

⌦ **TIP1-A_5040 Schlüssel sicher speichern**

Der Konfigurationsdienst MUSS Schlüssel sicher speichern und ihr Auslesen verhindern.⌫

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 26: Tab_KSR_025 Konfigurationsdienst

Name	`I_KSRS_Download`	
Version (KDV)	gemäß Produkttypversion	
Namensraum	http://ws.gematik.de/ksr/v1.0	
Namensraum-Kürzel	KSR	
Operationen	**Name**	**Kurzbeschreibung**
	`listUpdates`	Auflisten verfügbarer Updates
WSDL	`Konfigurationsdienst.wsdl`	
Schema	`Konfigurationsdienst.xsd`	

⌫

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 27: 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.
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:

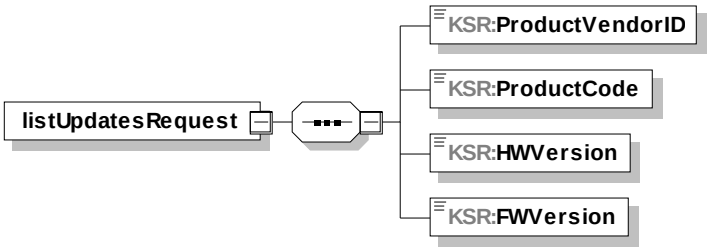


Abbildung 10: Abb_KSR_008 Operation I_KSRS_Download::listUpdates Request

Tabelle 28: 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 29: 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 30: 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 31: 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 32: 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:

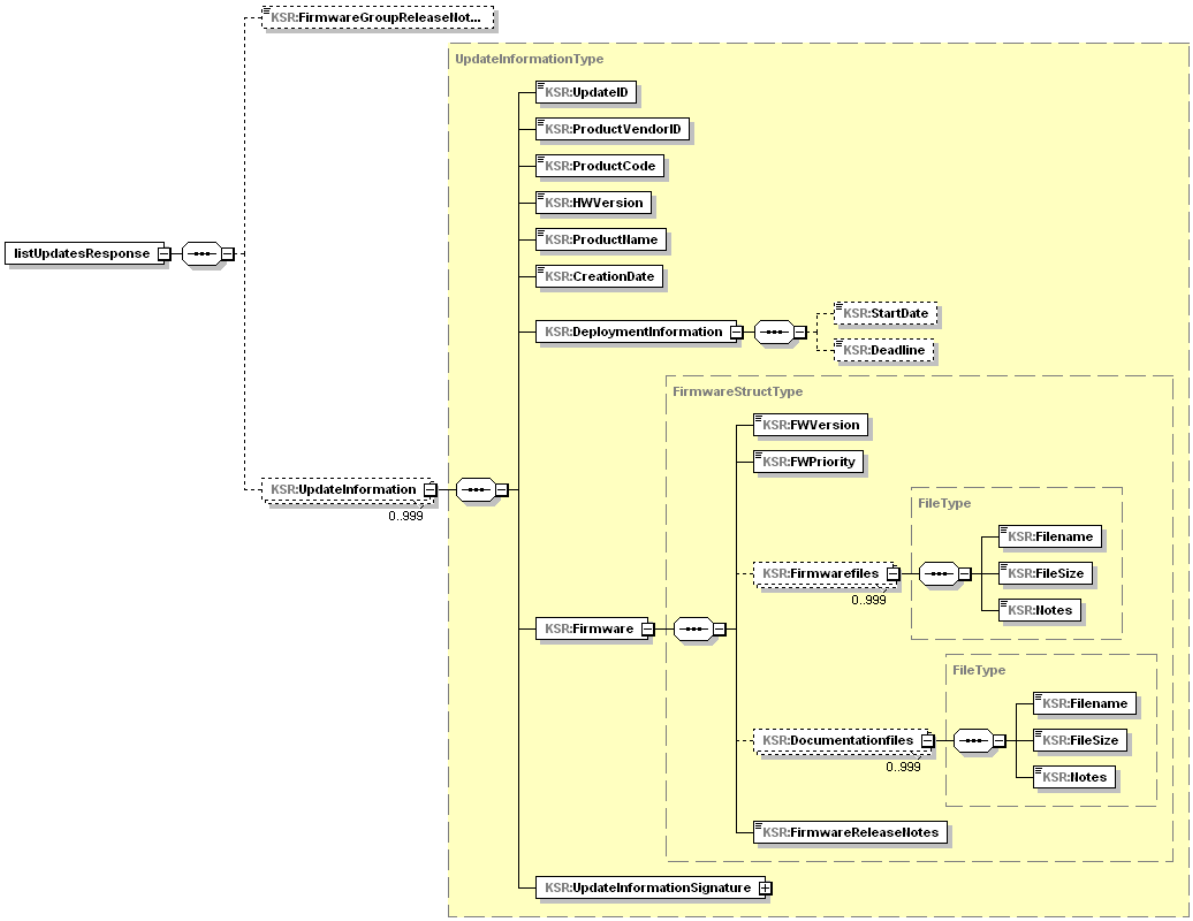


Abbildung 11: Abb_KSR_009 Operation I_KSRS_Download::listUpdates Response

Tabelle 33: 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 34: 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 35: 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.⌫

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 36: 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. Mit jedem Aufruf dieser Operation wird ein File übertragen.
Initiierender Akteur	Konnektor
Weitere Akteure	keine
Auslöser	Konnektor

Element	Beschreibung
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	Der Aufrufer (KSR-Client im Konnektor) ruft über die hier definierte Schnittstelle den Konfigurationsdienst auf. Eingangsdaten: https://<host>/ Konfigurationsdienst Downloadpunkt für angefragtes File der TI. <path> Identifiziert das angefragte File.
Standardablauf	Aufruf von TUC_KSR_001 „Get File“ mit Parametern https://<host>/ (entspricht DNS SRV Resource Record „_ksrfirmware._tcp.ksr.telematik“) <path> Dieser Wert entspricht den in Operation I_KSRS_Download::listUpdatesResponse zurückgegebenen „Filenamen“ oder kann den Hersteller-Update-Informationen entnommen werden.
Fehlerfälle	Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.

⌫

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 37: 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 die Update-Datei vorliegen und gespeichert.
Aufruf	Der Aufrufer (KSR-Client im Konnektor) ruft über die hier definierte Schnittstelle den Konfigurationsdienst auf. Eingangsdaten: • https://<host>/ Konfigurationsdienst Downloadpunkt für angefragtes File der TI. • <path> Identifiziert das angefragte File.
Standardablauf	Aufruf von TUC_KSR_001 „Get File“ mit Parametern • https://<host>/ (entspricht DNS SRV Resource Record „_ksrkonfig._tcp.ksr.telematik“) • <path> Filename des Konfigurationsdatenfiles.
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_035 bereitstellen.

Tabelle 38: 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.
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 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 39: 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 40: Tab_KSR_037 File Transfer HTTP Request – Element path

Bezeichnung	path
Beschreibung	Filename inklusive relativem Pfad.
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 KANN 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.⌫

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 in den Download-Bereichen der unterschiedlichen Umgebungen (RU, TU, PU) verfügbar zu machen beziehungsweise zu löschen. Dies wird durch Aufträge der berechtigten Akteure an den Anbieter des Konfigurationsdienstes realisiert.

6.2.1 Uploadschnittstelle P_KSRS_Upload

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

6.2.1.1 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 (PU) und den Testbetriebsverantwortlichen 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 41: Tab_KSR_039 P_KSRS_Upload Schema

Name	`P_KSRS_Upload`	
Version (KDV)	gemäß Produkttypversion	
Namensraum	http://ws.gematik.de/ksr/v1.0	
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, Servicebetriebsverantwortlicher TI-Plattform (PU), Testbetriebsverantwortlicher TU und Testbetriebsverantwortlicher RU) auf P_KSRS_Upload der jeweiligen Umgebung zugreifen können. ⌫

⌦ **TIP1-A_3348 Form und Inhalt Upload-Interface**

Der Anbieter des Konfigurationsdienstes MUSS Form und Inhalt des Upload-Interfaces inklusive Vorgaben zum Ausfüllen der Update-Informationen (z.B. falls relative Pfade in den „Filename“ Parametern vorgegeben werden), definieren und mit den berechtigten Akteuren abstimmen.⌫

⌦ **TIP1-A_3311 Schutz Upload-Interface**

Der Anbieter des Konfigurationsdienstes MUSS die Kommunikationsschnittstelle von KSR-Upload so auslegen, dass die Integrität und Authentizität der durch die authentisierten Hersteller übermittelten Update-Pakete und Firmware-Gruppen-Informationen gewährleistet wird. Die Schutzmechanismen bezüglich Integrität und Authentizität müssen mit den Herstellern abgestimmt werden. ⌫

⌦ **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_3346 Eingangsprüfung**

Der Anbieter des Konfigurationsdienstes MUSS die übermittelten Update-Pakete und Firmware-Gruppen-Informationen einer Eingangsprüfung unterziehen.

Die Eingangsprüfung MUSS folgende Prüfungen enthalten:

- Prüfung der Integrität und Authentizität
- Prüfung auf syntaktische Korrektheit (Update-Informationen und Firmware-Gruppen-Informationen)
- Prüfung auf Vollständigkeit (Vorhandensein aller aus den Update-Informationen referenzierten Files)⌫

6.2.2 Managementdienste P_KSRS_Operations

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

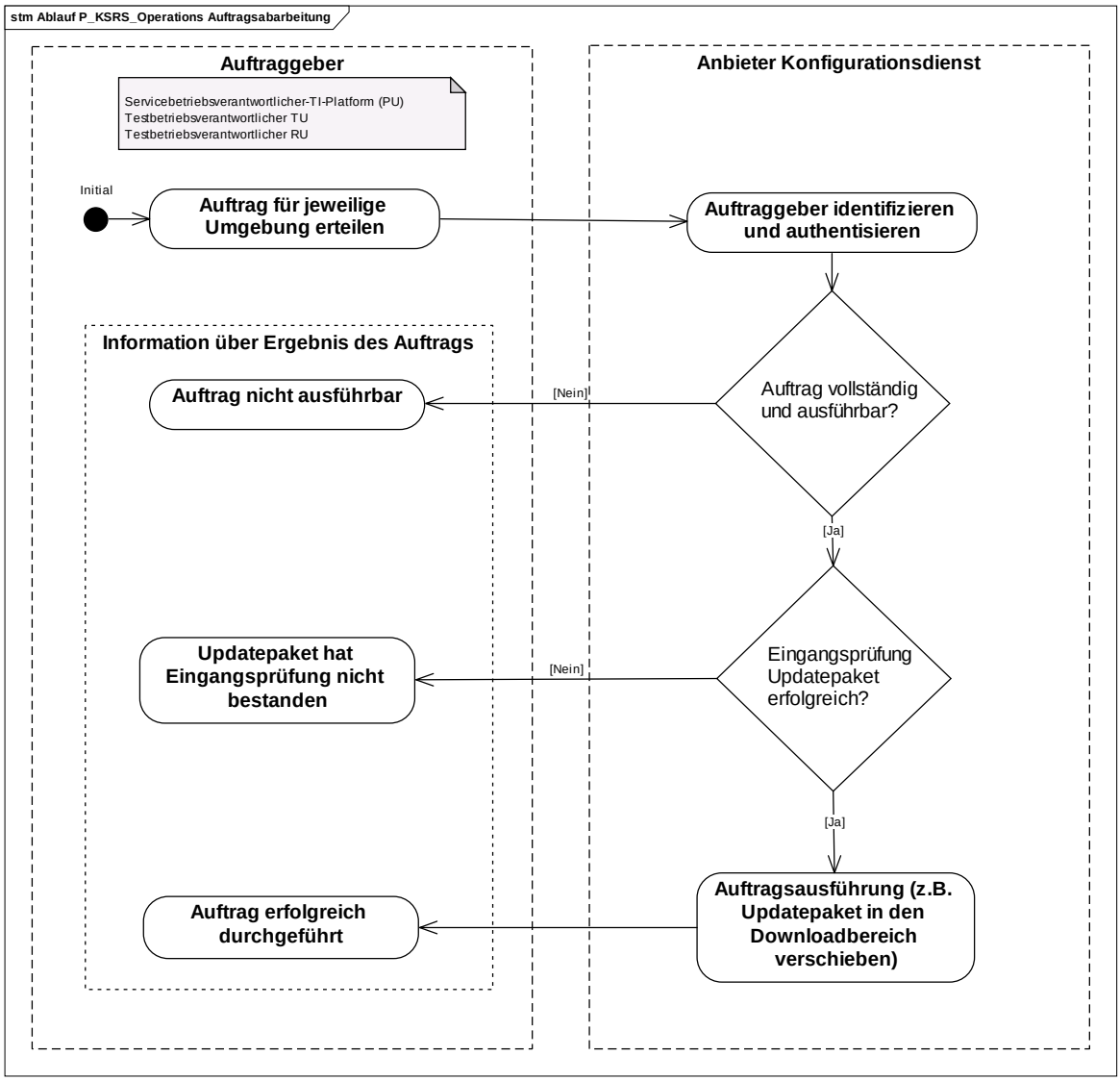


Abbildung 12: Abb_KSR_010 Beispiel Auftragsabarbeitung (P_KSRS_Operations)

6.2.2.1 Schnittstellendefinition

KSR-Management bietet für den Servicebetriebsverantwortlichen der TI-Plattform 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 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 Konfi-

gurationsdatenfiles 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_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.⌫

⌦ **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 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 dem Testbetriebsverantwortlichen 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 dem Testbetriebsverantwortlichen 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 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 dem Testbetriebsverantwortlichen RU zyklisch jeden Monat und zusätzlich auf Anfrage adhoc einen Bericht mit den statistischen Daten der Referenzumgebung (RU) übermitteln. ⌫

TIP1-A_3925 Organisatorische Schnittstelle zur Bereitstellung von statistischen Daten der TU

Der Anbieter des Konfigurationsdienstes MUSS dem Testbetriebsverantwortlichen TU zyklisch jeden Monat und zusätzlich auf Anfrage adhoc einen Bericht mit den statistischen Daten der Referenzumgebung (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.⌫

Anhang A – Verzeichnisse

A1 – Abkürzungen

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

A2 – Glossar

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

A3 – 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 10
Abbildung 4: Abb_KSR_003 Zerlegung Konfigurationsdienst 11
Abbildung 5: Abb_KSR_012 Verteilungsprozess Update-Paket (PU) 12
Abbildung 6: Abb_KSR_004 Inhalt von Firmware-Update-Paketen 16
Abbildung 7: Abb_KSR_005 Hersteller-Update-Informationen (UpdateInfo.xml) 19
Abbildung 8: Abb_KSR_013 Verteilungsprozess Firmware-Gruppen-Informationen 25
Abbildung 9: Abb_KSR_007 Firmware-Gruppen-Informationen 27
Abbildung 10: Abb_KSR_008 Operation I_KSRS_Download::listUpdates Request 34
Abbildung 11: Abb_KSR_009 Operation I_KSRS_Download::listUpdates Response 36
Abbildung 12: Abb_KSR_010 Beispiel Auftragsabarbeitung (P_KSRS_Operations) 45
Abbildung 13: Abb_KSR_015 Beispielablauf für ein Firmware Update 54
Abbildung 14: Abb_KSR_014 Schema InfrastrukturKonfig.xsd 55

A4 – Tabellenverzeichnis

Tabelle 1: Tab_KSR_001 Schnittstellen des Konfigurationsdienstes 14
Tabelle 2: Tab_KSR_002 Schnittstellen des Konfigurationsdienstes 15
Tabelle 3: Tab_KSR_003 Schutz der Firmware-Update-Pakete 17
Tabelle 4: Tab_KSR_004 Hersteller-UpdateInformation – Element UpdateID 19
Tabelle 5: Tab_KSR_005 Hersteller-UpdateInformation – Element ProductVendorID 20
Tabelle 6: Tab_KSR_006 Hersteller-UpdateInformation – Element ProductCode 20
Tabelle 7: Tab_KSR_007 Hersteller-UpdateInformation – Element HWVersion 20
Tabelle 8: Tab_KSR_008 Hersteller-UpdateInformation – Element ProductName 20
Tabelle 9: Tab_KSR_009 Hersteller-UpdateInformation – Element CreationDate 21
Tabelle 12: Tab_KSR_012 Hersteller-UpdateInformation – Element DeploymentInformation.StartDate 21
Tabelle 13: Tab_KSR_013 Hersteller-UpdateInformation – Element DeploymentInformation.Deadline 21
Tabelle 14: Tab_KSR_014 Hersteller-UpdateInformation – Element Firmware.FWVersion 22
Tabelle 15: Tab_KSR_040 Hersteller-UpdateInformation – Element Firmware.FWPriority 22
Tabelle 16: Tab_KSR_015 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.Filename 22
Tabelle 17: Tab_KSR_041 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.FileSize 22
Tabelle 18: Tab_KSR_016 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.Notes 23
Tabelle 19: Tab_KSR_017 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.Filename 23
Tabelle 20: Tab_KSR_042 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.FileSize 23
Tabelle 21: Tab_KSR_018 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.Notes 24
Tabelle 22: Tab_KSR_019 Hersteller-UpdateInformation – Element Firmware.FirmwareReleaseNotes 24
Tabelle 23: Tab_KSR_020 Hersteller-UpdateInformation – Element UpdateInformationSignature 24
Tabelle 24: Tab_KSR_021 Firmware-Gruppen-Information – Element FirmwareGroupID 27
Tabelle 25: Tab_KSR_022 Firmware-Gruppen-Information – Element FirmwareGroupVersion 27
Tabelle 26: Tab_KSR_023 Firmware-Gruppen-Information – Element FirmwareGroupReleaseNotes 27

Tabelle 27: Tab_KSR_024 Firmware-Gruppen-Information – Element FirmwareGroupSignature 28
Tabelle 28: Tab_KSR_025 Konfigurationsdienst 32
Tabelle 29: Tab_KSR_026 Operation I_KSRS_Download::listUpdates 33
Tabelle 30: Tab_KSR_027 I_KSRS_Download::listUpdates Request 34
Tabelle 31: Tab_KSR_028 Hersteller-Update-Informationen – Element ProductVendorID 34
Tabelle 32: Tab_KSR_029 Hersteller-Update-Informationen – Element ProductCode 34
Tabelle 33: Tab_KSR_030 Hersteller-Update-Informationen – Element HWVersion 35
Tabelle 34: Tab_KSR_031 Hersteller-Update-Informationen – Element FWVersion 35
Tabelle 35: Tab_KSR_032 I_KSRS_Download::listUpdates – Response 36
Tabelle 36: Tab_KSR_033 I_KSRS_Download::listUpdates – Element FirmwareGroupReleaseNotes 36
Tabelle 37: Tab_KSR_034 I_KSRS_Download::listUpdates – Element UpdateInformation 36
Tabelle 38: Tab_KSR_035 Operation I_KSRS_Download::getUpdates 37
Tabelle 39: Tab_KSR_044 Operation I_KSRS_Download::get_Ext_Net_Config 38
Tabelle 40: Tab_KSR_043 TUC_KSR_001 „Get File“ 40
Tabelle 41: Tab_KSR_036 File Transfer HTTP Request – Element host 40
Tabelle 42: Tab_KSR_037 File Transfer HTTP Request – Element path 41
Tabelle 43: Tab_KSR_039 P_KSRS_Upload Schema 43
Tabelle 44: Tab_KSR_045 Attribute des Konfigurationsdatenfiles zur Anbindung von Bestandsnetzen 55

A5 – Referenzierte Dokumente

A5.1 – 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 passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur

[Quelle]	Herausgeber: Titel
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemKPT_Betr_ORS1]	gematik: Betriebskonzept Online-Rollout (Stufe 1)
[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_SiBetrUmg]	gematik: Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI

A5.2 – 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

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.

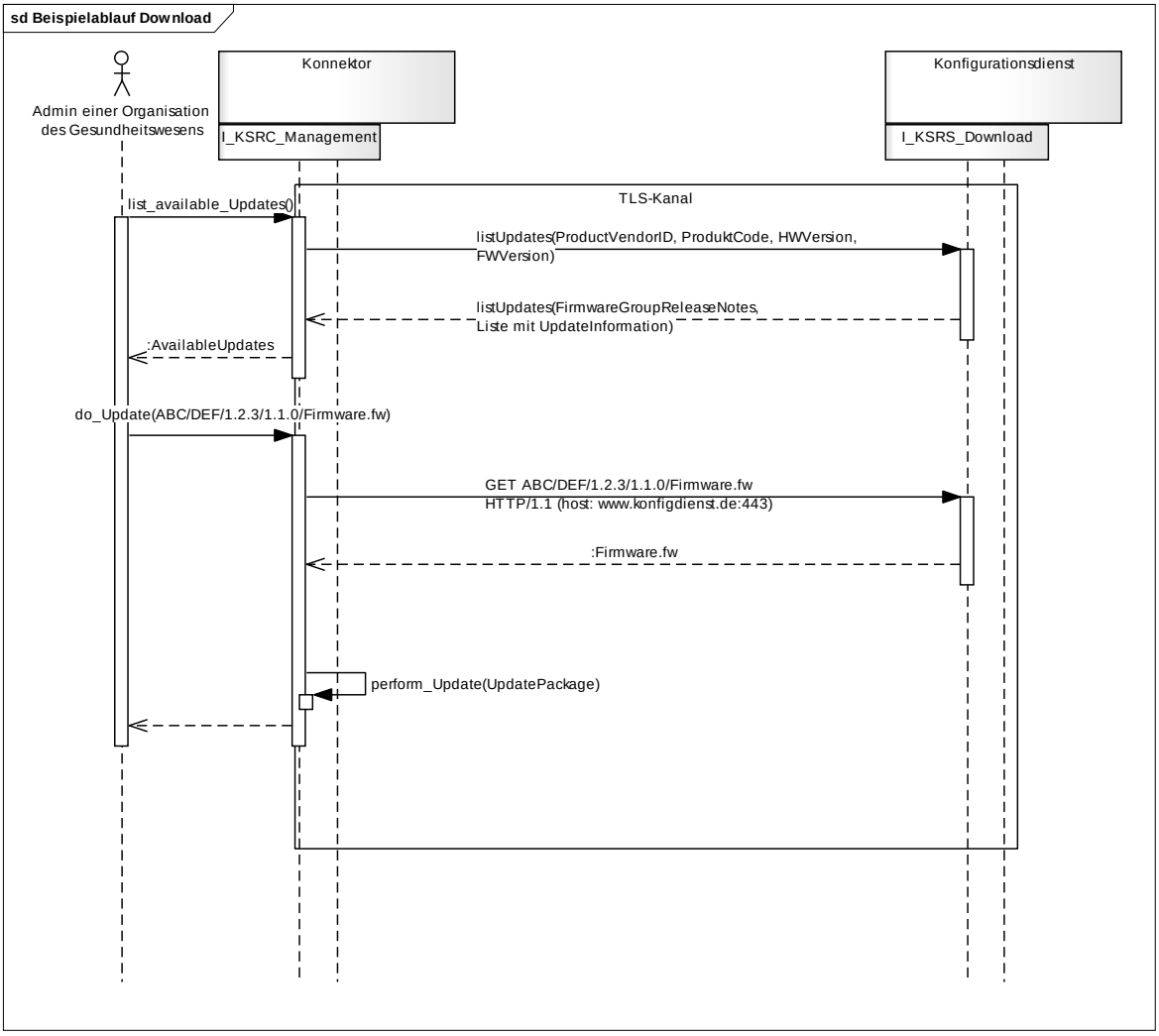


Abbildung 13: Abb_KSR_015 Beispielablauf für ein Firmware Update

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.

Anhang C – Konfigurationsdatenfile zur Anbindung von Bestandsnetzen

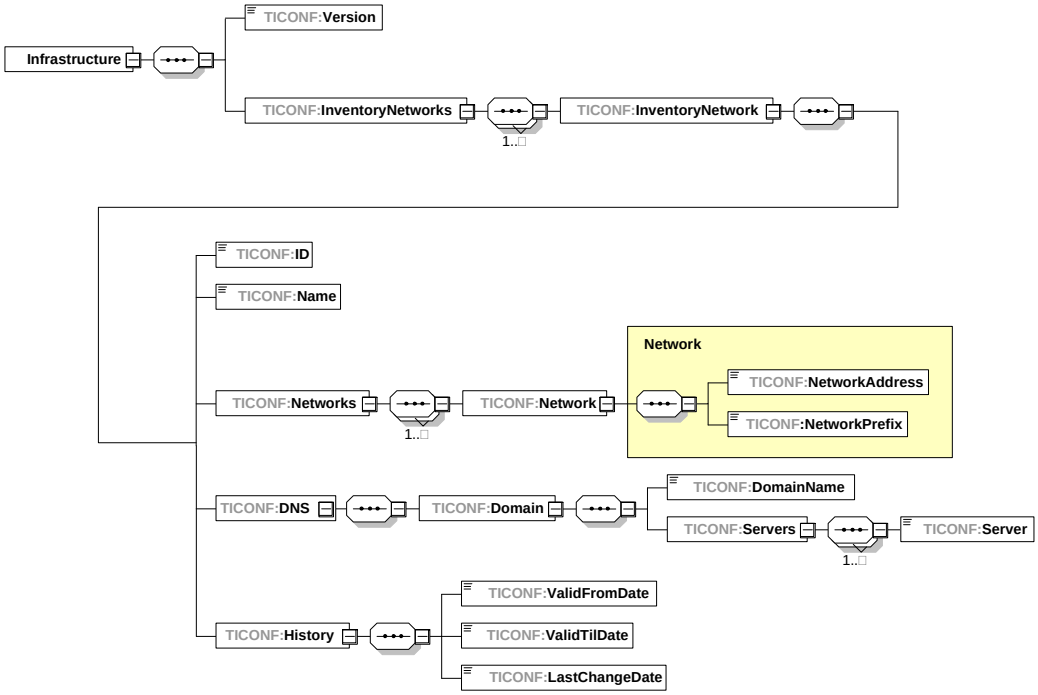


Abbildung 14: Abb_KSR_014 Schema InfrastrukturKonfig.xsd

Tabelle 42: 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	
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

Datenelement	Typ	Beschreibung	Wertebereich
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