

## Einführung der Gesundheitskarte

# Spezifikation Konfigurationsdienst

Version: 1.8.0  
Revision: \main\rel\_online\rel\_ors1\rel\_opb1\41  
Stand: 21.04.2017  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemSpec\_KSR

---

## Dokumentinformationen

---

### Änderungen zur Vorversion

Anpassung lt. Änderungsliste

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	23.07.12		zur Abstimmung freigegeben	gematik
1.0.0	15.10.12		Überarbeitung nach Kommentierung und Workshop	gematik
1.1.0	06.06.13		freigegeben	gematik
1.2.0	15.08.13		Einarbeitung lt. Änderungsliste vom 08.08.13	gematik
1.3.0	21.02.14		Losübergreifende Synchronisation	gematik
1.4.0	17.06.14		In der Auflistung der Schnittstellen des KSR wurde die benötigte Schnittstelle ergänzt, eine Referenz wurde gestrichen – gemäß P11-Änderungsliste.	gematik
1.5.0	24.08.16		Anpassungen zum Online-Produktivbetrieb (Stufe 1), Übernahme der arvato Spezifikation ARV_706.3_Spec_SST_KSR	gematik
1.6.0	16.10.16		Einarbeitung lt. Änderungsliste	
1.7.0	06.02.17		Einarbeitung lt. Änderungsliste	
			Einarbeitung lt. Änderungsliste	gematik
1.8.0	21.04.17		freigegeben	

---

## Inhaltsverzeichnis

---

<b>Dokumentinformationen .....</b>	<b>2</b>
<b>Inhaltsverzeichnis .....</b>	<b>3</b>
<b>1 Einordnung des Dokumentes .....</b>	<b>5</b>
1.1 Zielsetzung .....	5
1.2 Zielgruppe .....	5
1.3 Geltungsbereich .....	5
1.4 Abgrenzungen .....	5
1.5 Methodik .....	6
<b>2 Systemüberblick .....</b>	<b>7</b>
<b>3 Systemkontext .....</b>	<b>8</b>
3.1 Akteure und Rollen .....	8
3.2 Nachbarsysteme .....	10
<b>4 Zerlegung des Produkttyps .....</b>	<b>12</b>
4.1 KSR-Upload .....	14
4.2 KSR-Download .....	14
4.3 KSR-Management .....	15
4.4 Schnittstellen .....	15
<b>5 Übergreifende Festlegungen .....</b>	<b>17</b>
5.1 Inhalt von Firmware-Update-Paketen .....	17
5.2 Hersteller-Update-Informationen .....	19
5.3 Behandlung von Firmware-Gruppen im Konfigurationsdienst .....	27
5.3.1 Signatur der Datei „FirmwareGroupInfo.xml“ .....	33
5.4 Behandlung von Konfigurationsdatenfiles .....	35
5.5 Kommunikation .....	35
5.5.1 TLS Transport Layer Security (TLS) .....	35
5.5.2 IP Version .....	36
5.5.3 DNS Resource Record .....	36
5.6 Logging .....	37
5.7 Statistische Daten .....	40

5.8	Kryptographische Festlegungen .....	41
6	Funktionsmerkmale .....	42
6.1	Basisdienste .....	42
6.1.1	Schnittstelle I_KSRS_Download (Provided) .....	42
6.1.1.1	I_KSRS_Download::listUpdates .....	42
6.1.1.1.1	I_KSRS_Download::listUpdates Request .....	44
6.1.1.1.2	I_KSRS_Download::listUpdates Response .....	45
6.1.1.2	I_KSRS_Download::getUpdates .....	47
6.1.1.3	I_KSRS_Download::get_Ext_Net_Config .....	49
6.1.1.4	TUC_KSR_001 „Get File“ .....	51
6.1.1.5	KSR Download Cache .....	52
6.2	Organisatorische Schnittstellen .....	53
6.2.1	Registrierung berechtigter Nutzer .....	54
6.2.2	Berechtigungs- und Rollenkonzept .....	54
6.2.3	Uploadschnittstelle P_KSRS_Upload .....	55
6.2.3.1	Schnittstellendefinition .....	55
6.2.3.2	Eingangsprüfung durch den Konfigurationsdienst .....	57
6.2.3.3	Pfadreferenzen .....	61
6.2.3.4	Verfahren zum Erstellen eines signierten Update-Paketes .....	62
6.2.4	Managementdienste P_KSRS_Operations .....	63
6.2.4.1	Schnittstellendefinition .....	63
Anhang A	– Verzeichnisse .....	69
A1	– Abkürzungen .....	69
A2	– Glossar .....	69
A3	– Abbildungsverzeichnis .....	69
A4	– Tabellenverzeichnis .....	70
A5	– Referenzierte Dokumente .....	72
A5.1	– Dokumente der gematik .....	72
A5.2	– Weitere Dokumente .....	72
Anhang B	– Nutzungsbeispiel I_KSRS_Download .....	74
Anhang C	– Konfigurationsdatenfile zur Anbindung von Bestandsnetzen ..	76

---

## 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:

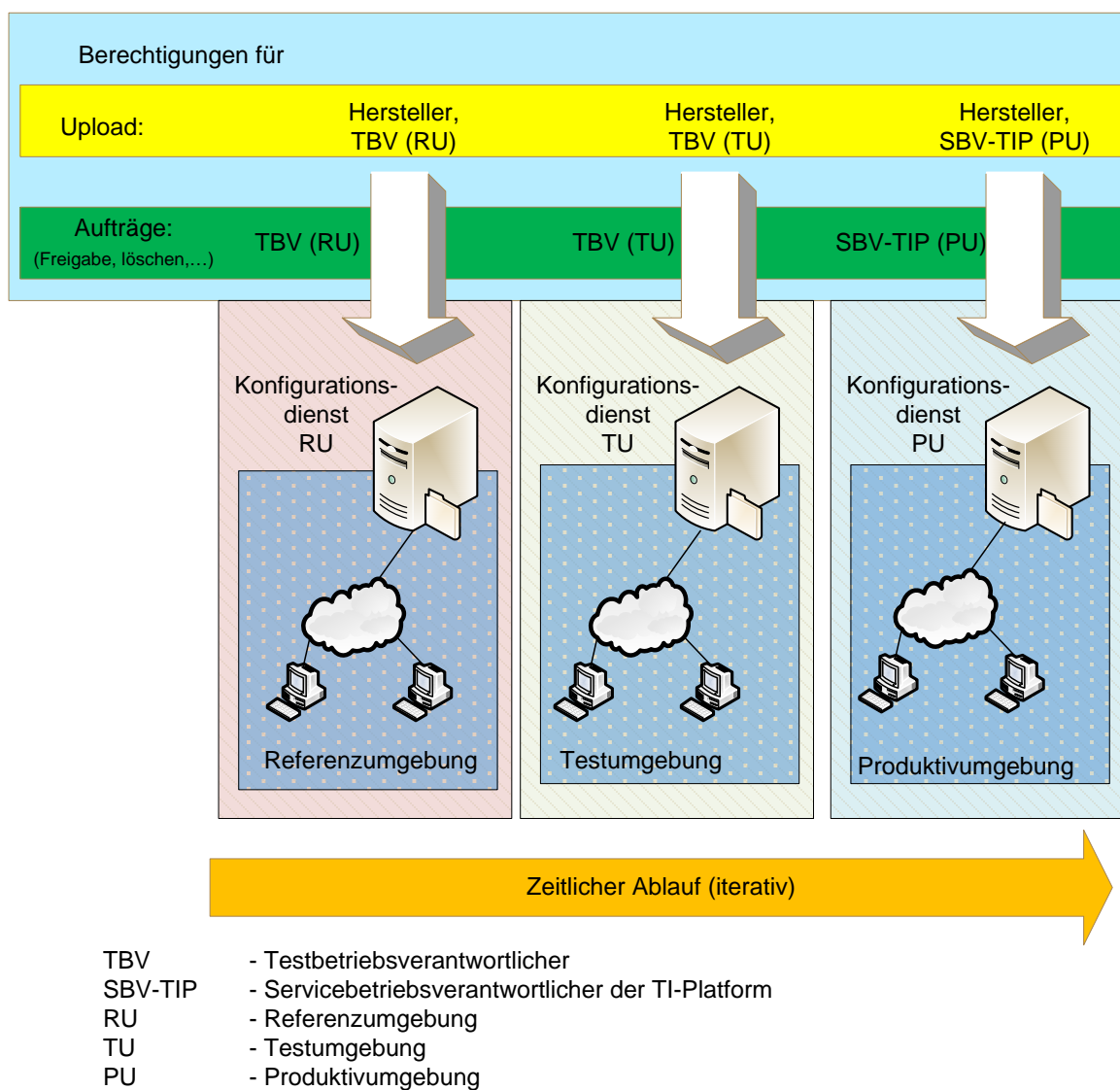
- der Bereitstellung der für den Wirkbetrieb zugelassenen Firmware-Versionen der dezentralen Produkte Konnektor und eHealth-Kartenterminal auf dem Konfigurationsdienst,
- der Bereitstellung der Firmware-Versionen der dezentralen Produkte für die Referenzumgebung und die Testumgebung auf dem Konfigurationsdienst,
- 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

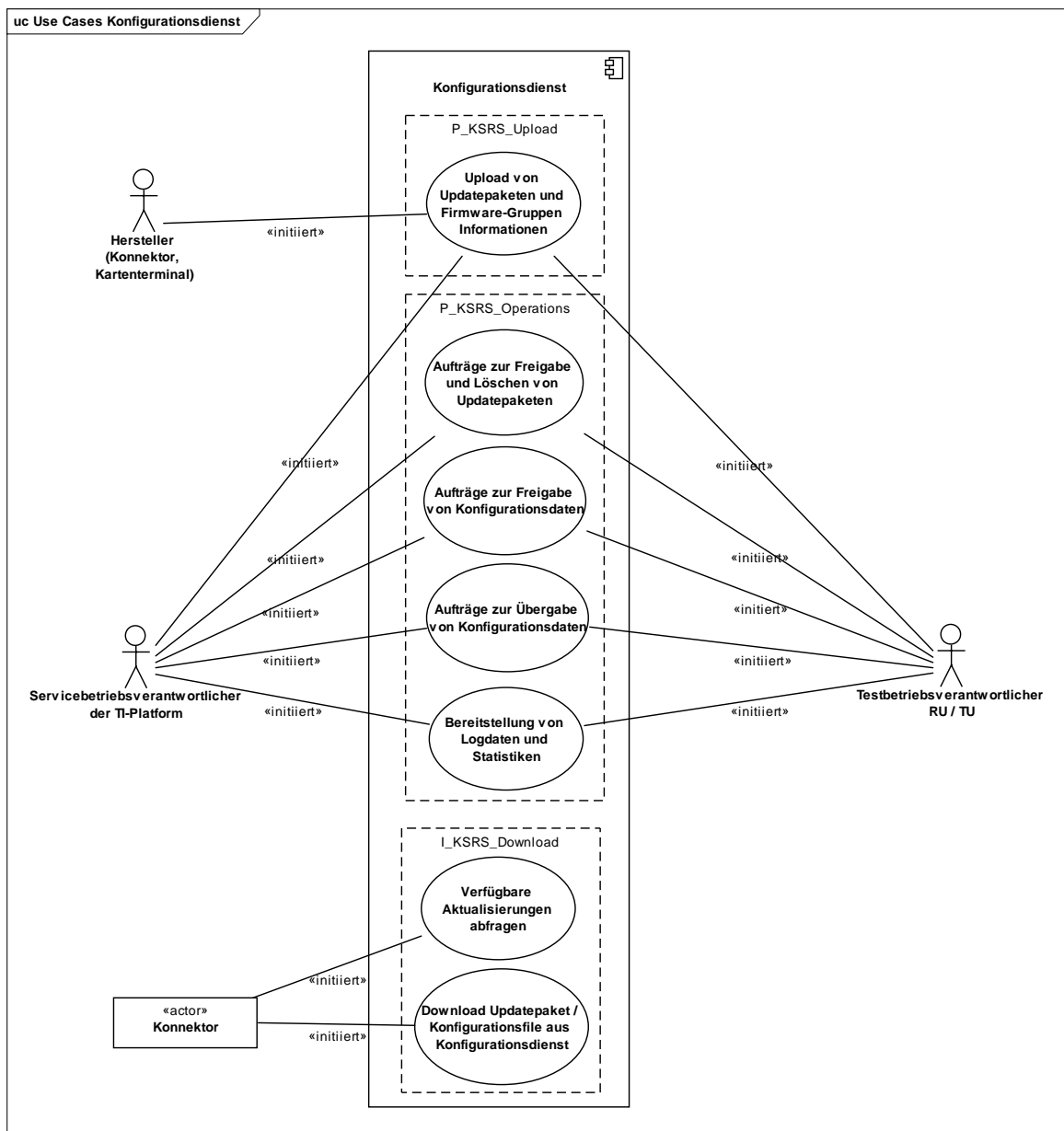
### 3.1 Akteure und Rollen

Die Abbildungen Abb\_KSR\_001 und Abb\_KSR\_011 geben einen Überblick über die externen Akteure und Use Cases des Konfigurationsdienstes.



**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 berechnigte 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.

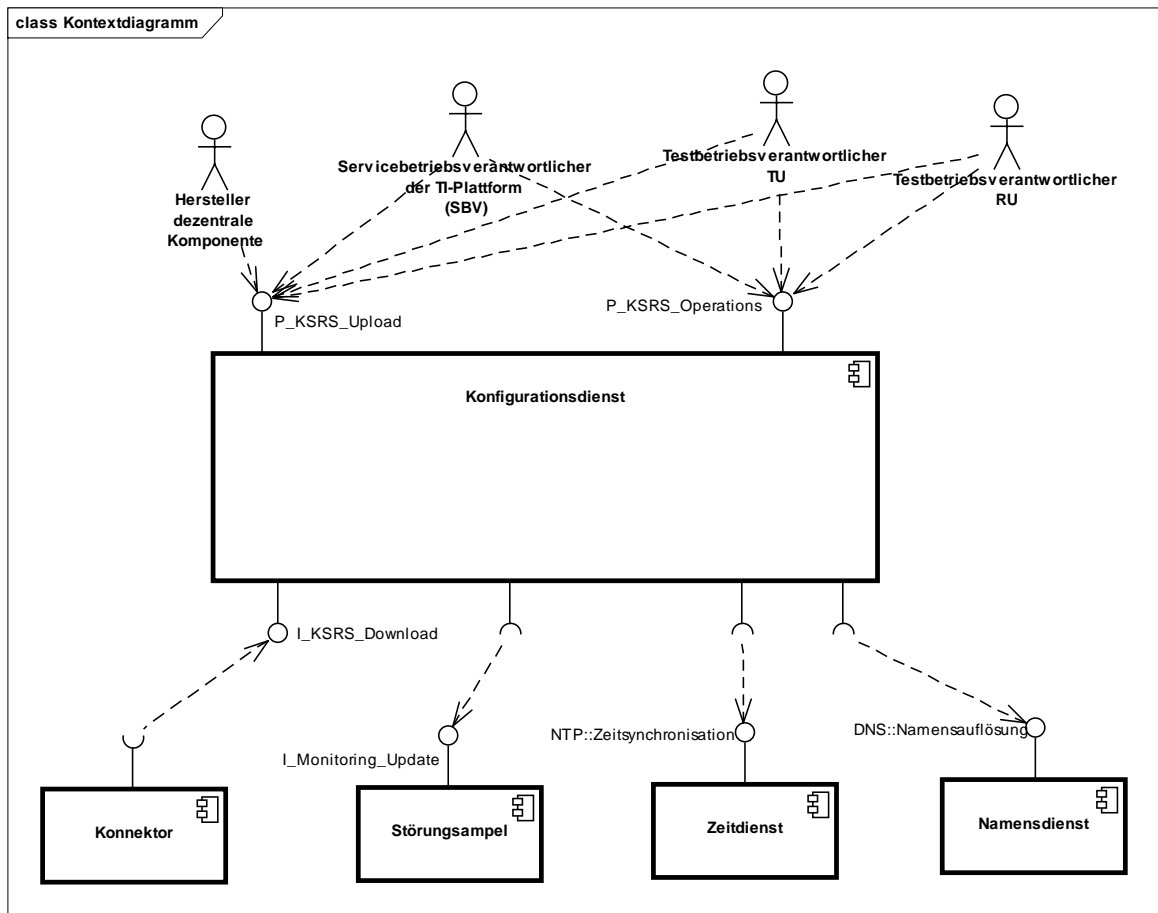


Abbildung 3: Abb\_KSR\_002 Kontextdiagramm Konfigurationsdienst

## 4 Zerlegung des Produkttyps

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

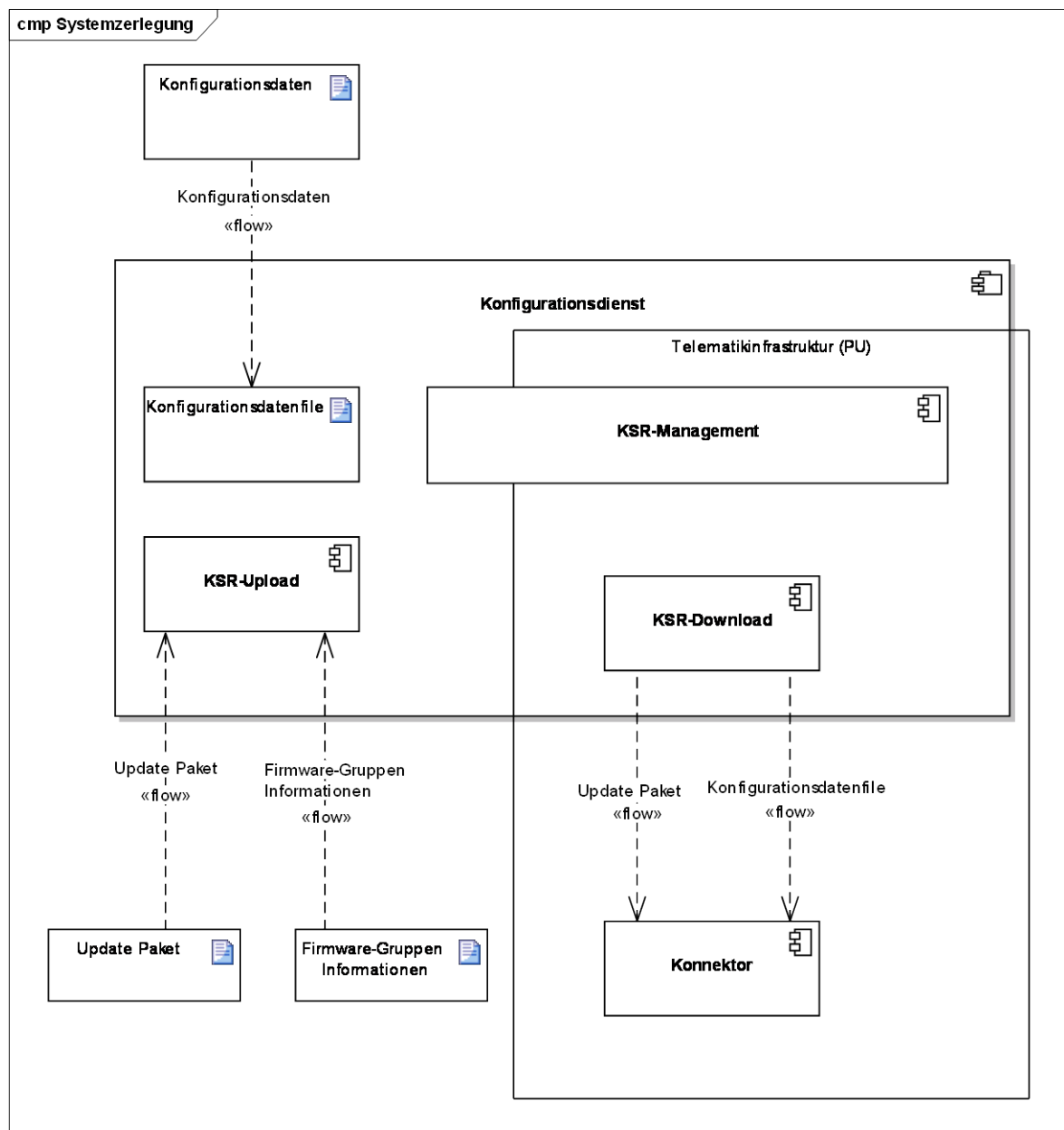
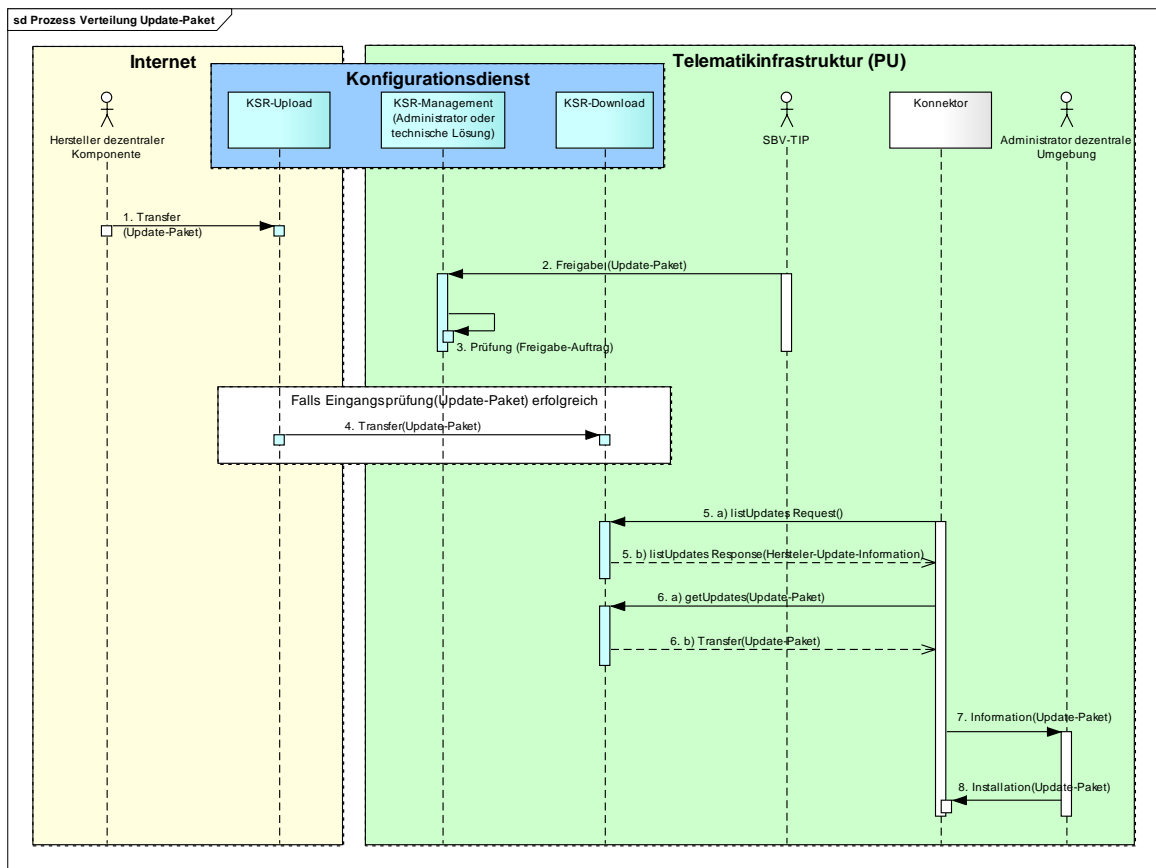


Abbildung 4: Abb\_KSR\_003 Zerlegung Konfigurationsdienst

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

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 Konfigurationsdateien im Downloadbereich der PU**

Der Konfigurationsdienst MUSS sicherstellen, dass nur Konfigurationsdateien 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. 

#### 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 Servicebetriebsverantwortlichen der TI-Plattform sowie zu den Testbetriebsverantwortlichen 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 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#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 Schnittstellenabbildung Konfigurationsdienst**

<b>Spezifikationsschnittstelle [gemSpec_KSR]</b>	<b>Konzeptionelle Schnittstelle [gemKPT_Arch_TIP]</b>
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.

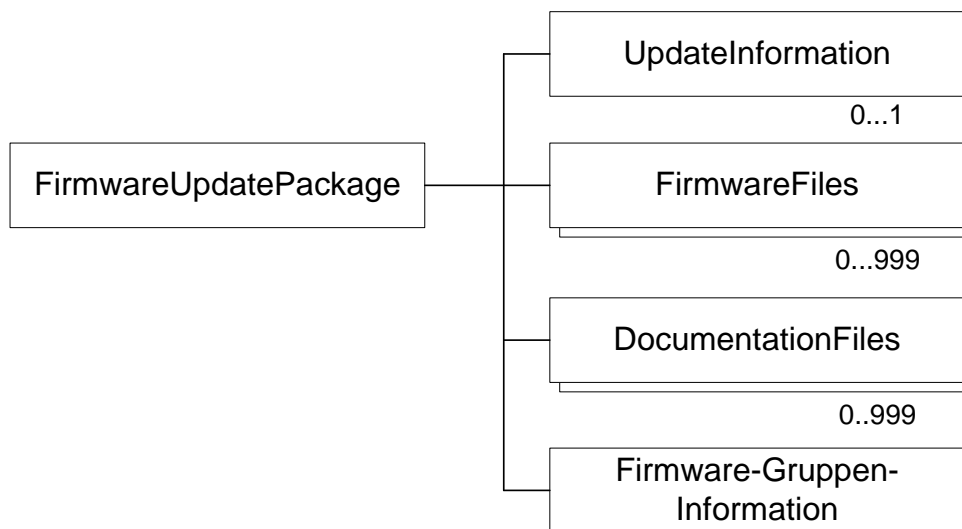


Abbildung 6: Abb\_KSR\_004 Inhalt von Firmware-Update-Paketen

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
<b>Updatepaket</b>	Integritäts- und Authentizitätsschutz Gesamtpaket durch Hersteller	Konfigurationsdienst	TIP1-A_3347
<b>UpdateInformation</b>	Integritäts- und Authentizitätsschutz durch Hersteller	Konnektor	TIP-A_3896 TIP-A_3897
<b>Firmwarefiles</b>	Integritäts- und Authentizitätsschutz durch Hersteller	Konnektor, Kartenterminal	siehe [gemSpec_Kon], [gemSpec_KT]
<b>DocumentationFiles</b>	Keine	-	Keine
<b>Firmware-Gruppen Information</b>	Integritäts- und Authentizitätsschutz durch Hersteller	Konfigurationsdienst	TIP1-A_3322
<b>Konfigurationsdatenfile</b>	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 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 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 durch die Prüfung der Update-Paket – Signatur (TIP1-A\_6123) 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:

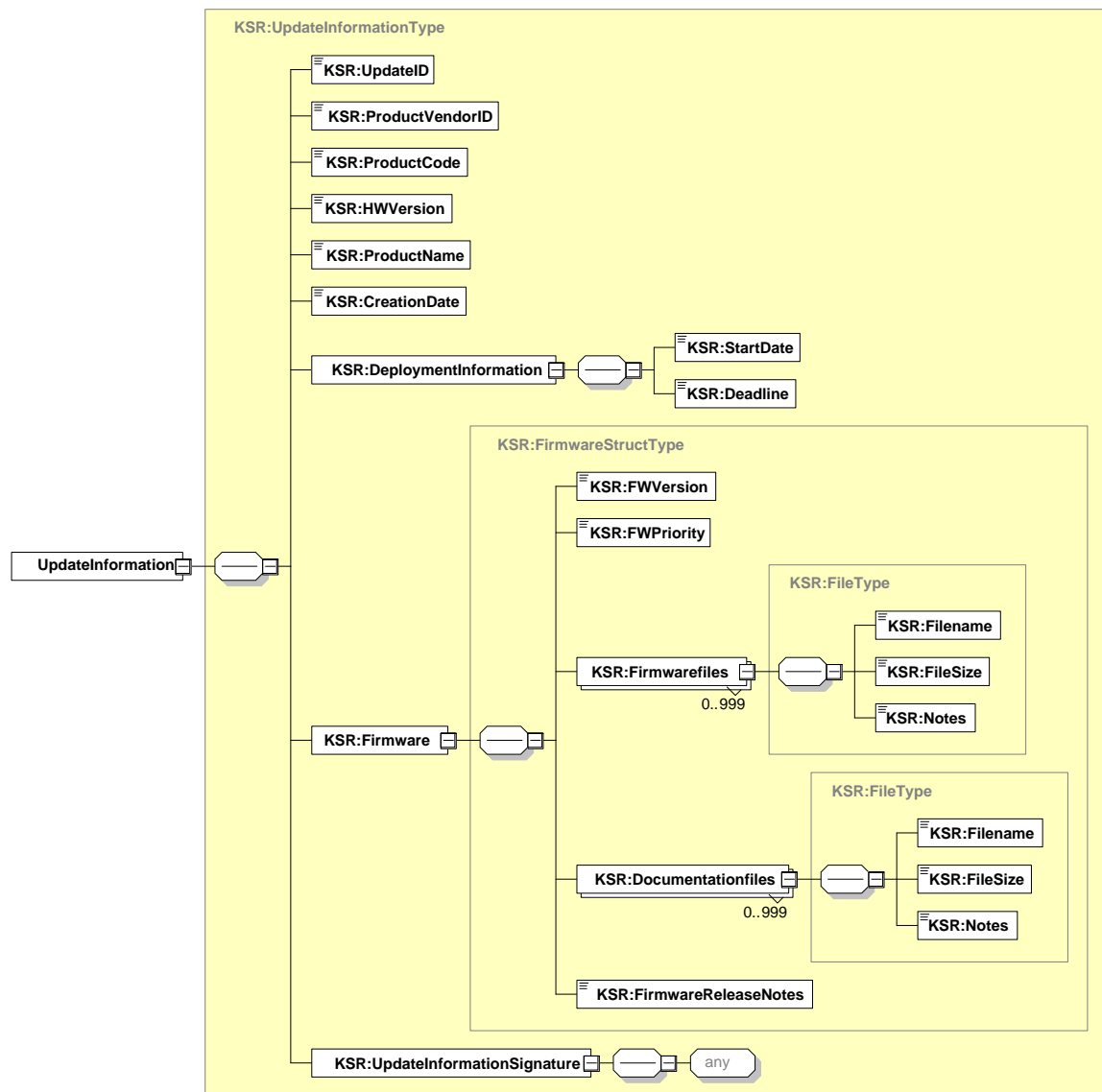


Abbildung 7: Abb\_KSR\_005 Hersteller-Update-Informationen (UpdateInfo.xml)

Tabelle 4: Tab\_KSR\_004 Hersteller-UpdateInformation – Element UpdateID

<b>Bezeichnung</b>	UpdateID
<b>Beschreibung</b>	Identifiziert das Update eindeutig.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals
<b>Optional</b>	Nein

<b>Wertebereich</b>	<p>Entspricht dem Wertebereich vom XML-Datentyp „string“ mit Pattern "[a-zA-Z0-9]{1,24}_[a-zA-Z0-9]{1,7}".</p> <p>Maximale Länge: 32 Zeichen</p> <p>Syntax: &lt;eindeutiger Teil, max. 24 Zeichen&gt;_&lt;OPB oder Name der Erprobung, max. 7 Zeichen&gt;</p> <p>Die UpdateID ist vom Hersteller des Update-Pakets 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.</p> <p>Der Suffix OPB gibt an, dass es sich um ein Update-Paket für den Online Produktivbetrieb handelt.</p> <p>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 GBV abstimmen.</p> <p>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.</p>
---------------------	---

**Tabelle 5: Tab\_KSR\_005 Hersteller-UpdateInformation – Element ProductVendorID**

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

**Tabelle 6: Tab\_KSR\_006 Hersteller-UpdateInformation – Element ProductCode**

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

**Tabelle 7: Tab\_KSR\_007 Hersteller-UpdateInformation – Element HWVersion**

<b>Bezeichnung</b>	HWVersion
<b>Beschreibung</b>	Identifiziert zusammen mit ProductCode und ProductVendorID die Hardware, für welche das Update geeignet ist. [gemSpec_OM] beschreibt dieses Element ausführlich.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals
<b>Optional</b>	nein
<b>Wertebereich</b>	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**

<b>Bezeichnung</b>	ProductName
<b>Beschreibung</b>	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.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals
<b>Optional</b>	nein
<b>Wertebereich</b>	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 256 Zeichen.

**Tabelle 9: Tab\_KSR\_009 Hersteller-UpdateInformation – Element CreationDate**

<b>Bezeichnung</b>	CreationDate
<b>Beschreibung</b>	Datum der Firmware. Es dient der Information des Clients zur Auswahl des Updates.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals
<b>Optional</b>	nein
<b>Wertebereich</b>	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**

<b>Bezeichnung</b>	DeploymentInformation.StartDate
--------------------	---------------------------------

<b>Beschreibung</b>	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.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals
<b>Optional</b>	ja
<b>Wertebereich</b>	Entspricht dem Wertebereich vom XML-Datentyp „date“.

**Tabelle 11: Tab\_KSR\_013 Hersteller-UpdateInformation – Element DeploymentInformation.Deadline**

<b>Bezeichnung</b>	DeploymentInformation.Deadline
<b>Beschreibung</b>	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.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals
<b>Optional</b>	ja
<b>Wertebereich</b>	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**

<b>Bezeichnung</b>	FWVersion
<b>Beschreibung</b>	Die Firmware-Version des vorliegenden Updates. [gemSpec_OM] beschreibt dieses Element ausführlich.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals
<b>Optional</b>	nein
<b>Wertebereich</b>	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**

<b>Bezeichnung</b>	FWPriority
<b>Beschreibung</b>	Mit diesem Element definiert der Hersteller der dezentralen Komponente die Kritikalität des Firmware Updates. Auf kritische Updates wird der Administrator des Konnektors besonders hingewiesen.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals

<b>Optional</b>	nein
<b>Wertebereich</b>	„Normal“, „Kritisch“

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

**Tabelle 14: Tab\_KSR\_015 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.Filename**

<b>Bezeichnung</b>	Files.Firmwarefiles.Filename
<b>Beschreibung</b>	Filename inklusive absolutem Pfad. Dieser Wert wird in der Operation getUpdates HTTP Request als Parameter <filename> genutzt.
<b>Befüllung</b>	Durch Hersteller von Konnektoren und Kartenterminals (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.
<b>Optional</b>	nein
<b>Wertebereich</b>	Entspricht dem Wertebereich vom XML-Datentyp „string“.

**Tabelle 15: Tab\_KSR\_041 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.FileSize**

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

**Tabelle 16: Tab\_KSR\_016 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.Notes**

<b>Bezeichnung</b>	Files.Firmwarefiles.Notes
<b>Beschreibung</b>	Kurze Erläuterung zum Inhalt/Zweck des zugehörigen Files. Diese Information dient der Information der dezentralen Komponente.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals
<b>Optional</b>	Nein
<b>Wertebereich</b>	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 256 Zeichen.



**Tabelle 17: Tab\_KSR\_017 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.Filename**

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

**Tabelle 18: Tab\_KSR\_042 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.FileSize**

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

**Tabelle 19: Tab\_KSR\_018 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.Notes**

<b>Bezeichnung</b>	Files.Documentationfiles.Notes
<b>Beschreibung</b>	Kurze Erläuterung des zugehörigen Files. Diese Information dient der Information der dezentralen Komponente.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals
<b>Optional</b>	Nein, falls zugehörigen File vorhanden.
<b>Wertebereich</b>	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 256 Zeichen.

**Tabelle 20: Tab\_KSR\_019 Hersteller-UpdateInformation – Element Firmware.FirmwareReleaseNotes**

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

**Tabelle 21: Tab\_KSR\_020 Hersteller-UpdateInformation – Element UpdateInformationSignature**

<b>Bezeichnung</b>	UpdateInformationSignature
<b>Beschreibung</b>	<p>Dieses Element kann der Konnektorhersteller zur Signatur der UpdateInformation nutzen.</p> <p>Hersteller von Kartenterminals sollen dieses Element nicht nutzen und die UpdateInformation nicht signieren.</p> <p>Die Signatur kann auch als „Detached-Signature“ in einer eigenen Datei übermittelt werden.</p> <p>Das Signaturverfahren liegt in Verantwortung des Herstellers, der Konfigurationsdienst wertet dieses Feld nicht aus.</p>
<b>Befüllung</b>	Hersteller von Konnektoren
<b>Optional</b>	Ja.
<b>Wertebereich</b>	Any (vom Hersteller festzulegen)

Das nachfolgende Beispiel zeigt eine ausgefüllte UpdateInfo.xml. Die Datei definiert zwei Firmware-Dateien 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_12122013</UpdateID>
  <ProductVendorID>CXX01</ProductVendorID>
  <ProductCode>KT25</ProductCode>
  <HWVersion>1.0.1</HWVersion>
  <ProductName>Kartenterminal 25</ProductName>
  <CreationDate>2014-01-14</CreationDate>
  <DeploymentInformation>
    <StartDate>2014-01-14</StartDate>
    <Deadline>2014-01-30</Deadline>
  </DeploymentInformation>
  <Firmware>
    <FWVersion>2.10.0</FWVersion>
    <FWPriority>Normal</FWPriority>
    <Firmwarefiles>
      <Filename>/CXX01/KT25/Update_12122013/FW10_2_10_0.bin</Filename>
      <FileSize>2345</FileSize>
      <Notes>Firmware Update 2.10.0</Notes>
    </Firmwarefiles>
    <Firmwarefiles>
      <Filename>/CXX01/KT25/Update_12122013/FW10_2_10_0.jpg</Filename>
      <FileSize>2655</FileSize>
      <Notes>Neues Logo</Notes>
    </Firmwarefiles>
    <Documentationfiles>
      <Filename>/CXX01/KT25/Update_12122013/FW10_2_10_0.pdf</Filename>
      <FileSize>8695</FileSize>
      <Notes>Dokumentation zu Firmware Update 2.10.0</Notes>
    </Documentationfiles>
    <FirmwareReleaseNotes>
      Release Notes der Version 2.10.0.
      Information zu den behobenen Fehlern finden sich auf der Webseite.
    </FirmwareReleaseNotes>
  </Firmware>
  <UpdateInformationSignature></UpdateInformationSignature>
</UpdateInformation>
```

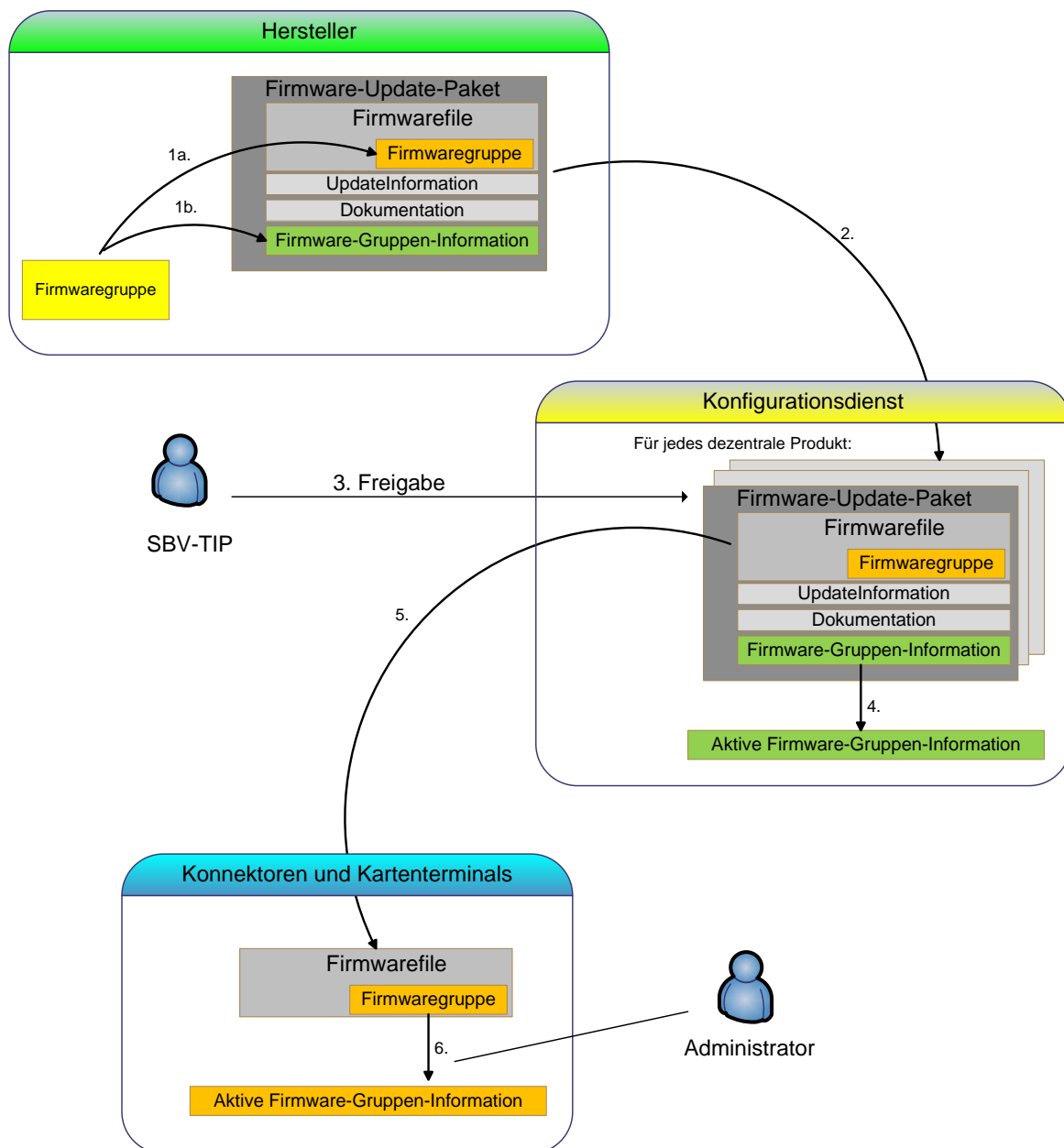
Abbildung 8 Abb\_KSR\_006 Beispiel UpdateInfo.xml

### 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 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 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 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:

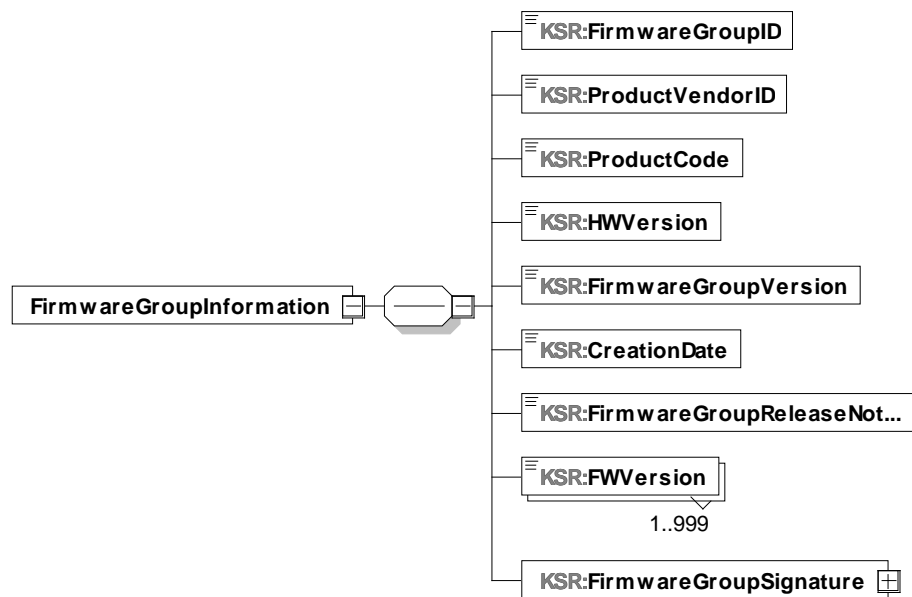


Abbildung 10: Abb\_KSR\_007 Firmware-Gruppen-Informationen

Tabelle 22: Tab\_KSR\_021 Firmware-Gruppen-Information – Element FirmwareGroupID

<b>Bezeichnung</b>	FirmwareGroupID
<b>Beschreibung</b>	Identifiziert die Firmware-Gruppe eindeutig.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals
<b>Optional</b>	Nein
<b>Wertebereich</b>	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit dem Pattern „[a-zA-Z0-9_]*“. Maximale Länge: 32 Zeichen

Tabelle 23: Tab\_KSR\_022 Firmware-Gruppen-Information – Element FirmwareGroupVersion

<b>Bezeichnung</b>	FirmwareGroupVersion
<b>Beschreibung</b>	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 numerisches Feld interpretiert.
<b>Optional</b>	nein
<b>Wertebereich</b>	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit dem Pattern „[0-9]*“ (ganzzahlige Zahlen). Maximale Länge 5 Zeichen.

**Tabelle 24: Tab\_KSR\_023 Firmware-Gruppen-Information – Element FirmwareGroupReleaseNotes**

<b>Bezeichnung</b>	FirmwareGroupReleaseNotes
<b>Beschreibung</b>	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.
<b>Optional</b>	nein
<b>Wertebereich</b>	Entspricht dem Wertebereich vom XML-Datentyp „string“. Maximale Länge 2048 Zeichen.

**Tabelle 25: Tab\_KSR\_024 Firmware-Gruppen-Information – Element FirmwareGroupSignature**

<b>Bezeichnung</b>	FirmwareGroupSignature
<b>Beschreibung</b>	Dieses Element kann der Hersteller von Konnektoren und Kartenterminals 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.
<b>Befüllung</b>	Hersteller von Konnektoren und Kartenterminals
<b>Optional</b>	Ja.
<b>Wertebereich</b>	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 FWVersionen in der Liste enthalten sein. ☒

#### ☒ **TIP1-A\_6131 FirmwareGroupInfo.xml - Format**

Der Konfigurationsdienst und Hersteller von Konnektoren und Kartenterminals MÜSSEN die Datei FirmwareGroupInfo.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 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. ☒

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/kar/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 Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals MÜSSEN die Detached-Signatur 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 Konnektoren und Kartenterminals 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 Signierer-Zertifikat im XML-Block des XML-Elementes KeyInfo.
- Die Signatur ist konform mit der Anforderung [gemSpec\_Krypt# GS-A\_4370] und verwendet den Signatur-Algorithmus "RSASSA-PKCS1-v1\_5 mit SHA256" oder "RSASSA-PSS mit SHA256". Die Signatur-Algorithmen sind in der [gemSpec\_Krypt# GS-A\_4371] definiert.
- 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 Konnektoren und Kartenterminals 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>"				
_ksrkongfig._tcp.ksr.<TOP_LEVEL_DOMAIN_TI>	<TTL3>	<IN>	<SRV>	<Priorität2>
<Gewicht2> <Port2> <FQDN2>				
_ksrkongfig._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 Konfigurationsdateien 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 26 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 Infold ist abhängig von dem Wert im Feld Action nach den Angaben folgenden Tabelle. Das Operator-Zeichen „|“ im Feld Infold 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 27 Tab\_KSR\_049 Werte im Feld Infold zu Action**

Action	Infold
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



#### **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 28: 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. [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	String „[0-9]{1,3}].[0-9]{1,3}].[0-9]{1,3}“ Wenn „listUpdates“ aufgerufen wurde, enthält dieses Feld den entsprechenden Parameter des



Position	Feld	Beschreibung	Typ
		ausführlich.	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. 

## 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 29: Tab\_KSR\_025 Konfigurationsdienst

Name	I_KSRS_Download	
Version (KDV)	gemäß Produkttypversion	
Namensraum	<a href="http://ws.gematik.de/ksr/v1.1">http://ws.gematik.de/ksr/v1.1</a>	
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:

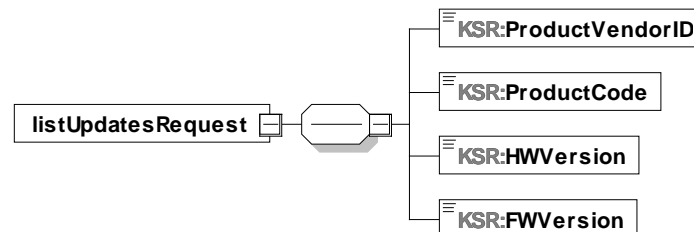


Abbildung 12: Abb\_KSR\_008 Operation I\_KSRS\_Download::listUpdates Request

Tabelle 31: Tab\_KSR\_027 I\_KSRS\_Download::listUpdates Request

<b>Bezeichnung</b>	I_KSRS_Download::listUpdates Request
<b>Beschreibung</b>	Operations-Element des Request der Operation I_KSRS_Download::listUpdates

Tabelle 32: Tab\_KSR\_028 Hersteller-Update-Informationen – Element ProductVendorID

<b>Bezeichnung</b>	ProductVendorID
<b>Beschreibung</b>	Identifiziert den Hersteller des Produkts, für welches auf Updates geprüft werden soll.
<b>Optional</b>	Nein
<b>Wertebereich</b>	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

<b>Bezeichnung</b>	ProductCode
<b>Beschreibung</b>	Identifiziert das Produkt zusammen mit dem ProductVendorID, für welches auf Updates geprüft werden soll.
<b>Optional</b>	Nein
<b>Wertebereich</b>	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

<b>Bezeichnung</b>	HWVersion
--------------------	-----------

<b>Beschreibung</b>	Identifiziert die Hardware zusammen mit ProductCode und ProductVendorID , für welches auf Updates geprüft werden soll. [gemSpec_OM] beschreibt dieses Element ausführlich.
<b>Optional</b>	Nein
<b>Wertebereich</b>	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**

<b>Bezeichnung</b>	FWVersion
<b>Beschreibung</b>	Die FirmwareVersion des Produkts, für welches auf Updates geprüft werden soll.
<b>Optional</b>	Nein
<b>Wertebereich</b>	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:

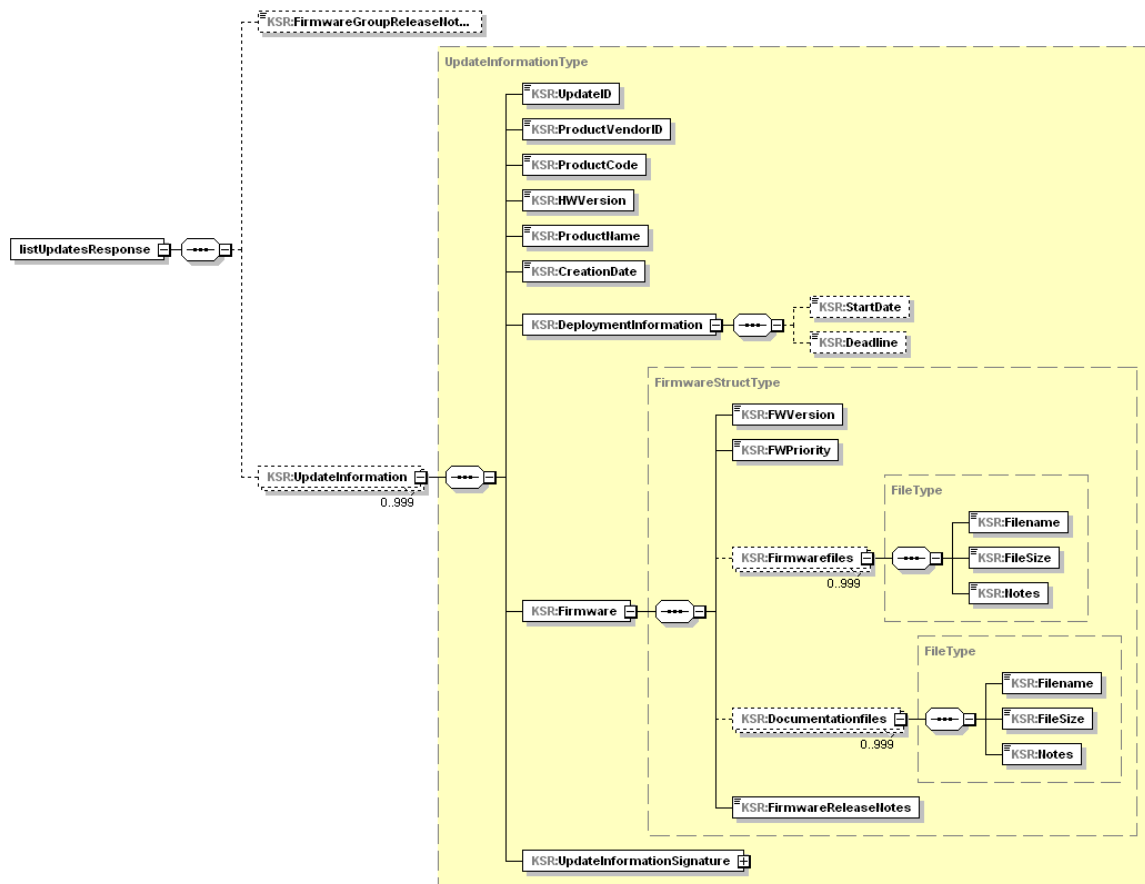


Abbildung 13: Abb\_KSR\_009 Operation I\_KSRS\_Download::listUpdates Response

Tabelle 36: Tab\_KSR\_032 I\_KSRS\_Download::listUpdates – Response

<b>Bezeichnung</b>	I_KSRS_Download::listUpdates Response
<b>Beschreibung</b>	Operations-Element des Response der Operation I_KSRS_Download::listUpdates

Tabelle 37: Tab\_KSR\_033 I\_KSRS\_Download::listUpdates – Element FirmwareGroupReleaseNotes

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

**Tabelle 38: Tab\_KSR\_034 I\_KSRS\_Download::listUpdates – Element UpdateInformation**

<b>Bezeichnung</b>	UpdateInformation
<b>Beschreibung</b>	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).
<b>Optional</b>	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-Konfigurationsdateien wird der technische Use Case TUC\_KSR\_001 „Get File“ (Kapitel 6.1.1.4) genutzt. Die Konnektor-Konfigurationsdateien 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-Konfigurationsdateien 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 „_ksrkongfig._tcp.ksr.telematik“ ermittelt. <path> wird durch Abfrage des DNS TXT Resource Record „_ksrkongfig._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.
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 43: Tab\_KSR\_036 File Transfer HTTP Request – Element host**

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

**Tabelle 44: Tab\_KSR\_037 File Transfer HTTP Request – Element path**

<b>Bezeichnung</b>	path
<b>Beschreibung</b>	Absoluter Pfad (siehe z.B. Tab_KSR_015, Tab_KSR_017)
<b>Optional</b>	nein
<b>Wertebereich</b>	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. ☒

#### 6.1.1.5 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 Störungssampel Monitoringdaten**

Der Konfigurationsdienst MUSS für alle seine Komponenten inklusive der KSR Download Cache Server Monitoringdaten an die Störungssampel 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 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 Registrierung berechtigter Nutzer

Hersteller (und TBV/SBV-TIP) 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 Konnektoren und Kartenterminals bekommen nur die Berechtigung sich im Upload-Bereich anzumelden, Update-Pakete hochzuladen und Statistikdaten herunterzuladen. Die TBV/SBV-TIP der jeweiligen Umgebung erhalten Berechtigung für den Upload- und dem Konfigurationsbereich. Die TBV/SBV-TIP können damit Update-Pakete im Upload-Bereich einspielen und die hoch geladenen Pakete im Konfigurationsbereich bearbeiten, d.h. Aufträge zum Löschen oder zur Freigabe des Update-Paketes erteilen. 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 Konnektoren und Kartenterminals, TBV, SBV-TIP 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

Rolle / Gruppe	Berechtigung
	herunterladen.
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_PU	Die Rolle kann sich an der Web-Applikation des Upload-Bereichs in PU anmelden, Pakete hochladen, den Status einsehen und Statistikdaten herunterladen.
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.
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.
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
TBV	Hersteller_TU, Hersteller_RU, TBV_RU, TBV_TU
SBV-TIP	Hersteller_PU, SBV_PU

## 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 (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 47: Tab\_KSR\_039 P\_KSRS\_Upload Schema**

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



☒ **TIP1-A\_3343 Berechtigung P\_KSRS\_Upload**

Der Anbieter des Konfigurationsdienstes MUSS sicherstellen, dass nur berechtigte Akteure (berechtigte Hersteller von Konnektoren und Kartenterminals, 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 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 Übermittels von Update-Paketen den Nutzer über den Fortschritt des Filetransfers informieren. ☒

**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/SBV-TIP 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 bzw. SBV Rolle für die jeweilige Umgebung besitzen. ☒

Der Hersteller von Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals DÜRFEN NICHT Update-Pakete hochladen, deren entkomprimierte Paketgröße den abgestimmten Maximalwert übersteigt und Konfigurationsdienst DARF NICHT Update-Pakete akzeptieren welche diesen Maximalwert übersteigen. ☒

Der maximale Wert ist durch das Mengengerüst in [gemSpec\_Perf#3.1.4] auf 750Mb spezifiziert.

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 Konnektoren und Kartenterminals 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 Konnektoren oder Kartenterminals 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 Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals 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. ☒

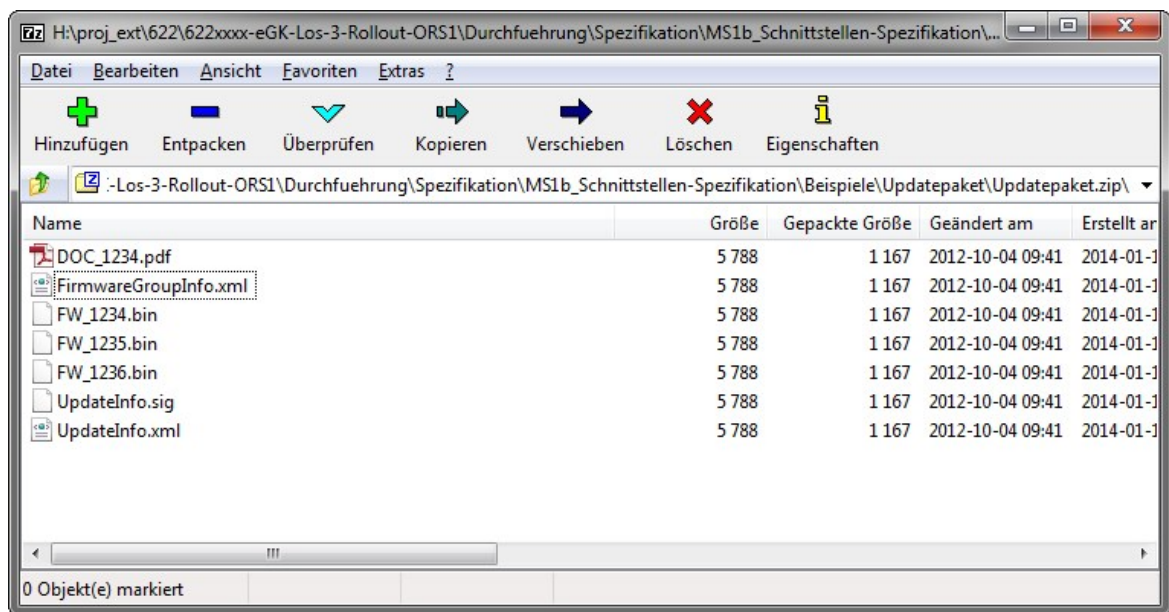


Abbildung 14 Abb\_KSR\_017 Beispiel Struktur Update-Paket

#### ☒ 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 Konnektoren und Kartenterminals 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 Konnektoren bzw. Kartenterminals 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-CAAdES] vorgegeben.

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

Folgendes Verfahren wird angewendet zur Verifikation der Signatur der Datei:

1. Der Hersteller von Konnektoren und Kartenterminals 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 Konnektoren und Kartenterminals MÜSSEN die detached PKCS#7-Signatur zum Update-Paket mit Signatur-Algorithmus "RSASSA-PKCS1-v1\_5 mit SHA256" oder "RSASSA-PSS mit SHA256" unterstützen. Das Feld certificates des Feldes signedData der Signatur MUSS das Zertifikat der Signatur enthalten (Validation Policy zu [ETSI-CAAdES#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-CAAdES#5.7]. Die Signatur-Algorithmen MÜSSEN entsprechend [gemSpec\_Krypt#GS-A\_5080] unterstützt werden. ☒

#### **☒ 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 Konnektoren und Kartenterminals 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. ☒

#### **☒ TIP1-A\_6066 KSR Bereitstellung "Signier-Tool"**

Der Anbieter des Konfigurationsdienstes MUSS berechtigten Herstellern dezentraler Komponenten der TI, dem Servicebetriebsverantwortlichen TI-Plattform



(PU) und den Testbetriebsverantwortlichen TU/RU ein Tool zur Signatur von Update-Paketen bereitstellen. ☒

## 6.2.4 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.

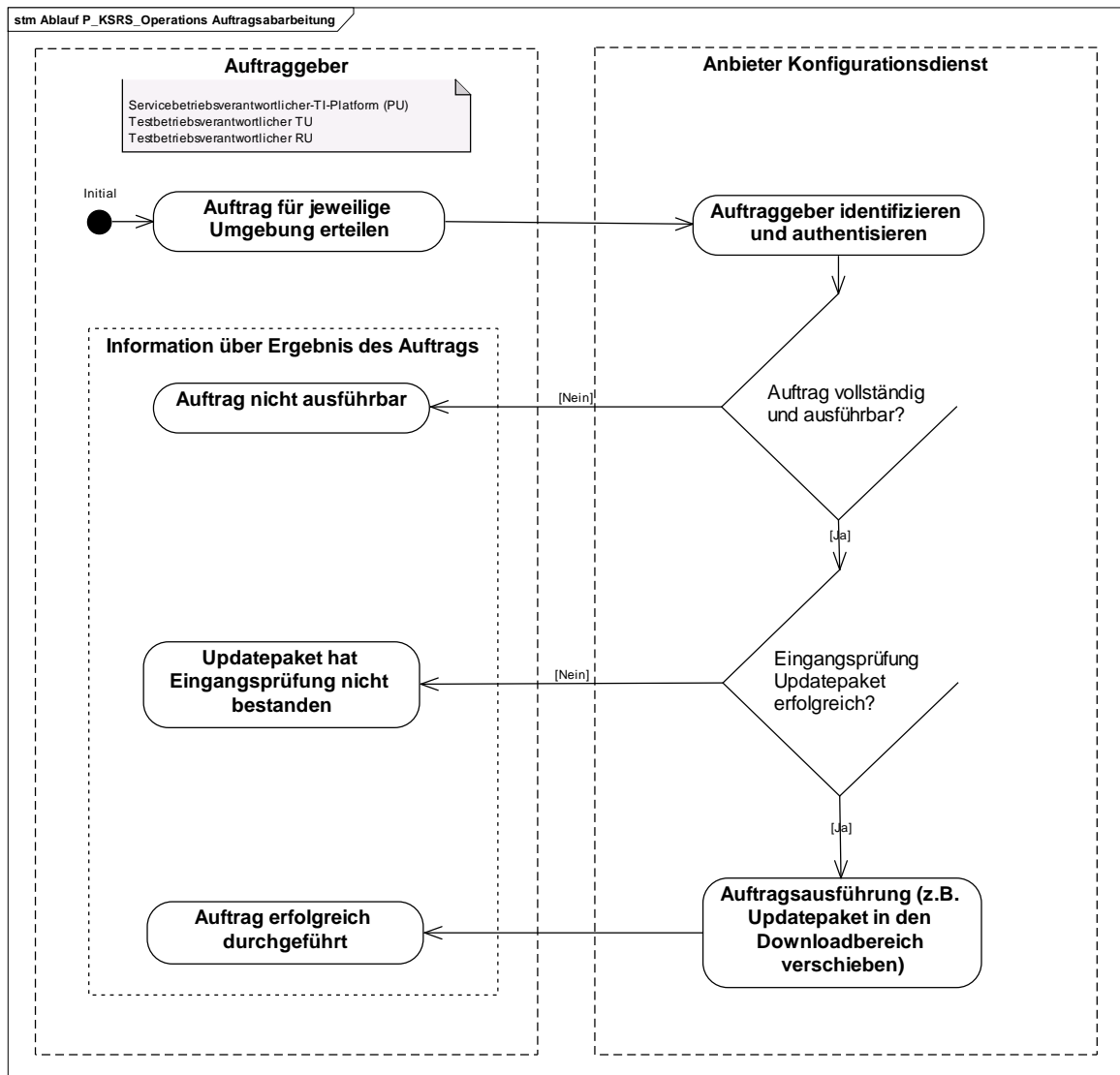


Abbildung 15: Abb\_KSR\_010 Beispiel Auftragsabarbeitung (P\_KSRS\_Operations)

### 6.2.4.1 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 berechnigte 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. Folgende Informationen MÜSSEN mindestens zwingend enthalten sein:

- Umgebung, in der der Auftrag ausgeführt wurde.
- 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.



Status	Beschreibung
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. ☒

☒ **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. ☒

☒ **TIP1-A\_6067 Organisatorische Schnittstelle zur Bereitstellung von KSR Statusberichten der PU**

Der Anbieter des Konfigurationsdienstes MUSS dem Servicebetriebsverantwortlichen der TI-Plattform 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. ☒

---

## 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.....	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.....	17
Abbildung 7: Abb_KSR_005 Hersteller-Update-Informationen (UpdateInfo.xml) .....	20
Abbildung 8: Abb_KSR_006 Beispiel UpdateInfo.xml .....	27
Abbildung 9: Abb_KSR_013 Verteilungsprozess Firmware-Gruppen-Informationen .....	28
Abbildung 10: Abb_KSR_007 Firmware-Gruppen-Informationen .....	30
Abbildung 11: Abb_KSR_016 Beispiel aus FirmwareGroupInfo.xml.....	33
Abbildung 12: Abb_KSR_008 Operation I_KSRS_Download::listUpdates Request .....	44
Abbildung 13: Abb_KSR_009 Operation I_KSRS_Download::listUpdates Response .....	46
Abbildung 14: Abb_KSR_017 Beispiel Struktur Update-Paket .....	61
Abbildung 15: Abb_KSR_010 Beispiel Auftragsabarbeitung (P_KSRS_Operations).....	63

Abbildung 16: Abb_KSR_015 Beispielablauf für ein Firmware Update.....	75
Abbildung 17: Abb_KSR_014 Schema InfrastrukturKonfig.xsd .....	76

## **A4 – Tabellenverzeichnis**

Tabelle 1: Tab_KSR_001 Schnittstellen des Konfigurationsdienstes .....	15
Tabelle 2: Tab_KSR_002 Schnittstellenabbildung Konfigurationsdienst.....	16
Tabelle 3: Tab_KSR_003 Schutz der Firmware-Update-Pakete .....	18
Tabelle 4: Tab_KSR_004 Hersteller-UpdateInformation – Element UpdateID.....	20
Tabelle 5: Tab_KSR_005 Hersteller-UpdateInformation – Element ProductVendorID.....	21
Tabelle 6: Tab_KSR_006 Hersteller-UpdateInformation – Element ProductCode .....	21
Tabelle 7: Tab_KSR_007 Hersteller-UpdateInformation – Element HWVersion.....	22
Tabelle 8: Tab_KSR_008 Hersteller-UpdateInformation – Element ProductName .....	22
Tabelle 9: Tab_KSR_009 Hersteller-UpdateInformation – Element CreationDate.....	22
Tabelle 10: Tab_KSR_012 Hersteller-UpdateInformation – Element DeploymentInformation.StartDate .....	22
Tabelle 11: Tab_KSR_013 Hersteller-UpdateInformation – Element DeploymentInformation.Deadline .....	23
Tabelle 12: Tab_KSR_014 Hersteller-UpdateInformation – Element Firmware.FWVersion .....	23
Tabelle 13: Tab_KSR_040 Hersteller-UpdateInformation – Element Firmware.FWPriority .....	23
Tabelle 14: Tab_KSR_015 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.FileName .....	24
Tabelle 15: Tab_KSR_041 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.FileSize .....	24
Tabelle 16: Tab_KSR_016 Hersteller-UpdateInformation – Element Firmware.Firmwarefiles.Notes .....	24
Tabelle 17: Tab_KSR_017 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.FileName .....	25
Tabelle 18: Tab_KSR_042 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.FileSize .....	25
Tabelle 19: Tab_KSR_018 Hersteller-UpdateInformation – Element Firmware.Documentationfiles.Notes .....	25
Tabelle 20: Tab_KSR_019 Hersteller-UpdateInformation – Element Firmware.FirmwareReleaseNotes.....	25
Tabelle 21: Tab_KSR_020 Hersteller-UpdateInformation – Element UpdateInformationSignature .....	26

Tabelle 22: Tab_KSR_021 Firmware-Gruppen-Information – Element FirmwareGroupID .....	30
Tabelle 23: Tab_KSR_022 Firmware-Gruppen-Information – Element FirmwareGroupVersion .....	30
Tabelle 24: Tab_KSR_023 Firmware-Gruppen-Information – Element FirmwareGroupReleaseNotes .....	31
Tabelle 25: Tab_KSR_024 Firmware-Gruppen-Information – Element FirmwareGroupSignature .....	31
Tabelle 26 Tab_KSR_048 Logdatenformat .....	38
Tabelle 27 Tab_KSR_049 Werte im Feld Infold zu Action .....	39
Tabelle 28: Tab_KSR_046 Statistikdatenformat .....	40
Tabelle 29: Tab_KSR_025 Konfigurationsdienst .....	42
Tabelle 30: Tab_KSR_026 Operation I_KSRS_Download::listUpdates .....	43
Tabelle 31: Tab_KSR_027 I_KSRS_Download::listUpdates Request .....	44
Tabelle 32: Tab_KSR_028 Hersteller-Update-Informationen – Element ProductVendorID .....	44
Tabelle 33: Tab_KSR_029 Hersteller-Update-Informationen – Element ProductCode ....	44
Tabelle 34: Tab_KSR_030 Hersteller-Update-Informationen – Element HWVersion .....	44
Tabelle 35: Tab_KSR_031 Hersteller-Update-Informationen – Element FWVersion .....	45
Tabelle 36: Tab_KSR_032 I_KSRS_Download::listUpdates – Response .....	46
Tabelle 37: Tab_KSR_033 I_KSRS_Download::listUpdates – Element FirmwareGroupReleaseNotes .....	46
Tabelle 38: Tab_KSR_034 I_KSRS_Download::listUpdates – Element UpdateInformation .....	47
Tabelle 39 Tab_KSR_047 I_KSRS_Download::listUpdates Fehlercodes .....	47
Tabelle 40: Tab_KSR_035 Operation I_KSRS_Download::getUpdates .....	48
Tabelle 41: Tab_KSR_044 Operation I_KSRS_Download::get_Ext_Net_Config .....	50
Tabelle 42: Tab_KSR_043 TUC_KSR_001 „Get File“ .....	51
Tabelle 43: Tab_KSR_036 File Transfer HTTP Request – Element host .....	52
Tabelle 44: Tab_KSR_037 File Transfer HTTP Request – Element path .....	52
Tabelle 45 Tab_KSR_011 Gruppen und Berechtigungen .....	54
Tabelle 46 Tab_KSR_038 Beispiel Gruppenzuordnung .....	55
Tabelle 47: Tab_KSR_039 P_KSRS_Upload Schema .....	56
<b>Tabelle 48: Tab_KSR_010 Struktur Update-Paket .....</b>	<b>59</b>
Tabelle 49: Tab_KSR_050 Status Definition .....	64
Tabelle 50: Tab_KSR_045 Attribute des Konfigurationsdatenfiles zur Anbindung von Bestandsnetzen .....	76



## 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
[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 v2.3.0
[gemSpec_Perf]	gematik: Performance und Mengengerüst TI-Plattform
[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, <a href="http://tools.ietf.org/html/rfc2109">http://tools.ietf.org/html/rfc2109</a>
[RFC2616]	Hypertext Transfer Protocol – http/1.1
[ZIP-APP]	<a href="http://www.pkware.com/documents/casestudies/APPNOTE.TXT">http://www.pkware.com/documents/casestudies/APPNOTE.TXT</a>
[XMLDSig]	XML Signature Syntax and Processing (Second Edition) W3C Recommendation 10 June 2008 <a href="http://www.w3.org/TR/2008/PER-xmlsig-core-20080326/">http://www.w3.org/TR/2008/PER-xmlsig-core-20080326/</a>
[ETSI-CADES]	ETSI TS 101 733 V1.7.4 (2008-07), Electronic Signatures and



[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)
[ETSI-XAdES]	ETSI TS 101 903 V1.4.2 (2010-12), Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)

---

## **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.

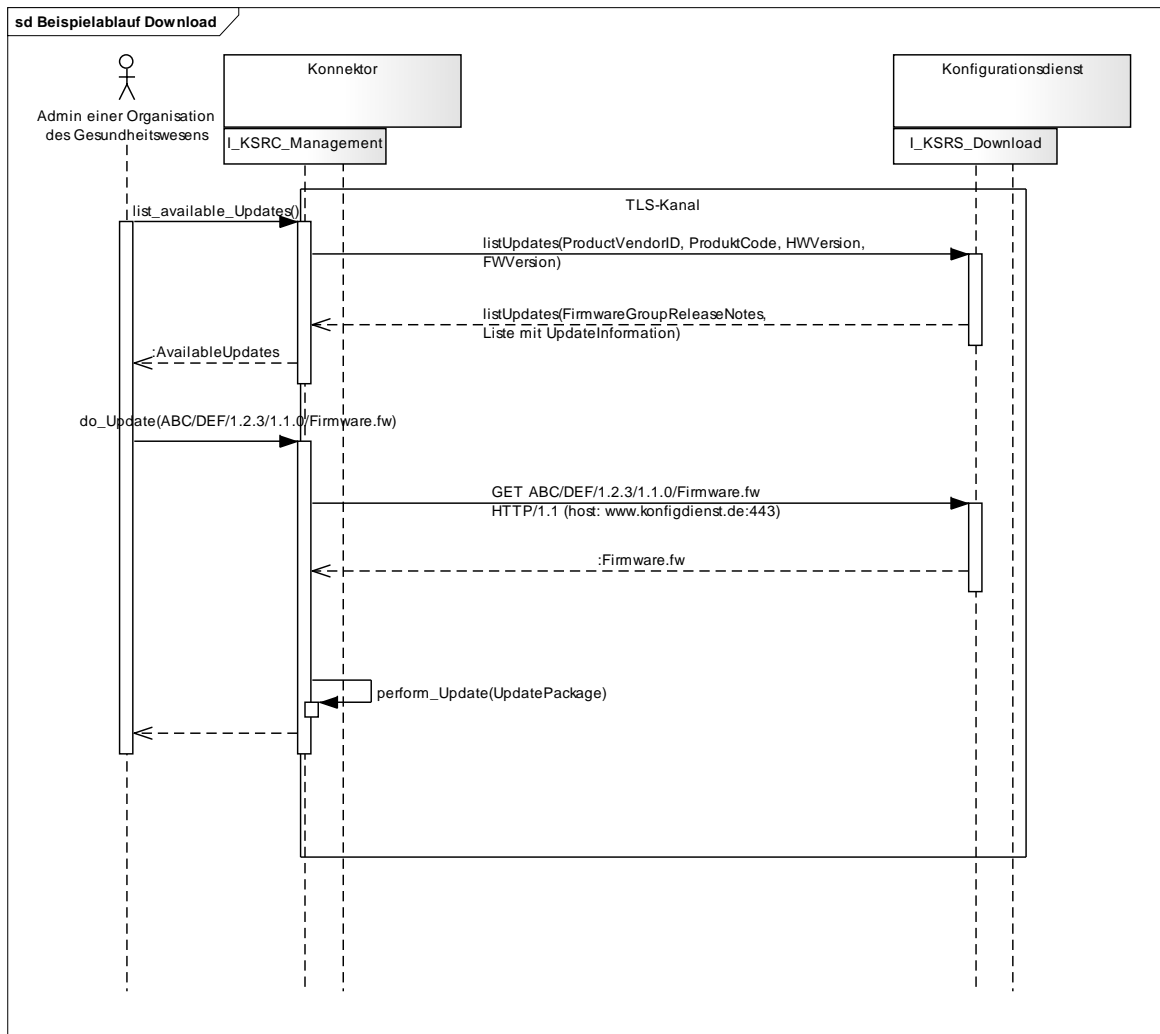


Abbildung 16: Abb\_KSR\_015 Beispielablauf für ein Firmware Update

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.

## Anhang C – Konfigurationsdatenfile zur Anbindung von Bestandsnetzen

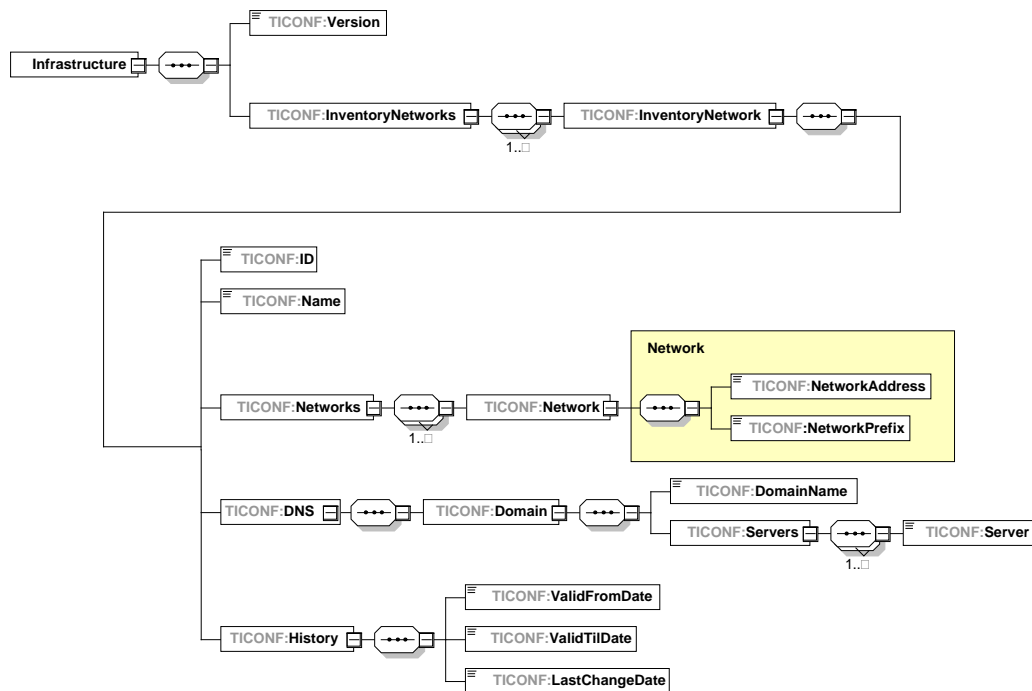


Abbildung 17: Abb\_KSR\_014 Schema InfrastrukturKonfig.xsd

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	Identifizier 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