Schnittstellen- und Prozessspezifikation Konfigurationsdienst

Version:	1.9.0
Stand:	01.04.2015
Status:	Freigegeben
Klassifizierung:	öffentlich
Referenzierung:	ARV_706.3_Spec_SST_KSR

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um eine überarbeitete Version des Dokumentes gemäß Güteprüfung. Die Änderungen zur letzten freigegebenen Version sind gelb markiert.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.1	09.01.14		Initiale Befüllung, Übernahme bisheriger Texte	ARV
0.0.2	13.01.14		Definition der Schnittstellen, Defintion Update-Pakete.	ARV
0.0.3	16.01.14		Review einarbeiten, Abstimmung, Signatur-Verfahren	ARV
0.0.4	17.01.14		Review zur 1. Abstimmung	ARV
0.0.5	22.01.14		Logging, Operations-Schnittstelle, Download-Schnittstelle, Statistikdaten	ARV
0.0.6	24.01.14		Definition Anforderungen, Signatur „FirmwareGroupInfo.xml“	ARV
0.0.7	27.01.14		Review-Ergebnisse einarbeiten	ARV
0.0.8	28.01.14		Review-Ergebnisse einarbeiten	ARV
0.9.0	29.01.14		Bereitstellung zur internen QS, Glossar	ARV
0.9.1	30.01.14	1.2	Abstimmung Los 1 & 2	ARV
0.9.2	30.01.14		Anforderungsregister, Logging-Datenformat	ARV
0.9.3	03.02.14		Review Ergebnisse einarbeiten	ARV
1.0.0	06.02.14	alle	Freigegeben durch Release Board	ARV
1.0.1	04.03.14	alle	Überarbeitung nach Güteprüfung	ARV
1.1.0	05.03.14		Freigabe durch Release Board	gematik, ARV
1.1.1	11.02.14	6.1.2.4	Überarbeitung nach Güteprüfung	ARV
1.2.0	13.03.14		Freigabe Release-Mngt.	gematik
1.2.1	30.03.14	5.2; 6.1.1.5; 6.1.1.6; 6.1.3	Überarbeitung nach P11-Prüfung	ARV
1.3.0	27.08.14		Freigabe Release-Mngt.	gematik
1.3.1	16.12.14	5.1.1	Anpassung Gruppen und Berechtigungen	ARV
1.4.0	19.12.14		Freigabe Release-Mngt.	gematik

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.4.1	27.01.15	6.1.1.4; 6.1.1.7; A5.2	Angaben zu notwendigen Parametern (signedAttrs) für die Erstellung von Signaturen	ARV
1.5.0	30.01.15		Freigabe Release-Mngt.	gematik
1.5.1	04.02.15	6.1.1.4	Korrektur OIDs	ARV
1.5.2	17.02.15	6.1.1.4; 6.1.1.7	Anpassung zu KSR Release 1.0.5	ARV
1.6.0	20.02.15		Freigabe durch Release-Mngt.	gematik
1.6.1	10.03.15	6.1.1.4; 6.1.1.7; 7.2	Anpassung zu KSR Release 1.0.7	ARV
1.6.2	11.03.15	6.1.1.4	Anpassung gemäß Mängelliste, Review	ARV
1.7.0	11.03.15		Freigabe Release Mngt.	gematik
1.7.1	24.03.15	6.1.1.7	Anpassung zu KSR Release 1.0.8	ARV
1.8.0	24.03.15		Freigabe Release Mngt.	gematik
1.8.1	31.03.15	6.1.1.7	Anpassung zu KSR Release 1.0.9	ARV
1.9.0	01.04.15		Freigabe Release Mgmt.	ARV
1.9.0	09.04.15	Titel	Status auf „Freigegeben“ umgesetzt	ARV

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Schnittstellen und Prozesse des Produkttyps Konfigurationsdienst und wird in Teilen mit den Herstellern von Konnektoren und Kartenterminals abgestimmt.

1.2 Zielgruppe

Das Dokument ist maßgeblich für die Anbieter der Lose 1, 2 und 3 des Vorhabens „Erprobung Online-Rollout (Stufe 1)“ sowie für Hersteller und Anbieter von weiteren Produkten zum Online-Rollout (Stufe 1).

Hinweis: Die vorliegende Version der Spezifikation wurde mit ORS1 Los 2 in den relevanten Spezifikationsanteilen (insbes. Integritäts- und Authentizitätsschutz von Update-Paketen) abgestimmt.

1.3 Geltungsbereich

Dieses Dokument enthält die Schnittstellenbeschreibung für den Produkttyp Konfigurationsdienst für die Telematikinfrastruktur des Deutschen Gesundheitswesens für den Online-Rollout (Stufe 1). Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Abgrenzungen

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang A5).

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

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zu den Themenbereichen

- Implementierung und Architektur,
- Layout der Webseiten,

- Prozesse anderer Produkttypen,
- Beantragung, Administration, Sperrung und Löschung von Benutzeraccounts für den Zugriff auf Produkte in der TI,
- Bereitstellung von Zertifikaten. Die Zertifikate werden über die Infrastructur-CA beantragt und werden im Folgenden zum Signieren der Update-Pakete durch den Hersteller von Konnektoren und Kartenterminals benötigt.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern 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:

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0000 <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Systemüberblick

2.1 Komponenten des Konfigurationsdienstes

Der Konfigurationsdienst besteht aus mehreren Komponenten, welche durch Firewalls getrennt in verschiedenen Sicherheitszonen verteilt sind. Der Konfigurationsdienst ist in drei Bereiche unterteilt:

- Upload-Bereich: Auf diesen Bereich greift der berechtigte Hersteller von Konnektoren oder Kartenterminals über das Internet zu, um Updates einzustellen. Er besteht aus einem Webserver, der das Frontend bereitstellt. Dieser Bereich implementiert die organisatorische Schnittstelle P_KSRS_Upload.
- Konfigurationsbereich: In diesem Bereich erfolgt die Freigabe der Updates. Eine Process Engine übernimmt die Ausführung der implementierten Prozesse. Der User erhält jeweils über das Frontend eine Aufgabenliste zur Abarbeitung der anstehenden Punkte innerhalb des Prozesses. Dieser Bereich implementiert die organisatorische Schnittstelle P_KSRS_Operations.
- Download-Bereich (incl. dem Download-Cache): In diesem Bereich werden die Updates für die dezentralen Komponenten zur Verfügung gestellt. Dieser Bereich stellt die Schnittstelle I_KSRS_Download zur Verfügung.

Eine Übertragung von Daten und Zuständen zwischen den einzelnen Umgebungen (RU, TU und PU) ist dabei wie gefordert ausgeschlossen, jede Umgebung verfügt über eine eigenständige Instanz des Produkttyps KSR und arbeitet unabhängig vom Zustand der anderen Umgebungen.

2.2 Übersicht

Schematisch stellt sich der Konfigurationsdienst wie auf folgendem Diagramm dar. Zu jedem der drei Bereiche gibt es eine Schnittstelle, die durch die jeweilige Benutzergruppe angesprochen werden kann. Die Bereiche sind inhaltlich und technisch voneinander getrennt und können nur über Schnittstellen durch Firewalls kommunizieren.

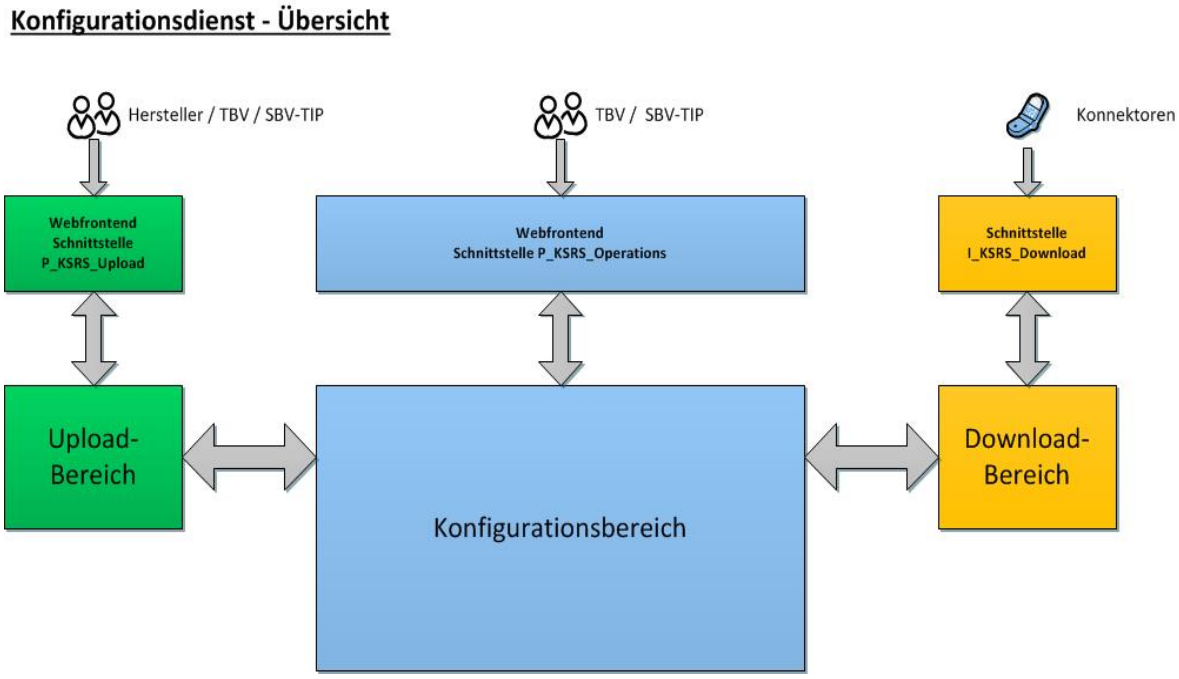

Abbildung 1 Konfigurationsdienst - Übersicht

3 Systemkontext

3.1 Akteure und Rollen

Die Akteure und Rollen sind in der Spezifikation [gemSpec_KSR#3.1] beschrieben, zum besseren Verständnis der Spezifikation, wird hier eine kurze Zusammenfassung dargestellt.

Grundsätzlich existieren drei getrennte Umgebungen, auf denen jeweils eine Instanz des Produkttyps Konfigurationsdienst installiert ist.

- Referenzumgebung (RU)
- Testumgebung (TU)
- Produktivumgebung (PU)

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

Durch den Hersteller der dezentralen Komponente wird das Update-Paket in die jeweilige Umgebung geladen und dort von dem jeweiligen Akteur bearbeitet (z.B. Freigegeben).

Der Akteur „Konnektor“ kann nur auf den Download-Bereich zugreifen und über die dort definierten Schnittstellen, die entsprechenden Informationen abrufen.

Im Folgenden bezeichnet der Begriff „Hersteller“, den Hersteller von Konnektoren und Kartenterminals.

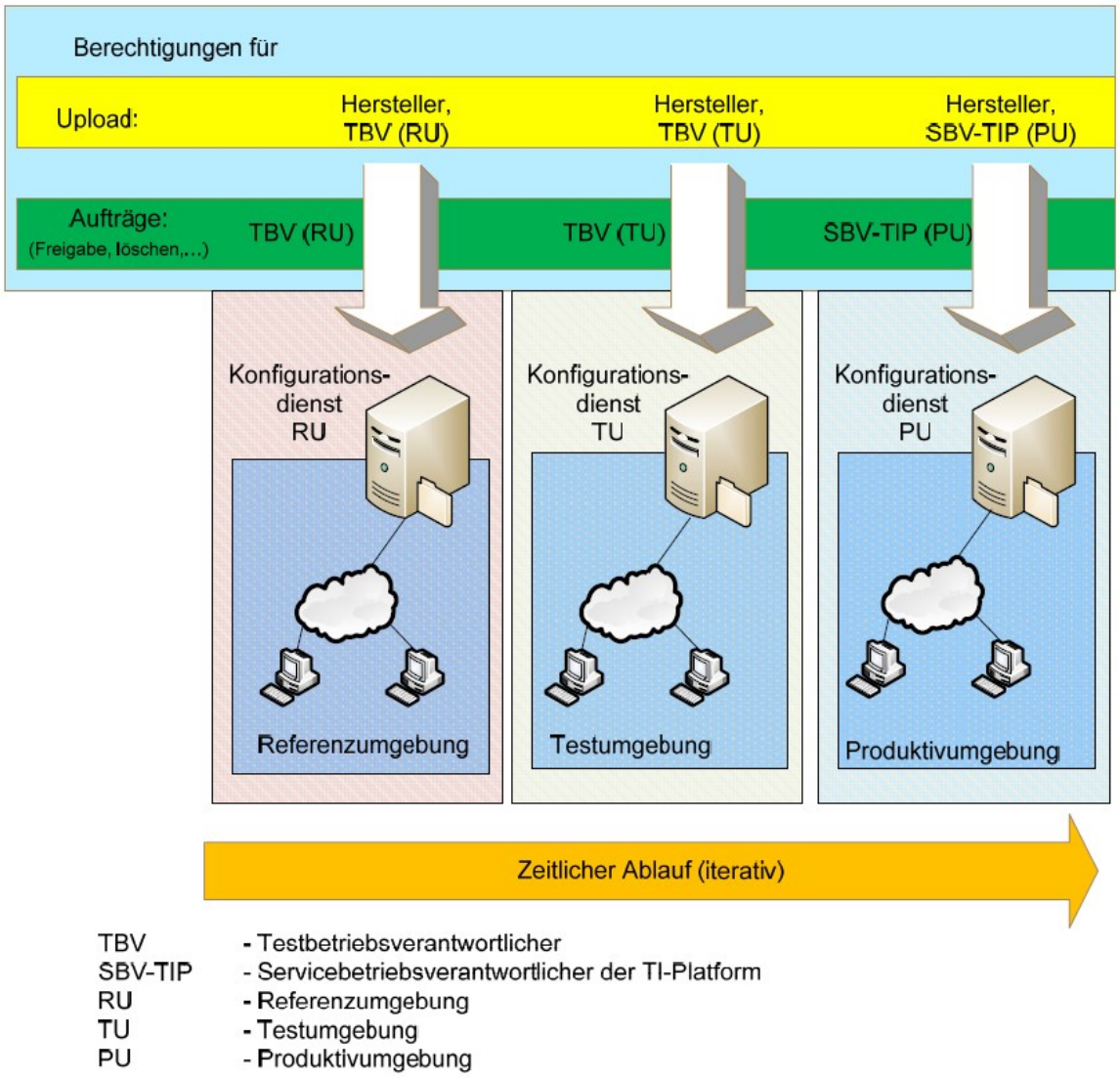

Abbildung 2 Überblick externe Akteure Konfigurationsdienst [gemSpec_KSR#Abb_KSR_001]

3.2 Nachbarsysteme

Die Nachbarsysteme sind in der Spezifikation [gemSpec_KSR#3.2] beschrieben.

4 Zerlegung des Produkttyps

Die Zerlegung des Produkttyps Konfigurationsdienst sind in der Spezifikation [gemSpec_KSR#4] beschrieben.

5 Übergreifende Festlegungen

5.1 Registrierung berechtigter Hersteller / TBV / SBV-TIP in KSR

Die Freischaltung von Herstellern (und TBV/SBV-TIP) zur Nutzung des Konfigurationsdienstes ist nicht Bestandteil des Konfigurationsdienstes. Die Beantragung eines Zuganges wird außerhalb des KSR in einem Betriebsprozess abgebildet, siehe dazu [ARV_706.3_KPT_Betr_V1#4.3.13]. Dieser Prozess sieht vor, dass der Versand der notwendigen Hardware Token und Authentifizierungsinformationen (User/Pin/Passwort) über getrennte Wege erfolgen. Der Hardware Token über Post per Einschreiben und der Versand von User/Pin/Passwort wird über zertifikatsbasierende verschlüsselte / signierte E-Mail erfolgen. 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 bekommen nur die Berechtigung sich im Upload-Bereich anzumelden, Update-Pakete hochzuladen und Statistikdaten (siehe Kapitel 7.1) 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 beim Login des Anwenders durch den Konfigurationsdienst durch die Zugehörigkeit eines Anwenders zu einer Berechtigungsgruppe des Konfigurationsdienstes ermittelt.

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0037 Registrierung berechtigter Akteure**

Der Hersteller, TBV, SBV-TIP MUSS den Zugang über einen Betriebsprozess [ARV_706.3_KPT_Betr_V1] beantragen.⌫

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0038 Login berechtigter Akteure**

Der Hersteller, TBV, SBV-TIP MUSS sich mit den Zugangsdaten anmelden, die er bei der Freischaltung für den Konfigurationsdienst erhalten hat.⌫

5.1.1 Berechtigungs- und Rollenkonzept

Sofern in dem hier vorliegenden Dokument von Herstellern, TBV, SBV-TIP oder allgemein von Akteuren (außer Konnektoren) gesprochen wird, sind damit aus technischer Sicht Anwender mit einer oder mehreren Rollen gemeint. Jede Rolle besitzt unterschiedliche Berechtigungen innerhalb des Konfigurationsdienstes.

Tabelle 1 Gruppen und Berechtigungen

Rolle / Gruppe	Berechtigung
Hersteller_RU	Die Rolle kann sich an der Web-Applikation des Upload-Bereichs in RU anmelden, Pakete hochladen, den Status einsehen und Statistikdaten herunterladen.

Rolle / Gruppe	Berechtigung
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.
~~CONFIG_RU~~	~~Die Rolle kann Konfigurationsdatenfiles für RU hochladen, freigeben oder ablehnen und kann zusätzlich zu TBV_RU erteilt werden.~~
~~CONFIG_TU~~	~~Die Rolle kann Konfigurationsdatenfiles für TU hochladen, freigeben oder ablehnen und kann zusätzlich zu TBV_TU erteilt werden.~~
~~CONFIG_PU~~	~~Die Rolle kann Konfigurationsdatenfiles für PU hochladen, freigeben oder ablehnen und kann zusätzlich zu SBV_PU erteilt werden.~~

Den Akteuren der Web-Applikationen sind jeweils Rollen ihrer Umgebung zugewiesen.

Im vorliegenden Dokument gehen wir von folgenden Rollenzugehörigkeiten aus. Die Zuordnung dient ausschließlich als Beispiel für dieses Dokument.

Tabelle 2 Beispiel Gruppenzuordnung

Akteur	Mitgliedschaft in Gruppe
Hersteller	Hersteller_PU, Hersteller_TU und Hersteller_RU
TBV	Hersteller_TU, Hersteller_RU, TBV_RU, TBV_TU~~, CONFIG_RU, CONFIG_TU~~
SBV-TIP	Hersteller_PU, SBV_PU~~, CONFIG_PU~~

5.2 Integritäts- und Authentizitätsschutz der Pakete in KSR

Zum Schutz der Integrität der Konnektoren und Kartenterminals ist es wichtig, jederzeit im Prozessablauf sicherzustellen, dass keine Manipulationen an den Update-Paketen des Herstellers vorgenommen wurden. Die Zertifikate für den KSR können analog zu den CMP-Identitäten von der Infrastruktur-CA [ARV_706.3_Spec_SST_Komponenten-PKI#2.1] ~~der TI~~ bezogen werden. Dazu wird ein eigenes Zertifikatsprofil erstellt werden. Der Prozess zur Zertifikatsausgabe ist in [ARV_706.3_Spec_SST_Komponenten-PKI#5.2.3] beschrieben. Mit dem erstellten Zertifikat kann der Hersteller der dezentralen Komponente die jeweiligen Update-Pakete (und Firmware-Gruppen-Informationen)

signieren. Durch die Signatur kann die Integrität und Authentizität der Update-Pakete jederzeit durch den Konfigurationsdienst sichergestellt werden. Die genaue Ausgestaltung dieses Schutzmechanismus wird in Kapitel 6.1.1.4 beschrieben.

Nach dem Upload werden die Update-Pakete einer Eingangsprüfung unterzogen, ungültige Pakete werden abgewiesen [TIP1-A_3346], siehe dazu Kapitel 6.1.2.4:

- Prüfung der Integrität und Authentizität
- Prüfung auf syntaktische Korrektheit
- Prüfung auf Vollständigkeit

Der Konfigurationsdienst enthält einen Service, der es während der Verarbeitung jederzeit ermöglicht, eine Überprüfung der Integrität des Update-Paketes durchzuführen. Insbesondere bei der Freigabe und der darauf folgenden Übermittlung an den Download-Bereich, wird die Signatur bzw. die Integrität überprüft. Damit wird sichergestellt, dass das im Download-Bereich bereitgestellte Update-Paket identisch mit dem vom Hersteller übertragenem Update-Paket ist und keine Manipulationen bei der Verarbeitung des Paketes vorgenommen wurden.

Alle Operationen wie Upload, Prüfung incl. Resultat oder Freigabe des Update-Pakets werden revisionssicher protokolliert [TIP1-A_3345], siehe dazu Kapitel 7.2.

5.3 Behandlung von Zertifikaten im KSR

Zum Schutz der Update-Pakete und deren Teilinformationen werden Signaturen verwendet. Der KSR verifiziert bzw. prüft nur die Signaturen der folgenden Informationsobjekte

- Update-Paket (Gesamtpaket)
- Firmware-Gruppen-Information (Teilinformation)

Die Signatur des Informationsobjekts „UpdateInformation“ wird vom KSR transparent behandelt und inhaltlich nicht geprüft.

Tabelle 3 Schutzanforderung der Update-Pakete [gemSpec_KSR#5.1]

Informationsobjekt	Schutzanforderungen	Prüfung durch
Update-Paket	Integritäts- und Authentizitätsschutz Gesamtpaket durch Hersteller.	Konfigurationsdienst, durch die Signatur des Update-Paketes, siehe Kapitel 6.1.1.4.
Update-Paket, Element UpdateInformation	Integritäts- und Authentizitätsschutz durch Hersteller	Konnektor
Update-Paket, Element Firmwarefiles	Integritäts- und Authentizitätsschutz durch Hersteller	Konnektor, Kartenterminals
Update-Paket, Element Documentationfiles	Keine	-

Informationsobjekt	Schutzanforderungen	Prüfung durch
Update-Paket, Element Firmware-Gruppen-Information	Integritäts- und Authentizitätsschutz durch Hersteller	Konfigurationsdienst, durch die Signatur des Update-Paketes, siehe Kapitel 6.1.1.7.

6 Funktionsmerkmale

6.1 Schnittstellen des Konfigurationsdienstes

Der Konfigurationsdienst stellt drei Schnittstellen bereit, die im Folgenden definiert werden.

Die Akteure benötigen für den Zugriff auf die organisatorischen Schnittstellen einen Zugang mit den entsprechenden Berechtigungen, der in einem separaten Prozess / System beantragt werden muss (siehe Kapitel 5.1). Im weiteren Verlauf wird davon ausgegangen, dass die Akteure entsprechende Zugänge beantragt haben und diese eingerichtet sind.

Es existiert keine Verbindung zwischen der Referenz-, Test- und Produktionsumgebung. Das Update-Paket muss jeweils vom Hersteller in den Upload-Bereich der jeweiligen Umgebung geladen werden. Durch einen organisatorischen Prozess erhält der TBV/SBV-TIP Arbeitsaufträge (z.B. Prüfung des Update-Paketes, Löschen eines Update-Paketes) und führt diese im Konfigurationsbereich der jeweiligen Umgebung aus. Ein Übergang der Update-Pakete zwischen den Umgebungen ist ausgeschlossen. Die beschriebenen Prozesse und Schnittstellen sind in den Umgebungen identisch implementiert. Die Bereitstellung eines Update-Paketes im Download-Bereich wird erst nach der Freigabe durch den TBV/SBV-TIP der Umgebung durchgeführt.

6.1.1 Schnittstelle P_KSRS_Upload

Die Schnittstelle P_KSRS_Upload ist eine organisatorische Schnittstelle und wird durch den Konfigurationsdienst in Form einer Web-Applikation bereitgestellt. Die berechtigten Akteure erhalten über diese Applikation die Möglichkeit Update-Pakete in die jeweilige Umgebung zur Überprüfung hoch zu laden. Die Überprüfung und Freigabe durch den TBV/SBV-TIP ist ein weiterer Prozess, der durch den Upload gestartet wird. Der Freigabe-Prozess wird in der Schnittstelle P_KSRS_Operations definiert (siehe Kapitel 6.1.2).

Alle Aktionen eines Benutzers werden mit Beauftragung, Auftragsbestätigung und Ausführung (inkl. Fehlerfall) geloggt, siehe dazu Kapitel 7.2.

Statistikdaten werden dem Akteur ebenfalls in dem Web-Frontend zum Download bereitgestellt. Das Format der Statistikdaten ist in Kapitel 7.1 definiert.

Das Web-Frontend erfüllt die Forderung der parallelen Nutzung durch mehrere Anwender [TIP1-A_5042].

Der Zugriff auf das Web_Frontend erfolgt ausschließlich über HTTPS (TLS 1.1/1.2). Die Web-Applikation erhält zur Absicherung der Verbindung ein entsprechendes Zertifikat durch TI.

6.1.1.1 Prozessdefinition „Upload“

Der Prozessablauf für den Upload eines Update-Paketes durch Hersteller, bzw. TBV/SBV-TIP wird wie folgt definiert:

(1) Der Hersteller ruft KSR-Web-Applikation für den Upload-Bereich der jeweiligen Umgebung auf und authentifiziert sich mittels des hierfür vorgegebenen Verfahrens.

(2) Auf der Übersichtsseite wählt der Hersteller die Funktionalität „Upload“ aus und wird auf eine weitere Webseite geleitet.

(3) Auf der Webseite werden das Update-Paket und die dazugehörige Signaturdatei ausgewählt und beim Druck des Buttons „Upload“ in den Upload-Bereich des Konfigurationsdienstes übertragen. Die Webseite wird geschlossen und die Übersichtsseite wird wieder angezeigt.

(4) Der Server nimmt die Dateien entgegen und speichert diese im Filesystem ab.

(5) Sobald der Upload der Dateien erfolgreich beendet wurde, schickt der Server eine Information über den erfolgten Upload an den Konfigurationsbereich des Konfigurationsdienstes und startet damit den Freigabeprozess.

(6) Der Hersteller kann den Status des hochgeladenen Update-Paketes in der Übersicht verfolgen (Siehe Tabelle 13 Status Definition). Sofern bei der Überprüfung Fehler aufgetreten sind, kann sich der Hersteller in der Übersichtseite eine Fehlerbeschreibung anzeigen lassen.

(7) Auf der Übersichtsseite kann der Akteur Statistikdaten des jeweiligen Update-Paketes als Datei herunterladen. Die Beschreibung des Inhaltes und des Dateiformates wird in Kapitel 7.1 aufgeführt.

6.1.1.2 Schnittstellendefinition

Der Hersteller 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.

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0018 Name des Update-Paketes**

Der Hersteller MUSS den Dateinamen so wählen, das er dem Pattern „[A-Za-z0-9_-.]*“ entspricht und nicht länger als 32 Zeichen ist.⌫

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0001 Definition Update-Paket Struktur**

Hersteller von Konnektoren oder Kartenterminals MÜSSEN Update-Pakete mit den in Tabelle 4 (Struktur Update-Paket) definierten Elementen in Form eines ZIP-Containers nach dem Standard [ZIP-APP] erzeugen.⌫

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0019 Passwort des Update-Paketes**

Der Hersteller DARF NICHT den ZIP-Container mit einem Passwort schützen.⌫

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0002 Größe des Update-Paketes**

Der Hersteller DARF NICHT Update-Pakete hochladen, deren entkomprimierte Paketgröße dem abgestimmten Maximalwert übersteigt. ⌫

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

Das Update-Paket enthält folgende Elemente im Wurzelverzeichnis des Containers:

Tabelle 4 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

⌦ ARV_706.3_Spec_SST_KSR_AFO_0003 Update-Paket - Dateinamen und Unterverzeichnisse

Der Hersteller MUSS folgende Vorgaben im ZIP-Container erfüllen:

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

⌦ ARV_706.3_Spec_SST_KSR_AFO_0004 Update-Paket – Übertragung „Firmware-Gruppen-Information“

Der Hersteller MUSS, 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.⌫

⌦ ARV_706.3_Spec_SST_KSR_AFO_0022 Update-Paket – Dateinamen der UpdateInformation Detached-Signatur

Der Hersteller MUSS, sofern das Update-Paket eine Detached-Signatur des Elementes „UpdateInformation“ enthält, die Signatur in der Datei mit dem Namen „UpdateInfo.sig“ speichern.⌫

⌦ ARV_706.3_Spec_SST_KSR_AFO_0023 Update-Paket – Dateinamen der FirmwareGroupInfo Detached-Signatur

Der Hersteller MUSS, sofern das Update-Paket eine Detached-Signatur des Elementes „Firmware-Gruppen-Information“ enthält, die Signatur in der Datei mit dem Namen „FirmwareGroupInfo.sig“ speichern.⌫

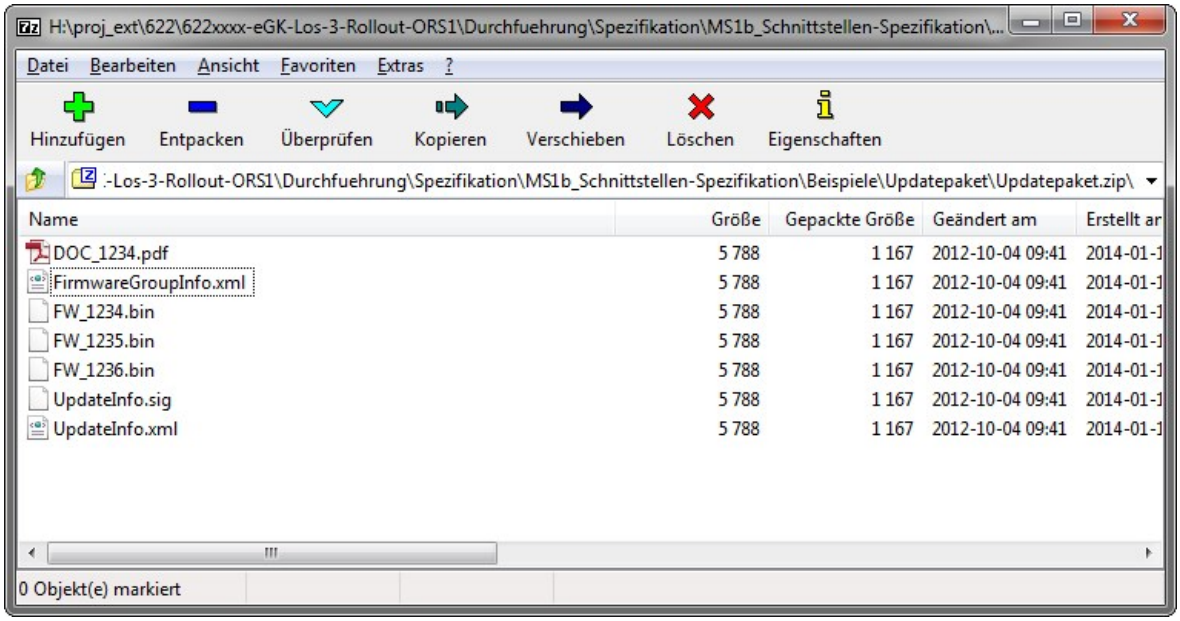

Abbildung 3 Beispiel Struktur Update-Paket

6.1.1.3 Pfadreferenzen

Sofern die Dateien des Update-Paketes über die Schnittstelle I_KSRS_Download::getUpdates heruntergeladen werden sollen, 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.

⌦ ARV_706.3_Spec_SST_KSR_AFO_0005 Pfadreferenz

Der Hersteller MUSS alle Pfadangaben nach folgenden Vorgaben aufbauen:

- Schema: /<ProductVendorId>/<ProductCode>/<UpdateID>/<Filename>
- Als Trennzeichen wird 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 6.1.1.2) 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.

6.1.1.4 Verfahren zum Erstellen eines signierten Update-Paketes

Der Hersteller hat durch die Infrastruktur-CA der TI [ARV_706.3_Spec_SST_Komponenten-PKI] ein X.509-Zertifikat mit einem Private-Key zum Signieren der Dateien erhalten. Mit diesem Zertifikat kann der Hersteller mit Hilfe eines Tools die Update-Pakete signieren. Die Grundlage des Signaturverfahrens ist in [gemSpec_Krypt#3.7] definiert. Darin ist der Signaturstandard [ETSI-CAdES] vorgegeben.

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

Folgendes Verfahren wird angewendet zur Verifikation der Signatur der Datei:

1. Der Hersteller erstellt ein Update-Paket.
2. Der Hersteller signiert das Update-Paket mit seinem Zertifikat 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.

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0007 Update-Paket – Signatur**

Der Hersteller MUSS eine detached PKCS#7-Signatur zum Update-Paket mit Signatur-Algorithmus Algorithmus "RSASSA-PKCS1-v1_5 mit SHA256" oder "RSASSA-PSS mit SHA256" erstellen. Das Feld certificates des Feldes signedData der Signatur MUSS das Zertifikat der Signatur enthalten (Validation Policy zu [ETSI-CAdES#5.4]). Das Feld signedAttrs der Signatur MUSS die Attribute content-type (OID 1.2.840.113549.1.9.3), message-digest (OID 1.2.840.113549.1.9.4) und ESS signing-certificate-v2 (OID 1.2.840.113549.1.9.16.2.47) enthalten laut [ETSI-CAdES#5.7]. Die Signatur-Algorithmen sind in [GS-A_5080] der [gemSpec_Krypt] definiert.⌫

~~Der Hersteller MUSS das Update-Paket mit einer gültigen Signatur nach den in [gemSpec_Krypt#3.7] definierten Anforderungen signieren, eine PKCS#7 Detached-Signature erstellen und beide Dateien in den Upload-Bereich hochladen.~~

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0029 Zertifikat**

Der Hersteller MUSS bei der Infrastruktur-CA der TI ein Zertifikat zum Signieren der Update-Pakete im Konfigurationsdienst bestellen und die Update-Paket mit diesem Zertifikat signieren. ⌫

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0030 Upload der Update-Paketes**

Der Hersteller MUSS das Update-Paket mit der erzeugten Signatur in den Konfigurationsdienst über die organisatorische Schnittstelle P_KSRS_Upload hochladen. ⌫

6.1.1.5 Definition Element „UpdateInformation“

Diese Definition ergänzt und verdeutlicht die Definition des Typs „UpdateInformation“ aus der Defintionsdatei „Konfigurationsdienst.xsd“ und der Spezifikation [gemSpec_KSR]. Konkretisierungen gegenüber der Spezifikation sind durch AFO’s definiert.

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0008 UpdateInfo.xml - Format**

Der Hersteller MUSS die Datei UpdateInfo.xml nach folgenden Vorgaben erstellen:

- Die Datei verwendet das charset-encoding „UTF-8“
- Die Datei definiert den Namespace http://ws.gematik.de/ksr/v1.1 ~~v1.0~~ als Default-Namespace. Es ist keine „schemaLocation“ enthalten. Die Validierung erfolgt ausschließlich mit lokalen Schema-Dateien im jeweiligen System.
- Die Datei kann gegen das XSD Schema „Konfigurationsdienst.xsd“ validiert werden.⌫

Tabelle 5 UpdateInformation - Element UpdateID

Bezeichnung	UpdateID
Beschreibung	Identifiziert das Update eindeutig.
Befüllung	Hersteller von Konnektoren und Kartenterminals
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML Datentyp „string“ mit dem Pattern „[a-zA-Z0-9_]*“. Maximale Länge: 32 Zeichen Die UpdateID ist vom Hersteller 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, siehe Kapitel 6.1.1.3.

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0009 UpdateInfo.xml – UpdateID**

Der Hersteller MUSS das Element UpdateID nach folgenden Vorgaben füllen:

- Die UpdateID entspricht dem Pattern „[a-zA-Z0-9_]*“
- Die UpdateID ist nicht länger als 32 Zeichen.
- Die UpdateID muss für jedes Update-Paket eindeutig sein und darf nicht wiederverwendet werden.⌫

Eine einmal benutzte ID für einen Upload kann auch im Falle einer nicht bestandenen Eingangsprüfung mit anschliessender Löschung des Paketes nicht ein weiteres mal genutzt werden.

Tabelle 6 UpdateInformation - Element Firmware.Firmwarefiles.Filename

Bezeichnung	Firmware.Firmwarefiles.Filename
Beschreibung	Filename inklusive relativem Pfad. Dieser Wert wird in Operation I_KSRS_Download::getUpdates HTTP Request als Parameter <path> genutzt.
Befüllung	Hersteller von Konnektoren und Kartenterminals. Der relative Pfad muss der Definition in Kapitel 6.1.1.3 genügen und am Ende einen Filename enthalten, der im Update-Paket eindeutig zu finden ist.
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML Datentyp „string“

Tabelle 7 UpdateInformation - Element Firmware.Documentationfiles.Filename

Bezeichnung	Firmware.Documentationfiles.Filename
Beschreibung	Filename inklusive relativem Pfad. Dieser Wert wird in Operation I_KSRS_Download::getUpdates HTTP Request als Parameter <path> genutzt.
Befüllung	Hersteller von Konnektoren und Kartenterminals. Der relative Pfad muss der Definition in Kapitel 6.1.1.3 genügen und am Ende einen Filename enthalten, der im Update-Paket eindeutig zu finden ist.
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML Datentyp „string“

Tabelle 8 UpdateInformation - Element UpdateInformationSignature

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

Wertebereich	Any (Vom Hersteller festzulegen)

Das nachfolgende Beispiel zeigt eine ausgefüllte UpdateInfo.xml. Die Datei definiert zwei Firmware-Dateien und eine Dokumentationsdatei. 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 4 Beispiel UpdateInfo.xml

6.1.1.6 Definition Element „Firmware-Gruppen-Information“

Diese Definition ergänzt und verdeutlicht die Definition des Typs „FirmwareGroupInformation“ aus der Definitionsdatei „Konfigurationsdienst.xsd“ und der Spezifikation [gemSpec_KSR].

Konkretisierungen gegenüber der Spezifikation sind durch AFO's definiert.

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0011 FirmwareGroupInfo.xml - Format**

Der Hersteller MUSS die Datei FirmwareGroupInfo.xml nach folgenden Vorgaben erstellen:

- Die Datei verwendet das charset-encoding „UTF-8"
- Die Datei definiert den Namespace http://ws.gematik.de/ksr/v1.1 ~~v1.0~~ als Default-Namespace.
- Es ist keine „schemaLocation" enthalten. Die Validierung erfolgt ausschließlich mit lokalen Schema-Dateien im jeweiligen System.
- Die Datei kann erfolgreich gegen das XSD Schema „Konfigurationsdienst.xsd" validiert werden. ⌫

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 Datei die aktuellen Firmware-Gruppen-Informationen. Das Dateiformat wird in diesem Kapitel genauer beschrieben. 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 liefert der Hersteller ein Update-Paket nach dem in Kapitel 6.1.1.2 beschriebenen Schema, das Paket ist jedoch nur mit dem Element „Firmware-Gruppen-Information" gefüllt (Siehe Kapitel 6.1.1.4). Die „Firmware-Gruppen-Information" wird durch den Hersteller so erstellt, dass das zurückgezogene Update nicht mehr im Download-Bereich über die Operation listUpdates angeboten wird.

Die Anforderung „[TIP1-A_3322] Firmware-Gruppenkonzept – Integritäts- und Authentizitätsschutz" wird durch die Signatur des Update-Paketes in Verbindung mit der Authentifizierung eines für den KSR-Upload berechtigten Akteurs erfüllt. Da eine Firmware-Gruppen-Information immer in einem Update-Paket verpackt und signiert wird, ist die Integrität und Authentizität der Information über die gesamte Lebenszeit gewährleistet.

Tabelle 9 Firmware-Gruppen-Information - Element FirmwareGroupID

Bezeichnung	FirmwareGroupID
Beschreibung	Identifiziert die Firmware-Gruppe eindeutig.

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

⌦ ARV_706.3_Spec_SST_KSR_AFO_0012 FirmwareGroupInfo.xml – FirmwareGroupID

Der Hersteller MUSS das Element FirmwareGroupID nach folgenden Vorgaben füllen:

- Die FirmwareGroupID entspricht dem Pattern „[a-zA-Z0-9_]*“
- Die FirmwareGroupID ist nicht länger als 32 Zeichen.⌫

Tabelle 10 Firmware-Gruppen-Information - Element FirmwareGroupVersion

Bezeichnung	FirmwareGroupVersion
Beschreibung	Die Versionsnummer der aktuellen Firmware-Gruppe. Laut GS-A_4868 [gemSpec_OM] muss die Firmware-Gruppe mit aufsteigenden Nummern versioniert werden. Der Inhalt wird als nummerisches Feld interpretiert.
Befüllung	Hersteller von Konnektoren und Kartenterminals
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML Datentyp „string“ mit dem Pattern „[0-9]*“. Maximale Länge 5 Zeichen.

⌦ ARV_706.3_Spec_SST_KSR_AFO_0016 FirmwareGroupInfo.xml – FirmwareGroupVersion

Der Hersteller MUSS das Element FirmwareGroupVersion nach folgenden Vorgaben füllen:

- Die FirmwareGroupVersion entspricht dem Pattern „[0-9]*“
- Die FirmwareGroupVersion ist nicht länger als 5 Zeichen.
- Die Versionierung der Firmware-Gruppe erfolgt mit aufsteigenden Nummern.⌫

Tabelle 11 Firmware-Gruppen-Information - Element FirmwareGroupSignature

Bezeichnung	FirmwareGroupSignature

Beschreibung	Dieses Element kann der Hersteller von Konnektoren und Kartenterminals zur Signatur der Firmware-Gruppen-Information nutzen. Die Signatur wird in Kapitel 6.1.1.7 definiert. Der Hersteller kann die Signatur auch als „Detached“-Signature nach dem in 6.1.1.7 definierten Verfahren im Update-Paket speichern. Sofern dieses Feld durch den Hersteller verwendet wird, entspricht der Inhalt des Feldes einer Detached-Signature in einem Base64-Codierten String.
Befüllung	Hersteller von Konnektoren und Kartenterminals
Optional	Ja
Wertebereich	Base64 codierter String, mit der Detached-Signature.

Das nachfolgende Beispiel zeigt eine ausgefüllte FirmwareGroupInfo.xml.

```
<?xml version="1.0" encoding="UTF-8"?>

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

</FirmwareGroupInformation>
```

Abbildung 5 Beispiel FirmwareGroupInfo.xml

6.1.1.7 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].

⌦ ARV_706.3_Spec_SST_KSR_AFO_0024 Detached-Signature der FirmwareGroupInfo.xml

~~Der Hersteller MUSS die Signatur~~ Wenn eine Detached-Signature der FirmwareGroupInfo.xml ~~nach~~ genutzt wird, darf nicht gleichzeitig das in

ARV_706.3_Spec_SST_KSR_AFO_0025 beschriebene FirmwareGroupInfo.xml - Element „FirmwareGroupSignature“ genutzt werden.

KSR erwartet eine Detached-Signature (UTF-8-kodierte XML-Datei) mit folgenden ~~Vorgaben erstellen:~~ Eigenschaften zur Datei „FirmwareGroupInfo.xml“.

- Die Signatur ~~ist eine Detached-Signature~~ hat die XAdES-Form. Optionale XAdES-Attribute sind erlaubt, werden aber bei der Signaturprüfung ignoriert.
- Die Signatur erfolgt über das gesamte XML-Dokument nach ~~[XMLDSig]~~ 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 [GS-A_4370] aus [gemSpec_Krypt~~#3.1~~] und verwendet den Signatur-Algorithmus "RSASSA-PKCS1-v1_5 mit SHA256" oder "RSASSA-PSS mit SHA256". Die Signatur-Algorithmen sind in [GS-A_4371] der [gemSpec_Krypt] 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.

⌦ ARV_706.3_Spec_SST_KSR_AFO_0025 FirmwareGroupInfo.xml - Element „FirmwareGroupSignature“

Wenn das FirmwareGroupInfo.xml - Element „FirmwareGroupSignature“ genutzt wird, darf nicht gleichzeitig die in ARV_706.3_Spec_SST_KSR_AFO_0024 beschriebene Detached-Signature der FirmwareGroupInfo.xml im Paket enthalten sein bzw. genutzt werden. Der Hersteller MUSS bei Nutzung des Elementes „FirmwareGroupSignature“ in der Datei „FirmwareGroupInfo.xml“ - den Inhalt nach folgender Vorgabe erstellen:

- Die Signatur wird als Detached-Signature [ARV_706.3_Spec_SST_KSR_AFO_0024] erstellt.

- Die erstellte Signatur wird in einer UTF-8 kodierte XML-Datei gespeichert und diese als Base64-Codierter String in das Feld „FirmwareGroupSignature“ geschrieben⌫

6.1.1.8 UI-Masken

Disclaimer:

Die im Folgenden dargestellten UI-Masken dienen nur zur Übersicht und zur Visualisierung des Upload-Prozesses. Spätere Implementierungen werden dem zu definierenden Standard-Layout angepasst und können weitere Informationen und Aktionen enthalten.

Abbildung 6 UI-Maske Hersteller Login

Login-Maske des Upload-Bereichs. Zur Anmeldung am Upload-Bereich des Konfigurationsdienstes muss der Akteur seinen Benutzernamen, sein Passwort und das RSA-Token eingeben. Der Konfigurationsdienst verifiziert die eingegebenen Daten gegenüber IAM (Authentifizierungs- und Authorisierungsmanagement) und ermittelt die Rollen des angemeldeten Akteurs (siehe Kapitel 5.1.1). In den weiteren Masken kann der Akteur entsprechend seiner Rollen die Aktionen durchführen, bzw. Daten einsehen.

Sofern die Kombination aus Benutzername, Passwort und RSA-Token nicht korrekt authentifiziert werden konnte, wird eine Fehlermeldung eingeblendet und der Benutzer bleibt auf dieser Maske.

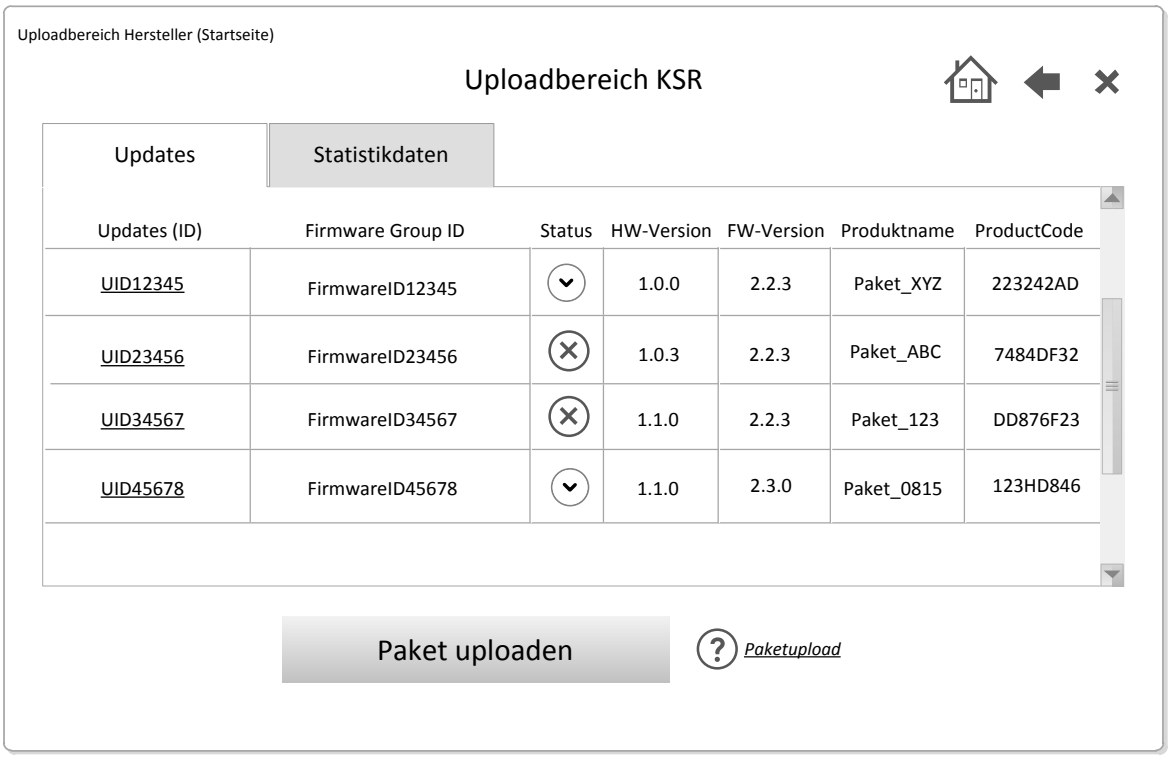

Abbildung 7 UI-Maske Übersicht Upload-Bereich – Updates

Hier hat der Akteur einen Überblick in alle seine bereits hochgeladenen Update-Pakete und kann die UpdateID sowie die FirmwareGroupID, den Status (z.B. genehmigt/abgelehnt), die Hardware- und Firmware-Version(en), den ProductCode, sowie den Produktnamen einsehen. Des Weiteren wird auf dieser Seite die Funktion des Paket-Uploads (Button) bereitgestellt (Weiterleitung auf die Uploadmaske).

Die oben rechts auffindbare Navigation erstreckt sich über alle Usermasken gleich (ausgenommen Login). Mit Klick auf das Haussymbol gelangt man auf die Startseite, die Übersichtseite der Updates des Upload-Bereichs. Der nach links zeigende Pfeil in der Mitte führt auf die vorherige Seite zurück. Das Kreuz rechts in der Navigation ist der Logout-Button.

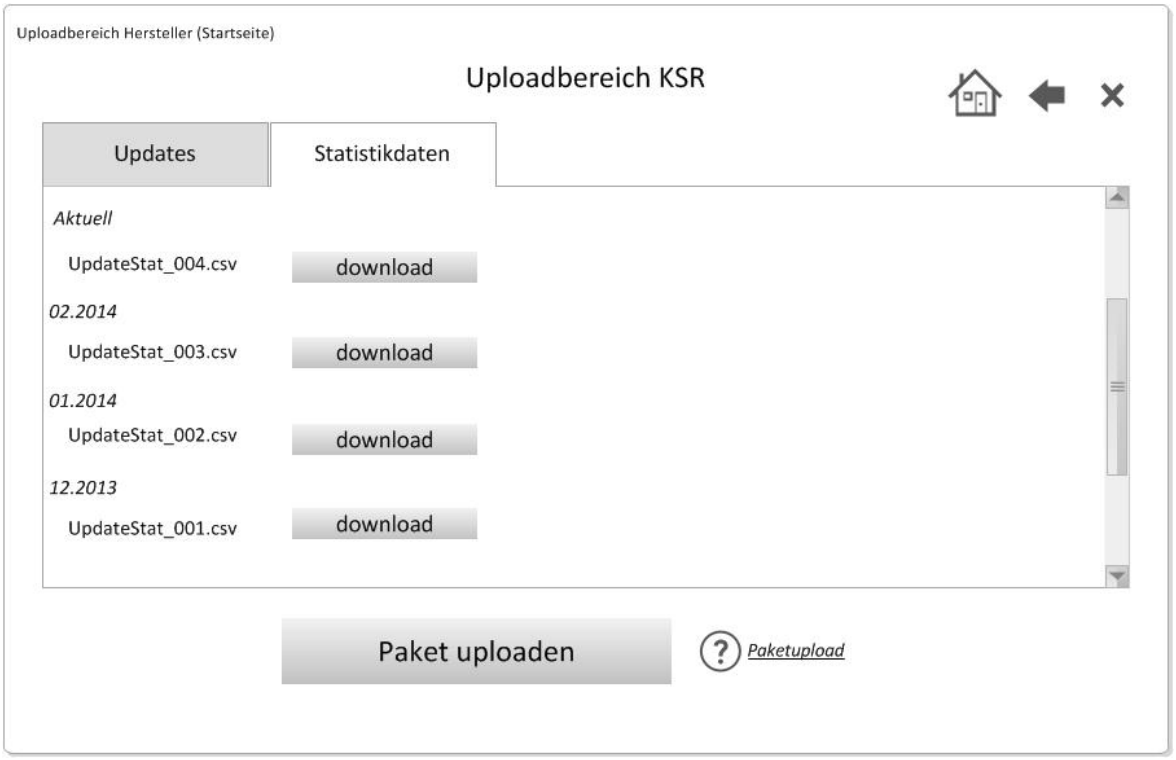

Abbildung 8 UI-Maske Übersicht Upload-Bereich - Statistikdaten

In der UI Maske „Upload-Bereich Statistikdaten“ kann der Akteur eine chronologische Auflistung (nach Monat absteigend) aller, für sein Produkte zur Verfügung stehenden Statistikdateien einsehen bzw. diese in Form einer CSV-Datei herunterladen. Ebenfalls wie in der Übersicht-Maske der Updates wird auch hier an selber Stelle der Paket-Upload bereitgestellt (Weiterleitung auf die Upload-Maske).Im Upload-Bereich werden nur Statistikdateien für die Produkte des jeweiligen Akteurs zum Download angeboten. Logging-Daten stehen dem TBV/SBV-TIP der Umgebung nur im Konfigurationsbereich zum Download zur Verfügung.

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0026 Berechtigung Statistikdaten**

Der Konfigurationsdienst DARF NICHT Statistikdaten anderer Hersteller anzeigen oder zum Download bereitstellen.⌫

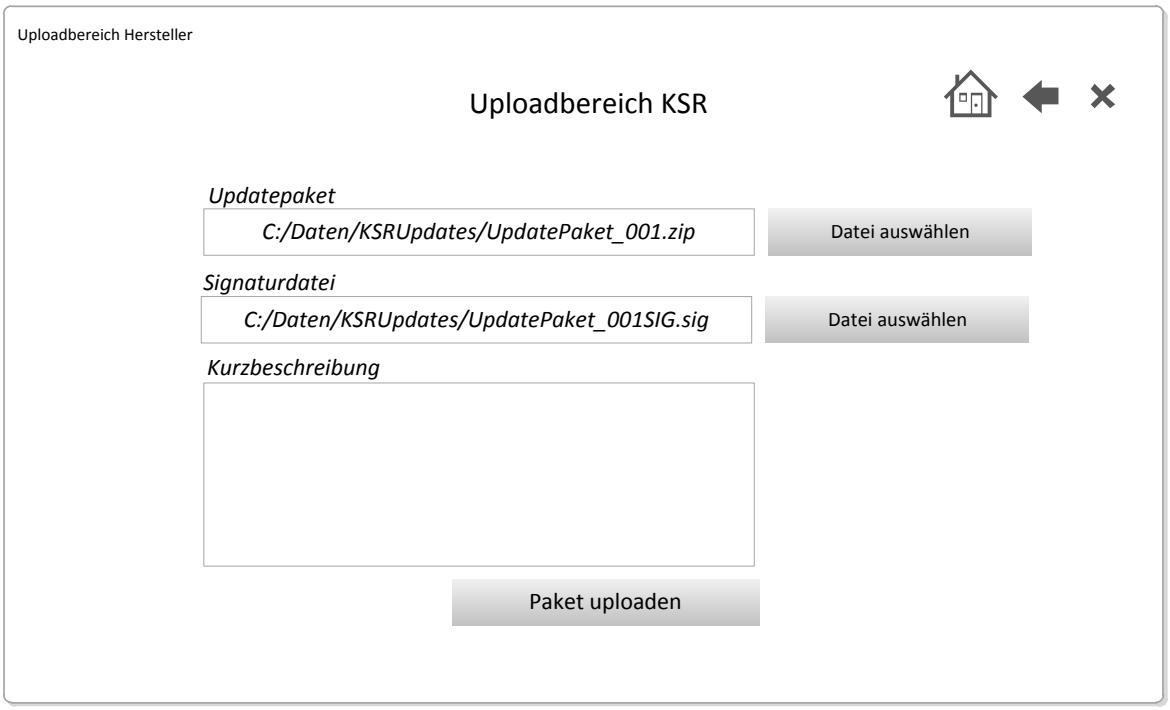

Abbildung 9 UI-Maske Upload

In der Upload-Maske lädt der Hersteller seine Update-Pakete hoch. Hierfür muss er das eigentliche Paket (zip-Datei), sowie eine entsprechende Signaturdatei (sig-Datei) auswählen und hat außerdem die Möglichkeit eine Kurzbeschreibung zu dem Paket für den Upload zu hinterlegen.

6.1.2 Schnittstelle P_KSRS_Operations

Die Schnittstelle P_KSRS_Operations ist eine organisatorische Schnittstelle für die verantwortlichen Akteure des Konfigurationsbereichs. Hersteller haben keinen Zugriff auf diese Schnittstelle, der Zugriff ist nur innerhalb der TI-Plattform möglich.

Wie die Schnittstelle P_KSRS_Upload wird die Schnittstelle in Form eines Web-Frontend durch den Konfigurationsdienst zur Verfügung gestellt (allerdings als eigenständige Komponente). Die Aufträge durch die berechtigten Akteure werden durch Aktionen auf der Web-Oberfläche abgebildet. Die vom Hersteller hochgeladenen Pakete werden dabei in Form einer Aufgaben-Liste angezeigt. Für diese Pakete kann der Akteur der Umgebung Aktionen starten, die die Aufträge des Akteurs an den Konfigurationsbereich abbilden. Eine Aktion wäre z.B. die Freigabe des Paketes für den Download-Bereich oder das Löschen eines Update-Paketes.

Das Web-Frontend erfüllt die Forderung der parallelen Nutzung durch mehrere Anwender [TIP1-A_5043].

Der Zugriff auf das Web_Frontend erfolgt ausschließlich über HTTPS (TLS 1.1/1.2). Die Web-Applikation erhält zur Absicherung der Verbindung ein entsprechendes Zertifikat durch TI. In der Aufgabenliste erscheinen für den Akteur nur die aktuell, in der jeweiligen Umgebung noch nicht freigegebenen Pakete, die einer seiner Berechtigungsgruppen zugeordnet sind (siehe Kapitel 5.1.1).

Alle Aktionen eines Benutzers werden mit Beauftragung, Auftragsbestätigung und Ausführung (incl. Fehlerfall) geloggt, siehe dazu Kapitel 7.2. Die Bereitstellung der geloggten Daten geschieht nach dem Verfahren für die Statistikdaten. Die Log-Dateien werden monatlich zusammengefasst und als CSV-Download dem jeweiligen TBV/SBV-TIP der Umgebung bereitgestellt.

Statistikdaten werden dem TBV/SBV-TIP ebenfalls im Web-Frontend des Konfigurationsbereiches der jeweiligen Umgebung zum Download bereitgestellt. Das Format der Statistikdaten ist in Kapitel 7.1 definiert.

Tabelle 12 Kurzbeschreibung Use Cases im Konfigurationsbereich

Use-Case	Beschreibung
Zugang	Die Anwender authentifizieren sich.
Updatedaten inkl. Dateien	Die Update-Pakete werden durch den Konfigurationsdienst vom Upload-Bereich abgeholt (pull).
Update-Pakete und Firmware-Gruppen-Informationen	Der TBV/SBV-TIP sieht in der Oberfläche alle Update-Pakete. Dabei kann er entsprechende Filterungen (Hersteller, Produkt, Status etc.) vornehmen. Der TBV/SBV-TIP gibt in dieser Oberfläche das Update-Paket frei. Nach dieser Freigabe kann die Weiterleitung der Updates inkl. Dateien in den Download-Bereich erfolgen. Alternativ dazu wird der Status „Abgelehnt“ für Update-Pakete, die nicht freigegeben werden können eingetragen.
Auftrag zur Deaktivierung von Update-Paketen	Der TBV/SBV-TIP kann die Deaktivierung (Löschung) von Update-Paketen beauftragen. Der Auftrag wird vom Konfigurationsdienst ausgeführt. Diese Update-Pakete werden im Download-Bereich und dem entsprechenden Service dann nicht mehr zur Verfügung gestellt. In Konfigurationsbereich wird dieses Paket als Archivversion aufbewahrt.
Statistikdaten	Die Statistikdaten werden aus den Download-Bereichen gesammelt und für die Hersteller aufbereitet. Diese Daten werden für die Hersteller im Upload-Bereich als CSV-Datei angeboten. Diese Statistikdaten können von den TBV/SBV-TIP ebenfalls als CSV-Datei heruntergeladen werden.
Logging-Daten	Die Logging-Daten der ausgeführten Aktionen werden gesammelt und ähnlich den Statistikdaten aufbereitet. Die gesammelten Logging-Daten können von den TBV/SBV-TIP als CSV-Datei heruntergeladen werden.
Übergabe von Konfigurationsdaten	Der TBV/SBV-TIP erstellt die Konfigurationsdaten und lädt diese in den Konfigurationsbereich.
Auftrag Freigabe von Konfigurationsdaten	Der TBV/SBV-TIP gibt die Konfigurationsdaten für den Download-Bereich frei. In der Oberfläche können die Beteiligten (TBV/SBV-TIP) ihre Aufträge mit dem jeweiligen Status einsehen und nach Datum, Produkt, Status usw. filtern.

6.1.2.1 Prozessdefintion „Freigabe“

Zentraler Bestandteil des Konfigurationsdienstes ist die Freigabe der bereitgestellten Pakete (Update-Pakete / Konfigurationsdatenfiles) durch den TBV/SBV-TIP der jeweiligen Umgebung und die Bereitstellung der Dateien im Download-Bereich.

Für die Produktivumgebung kann sich nur der SBV-TIP am Konfigurationsbereich anmelden und die Freigabe des Update-Paketes für den Download-Bereich beauftragen. [TIP1-A_3312]

Das Loggen der Aktionen wird in der Beschreibung nicht erwähnt, es werden jedoch alle relevanten Aktionen, wie in Kapitel 7.2 beschrieben, geloggt.

Der Prozess „Freigabe“ wird wie folgt definiert:

1. Der Konfigurationsbereich erhält die Informationen über ein neu hochgeladenes Update-Paket durch den Upload-Bereich. Dem Konfigurationsdienst werden neben dem Pfad zum Update-Paket auch die Daten der Signatur übermittelt. Durch die Übermittlung der Daten wird der Freigabe-Prozess gestartet.
2. Die Update-Pakete werden aus dem Upload-Bereich in den Konfigurationsbereich transferiert.
3. Die Signatur des Update-Paketes wird überprüft, um die sichere Übertragung zu verifizieren.
4. Das Update-Paket wird entpackt und eine Eingangsprüfung der übermittelten Daten wird durchgeführt. (Siehe Kapitel 6.1.2.4)
5. Nach erfolgreicher Eingangsprüfung wird mit Schritt 6 fortgefahren, ansonsten wird eine Fehlermeldung generiert und der Akteur wird über die Statusmeldung im Upload-Bereich informiert, dass das Paket nicht verarbeitet werden kann.
6. Ein neuer Auftrag zur Freigabe des Update-Paketes wird erzeugt und der Gruppe der TBV/SBV-TIP zugewiesen.
7. Der TBV/SBV-TIP meldet sich an dem Web-Frontend des Konfigurationsbereiches an und erhält eine Liste der zur Bearbeitung anstehenden Aufträge.
8. Der TBV/SBV-TIP wählt einen Auftrag aus der Liste zur Bearbeitung aus.
9. Der TBV/SBV-TIP wählt die auszuführende Aktion (Freigabe, Ablehnen, Deaktivieren…) für diesen Auftrag und gibt eventuell benötigte Parameter ein. Der TBV/SBV-TIP ist dafür verantwortlich, nur Freigaben von Update-Paketen durchzuführen, die durch die gematik zugelassen sind. Der Test der Pakete erfolgt extern und ist nicht Bestandteil des Konfigurationsdienstes.
10. Die Aktion wird durch den Konfigurationsbereich ausgeführt.
    a. Aktion Freigabe: Das Paket wird in den Download-Bereich übernommen und für den Download durch die Konnektoren vorbereitet.
    b. Aktion Ablehnung: Das Paket wird nicht in den Download-Bereich übernommen. Der Hersteller erhält im Upload-Bereich eine Information mit dem Ablehnungsgrund. Das Paket wird in das Archiv verschoben und der Auftrag ist beendet.

11. In der Gruppe „Aktive Pakete“ wird das freigegebene Paket eingetragen und bis zur Deaktivierung dort aufgelistet.

12. Der TBV/SBV-TIP kann das Paket deaktivieren. Das Deaktivieren eines Paketes entspricht einem Löschauftrag durch den TBV/SBV-TIP [TIP1-A_3913]. Das Paket wird dann nicht mehr im Frontend angezeigt und liegt nur noch im Archiv auf dem Filesystem. Die Deaktivierung eines Update-Paketes durch den Hersteller erfolgt durch das Einspielen einer neuen Firmware-Gruppen-Information über den Upload-Bereich.

13. Der TBV/SBV-TIP kann sich auf der Übersichtsmaske die zur Verfügung stehenden Statistikdaten / Logdaten ansehen und herunterladen. (Siehe Kapitel 7.1)

Durch den dargestellten Prozess wird in der PU sichergestellt, dass nur durch einen SBV-TIP freigegebene Pakete im Download-Bereich zur Verfügung stehen. Der SBV-TIP ist dafür verantwortlich, dass vor einer Freigabe entsprechende inhaltliche Tests und Überprüfungen der Pakete stattfinden.

⌦ ARV_706.3_Spec_SST_KSR_AFO_0017 Prüfung des Update-Paketes durch den SBV-TIP

Der SBV-TIP MUSS vor der Freigabe eines Update-Paketes in der PU eine inhaltliche Prüfung des Paketes durchführen. Die inhaltliche Prüfung enthält auch die Zulassung der Firmware durch die gematik.⌫

Eine zusätzliche Signatur des Update-Paketes durch die gematik ist nicht notwendig, da durch den Signatur-Prozess bereits sichergestellt ist, dass das Paket bis zum Download nicht durch den Konfigurationsdienst verändert wurde und das Paket nur nach manueller Prüfung und Freigabe durch den SBV-TIP in den Download-Bereich PU gelangen kann. [TIP1-A_3312]

6.1.2.2 Konfigurationsdatenfiles

Die einzige Ausprägung eines zentralen Konfigurationsdatenfiles ist zu diesem Zeitpunkt das Konfigurationsdatenfile zur Anbindung von Bestandsnetzen, siehe [gemSpec_KSR#Anhang_C]. Die Konfigurationsdatenfiles werden über den Download-Bereich zur Verfügung gestellt. Die Daten werden innerhalb der Telematikinfrastruktur erstellt und durch den TBV/SBV-TIP in den Konfigurationsdienst eingespielt. Konfigurationsdatenfiles werden weitestgehend wie Update-Pakete behandelt und besitzen einen ähnlichen Freigabe-Prozess.

1. Die Konfigurationsdaten-Datei wird nach dem Schema „InfrastrukturKonfig.xsd“ erstellt und liegt dem TBV/SBV-TIP zum Einspielen vor.

2. Der TBV/SBV-TIP meldet sich an dem Web-Frontend des Konfigurationsbereiches an.

3. Auf der Seite der Konfigurationsdaten wird eine neue Konfigurationsdaten-Datei hochgeladen, schemavalidiert und ein neuer Auftrag zur Freigabe wird erstellt.

4. Der TBV/SBV-TIP kann sich den Inhalt der Datei in der Übersicht anzeigen lassen.

5. Der TBV/SBV-TIP wählt einen Auftrag aus der Liste der Konfigurationsdaten zur Bearbeitung aus.

6. Der TBV/SBV-TIP wählt die auszuführende Aktion (Übergabe, Ablehnen,…) für diesen Auftrag und gibt eventuell benötigte Parameter ein.
7. Die Aktion wird durch den Konfigurationsbereich ausgeführt.
    a. Aktion Freigabe: Das Paket wird in den Download-Bereich übernommen und für den Download durch die Konnektoren vorbereitet.
    b. Aktion Ablehnung: Das Paket wird nicht in den Download-Bereich übernommen. Das Paket wird in das Archiv verschoben und der Auftrag ist beendet.

Das Format der Konfigurationsdaten wird durch das Schema „InfrastrukturKonfig.xsd“ definiert.

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0013 Konfigurationsdatenfile - Format**

Der TBV/SBV-TIP MUSS die Konfigurationsdaten nach folgenden Vorgaben erstellen:

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

⌦ ARV_706.3_Spec_SST_KSR_AFO_0036 Prüfung des Konfigurationsdatenfiles durch den TBV/SBV-TIP

Der TBV/SBV-TIP MUSS vor der Freigabe eines Konfigurationsdatenfiles in der jeweiligen Umgebung eine inhaltliche Prüfung des Paketes durchführen. ⌫

6.1.2.3 Status Definitionen

Der Weg eines Update-Paketes durch den Freigabe-Prozess kann durch den jeweiligen Status des Paketes nachvollzogen werden. Der Status des jeweiligen Paketes wird im Frontend angezeigt. Die Tabelle 13 beschreibt die unterschiedlichen Zustände.

Tabelle 13 Status Definition

Status	Beschreibung
Neu	Das Paket wurde an den Konfigurationsbereich übergeben und wartet auf den Start der Eingangsprüfung. Der Start erfolgt automatisch nach der abgeschlossenen Übertragung des Update-Paketes.
Test	Die Eingangsprüfung wird gerade durchgeführt (für Update-Pakete).
Akzeptiert	Die Eingangsprüfung wurde erfolgreich durchgeführt. Das Paket wartet auf die Freigabe durch den TBV/SBV-TIP.
Abgelehnt	Die Eingangsprüfung meldete einen Fehler, das Update-Paket wird zurückgewiesen.

Status	Beschreibung
Freigegeben	Das Paket wurde durch den TBV/SBV-TIP 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.

6.1.2.4 Eingangsprüfung

Nach dem Upload werden die Update-Pakete einer Eingangsprüfung [TIP1-A_3346] unterzogen, ungültige Pakete werden mit einer Fehlermeldung abgewiesen. Die Eingangsprüfung wird im Konfigurationsbereich durchgeführt. Der Hersteller erhält in der Übersicht des Upload-Bereiches einen Status des Update-Paketes angezeigt, am Status kann er erkennen, ob das Paket noch geprüft, akzeptiert oder abgelehnt wurde. Bei einer Ablehnung erfolgt eine detaillierte Fehlerbeschreibung, die der Hersteller in der Upload-Übersicht abrufen kann.

Bei der Eingangsprüfung werden folgende Punkte geprüft:

- Die Signatur des Update-Paketes wird beim Übergang zwischen Upload-Bereich und Konfigurationsbereich geprüft. Die Prüfung umfasst mindestens die folgende Schritte:
  - Prüfung der Gültigkeit des Zertifikats über den (internen) OCSP-Responder (OCSP-ICA) der Infrastruktur-CA,
  - Prüfung der Zertifikatstyp-OID auf Zulässigkeit,
  - Prüfung der mathematischen Korrektheit des Zertifikats.
- Die Integrität des ZIP-Containers
- Das Update-Paket wird geöffnet und festgestellt, dass alle notwendigen Dateien im ZIP-Container enthalten sind. (FirmwareGroupInfo.xml, ev. UpdateInfo.xml)
- 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 Kapitel 6.1.1.3 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.
- Es dürfen nicht mehr Dateien im Container enthalten sein, als die in 6.1.1.2 definierten Elemente. Die Firmware- und Dokumentationsdateien müssen alle durch UpdateInfo.xml referenziert werden. Update-Pakete mit Dateien ohne Referenz werden abgelehnt.

- Die Datei „FirmwareGroupInfo.xml“ wird mit dem XSD-Schema validiert und sichergestellt, dass die Version aktueller ist, als die bereits vorhandene.

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0020 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.⌫

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0021 Zusätzliche Dateien im Update-Paket**

Der Hersteller von Konnektoren oder Kartenterminals MUSS das Update-Paket so erstellen, das nur die in Tabelle 4 definierten Elemente in ihr enthalten sind. ⌫

Grundsätzlich werden nur vollständig korrekte Update-Pakete für die weitere Verarbeitung freigegeben. Eine Verarbeitung von Teilen des Update-Paketes findet nicht statt.

Sofern die Signatur verifiziert werden konnte, wird das Update-Paket möglichst vollständig überprüft, d.h. es wird nicht bei dem ersten Fehler mit einer Fehlermeldung abgebrochen. Eine nicht verifizierbare Signatur führt zu einer sofortigen Ablehnung des Update-Paketes.

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0031 Fehlerhafte Signaturen**

Der Anbieter des Konfigurationsdienstes DARF Pakete mit einer Fehlerhaften oder nicht verifizierten Signatur NICHT weiter verarbeiten.⌫

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0032 Vollständige Update-Pakete**

Der Anbieter des Konfigurationsdienstes DARF unvollständige Update-Pakete NICHT verarbeiten.⌫

Fehlermeldungen erhalten eine eindeutige ID und eine Fehlerbeschreibung in Deutsch.

Beispiel:

EC102 Fehlende Datei FW_122.fw

EC200 FirmwareGroupInfo.xml ist nicht vorhanden

6.1.2.5 UI-Masken

Disclaimer:

Die im Folgenden dargestellten UI-Masken dienen nur zur Übersicht und zur Visualisierung des Freigabe-Prozesses. Spätere Implementierungen werden dem zu definierenden Standard-Layout angepasst und können weitere Informationen und Aktionen enthalten.

Abbildung 10 UI-Maske Login Konfigurationsbereich

Auf der Authentifizierungsseite des Konfigurationsbereichs meldet sich der TBV bzw. SBV-TIP an, um zum Konfigurationsbereich zu gelangen. Dazu muss der Akteur seinen Benutzernamen, sein Passwort und das RSA-Token eingeben. Der Konfigurationsdienst verifiziert die eingegebenen Daten gegenüber IAM (Authentifizierungs- und Authorisierungsmanagement) und ermittelt die Rollen des angemeldeten Akteurs (siehe Kapitel 5.1.1). In den weiteren Masken kann der Akteur entsprechend seiner Rollen die Aktionen durchführen, bzw. Daten einsehen. Sofern die Kombination aus Benutzername, Passwort und RSA-Token nicht korrekt authentifiziert werden konnte, wird eine Fehlermeldung eingeblendet und der Benutzer bleibt auf dieser Maske.

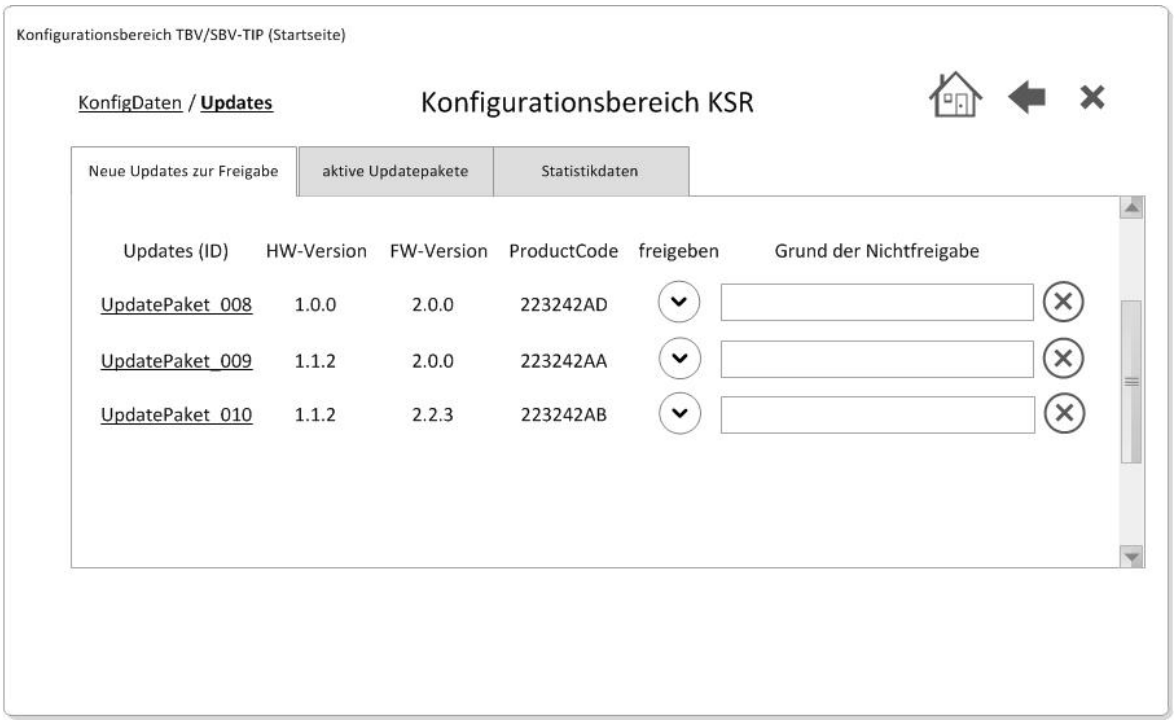

Abbildung 11 UI-Maske Neue Updates zur Freigabe

Auf der Freigabe Updates-Maske wird dem TBV/SBV-TIP die Möglichkeit gegeben, neue vom Hersteller hochgeladene Updates für den Download freizugeben bzw. nicht freizugeben. Neben der Update-ID sind des Weiteren die Hardware-Version, die Firmware-Version sowie der ProductCode aufgelistet (weitere Felder sind aus Platzgründen nicht dargestellt). Mit Klick auf die UpdateID eines Pakets wird die beim Upload vom Hersteller erfasste Kurzbeschreibung angezeigt.

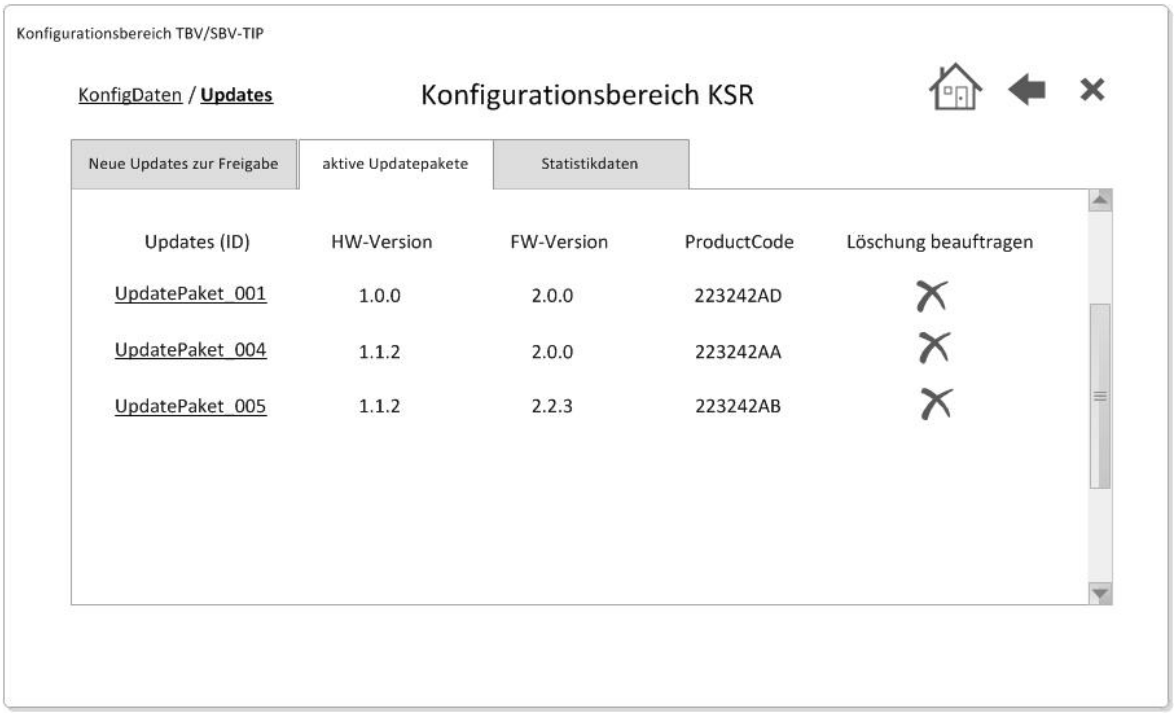

Abbildung 12 UI-Maske aktive Update-Pakete

Hier sind die bereits aktiven, also zum Download bereitgestellten Updates der Hersteller aufgelistet. Zusätzlich werden die Informationen Hardware-Version, Firmware-Version und der ProductCode mit angezeigt. Das Update-Paket mit einer aktiven Firmware-Gruppen-Information für ein Produkt des Herstellers wird mit der FirmwareGroupID in der Tabelle angezeigt. Mit Klick auf die Update-ID erscheint eine vom Hersteller erfasste Kurzbeschreibung zum Paket. Der TBV oder SBV-TIP hat hier die Möglichkeit die Löschung der Pakete zu beantragen.

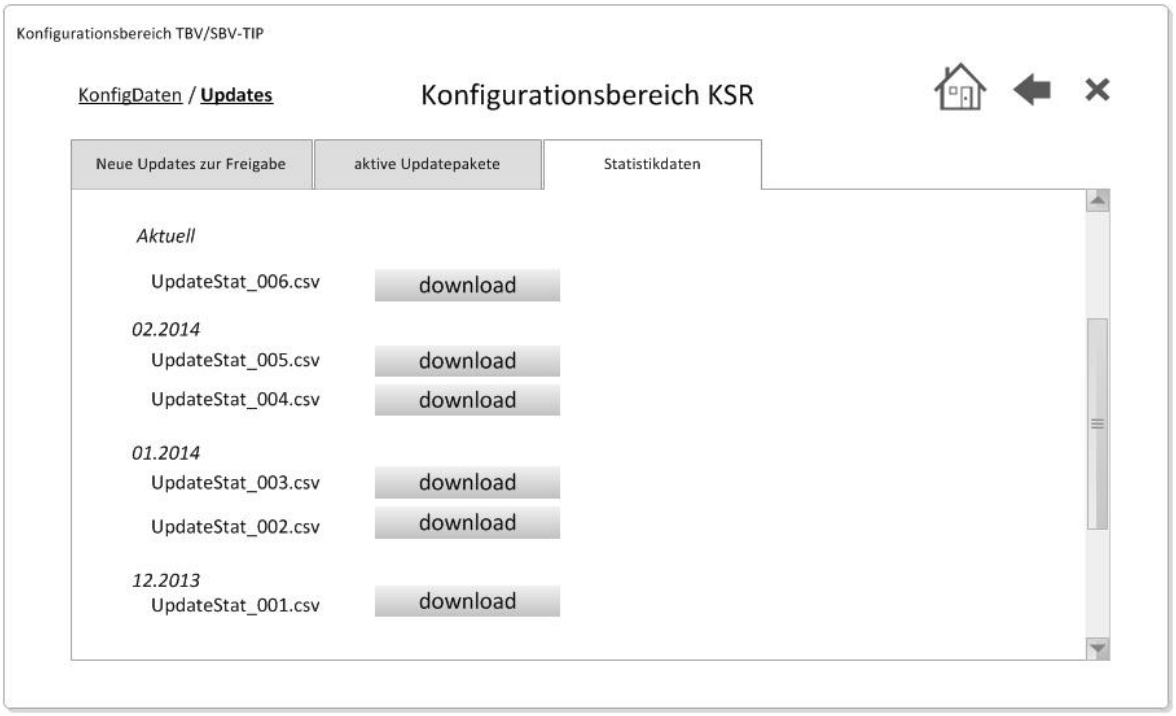

Abbildung 13 UI-Maske Statistikdaten

Die Statistik-Maske des Konfigurationsbereichs bietet eine Auflistung aller zur Verfügung stehenden, chronologisch zum Download bereitgestellten Statistik- bzw. Logdaten. Die Dateien enthalten jeweils Statistik- bzw. Logdaten für einen Monat, bzw. alle bisherigen Daten für den aktuell laufenden Monat. [TIP1-A_3352,TIP1-A_3924, TIP1-A_3925]

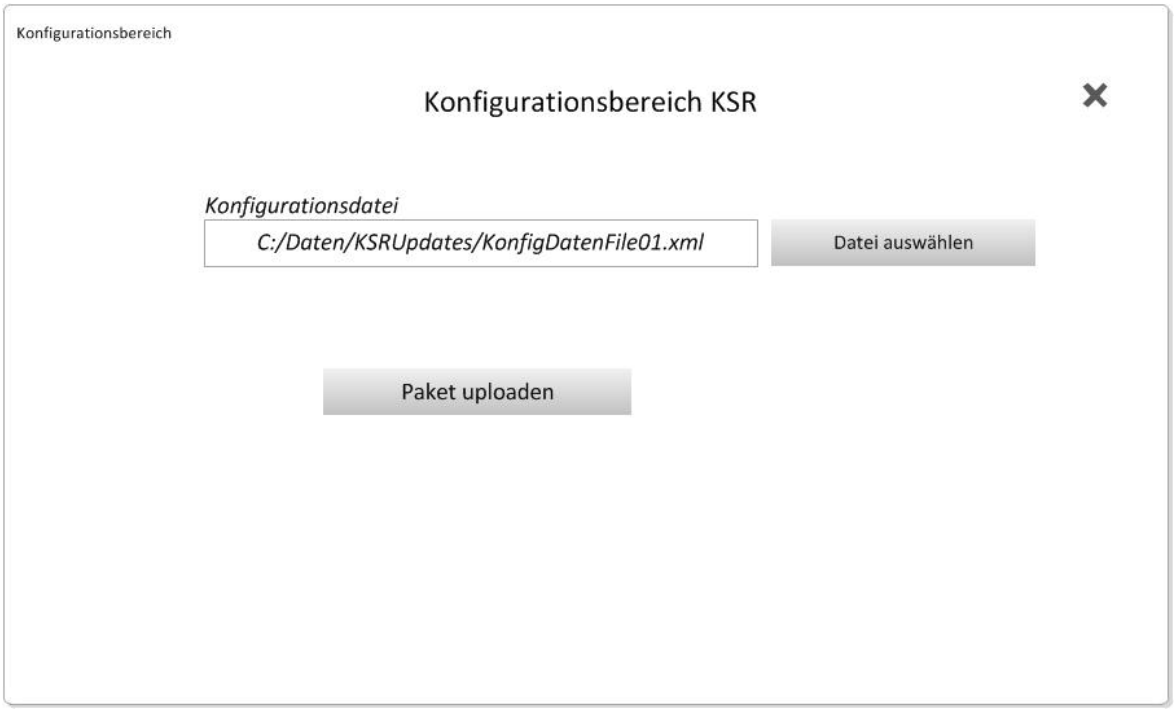

Abbildung 14 UI-Maske Upload Konfigurationsdaten

In dieser Maske wird das Konfigurationsdatenfile in den Konfigurationsbereich hochgeladen, anschließend technisch durch die Validierung und inhaltlich durch den jeweiligen TBV/SBV-TIP geprüft und entsprechend freigegeben oder abgelehnt.

Abbildung 15 UI-Maske Übergabe Konfigurationsdaten freigeben/nicht freigeben

Die Maske „Übergabe Konfigurationsdaten“ listet sämtliche hochgeladenen Konfigurationsdateien mit den zusätzlichen Informationen des Auftraggebers und des Formats auf. Mit Klick auf den Dateinamen erscheint ein Fenster, welches das Konfigurationsdatenfile anzeigt. Nach einer Sichtprüfung haben die TBV bzw. SBV-TIP die Möglichkeit, die hochgeladenen Konfigurationsdatenfiles zur Übergabe freizugeben oder abzulehnen.

6.1.3 Schnittstelle I_KSRS_Download

Die nachfolgende Beschreibung spezifiziert das technische Interface I_KSRS_Download. Über diese Schnittstelle können die zur Verfügung stehenden Update-Pakete vom Konfigurationsdienst abgefragt und heruntergeladen werden.

Die Schnittstelle wird technisch durch eine „SOAP (Version 1.1) über http“ Schnittstelle realisiert. Die Definition der Schnittstelle ist durch die gematik vorgegeben.

⌦ ARV_706.3_Spec_SST_KSR_AFO_0014 SOAP-Version

Der aufrufende KSR-Client (Konnektor) MUSS „SOAP über http“, Version 1.1 verwenden.⌫

Tabelle 14 I_KSRS_Download

Name	I_KSRS_Download	
Version (KDV)	Gemäß Produkttypversion	
Namensraum	http://ws.gematik.de/ksr/v1.1 ~~v1.0~~	
Namensraum-Kürzel	KSR	
Operationen	**Name**	**Kurzbeschreibung**
	listUpdates	Auflisten verfügbarer Updates
WSDL	Konfigurationsdienst.wsdl	
Schema	Konfigurationsdienst.xsd	

Die Operationen I_KSRS_Download::getUpdates und I_KSRS_Download::get_Ext_Net_Config sind Abrufe einer Datei und werden durch einen http GET Filetransfer (HTTP/1.1) realisiert.

Die Schnittstelle unterstützt das „Content Coding“ [RFC2616] „gzip“. [TIP1-A_3910]

6.1.3.1 Kommunikation

Wie in [gemKPT_Arch_TIP] dargestellt, wird die Verbindung zwischen Konnektor und Konfigurationsdienst durch TLS 1.2 abgesichert, um dem Schutzbedarf der übertragenen Informationen zu entsprechen. Die Verwendung von TLS 1.1 darf aus wichtigen Gründen erfolgen, bedarf allerdings der Absprache mit dem Anbieter des Konfigurationsdienstes.

Verbindungen mit einer anderen Verschlüsselung, bzw. unverschlüsselte Verbindungen werden vom Konfigurationsdienst zurückgewiesen.

6.1.3.2 Operation I_KSRS_Download::listUpdates

Die Operation listet die auf dem Konfigurationsdienst verfügbaren Update-Pakete für eine dezentrale Komponente der TI-Plattform auf.

Tabelle 15 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
Berechtigung	Konnektor
Vorbedingungen	Aufgebaute TLS-Verbindung vom Konnektor zum Konfigurationsdienst entsprechend Kapitel 6.1.3.1.
Nachbedingungen	Konfigurationsdienst hat Log-Daten der Abfrage gespeichert und der KSR-Client hat UpdateInformations vorliegen sowie gespeichert.
Aufruf	Der Aufrufer (Konnektor) ruft über die hier definierte Schnittstelle den Konfigurationsdienst mit den in Kapitel 6.1.3.2.1 definierten Parametern auf.
Antwort	Die Liste der auf dem Konfigurationsdienst verfügbaren Update-Pakete für die dezentrale Komponente entsprechend Beschreibung in Kapitel 6.1.3.2.2.
Standardablauf	Der Konfigurationsdienst stellt die Liste der verfügbaren Updates für die dezentrale Komponente der TI-Plattform zusammen. Diese Liste entspricht dem Element Firmware-Version der „aktiven“ Firmware-Gruppe für die Komponente. Der Konfigurationsdienst sendet im Response die Liste der verfügbaren Updates, sowie die FirmwareGroupReleaseNotes an den Client.
Fehlerfälle	Tritt während der Verarbeitung ein Fehler auf, beantwortet der Konfigurationsdienst die Anfrage mit einem SOAP-Fault entsprechend [gemSpec_OM]. Die verwendeten Fehlercodes aus [gemSpec_OM] sind in Kapitel 6.1.3.2.3 definiert.

6.1.3.2.1 Request

Im listUpdates-Request müssen folgende Parameter mit angegeben werden:

Tabelle 16 I_KSRS_Download::listUpdates Request

Element	Kurzbeschreibung	Optional	Wertebereich
ProductVendorID	Identifiziert den Hersteller des Produkts, für welches auf Updates geprüft werden soll.	nein	String, max. 5 Zeichen „[a-zA-Z0-9_]*“
ProductCode	Identifiziert das Produkt zusammen mit dem ProductVendorID, für welches auf	nein	String, max. 8 Zeichen

Element	Kurzbeschreibung	Optional	Wertebereich
	Updates geprüft werden soll.		„[a-zA-Z0-9_]*“
HWVersion	Identifiziert die Hardware zusammen mit ProductCode und ProductVendorID , für welches auf Updates geprüft werden soll.	nein	String „[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}“
FWVersion	Die FirmwareVersion des Produkts, für welches auf Updates geprüft werden soll.	nein	String „[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}“

6.1.3.2.2 Response

Der Download-Bereich sucht die Update-Pakete für die im Request beschriebenen Kriterien heraus und übermittelt sie zusammen mit den Release Notes der Firmware-Gruppe. Die Daten werden dabei aus dem Update-Paket entnommen und zu einer Liste zusammengeführt. Maximal 999 Update-Pakete können auf diesem Weg angeboten werden. Der Response ist leer, wenn zu diesen Kriterien kein Update-Paket gefunden wurde. Eine leere Response ist kein Fehler und wird nicht mit einem SOAP-Fault beantwortet.

Im listUpdates-Response werden folgende Elemente geliefert. Die genaue Spezifikation der Elemente entspricht den Definitionen in Kapitel 6.1.1.5 und Kapitel 6.1.1.6, die Elemente werden aus den Dateien UpdateInfo.xml und FirmwareGroupInfo.xml ausgelesen und in die Response-Struktur übertragen.

Tabelle 17 I_KSRS_Download::listUpdates Response

Element	Kurzbeschreibung	Optional
FirmwareGroupReleaseNotes	Dieses Element enthält die Release Notes der Firmware-Gruppen-Information. Es beschreibt die Update-Pakete bzw. Firmware der Firmware-Gruppe.	Ja*
UpdateInformation	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 6.1.1.5)	Ja*

*) falls keine Update-Pakete auf dem Konfigurationsdienst vorhanden sind

6.1.3.2.3 Fehlercodes

Folgende Fehlercodes aus [gemSpec_OM] werden durch die listUpdates-Operation abdeckt:

Tabelle 18 I_KSRS_Download::listUpdates Fehlercodes

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

Code	ErrorType	Severity	ErrorText	Auslösende Bedingung
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 Aufschlüsslung des Protokollfehlers werden in den Details erfasst

6.1.3.3 Operation I_KSRS_Download::getUpdates

Tabelle 19 I_KSRS_Download::getUpdates

Element	Beschreibung
Name	I_KSRS_Download::getUpdates
Beschreibung	Mit dieser Operation ruft der Konnektor verfügbare Updates für eine dezentrale Komponente der TI-Plattform vom Konfigurationsdienst ab. Die Auswahl der Files zum Download erfolgt auf Grundlage der zurückgegebenen Werte in Operation listUpdates Response. Mit jedem Aufruf dieser Operation wird ein File übertragen.
Initiierender Akteur	Konnektor
Weitere Akteure	keine
Auslöser	Konnektor
Berechtigung	Konnektor
Vorbedingungen	Aufgebaute TLS-Verbindung vom Konnektor zum Konfigurationsdienst entsprechend Kapitel 6.1.3.1.
Nachbedingungen	Konfigurationsdienst hat Log-Daten der Abfrage gespeichert und der Konnektor hat die Update-Datei vorliegen und gespeichert.
Aufruf	Der Aufrufer (Konnektor) ruft über die hier definierte Schnittstelle den Konfigurationsdienst auf. Eingangsdaten: • https://<host>/ Konfigurationsdienst Downloadpunkt für angefragtes File der TI. • <path> Identifiziert das angefragte File. Der Dateiname referenziert die angeforderte Datei aus dem Update-Paket. Die Pfadangabe entspricht der Definition in Kapitel 6.1.1.3.
Antwort	Das angeforderte File aus dem Update-Paket.
Standardablauf	Aufruf von TUC_KSR_001 „Get File“ mit Parametern, siehe Kapitel 6.1.3.5. Eingangsdaten:

Element	Beschreibung
	• https://<host>/ (entspricht DNS SRV Resource Record „_ksrfirmware._tcp.ksr.telematik“ • <path> Dieser Wert entspricht den in Operation I_KSRS_Download::listUpdatesResponse zurückgegebenen „Filenamen“ oder kann den Hersteller-Update-Informationen entnommen werden.
Fehlerfälle	Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.

6.1.3.4 Operation I_KSRS_Download::get_Ext_Net_Config

Tabelle 20 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
Berechtigung	Konnektor
Vorbedingungen	Aufgebaute TLS-Verbindung vom Konnektor zum Konfigurationsdienst entsprechend Kapitel 6.1.3.1.
Nachbedingungen	Konfigurationsdienst hat Log-Daten der Abfrage gespeichert und der Konnektor hat die Konfigurationsdaten-Datei vorliegen und gespeichert.
Aufruf	Der Aufrufer (Konnektor) ruft über die hier definierte Schnittstelle den Konfigurationsdienst auf. Eingangsdaten: • https://<host>/ Konfigurationsdienst Downloadpunkt für angefragtes File der TI. • <path> Identifiziert das angefragte File.
Antwort	Das angeforderte File aus dem Update-Paket.
Standardablauf	Aufruf von TUC_KSR_001 „Get File“ mit Parametern, siehe Kapitel 6.1.3.5. Eingangsdaten:

Element	Beschreibung
	• https://<host>/ (entspricht DNS SRV Resource Record „_ksrkonfig._tcp.ksr.telematik“ • <path> Dateiname des Konfigurationsdatenfiles. Der Dateiname des Konfigurationsdatenfile ist festgelegt auf „Bestandsnetze.xml“ [TIP1-A_5375]. Der Aufruf anderer Dateinamen erzeugt eine Fehlermeldung.
Fehlerfälle	Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.

6.1.3.5 Operation „Get File“

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.

Die Operation wird nur indirekt durch den Aufruf der Operation I_KSRS_Download::getUpdates und I_KSRS_Download::get_Ext_Net_Config angesprochen und darf nicht direkt aufgerufen werden. Die Operation der Schnittstelle wird nicht veröffentlicht.

Tabelle 21 TUC_KSR_001 "Get File"

Element	Beschreibung
Name	TUC_KSR_001 “Get File”
Beschreibung	Mit dieser Operation ruft der Konnektor verfügbare Dateien vom Konfigurationsdienst ab. Mit jedem Aufruf dieser Operation wird ein File übertragen.
Initiierender Akteur	Konnektor, indirekt über die I_KSRS_Download::getUpdates und I_KSRS_Download::get_Ext_Net_Config
Weitere Akteure	keine
Auslöser	Konnektor, indirekt über die I_KSRS_Download::getUpdates und I_KSRS_Download::get_Ext_Net_Config
Berechtigung	Nicht öffentlich
Vorbedingungen	Aufgebaute TLS-Verbindung vom Konnektor zum Konfigurationsdienst entsprechend Kapitel 6.1.3.1.
Nachbedingungen	Die angeforderte Datei wurde durch die aufrufende Operation an den Aufrufer weitergegeben.
Aufruf	http GET entsprechend Kapitel 6.1.3.5.1
Antwort	Die angeforderte Datei.
Standardablauf	Der Konfigurationsdienst überträgt die angeforderte Datei entsprechend http 1.1 [RFC2616]. Der Konfigurationsdienst speichert Log-Daten dieser Aktion, siehe Kapitel 7.2.

Element	Beschreibung
Fehlerfälle	Tritt während der Verarbeitung ein Fehler auf, sendet der Konfigurationsdienst im http-Response einen entsprechenden http Status Code. [TIP1-A_4120]

6.1.3.5.1 Request

Der Aufruf des Requests „get File“ erfolgt indirekt über die Operationen getUpdates und get_Ext_Net_Config. Beide Operationen unterstützen den Aufruf http GET nach [RFC2616]. Der Aufruf erfolgt mittels einer URL [RFC1738] nach folgendem Schema:

https://<host>/<path>

Der Aufruf muss die in Kapitel 6.1.3.1 definierte Verschlüsselung nach TLS 1.2 unterstützen.

Der Parameter <host> wird in den jeweiligen DNS Einträge definiert.

Der Parameter <path> definiert die angeforderte Datei und kann bei einem Aufruf über die Operation getUpdates eine Pfadangabe enthalten. Der Aufruf der Operation get_Ext_Net_Config darf in diesem Parameter nur den Dateinamen „Bestandsnetze.xml“ enthalten. [TIP1-A_5375]

6.1.3.5.2 Response

Sofern die im Pfad angegebene Datei gefunden wird, gibt der Konfigurationsdienst den Inhalt der Datei im http-Body, gemäß [RFC2616] zurück [TIP1-A_3336]. Der http Status Code ist in diesem Fall 200 „OK“.

Der Konfigurationsdienst füllt die notwendigen Header-Datenfelder in der http-Response, gemäß [RFC2616].

In dem http-Response Header „content-length“ wird die Größe der Datei in Bytes angegeben.

Der Content-Type der zurückgelieferten Datei ist „application/octet-stream“.

Sofern der Konfigurationsdienst überlastet oder der Zeitraum der Nichtverfügbarkeit bekannt ist, wird das Attribut „retry-after“ im Header der http-Response mit einem entsprechenden Wert gesetzt und der http Status Code 503 „Service Unavailable“ zurückgegeben. Das Feld wird entweder mit einem Wert im http-Date Format oder einer Anzahl von Sekunden belegt. (Siehe dazu [RFC2616#14.37]).

Beispiel:

Retry-After: Fri, 31 Dec 1999 23:59:59 GMT

Retry-After: 120

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0015 Unterstützung „retry-after“**

Der aufrufende KSR-Klient MUSS das Attribut „retry-after“ auswerten und bei einer Wiederholung der Abfrage beachten.

- Sofern das Attribut einen Zeitpunkt liefert, darf eine Wiederholung erst nach diesem Zeitpunkt erfolgen.

- bei der Angabe von Sekunden muss diese Zeitspanne eingehalten werden, bevor ein erneuter Aufruf gestartet wird.⌫

7 Informationsmodell

7.1 Definition Statistikdaten

Der Konfigurationsdienst ermittelt im laufenden Betrieb statistische Informationen über den Download der Update-Pakete. Die Daten werden den berechtigten Akteuren in einer Datei zum Download in den organisatorischen Schnittstellen zur Verfügung gestellt.

Der Inhalt der statistischen Daten, die der KSR zur Verfügung stellt, besteht aus einer Auflistung der im Download-Bereich angefragten, sowie bereitgestellten Updates, aufgeschlüsselt nach Produkt und Update-Paket im zeitlichen Verlauf und beinhaltet folgende Elemente in entsprechend aufgelisteter Reihenfolge, getrennt durch ein Semikolon:

Tabelle 22 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 ausführlich.	String „[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}") Wenn „listUpdates" aufgerufen wurde, enthält dieses Feld den entsprechenden Parameter des Requests, beim Aufruf von „getUpdates" die Hardware-Version der gesendeten Datei.
5	FWVersion	Firmware Version des heruntergeladenen Updates. [gemSpec_OM] beschreibt	String „[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}") Wenn „listUpdates" aufgerufen

Position	Feld	Beschreibung	Typ
		dieses Element ausführlich.	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.

Die Statistikdaten werden als CSV-Datei zum Download in den jeweiligen Frontends zur Verfügung gestellt (siehe Kapitel 6.1.1.8).

Die CSV-Datei verwendet UTF-8 Codierung und schließt die Zeilen mit einem Zeilenende Zeichen im UNIX-Format (LF).

Beispiel:

Der Aufbau einer Statistikdatei könnte für einen Aufruf von „getUpdates“ beispielsweise wie folgt aussehen:

„2014-01-08 09:46:18,780;12345;223345;1.0.0;1.1.2;getUpdates;345XYZ;Statistikdatei01“

Für einen Aufruf von „listUpdates“:

„2014-01-08 09:46:18,780;12345;223345;1.0.0;1.1.2;listUpdates;;“

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0033 Datei-Format Statistik-Daten**

Der Konfigurationsdienst MUSS die 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 „;“⌫

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0035 Umfang der gespeicherten Statistik-Daten**

Der Konfigurationsdienst MUSS die in Tabelle 22 „Statistikdatenformat“ enthaltenen Felder entsprechend ihrer Definition füllen und persistent speichern. ⌫

7.2 Logging

Das geforderte Logging des Konfigurationsdienstes bezieht sich auf die persistente Speicherung der ausgeführten Aktionen. Zugang zu Logging-Daten erhalten nur berechtigte Akteure. Die Logging-Daten werden nach einer konfigurierbaren Zeitspanne, spätestens nach 90 Tagen entfernt.

Der Konfigurationsdienst speichert sämtliche Aktionen (Aufträge und deren Auftragsbestätigungen) an den Schnittstellen P_KSRS_Upload, P_KSRS_Operations und I_KSRS_Download. Aktionen sind zum Beispiel der Upload eines Update-Paketes, die Freigabe eines Update-Paketes und der Download einer Firmware aus einem Update-Paket. Der Download wird zusätzlich in den Statistikdaten (Kapitel 7.1) aufgeführt.

Das Logging [TIP1-A_3328] gibt auf folgende Fragen (Tabelle 23) Auskunft:

Tabelle 23 Logging

Frage	Beispiel
Wer hat was getan?	UserIdD/ VendorID
Was hat er getan?	Durchgeführte Aktion, z.B. „FREIGABE“
Mit welchem Informationsobjekt?	UpdateID, FirmwareGroupID
Zu welchem Zeitpunkt?	Timestamp der Aktion
Welches Ergebnis hatte die Aktion?	• es ist kein Fehler aufgetreten • es ist ein internen Fehler aufgetreten und die Aktion wurde abgebrochen • es ist ein remote Fehler aufgetreten und die Aktion konnte nicht ausgeführt werden

Tabelle 24 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	String, max. 32 Zeichen

Position	Feld	Beschreibung	Typ
		Aktion, z.B. „FREIGABE“, „UPLOAD“,	
5	State	Status-Ergebnis der durchgeführten Aktion.	String, entweder „ERFOLG“, „FEHLER“ oder „REMOTE-FEHLER“
6	Description	Textuelle Beschreibung des Ergebnisses der ausgeführten Aktion. Kann leer sein, wenn die Aktion korrekt ausgeführt wurde, enthält in einem Fehlerfall, die Fehlerbeschreibung.	String, max. 2048 Zeichen

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

Tabelle 25 Werte im Feld InfoId zu Action

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

Die Logdaten werden als CSV-Datei zum Download in dem jeweiligen Konfigurationsbereich zur Verfügung gestellt. Der TBV/SBV/TIP der Umgebung kann die Dateien im Web-Frontend herunterladen. Die Daten werden jeweils pro Monat, am Monatsanfang zur Verfügung gestellt. Für den aktuellen Monat werden alle bisher angefallenen Daten bereitgestellt, siehe Kapitel 6.1.2.5

Das Feld „State“ ist ein Indikator für das Ergebnis der Aktion. Ist diese Erfolgreich abgeschlossen ist der Status „ERFOLG“, bei einer Fehlermeldung „FEHLER“ und bei einem aufgetretenen Remote-Fehler „REMOTE-FEHLER“. In dem Feld „Description“ kann bei einem Fehler die Fehlerbeschreibung eingesehen werden.

Die CSV-Datei verwendet UTF-8 Codierung und schließt die Zeilen mit einem Zeilenende Zeichen im UNIX-Format (LF).

Beispiel:

Der Aufbau einer Logdatei könnte beispielsweise wie folgt aussehen:

„2014-01-08 09:46:18,780;SBV_PU_01;223345;FREIGABE;OK;Freigabe erfolgt“

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0027 Löschen der Logging-Daten**

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

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0028 Umfang der gespeicherten Daten**

Der Konfigurationsdienst MUSS die in Tabelle 24 „Logdatenformat“ enthaltenen Felder entsprechend ihrer Definition füllen und persistent speichern. ⌫

⌦ **ARV_706.3_Spec_SST_KSR_AFO_0034 Datei-Format Logging-Daten**

Der Konfigurationsdienst MUSS die Logging-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 „;“⌫

Anhang A - Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
Base64	Base64 beschreibt ein Verfahren zur Kodierung von 8-Bit-Binärdaten (z. B. ausführbare Programme, ZIP-Dateien oder Bilder) in eine Zeichenfolge, die nur aus lesbaren, Codepage-unabhängigen ASCII-Zeichen besteht.
CSV	Comma-separated values
http	Hypertext Transfer Protocol
IAM	Authentifizierungs- und Authorisierungsmanagement
KSR	Konfigurations- und Software Repository
SBV-TIP	Servicebetriebsverantwortlicher der TI-Plattform
SOAP	Simple Object Access Protocol
TBV	Testbetriebsverantwortlicher
TLS	Transport Layer Security
UI	User Interface
XML	Extensible Markup Language
XSD	XML Schema
X.509	X.509 ist ein Standard für eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate.

A2 – Glossar

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

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

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
[gemSpec_KSR]	gematik: Spezifikation Konfigurationsdienst
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemSpec_OM]	gematik: Operations und Maintenance Spezifikation
[gemSpec_Krypt]	gematik. Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[ARV_706.3_KPT_Betr_V1]	Betriebskonzept
[ARV_706.3_Spec_SST_Komponenten-PKI]	Schnittstellen- und Prozessspezifikation Komponenten-PKI
[gemSpec_Perf]	gematik: Performance und Mengengerüst TI-Plattform

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC2616]	Hypertext Transfer Protocol – http/1.1
[RFC1738]	Uniform Resource Locators (URL)
[ZIP-APP]	http://www.pkware.com/documents/casestudies/APPNOTE.TXT
[XMLDSig]	XML Signature Syntax and Processing (Second Edition) W3C Recommendation 10 June 2008 http://www.w3.org/TR/2008/PER-xmldsig-core-20080326/
[ETSI-CAdES]	ETSI TS 101 733 V1.7.4 (2008-07), Electronic Signatures and Infrastructures (ESI); CMS AdvancedElectronic Signatures (CAdES)

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

Anhang B - Anforderungsregister

Eingangs-anforderung	Quelle	Umgesetzt durch
TIP1-A_3311	[gemSpec_KSR]	Kapitel 5
TIP1-A_3312	[gemSpec_KSR]	Kapitel 6.1.2.1 ARV_706.3_Spec_SST_KSR_AFO_0017
TIP1-A_3316	[gemSpec_KSR]	Kapitel 6.1.1.7 ARV_706.3_Spec_SST_KSR_AFO_0024, ARV_706.3_Spec_SST_KSR_AFO_0025
TIP1-A_3319	[gemSpec_KSR]	Kapitel 6.1.1.2/6.1.1.6
TIP1-A_3320	[gemSpec_KSR]	Kapitel 6.1.1.6
TIP1-A_3321	[gemSpec_KSR]	Kapitel 6.1.1.6
TIP1-A_3322	[gemSpec_KSR]	Kapitel 6.1.1.6
TIP1-A_3323	[gemSpec_KSR]	Kapitel 6.1.3.1
TIP1-A_3325	[gemSpec_KSR]	Kapitel 6.1.3.1
TIP1-A_3328	[gemSpec_KSR]	Kapitel 7.2 ARV_706.3_Spec_SST_KSR_AFO_0027, ARV_706.3_Spec_SST_KSR_AFO_0028
TIP1-A_3330	[gemSpec_KSR]	Kapitel 6.1.3.2
TIP1-A_3331	[gemSpec_KSR]	Kapitel 6.1.3.2
TIP1-A_3332	[gemSpec_KSR]	Kapitel 6.1.3.2
TIP1-A_3333	[gemSpec_KSR]	Kapitel 6.1.3.2.3
TIP1-A_3334	[gemSpec_KSR]	Kapitel 6.1.3.3
TIP1-A_3335	[gemSpec_KSR]	Kapitel 6.1.3
TIP1-A_3336	[gemSpec_KSR]	Kapitel 6.1.3.5.2
TIP1-A_3342	[gemSpec_KSR]	Kapitel 6.1.1 ARV_706.3_Spec_SST_KSR_AFO_0001, ARV_706.3_Spec_SST_KSR_AFO_0002, ARV_706.3_Spec_SST_KSR_AFO_0003, ARV_706.3_Spec_SST_KSR_AFO_0004, ARV_706.3_Spec_SST_KSR_AFO_0005, ARV_706.3_Spec_SST_KSR_AFO_0007, ARV_706.3_Spec_SST_KSR_AFO_0008, ARV_706.3_Spec_SST_KSR_AFO_0009, ARV_706.3_Spec_SST_KSR_AFO_0011, ARV_706.3_Spec_SST_KSR_AFO_0012, ARV_706.3_Spec_SST_KSR_AFO_0016,

Eingangs-anforderung	Quelle	Umgesetzt durch
		ARV_706.3_Spec_SST_KSR_AFO_0018, ARV_706.3_Spec_SST_KSR_AFO_0019, ARV_706.3_Spec_SST_KSR_AFO_0022, ARV_706.3_Spec_SST_KSR_AFO_0023, ARV_706.3_Spec_SST_KSR_AFO_0029, ARV_706.3_Spec_SST_KSR_AFO_0030
TIP1-A_3343	[gemSpec_KSR]	Kapitel 6.1.1 ARV_706.3_Spec_SST_KSR_AFO_0037, ARV_706.3_Spec_SST_KSR_AFO_0038
TIP1-A_3345	[gemSpec_KSR]	Kapitel 7.2
TIP1-A_3346	[gemSpec_KSR]	Kapitel 6.1.2.4 ARV_706.3_Spec_SST_KSR_AFO_0020, ARV_706.3_Spec_SST_KSR_AFO_0021, ARV_706.3_Spec_SST_KSR_AFO_0031, ARV_706.3_Spec_SST_KSR_AFO_0032
TIP1-A_3347	[gemSpec_KSR]	Kapitel 5.2
TIP1-A_3348	[gemSpec_KSR]	Kapitel 6.1.1
TIP1-A_3349	[gemSpec_KSR]	Kapitel 6.1.2
TIP1-A_3350	[gemSpec_KSR]	Kapitel 6.1.2
TIP1-A_3351	[gemSpec_KSR]	Kapitel 6.1.2
TIP1-A_3352	[gemSpec_KSR]	Kapitel 6.1.2
TIP1-A_3353	[gemSpec_KSR]	Kapitel 7.1
TIP1-A_3354	[gemSpec_KSR]	Kapitel 7.1 ARV_706.3_Spec_SST_KSR_AFO_0026, ARV_706.3_Spec_SST_KSR_AFO_0033, ARV_706.3_Spec_SST_KSR_AFO_0035
TIP1-A_3355	[gemSpec_KSR]	Kapitel 5.1 ARV_706.3_Spec_SST_KSR_AFO_0037, ARV_706.3_Spec_SST_KSR_AFO_0038
TIP1-A_3909	[gemSpec_KSR]	Kapitel 6.1.3, ARV_706.3_Spec_SST_KSR_AFO_0014
TIP1-A_3910	[gemSpec_KSR]	Kapitel 6.1.3
TIP1-A_3913	[gemSpec_KSR]	Kapitel 6.1.2.1
TIP1-A_3914	[gemSpec_KSR]	Kapitel 5.1
TIP1-A_3915	[gemSpec_KSR]	Kapitel 5.1
TIP1-A_3916	[gemSpec_KSR]	Kapitel 5.1
TIP1-A_3917	[gemSpec_KSR]	Kapitel 6.1.2.4
TIP1-A_3918	[gemSpec_KSR]	Kapitel 6.1.2.4
TIP1-A_3919	[gemSpec_KSR]	Kapitel 6.1.1.2/6.1.1.6/6.1.2.3

Eingangs-anforderung	Quelle	Umgesetzt durch
TIP1-A_3920	[gemSpec_KSR]	Kapitel 6.1.2
TIP1-A_3921	[gemSpec_KSR]	Kapitel 7.2
TIP1-A_3922	[gemSpec_KSR]	Kapitel 6.1.2.5
TIP1-A_3923	[gemSpec_KSR]	Kapitel 6.1.2.5
TIP1-A_3924	[gemSpec_KSR]	Kapitel 6.1.2.5
TIP1-A_3925	[gemSpec_KSR]	Kapitel 6.1.2.5
TIP1-A_4120	[gemSpec_KSR]	Kapitel 6.1.3.5.2
TIP1-A_5038	[gemSpec_KSR]	Kapitel 7.2
TIP1-A_5039	[gemSpec_KSR]	Kapitel 7.2
TIP1-A_5042	[gemSpec_KSR]	Kapitel 6.1.1
TIP1-A_5043	[gemSpec_KSR]	Kapitel 6.1.2
TIP1-A_5154	[gemSpec_KSR]	Kapitel 6.1.3.4
TIP1-A_5160	[gemSpec_KSR]	Kapitel 6.1.3.4
TIP1-A_5161	[gemSpec_KSR]	Kapitel 6.1.3.5
TIP1-A_5162	[gemSpec_KSR]	Kapitel 6.1.3.5.2, ARV_706.3_Spec_SST_KSR_AFO_0015
TIP1-A_5163	[gemSpec_KSR]	Kapitel 6.1.2.2, ARV_706.3_Spec_SST_KSR_AFO_0013, ARV_706.3_Spec_SST_KSR_AFO_0036
TIP1-A_5375	[gemSpec_KSR]	Kapitel 6.1.3.4
GS-A_4371	[gemSpec_Krypt]	Kapitel 6.1.1.7
GS-A_4385	[gemSpec_Krypt]	Kapitel 6.1.3.1
GS-A_4386	[gemSpec_Krypt]	Kapitel 6.1.3.1
GS-A_4387	[gemSpec_Krypt]	Kapitel 6.1.3.1
GS-A_5035	[gemSpec_Krypt]	Kapitel 6.1.3.1