vHGS eTicket RheinMain

Pflichtenheft

Schnittstellenspezifikation
PH 06-02 Terminalmanagementsysteme (TMS)

Erstellt für

Rhein Main Service

Version:	2.2
Datum:	15.06.2017
Dok-Ref.:	PH 06-02
Datei:	vHGS_PH06-02_TeminalMgmtSys_v2.2.docx

Versionshistorie

Version	Anlass	Datum
1.1	Ersterstellung (herausgelöst aus PH05, Version 1.0)	08.11.2010
1.2.1	Einarbeitung der Reviewkommentare vom 17.12.2010 sowie weiterer Änderungen	02.02.2011
1.3	Einarbeitung der Change Requests des CR –Pakets 2 (CR 002, 003, 006, 008, 009, 012, 017)	04.02.2011
1.4	Einarbeitung der Änderungen resultierend aus der aktualisierten KA 1.107 XSD	25.05.2011
1.4.1	Aktualisierung der Referenz auf die KA-XSD auf die mit KA KG abgestimmte KA_XML_Schema_V1107_K20110623.xsd.	30.06.2011
1.4.2	Aktualisierung der Referenz auf die KA-XSD auf die mit KA KG abgestimmte KA_XML_Schema_V1107_K20110801.xsd. Siehe auch Änderungsdokumentation zur KA XSD. Authentisierung per Nutzername/Kennwort statt per Zertifikat. Ergänzung einer Übersicht der in den TX_BASE verwendeten Org-IDs und KA Rollen	10.08.2011
1.4.3	Korrektur der Beschreibung zum Herunterladen der Paket-Quittungen Konkretisierung der Beschreibung zur Authentifizierung. Umbenennung Nachrichtentyp „RMVTariffModule“ in „RMVKontrollmodul“ im Manifest. Erweiterung der Datenstruktur PACKAGEACK um das Attribut „packageerrorcode“ Änderung der zu verwendenden Org-IDs und Rollen in den Attributen transSender und transEmpfänger des TX_BASE Ergänzung TXKNAWDM, TXKNAWA, TXKNAWB	07.10.2011
1.4.4	Ergänzung Hinweis bzgl. Eindeutigkeit der ID im TX_BASE, ggf. Bildung von Nummernkreisen für transSequenznummern Hinweis zur Durchführung der Kontrolltransaktion (TXEBER) unter Offene Punkte ergänzt.	-
1.5.1	Versand an üfB	08.11.2012
1.6	Erweiterung für SCG Ticketinfo Mobil Kontrollgeräte Änderung der referenzierten XSD von Version K20110801 auf K20120104. Verschiebung des Texts zu „Durchführung der Kontrolltransaktion (TXEBER)“ aus dem Kapitel „Offene Punkte“ in ein neues Kapitel „Hinweise zur technischen Umsetzung“. Hinweis: Die Änderungen haben für vorhandene TMS, die gemäß Version 1.4.3 (oder folgende) dieser Spezifikation realisiert wurden, keine Auswirkungen.	19.04.2013
1.7	Umsetzung vHGS CR 052: • TGZ als alternatives Format für Upload-Dateien und neue Grenz-	19.07.2013

Version	Anlass	Datum
	werte für die zulässige Dateigröße; • Ergänzung einer Namenskonvention für Upload-Dateien • Erweiterung der Paket-Quittung um TXB-Dateien und ERR-Dateien. • Behandlung von Duplikaten und wiederholtes Senden Hinweis zur Kodierung von Nullwerten in KA-Bytestrings ergänzt. Beschreibung zur Erkennung von Duplikaten und zur Behandlung des wiederholten Sendens erweitert und in neues Kap. 5.3 konsolidiert. Hinweis: Der erweiterte Inhalt der Paket-Quittung muss von TMS, die nach bisheriger SST-Spezifikation realisiert wurden, mindestens toleriert werden. Die Produktivsetzung der erweiterten SST im vHGS ist für den 30. Juli 2013 geplant.	
1.7.1	In Kapitel 2.2.5 die Vorgabe „Preemptive Authentication“ für die Basic Authentication ergänzt. Neues Kapitel 2.2.6 „Reaktion auf Verbindungsfehler“ (empfohlenes Muster für Wiederholungsversuche).	25.09.2013
1.8	Überarbeitung im Rahmen der Einführung der KA Version 1.3.0.	09.03.2016
1.9	Einarbeitung Kommentare aus dem Review der RMS (C. Gumbert)	13.06.2016
1.10	Einarbeitung weiterer Kommentare nach Abstimmung mit der RMS	22.06.2016
2.1	Finalisierung	21.07.2016
2.2	Ergänzung des KeyTypes 7 in TXCVCERTL. Hinweis auf Wegfall des Rollen-Code 31 (ALISE) in KA 1.3.0 Hinweis auf das Nullen datenschutzsensitiver Attribute in den TXEBER aus Kontrolle	15.06.2017

Verteiler

Organisation
rms - Rhein-Main-Verkehrsverbund Servicegesellschaft mbH
RMV - Rhein-Main-Verkehrsverbund
Cubic - Cubic Transportation Systems Deutschland GmbH
Verkehrsunternehmen und Lokale Nahverkehrsorganisationen (LNO) im RMV

Hinweis zum Urheberrecht

Vertraulichkeitsvermerk

Diese Arbeit wurde für das Projekt vHGS des RMV für die rms im Rahmen des eTicket RheinMain verfasst und vorgelegt. Alle Inhalte sind vertraulich zu behandeln.

Diese Arbeit unterliegt den zwischen rms und Cubic vereinbarten Nutzungsregelungen gem. §3 und den Vertraulichkeitsregelungen gem. §19 (2) des „Vertrages für ein verbundweites mandantenfähiges Hintergrundsystem eTicket RheinMain (vHGS)“ vom 07.10.2009.

Über den vertraglich zugelassenen Umfang hinaus darf diese Arbeit ohne die vorherige schriftliche Zustimmung von Cubic Transportation Systems (Deutschland) GmbH (weder vollständig noch in Auszügen) verändert, vervielfältigt, veröffentlicht oder an Dritte weitergegeben oder für andere Zwecke, als für jene, für die sie vorgelegt wurde, verwendet werden.

Inhalt

Referenzen

[KA_SPEC_SST_1107] Schnittstellenspezifikationen der Referenzsysteme KVP, DL, PV, AH, KOSE
VDV KA KG, Version 1.107, August 2010

[KA_SPEC_AktM_1107] Aktionsmanagement
VDV KA KG, Version 1.107, August 2010

[KA_SPEC_BOM_1107] Hauptdokument mit Basisobjektmodell (BOM)
VDV KA KG, Version 1.107, August 2010

[KA_SPEC_SAM_1107] Spezifikation des SAM
VDV KA KG, Version 1.107, August 2010

[KA_XSD_1107K] KA XML-Schema
VDV KA KG, Version 1.107 K20120104, 04.01.2012
KA_XML-Schema_V1107_K20120104.xsd
Hinweis: Die Version K20120104 enthält gegenüber der Version K20110801 Ergänzungen / Korrekturen im Bereich der Schnittstelle zum Massenpersonalisierer (Spec-PE). Die für die TMS-Schnittstelle relevanten Datenstrukturen sind in Version K20120104 gegenüber der Version K20110801 unverändert.

[KA_SPEC_SST_1300] Schnittstellenspezifikationen der Referenzsysteme KVP, DL, PV, AH, KOSE
VDV KA KG, Version 1.3.0, Juni 2014

[KA_SPEC_AktM_1300] Aktionsmanagement
VDV KA KG, Version 1.3.0, Juni 2014

[KA_SPEC_BOM_1300]	Hauptdokument mit Basisobjektmodell (BOM) VDV KA KG, Version 1.3.0, Juni 2014
[KA_SPEC_SAM_1300]	Spezifikation des SAM VDV KA KG, Version 1.300, Juni 2014
[KA_SPEC_MULTIBER_1300]	Spezifikation Multiberechtigung VDV KA KG, Version 1.300, Juni 2014
[KA_XSD_1300]	KA XML-Schema VDV KA KG, Version 1.300 Neben den originalen XSDs der KA liegen 4 weitere XSDs zur fachlichen Bündelung der getrennt vorliegenden XSDs bei. Die Bündelung bezieht sich auf AH, KOSE, KVP/PV/DL und PE. Eine weitere XSD enthält vHGS-TMS spezifische Definitionen.
[RMV KA 1.3.0 MBER]	RMV KA 1.3.0 inkl. Multiberechtigung im eTicket RheinMain, RMV, Version 1.0
[RMV_KA130_MBER]	RMV KA 1.3.0 MBER Konfiguration, RMV, Version 0001

1 Einleitung

1.1 Einordnung in das Gesamtsystem

Dieses Dokument spezifiziert die Schnittstelle des vHGS zur Verteilung von Daten an KA-Terminals (Mobile Kontrollgeräte, Einstiegskontrollgeräte sowie Verkaufsgeräte) und zur Übernahme von Daten aus den KA-Terminals. Die Datenformate orientieren sich an denen der VDV KA Spezifikation.

Die VDV KA Spezifikation unterscheidet zwischen DL-Terminals und DL-System bzw. KVP-Terminals und KVP-System, wobei lediglich die Schnittstellen des DL- bzw. KVP-Terminals zum Nutzermedium sowie die Schnittstelle des DL- bzw. KVP-Systems zu anderen KA-Hintergrundsystemen durch die VDV KA spezifiziert werden.

Die Schnittstelle zwischen den Terminals und dem jeweiligen (eigenen) Hintergrundsystem bleibt der Gestaltung durch den jeweiligen Systemlieferanten und das Verkehrsunternehmen vorbehalten. Seitens der VDV KA besteht lediglich die Anforderung, dass die VDV KA Transaktionsdaten auf dem Transportweg zwischen Terminal und Hintergrundsystem durch digitale Signaturen zu sichern sind.

Das Konzept des verbundweiten, mandantenfähigen Hintergrundsystems (vHGS) sieht vor, dass das DLS und/oder KVPS der Mandanten im vHGS repräsentiert ist und der Datenaustausch mit anderen KA-Rollen (insbesondere auch externen KA-Teilnehmern) mindestens in Bezug auf die EFM-Produkte des eTicket RheinMain über das vHGS realisiert wird.

Aufgrund dieses Zuschnitts der Systemgrenzen entsteht die Notwendigkeit zur Spezifikation einer vHGS-Schnittstelle für Terminalmanagementsysteme (bzw. Terminals) verschiedener Systemlieferanten. Das Terminalmanagementsystem stellt dabei eine Zwischenstation auf dem Weg von der normierten Schnittstelle des DLS (bzw. KVPS) mit anderen KA-Systemen (KOSES, PVS, AHS) zu der ebenfalls normierten Schnittstelle des DL-Terminals (bzw. KVP-Terminals) mit dem KA-Nutzermedium dar. Dieses Dokument beschreibt die Schnittstelle zwischen vHGS und den Terminalmanagementsystemen.

Die Terminals erfüllen hauptsächlich folgende Funktionen im Kontext des vHGS:

1. Kontrolle der Fahrtberechtigung (EFS) und NmApplikation unter Berücksichtigung von Sperrlisten
2. Ausführung von KVP-Transaktionen, die über eine Aktionsliste beauftragt werden.

Während Punkt 1 zwingend ist, kann es im Einzelfall Gruppen von Terminals geben, die den Punkt 2 nicht unterstützen.

Darüber hinaus werden von Verkaufsgeräten (personalbediente Verkaufsgeräte in Vertriebsstellen, Fahrerverkauf, Fahrkartenautomaten)

3. Fahrtberechtigungen (EFS) verkauft und ggf. Chipkarten mit NmApplikation ausgegeben.

Die Funktion dieser „Offline“-Verkaufsgeräte beschränkt sich auf den Barverkauf. Die Ausgabe von Fahrtberechtigungen aufgrund von Abonnements und anderen Vertragsprodukten ist ausgeschlossen.

Die auszutauschenden Daten ergeben sich im Wesentlichen aus der VDV KA.

1.2 KA-Rollen und Datenflüsse

1.2.1 Sperrmanagement

Der Datenaustausch gestaltet sich für Sperrlisten und die daraus resultierenden Sperrnachweise und Kontrollnachweise wie folgt:

- Jedes DLS (Mandant im vHGS) führt einen Sperrlistenabruf gegenüber dem KOSES (im vHGS) durch.
- Jedes Terminalmanagementsystem adressiert das eigene DLS im vHGS zum Abruf der Sperrlisten.
- Jedes Terminalmanagementsystem adressiert das eigene DLS im vHGS zur Ablieferung von Sperrnachweisen und Kontrollnachweisen.
- Das DLS leitet Sperrnachweise an das KOSES weiter.
- Das DLS leitet Kontrollnachweise an das PVS weiter.
- Das DLS erzeugt Sperranfragen aus Meldungen über defekte Medien.

Ergänzende Hinweise:

- Das DLS speichert die Sperrnachweise und Kontrollnachweise, jedoch nur für kurze Zeit (Systemparameter des vHGS mit RMV und Datenschutz abzustimmen, erwartete Größenordnung: 1 Woche), in der Online-Datenbank des vHGS.
- Das DLS bietet grundlegende Auswertungsmöglichkeiten (Reports/Statistik).
- Die im Konzept des eTicket RheinMain vorgesehene Verwendung einer „DL-Agentur“ bedingt, dass gegenüber externen KA-Teilnehmern nur diese „DL-Agentur“ in Erscheinung tritt. Die Zuordnung zu den einzelnen „handelnden DL“ (Verkehrsunternehmen) innerhalb des eTicket RheinMain wird durch das vHGS geleistet.

Für KVP-Terminals gelten die oben dargestellten Datenflüsse analog („KVPS“ an Stelle „DLS“).

1.2.2 Aktionsmanagement

Der Datenaustausch gestaltet sich für Aktionslisten und die daraus resultierenden Transaktionsnachweise wie folgt:

- Jedes KVPS (Mandant im vHGS) führt einen Aktionslistenabruf gegen das ALISES (im vHGS) durch.
- Jedes Terminalmanagementsystem adressiert das eigene KVPS im vHGS zum Abruf der Aktionsliste.
- Jedes Terminalmanagementsystem adressiert das eigene KVPS im vHGS zur Ablieferung von Transaktionsnachweisen aus der Ausführung von Einträgen aus der Aktionsliste.
- Das KVPS leitet als „ausführender KVP“ Transaktionsnachweise an PVS/ALISES weiter.

Ergänzende Hinweise:

- Das KVPS des ausführenden KVP speichert die Transaktionsnachweise nur für kurze Zeit. Eine dauerhafte Speicherung findet erst beim „beauftragenden KVP“ statt, der die Aktion beauftragt hat und die wirtschaftliche Verantwortung trägt.
- Das KVPS bietet grundlegende Auswertungsmöglichkeiten (Reports/Statistik) für den ausführenden KVP.

- Die im Konzept des eTicket RheinMain vorgesehene Verwendung einer „KVP-Agentur“ bedingt, dass gegenüber externen KA-Teilnehmern nur diese „KVP-Agentur“ in Erscheinung tritt. Die Zuordnung zu den einzelnen „handelnden KVP“ (Verkehrsunternehmen) innerhalb des eTicket RheinMain wird durch das vHGS geleistet.

1.2.3 Berechtigungsausgabe und Applikationsausgabe

Der Datenaustausch gestaltet sich für die Ausgabe von Berechtigungen und Applikationen wie folgt:

- Jedes Terminalmanagementsystem adressiert das eigene KVPS im vHGS zur Ablieferung von Transaktionsnachweisen über die Ausgabe von Berechtigungen und Applikationen.
- Das KVPS (Mandant im vHGS) leitet die Berechtigungsausgabe-Transaktionsnachweise an das PVS weiter.
- Das KVPS (Mandant im vHGS) leitet die Applikationsausgabe-Transaktionsnachweise an das AHS weiter.

Die Verkaufsgeräte nehmen wie alle KA-Terminals am Sperrmanagement teil. Es gelten die Ausführungen in Abschnitt 1.2.1.

Ergänzende Hinweise:

- Das KVPS (Mandant im vHGS) speichert die Transaktionsnachweise dauerhaft.
- Das KVPS erlaubt dem Mandanten die Verwaltung der ausgegebenen Berechtigung bzw. Chipkarte. Diesbezüglich unterscheidet sich die „offline“ ausgegebene Berechtigung bzw. Chipkarte nicht von einer „online“ durch die vHGS-pVKS ausgegebenen Berechtigung oder Chipkarte.
- Das KVPS erstellt aus den Transaktionsnachweisen Datensätze für die RMV-Verkaufsdatenmeldung. Das Pflichtenheft PH05-A1 enthält umfangreiche Vorgaben zu den im TXABER erwarteten Daten.
- Die im Konzept des eTicket RheinMain vorgesehene Verwendung einer „KVP-Agentur“ bedingt, dass gegenüber externen KA-Teilnehmern nur diese „KVP-Agentur“ in Erscheinung tritt. Die Zuordnung zu den einzelnen „handelnden KVP“ (Verkehrsunternehmen) innerhalb des eTicket RheinMain wird durch das vHGS geleistet.

1.3 Kontrollgeräte, Verkaufsgeräte und Terminalmanagementsysteme

Als Kontrollgeräte werden hier zusammenfassend die Mobilen Kontrollgeräte sowie die Einstiegskontrollgeräte bezeichnet, die im eTicket RheinMain der Kontrolle der Fahrtberechtigung sowie der Ausführung von KVP-Transaktionen aus einer Aktionsliste dienen.

Als Verkaufsgeräte werden hier zusammenfassend alle Geräte bezeichnet, die im eTicket RheinMain dem Verkauf von Fahrtberechtigungen dienen, ohne während des Verkaufsvorgangs mit dem vHGS verbunden zu sein. Typische Verkaufsgeräte sind Fahrerverkaufsgeräte („Busdrucker“), Fahrkartenautomaten, Verkaufsstellenarbeitsplatzsysteme.

Die Kontrollgeräte und Verkaufsgeräte werden von den Verkehrsunternehmen beschafft und betrieben.

Es wird davon ausgegangen, dass die Kontrollgeräte und Verkaufsgeräte in der Regel ein eigenes Managementsystem (im Folgenden als Terminalmanagementsystem bezeichnet) mitbringen, das

- den Datenaustausch mit den Geräten abwickelt,

- die Geräte mit Softwareaktualisierungen versorgt,
- die Geräte mit herstellerspezifisch für das Gerät aufbereiteten Grunddaten (Tarifmodul, Konfigurationsdaten, …) versorgt,
- den Status der Geräte überwacht (Auswertung der von den Geräten gelieferten Betriebsprotokolle/Störungsmeldungen, Bestandsführung über aktive und außer Betrieb befindliche Geräte, …).

Unbeschadet der Tatsache, dass das vHGS-Lastenheft auch die Möglichkeit einer direkten Kommunikation zwischen vHGS und Terminals zulässt, wird im Folgenden die Schnittstelle zwischen vHGS und Terminalmanagementsystemen beschrieben. Für den direkten Datenaustausch zwischen vHGS und einzelnen Terminals ist prinzipiell von der gleichen Schnittstelle auszugehen.

1.4 Anpassungen bzgl. KA 1.3.0

Mit der Erweiterung des vHGS dahingehend, dass neben der bisher unterstützten KA Version 1.107 (an der Schnittstelle 1.107K) auch die KA Version 1.3.0 unterstützt werden soll, wurde auch die TMS Schnittstelle angepasst.

Ob ein TMS KA 1.107K konforme Daten liefert und erhält oder KA 1.3.0 konforme Daten, muss im vHGS konfiguriert werden. Je nach Konfiguration werden auch nur die jeweils Versionskompatiblen Daten akzeptiert bzw. geliefert.

Der Mechanismus zur Datenübertragung bleibt grundsätzlich bestehen. Es ändern sich mit einer Umstellung auf KA 1.3.0 lediglich die ausgetauschten Daten.

In den folgenden Kapiteln gibt es, sofern notwendig, einen Unterpunkt bzgl. der Anpassung zur KA 1.3.0 Konformität.

2 Grundlagen

2.1 Daten

2.1.1 RMV EFS

Die in PH05-A1 festgelegte Datenstruktur „RMV EFS“ für den im eTicket RheinMain eingesetzten KA-konformen EFS ist geeignet, alle existierenden Produkte des regulären RMV-Tarifs abzubilden. Die Datenstruktur des RMV EFS ist von allen im eTicket RheinMain eingesetzten Geräten auf Grundlage der Spezifikation im PH05-A1 zu implementieren.

Neben der Datenstruktur „RMV-EFS“ wird in PH05-A1 auch der BerechtigungTarifbereichZusatz spezifiziert, wie er in der Datenstruktur TXABER im eTicket RheinMain zu verwenden ist.

Weiterhin enthält PH05-A1 detaillierte Vorgaben zu den zu verwendenden KA Typ-Codes (Terminal-Typen, Ort-Typen, …), zur Verwendung der Attribute des RMV-EFS und des BerechtigungTarifbereichZusatz und den in der Stammdatenverwaltung des vHGS zu pflegenden Daten.

2.1.2 KA Transaktionsdatensätze (TX*)

Es werden die XML-Datenstrukturen aus der VDV KA Spezifikation [KA_SPEC_SST_1107] bzw. [KA_SPEC_SST_1300] verwendet. Diese Datenstrukturen wurden ursprünglich für den Datenaustausch zwischen KA-Hintergrundsystemen entworfen. Für den Einsatz an der Schnittstelle zwischen vHGS und Terminalmanagementsystemen sind einige ergänzende Festlegungen erforderlich, siehe Kapitel 4.

Die Festlegungen in Kapitel 4.zur Verwendung der KA-Datenstrukturen (insbes. zu den Sender-/Empfänger-Attributen des TX_BASE) folgen pragmatischen Erwägungen. Wie in Abschnitt 1.2 ausgeführt, ist die Kommunikation an der Schnittstelle zwischen vHGS und Terminalmanagementsystem eine interne Kommunikation zwischen zwei IT-Systemen eines Verkehrsunternehmens. Die Zuordnung des Datenverkehrs zu einem Mandanten erfolgt im vHGS einzig anhand der Device-ID des Terminalmanagementsystems und nicht anhand der Sender-/Empfänger-Attribute des TX_BASE. Ein Mandant (Verkehrsunternehmen) kann mehr als ein Terminalmanagementsystem betreiben und diese unter getrennten Device-IDs im vHGS registrieren.

Für das Schlüsselmanagement (siehe Abschnitt 2.1.6) wurden proprietäre Transaktionen spezifiziert, die der KA TX Struktur folgen. Dabei werden die folgenden Transaktionstypcodes aus dem für proprietäre Verwendung reservierten Wertebereich des IONTransaktionsTyp_Code, vgl. [KA_SPEC_BOM_1107] / [KA_SPEC_BOM_1300]verwendet:

- 252 TXSYMKEYL
- 253 TXSYMKEYACK
- 254 TXCVCERTL

2.1.3 RMV Tarifmodul (Kontrollmodul)

Für die Durchführung der Kontrolle der RMV EFS wird dem Terminalmanagementsystem seitens des vHGS das RMV Kontrollmodul (Tarifmodul zur Kontrolle von RMV-EFS) bereitgestellt. Das RMV Tarifmodul (Kontrollmodul) dient dem gleichen Zweck wie das in der [KA_SPEC_SST_1107] bzw. [KA_SPEC_SST_1300] beschriebene „Produktmodul“, hat aber technisch eine andere Gestalt.

Ergänzungen / Änderungen mit Einführung KA 1.3.0

RMV-seitig wurde entschieden, dass die Funktionalität zur Bereitstellung des RMV-Tarifmoduls ab der Schnittstellenversion KA 1.3.0 eingestellt wird.

Der Mechanismus zur Verteilung des Tarifmoduls wird stattdessen zur Verteilung von weiterhin tariflich relevanten Konfigurationsdateien wie z. B. der Multiberechtigungs-Konfiguration verwendet.
Vgl. hierzu Dokument [RMV KA 1.3.0 MBER] und Konfigurationsdatei [RMV_KA130_MBER].

2.1.4 Kontrolle

2.1.4.1 Sperrlisten und Sperrnachweise

Die auszutauschenden Daten sind in [KA_SPEC_SST_1107] spezifiziert.

Das Terminalmanagementsystem erhält vom vHGS:

- Sperrlisten TXSLNM, TXSLK, TXSLOS

Das Terminalmanagementsystem liefert an das vHGS:

- Sperrnachweise TXSNAWA, TXSNAWB

Ergänzungen / Änderungen mit Einführung KA 1.3.0

Sofern die Schnittstelle nach KA 1.3.0 betrieben wird, erhält das Terminalmanagementsystem vom vHGS folgende, in [KA_SPEC_SST_1300] spezifizierte, Listen:

- Sperrlisten TXSLNMRESP, TXSLKASYMRESP, TXSLKSYMRESP, TXSLORGRESP, TXSLSAMRESP

Die Sperrnachweise werden wie bisher als TXSNAWA bzw. TXSNAWB durch das TMS an das vHGS übertragen.

2.1.4.2 Kontrollnachweise

Die auszutauschenden Daten sind in [KA_SPEC_SST_1107], [KA_SPEC_SST_1300] spezifiziert.

Das Terminalmanagementsystem liefert an das vHGS:

- Kontrollnachweise TXEBER
- Meldung defekter Medien TXKNAWDM
- Rumpfkontrollnachweise TXKNAWA, TXKNAWB

Gemäß den Vorgaben des RMV (in Übereinstimmung mit denen der VDV KA) sollen bei Kontrollen im Regelfall Kontrollnachweise TXEBER erzeugt werden.

Ergänzungen / Änderungen mit Einführung KA 1.3.0

Neben den bisher ausgetauschten Transaktionen können nach der Umstellung auf KA 1.3.0 auch die Transaktionen bzgl. Multiberechtigungen (siehe [KA_SPEC_MULTIBER_1300]) übermittelt werden:

- TXEMBER

2.1.5 Aktionsausführung

Die auszutauschenden Daten sind in [KA_SPEC_AktM_1107], [KA_SPEC_SST_1300] spezifiziert.

Gegenstand des Aktionsmanagements ist die Ausführung folgender KVP-Aktionen über eine Aktionsliste: Berechtigung-Ausgabe, Berechtigung-Rücknahme, Berechtigung-Entsperrung.

Das Terminalmanagementsystem erhält vom vHGS:

- Aktionsliste TXAML

Das Terminalmanagementsystem liefert an das vHGS:

- Transaktionsnachweise TXABER, TXRBER, TXSNAWB (Entsperrung), wobei die Transaktionsnachweise entsprechend den Vorgaben der [KA_SPEC_AktM_1107], [KA_SPEC_AktM_1300] über spezifische KA-Transaktionstyp-Codes[1] als Ergebnis der Ausführung eines Aktionslisteneintrags gekennzeichnet sind.

Die in der Spezifikation [KA_SPEC_AktM_1107], [KA_SPEC_AktM_1300] beschriebenen Mechanismen (a) Differenzlisten und (b) spezifische Aktionslisten für einzelne Terminals bzw. Terminalgruppen werden zum Systemstart des eTicket RheinMain nicht eingesetzt. Es ist geplant, diese Mechanismen in einer nachfolgenden Ausbaustufe des Systems zu ergänzen.

Ergänzungen / Änderungen mit Einführung KA 1.3.0

Neben den bisher ausgetauschten Transaktionen können nach der Umstellung auf KA 1.3.0 auch die Transaktionen bzgl. Multiberechtigungen (siehe [KA_SPEC_MULTIBER_1300]) übermittelt werden:

- TXAMBER, TXRMBER

2.1.6 Verkauf

Die auszutauschenden Daten sind in [KA_SPEC_SST_1107], [KA_SPEC_SST_1300] spezifiziert.

Das Terminalmanagementsystem liefert an das vHGS:

- Ausgabenachweise TXABER und TXAA

Es sind die Vorgaben des PH05-A1 zur Verwendung des TXABER zu berücksichtigen.

Ergänzungen / Änderungen mit Einführung KA 1.3.0

Neben den bisher ausgetauschten Transaktionen können nach der Umstellung auf KA 1.3.0 auch die Transaktionen bzgl. Multiberechtigungen (siehe [KA_SPEC_MULTIBER_1300]) übermittelt werden:

- TXAMBER, TXRMBER

2.1.7 Schlüsselmanagement

Die auszutauschenden Daten ergeben sich aus verschiedenen Dokumenten der VDV KA KG zur Umsetzung des Schlüsselmanagements.

---

[1] logTransaktionsTyp (NmTransaktionsTyp_CODE): TXABER – Ausgabe EFS über Aktionsliste = 37, TXSNAWB - Entsperrtransaktion EFS über Aktionsliste = 38 und Rückgabetransaktion EFS über Aktionsliste = 39

Das Terminalmanagementsystem erhält vom vHGS:

- TXSYMKEYL - Kryptogramme der in die SAMs zu ladenden symmetrischen Schlüssel,
- TXCVCERTL - CV Zertifikate der in die SAMs zu ladenden Zertifikate.

Das Terminalmanagementsystem liefert an das vHGS:

- Bestätigungen, dass es die Kryptogramme bzw. Zertifikate erhalten hat;
- TXSYMKEYACK - Bestätigungen, dass SAMs die für sie bestimmten Schlüssel geladen haben.

2.2 Technische Festlegungen

2.2.1 Simple Web-Services

Für die Kommunikation werden simple Webservices durch das vHGS angeboten.

Der Aufruf einer Schnittstelle ist einerseits durch die URL und andererseits durch HTTP-Methoden und HTTP-Attribute definiert. Die in diesem Dokument spezifizierten WebServices verwenden die HTTP-Methoden GET und POST.

Die Schnittstelle ist so gestaltet, dass die Terminalmanagementsysteme stets als Web-Service-Nutzer die vom vHGS angebotenen Web-Services aufrufen. Die Terminalmanagementsysteme müssen ihrerseits keine Web-Services anbieten.

2.2.2 HTTP Methoden und Attribute

Sofern in den nachfolgenden Detailspezifikationen nichts Abweichendes festgelegt wird, werden für die eingesetzten Methoden GET und POST die folgenden Attribute verwendet:

- GET: Herunterladen von Dateien
  - Aufrufparameter sind Bestandteil der URL.
  - Herunterzuladende Datei ist im HTTP-CONTENT der Antwort enthalten.
  - Content-Type (Mimetype) ist “application/x-zip-compressed oder “application/x-tgz””.
- POST: Hochladen von Dateien
  - Aufrufparameter sind Bestandteil der URL.
  - Hochzuladende Datei ist im HTTP-CONTENT enthalten.
  - Content-Type (Mimetype) ist “application/x-zip-compressed” oder “application/x-tgz”.
  - Content-Length enthält die Größe der hochgeladenen Datei in Bytes. Sofern diese Angabe nicht mit der tatsächlichen Größe der Datei im HTTP-CONTENT übereinstimmt, wird die Datei abgewiesen.

2.2.3 HTTP Rückgabewerte

Es werden standardkonforme HTTP Status-Codes als Rückgabewerte verwendet. Die HTTP Status-Codes sind im RFC 2616 (sowie RFC 2518, RFC 2817, RFC 2295, RFC 2774, RFC 4918) spezifiziert.

2.2.4 Dateiformate ZIP/TGZ und XML

Daten werden generell komprimiert als ZIP-Dateien (Dateiendung „.zip“) übertragen. Eine ZIP-Datei kann ein oder mehrere Dateien enthalten. In den meisten Fällen handelt es sich um XML-Dateien, siehe Detailbeschreibungen der Web-Services.

Für das Hochladen von Transaktionsdaten (siehe Kap. 3.8) kann alternativ auch eine TGZ-Datei (Dateiendung „.tgz“ oder „.tar.gz“) verwendet werden. Eine TGZ-Datei ist ein ZIP-Archiv, das eine TAR-Datei enthält, die wiederum ein oder mehrere Dateien enthält. Wenn ein Transaktionsdatenpaket als TGZ-Datei hochgeladen wurde, wird die zugehörige Paketquittung (siehe Kap. 0) vom vHGS als TGZ-Datei bereitgestellt.

Die Kodierung von XML-Dateien steht grundsätzlich in der ersten Zeile jeder XML-Datei. Enthält eine Datei keine Angaben, so wird UTF-8 verwendet.

Erste Zeile einer XML-Datei:

```
<?xml version="1.0" encoding="UTF-8"?>
```
[2]

Zur Gewährleistung eines reibungslosen Betriebs für alle Beteiligten (Antwortzeiten, Durchsatz) werden folgende Beschränkungen für die von den Terminalmanagementsystemen in das vHGS hochgeladenen Dateien festgelegt:

- ZIP-Datei
  - Maximal Anzahl von Dateien in der ZIP-Datei: 32 000
  - Maximale Größe einer ZIP-Datei: 2 MB
- TGZ-Datei
  - Maximal Anzahl von Dateien in der TAR-Datei: 32 000
  - Maximale Größe einer ZIP-Datei: 1 MB

Die Kontrollgeräte bzw. deren Terminalmanagementsysteme müssen die Erzeugung der von ihnen an das vHGS zu liefernden Dateien so steuern, dass die oben genannten Grenzwerte nicht überschritten werden. Das vHGS wird Dateien, die die oben genannten Grenzwerte überschreiten abweisen. Die Grenzwerte sind im vHGS als Systemparameter einstellbar und können ggf. angepasst werden, um den Erfordernissen des realen Betriebsgeschehens gerecht zu werden.

2.2.5 Authentifizierung

Die Terminalmanagementsysteme (bzw. einzelne Kontrollgeräte, soweit sie direkt mit dem vHGS kommunizieren sollten) erhalten eindeutige Kennungen (Device-ID), unter denen sie im vHGS geführt werden. Die Device-ID wird von der Betriebsführung des vHGS vergeben und ist in den Konfigurationsdaten des vHGS und des Terminalmanagementsystems einzutragen.

Beim Aufruf eines der Web-Services teilt das aufrufende System seine Kennung im Aufrufparameter Device-ID mit.

Die Authentifizierung gegenüber dem Web-Service erfolgt mittels http Basic Authentication (Preemptive Authentication[3]) durch Angabe einer Benutzername-Passwort-Kombination. Damit authentifiziert sich der Web-Service-Nutzer (d.h. das jeweilige Terminalmanagementsystem) nach Etablierung des SSL-gesicherten Kommunikationskanals (https). Die Authentifizierung ist für jeden Aufruf der Schnittstelle erforderlich (es werden keine Sessions etabliert). Als Benutzername wird die Device-ID verwendet. Das Passwort wird von der Betriebsführung des vHGS vergeben und ist in den Konfigurationsdaten des vHGS und des Terminalmanagementsystems einzutragen.

Es wird seitens des vHGS sichergestellt, dass jedes Terminalmanagementsystem nur seine eigenen Daten abholen kann.

2.2.6 Reaktion auf Verbindungsfehler

Sofern der Aufbau der Verbindung vom TMS zum vHGS scheitert, soll das TMS Wiederholungsversuche nach folgendem Muster durchführen:

---

[2] Die Reihenfolge der Attribute version und encoding kann – wie es der XML Standard erlaubt – variieren.

[3] Preemptive Authentication - Dies bedeutet, dass der Client User und Passwort ohne Aufforderung durch den Server zu schicken hat.

- 3 Wiederholungsversuche jeweils im Abstand von 3 Minuten,
- erneuter Versuch nach 1 Stunde,
- erneuter Versuch nach 1 weiteren Stunde.

Es ist auszuschließen, dass das TMS eine Vielzahl von Versuchen innerhalb weniger Sekunden unternimmt, da dies ggf. von den beteiligten Firewalls als Bedrohung gewertet wird. Ebenso muss gewährleistet werden, dass bei einem Wiederholungsversuch nur die Daten heruntergeladen bzw. hochgeladen werden, die noch nicht übertragen wurden.

Zum Umgang mit Duplikaten und „Wiederholtem Senden“ von KA Transaktionsdaten siehe Kapitel 5.3.

Im Rahmen der Abstimmung zwischen dem vHGS und den TMS Herstellern bzw. Betreibern soll weiterhin ein HTTP Timeout festgelegt werden. Zunächst wird eine Zeitspanne von 180 Sekunden festgelegt. Diese müssen sowohl das vHGS als auch die TMS berücksichtigen.

3 Anwendungsfälle

3.1 Allgemeiner Ablauf

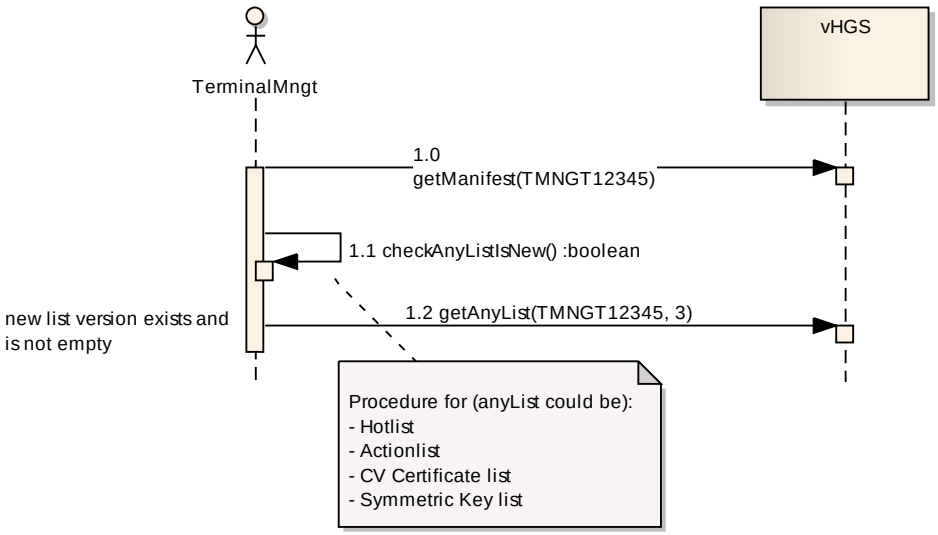
Zum Abrufen einer Nachricht (z.B. Aktionsliste) gilt folgender grundlegender Ablauf:

1.0 Aufrufer lädt die Manifest-Datei herunter.

1.1 Aufrufer prüft anhand der Nachrichtentypen und der Nachricht-ID, ob eine neue Nachricht vorhanden ist. Die Prüfung erfolgt gegenüber lokal gespeicherten Informationen über bereits heruntergeladene Nachrichten.

1.2 Nur falls eine neue Nachricht existiert, lädt der Aufrufer die Nachricht (z.B. die aktuelle Version der Aktionsliste) herunter.

Die nachfolgende Abbildung veranschaulicht den Ablauf.



Für das Einreichen von Transaktionen gilt der folgende Ablauf:

1.0 Der Aufrufer sendet ein Paket mit Transaktionsdaten an das vHGS. Jede Transaktion hat eine eindeutige Referenznummer. Das vHGS speichert das Paket, generiert eine Paketnummer und gibt diese zurück.

1.1 Der Scheduler startet die Verarbeitung der Transaktionen.

1.2 Das vHGS verarbeitet die Transaktionen. Das vHGS stellt dabei für jede abzulehnende Transaktion (z.B. fehlerhafte Formate, negatives Ergebnis der MAC-Prüfung, inkonsistente Daten) einen Ablehnungsdatensatz TXA und für jede akzeptierte Transaktion einen Bestätigungsdatensatz TXB aus.

1.3 Das vHGS erstellt eine Zusammenfassung und stellt diese zusammen mit den TXB, TXA und ERR-Dateien in einer Antwort-Datei als Paket-Quittung bereit.

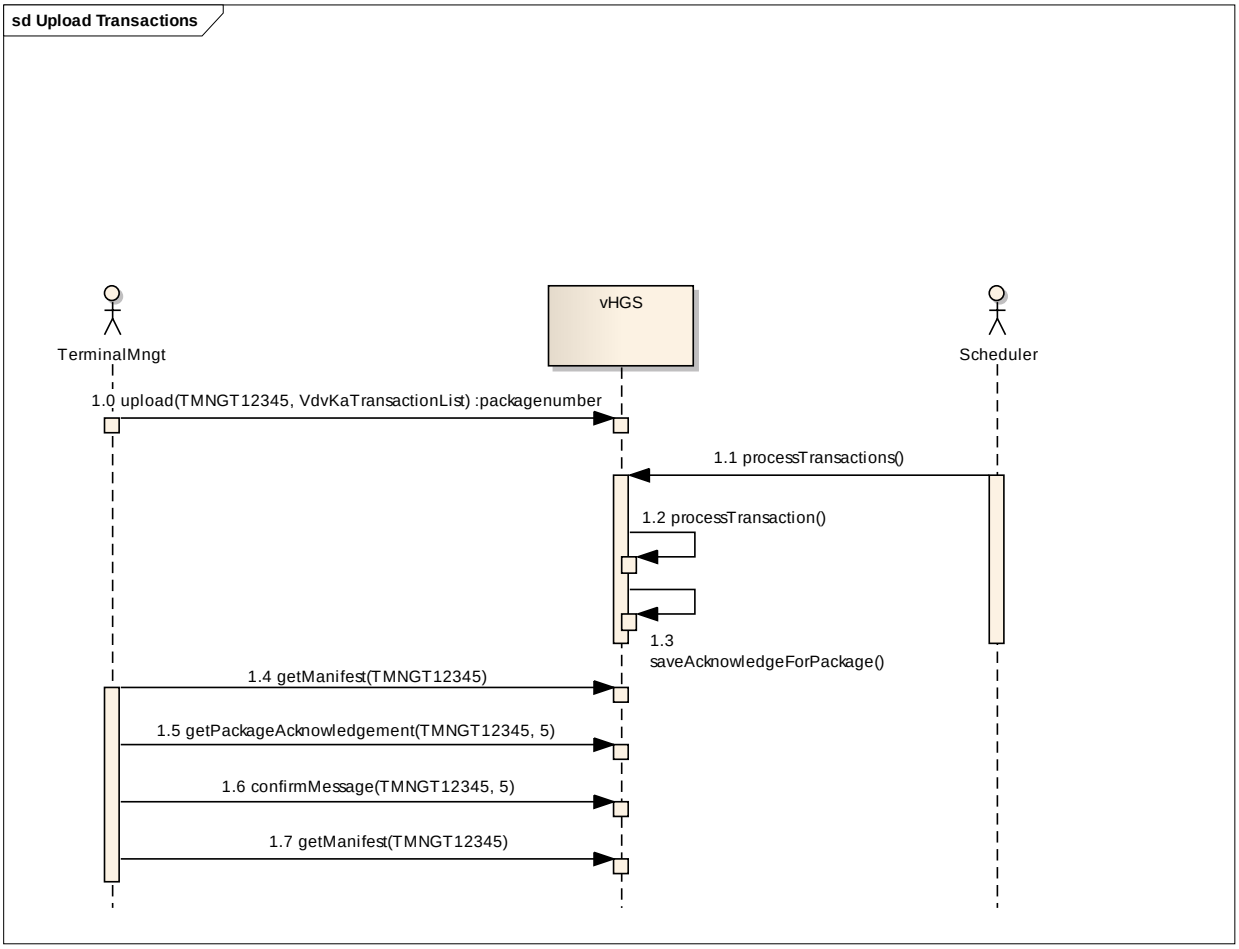
1.4 Zu einem späteren Zeitpunkt lädt der Aufrufer die Manifest-Datei herunter. In der Manifest-Datei wird die neu zur Verfügung stehende Paket-Quittung angegeben.

1.5 Der Aufrufer holt diese Paket-Quittung und verarbeitet diese Antwort. Die Transaktionen, auf die sich die Paket-Quittung bezieht, können anhand der in der Paket-Quittung enthalte-

nen Paketnummer identifiziert werden. Zum Beispiel kann jetzt die in Schritt 1.0 hochgeladene Liste als „erfolgreich geliefert“ markiert und archiviert bzw. gelöscht werden.

1.6 Der Aufrufer bestätigt den Erhalt der Paket-Quittung. Das vHGS entfernt die Paket-Quittung aus dem Manifest.

1.7 Beim erneuten Abruf der Manifest-Datei ist die Paket-Quittung in der Paket-Quittungs-Liste nicht mehr aufgeführt.



3.2 Manifest herunterladen

Get Manifest

https://..../ManifestServlet?DeviceId=<terminalMngtID>

Beschreibung

Diese Schnittstelle liefert eine Beschreibung der aktuellen Daten („Nachrichten“, engl. „Messages“), die für den Aufrufer bereitstehen. Der Aufrufer kann anhand dieser Manifest-Daten entscheiden, ob die entsprechenden Nachrichten (insbes. Sperr- und Aktionslisten) geholt werden müssen.

Intervall zur Abfrage einer Manifest-Datei zum Bezug aller verfügbaren Listen ist einmal täglich, da insbesondere die Sperr- und Aktionslisten auch nur einmal täglich erstellt und bereitgestellt werden.

Der Zeitpunkt zum Upload von Transaktionen bzw. Download von Listen wird für jedes TMS durch die Übergeordnete Fachliche Betriebsführung vHGS vorgegeben.

Sollte ein Terminalmanagementsystem die Listen permanent (Schwellwerte werden über Systemparameter konfiguriert) abrufen, wertet das System dies als Fehlfunktion und lehnt den Aufruf ab.

HTTP-Request-Methode

GET

Parameter

- terminalMngtID
  Identifiziert eindeutig ein externes Terminal Management System

Rückgabewert

ZIP-Datei (ManifestServlet.zip), die die Manifest-Datei (*OpNTCIPManifest.xml*) mit Informationen über die aktuellen Daten, die für den Aufrufer bereitstehen, enthält.

Ausnahmen

Sollten bei einer Anfrage Probleme auftreten und der Request wird nicht sauber bearbeitet, so wird ein entsprechender HTTP CODE zurückgegeben.

- CODE 404: terminalMngtID existiert nicht

Beispiel

Aufruf: https://vhgs.rmv.de/tl/ManifestServlet?DeviceId= 10001-201-00001

Rückgabe: ZIP-Datei mit der Manifest-Datei OpNTCIPManifest.xml

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<OpNTCIPManifestCollection Created="2016-06-13T09:39:42Z"
    DeviceId="DEHAMD-QA01" MessageId="21" MajorVersion="2" MinorVersion="0">
    <OpNTCIPManifest DeviceId="DEHAMD-QA01">
        <config-id>0</config-id>
        <device-id>DEHAMD-QA01</device-id>
        <location-id>0</location-id>
        <message-list>
            <OpNTCIPManifest_message>
                <message-name>TXAML</message-name>
                <major-version>1</major-version>
```

```
                <minor-version>0</minor-version>
                <message-id>615</message-id>
                <created-date>2016-06-10T15:57:04Z</created-date>
            </OpNTCIPManifest_message>
            <OpNTCIPManifest_message>
                <message-name>TXSLOS</message-name>
                <major-version>1</major-version>
                <minor-version>0</minor-version>
                <message-id>602</message-id>
                <created-date>2016-05-24T22:15:00Z</created-date>
            </OpNTCIPManifest_message>
            <OpNTCIPManifest_message>
                <message-name>TXSLNM</message-name>
                <major-version>1</major-version>
                <minor-version>0</minor-version>
                <message-id>614</message-id>
                <created-date>2016-06-08T22:15:00Z</created-date>
            </OpNTCIPManifest_message>
            <OpNTCIPManifest_message>
                <message-name>TXSLK</message-name>
                <major-version>1</major-version>
                <minor-version>0</minor-version>
                <message-id>141</message-id>
                <created-date>2015-10-12T22:15:00Z</created-date>
            </OpNTCIPManifest_message>
            <OpNTCIPManifest_message>
                <message-name>TXCVCERTL</message-name>
                <major-version>1</major-version>
                <minor-version>0</minor-version>
                <message-id>447</message-id>
                <created-date>2016-02-23T12:31:25Z</created-date>
            </OpNTCIPManifest_message>
        </message-list>
    </OpNTCIPManifest>
</OpNTCIPManifestCollection>
```

3.3 Sperrlisten herunterladen

Get Hotlists

https://..../MessageServlet?DeviceId=<terminalMngtID>&MessageId=<messageID>

Beschreibung

Diese Schnittstelle liefert die angeforderte Sperrliste über

- Berechtigungen und Applikationen,
- SAMs und Organisationen oder
- Schlüssel.

Die zu verwendende Nachricht-ID für die aktuelle Version der jeweiligen Liste ist in der Manifest-Datei abzulesen.

Durch die Anwendung der Sperrlisten in den Terminals (siehe KA Spezifikationen) entstehen Sperrnachweise. Diese werden über die Schnittstelle „Post VDV KA Transaction List“ an das vHGS geschickt.

HTTP-Request-Methode

GET

Parameter

- terminalMngtID
  Identifiziert eindeutig ein externes Terminal Management System
- messageID
  Nachricht-ID der Sperrliste. Siehe Manifest-Datei (Kapitel 3.2).

Rückgabewert

Als Rückgabe wird eine ZIP-Datei (MessageServlet.zip) geschickt, welche die angeforderte Sperrliste in der für das TMS konfigurierten KA Version enthält.

Ausnahmen

Sollten bei einer Anfrage Probleme auftreten und der Request wird nicht sauber bearbeitet, so wird ein entsprechender HTTP CODE zurückgegeben.

CODE 404: terminalMngtID oder messageID existiert nicht. Siehe http-Content für Details. Falls die angegebene Nachricht-ID nicht existiert, kann über einen erneuten Abruf der Manifest-Datei überprüft werden, ob die richtige Nachricht-ID verwendet wurde.

Beispiel:

Aufruf:
https://vhgs.rmv.de/tl/MessageServlet?DeviceId=10003-000-00001&MessageId=23

Rückgabe: ZIP-Datei mit der Datei TXSLNM.XML

TXSLNM.XML

3.4 Aktionsliste herunterladen

Get Actionlist

https://.../MessageServlet?DeviceId=<terminalMngtID>&MessageId=<messageID>

Beschreibung

Diese Schnittstelle liefert die angeforderte Aktionsliste für den Aufrufer zurück. Die zu verwendende Nachricht-ID für die aktuelle Version der Aktionsliste ist in der Manifest-Datei abzulesen.

HTTP-Request-Methode:

GET

Parameter

- terminalMngtID
  Identifiziert eindeutig ein externes Terminal Management System
- messageID
  Nachricht-ID der Aktionsliste. Siehe Manifest-Datei (Kapitel 3.2).

Rückgabewert

Als Rückgabe wird eine ZIP-Datei (MessageServlet.zip) geschickt, welche die angeforderte Aktionsliste in der für das TMS konfigurierten KA Version enthält.

Ausnahmen

Sollten bei einer Anfrage Probleme auftreten und der Request wird nicht sauber bearbeitet, so wird ein entsprechender HTTP CODE zurückgegeben.

- CODE 404: terminalMngtID oder messageID existiert nicht. Siehe http-Content für Details. Falls die angegebene Nachricht-ID nicht existiert, kann über einen erneuten Abruf der Manifest-Datei überprüft werden, ob die richtige Nachricht-ID verwendet wurde.

Beispiel

Aufruf:
https://vhgs.rmv.de/tl/MessageServlet?DeviceId=10003-000-00001&MessageId=25

Rückgabe: ZIP-Datei mit der Datei TXAML.XML

3.5 Kryptogrammliste (symmetrische Schlüssel) herunterladen

Get Symmetric Key List

https://..../MessageServlet?DeviceId=<terminalMngtID>&MessageId=<messageID>

Beschreibung

Diese Schnittstelle liefert die angeforderte Liste von symmetrischen Schlüsseln für den Aufrufer zurück. Die zu verwendende Nachricht-ID für die Liste ist in der Manifest-Datei abzulesen.

Die symmetrischen Schlüssel werden für ein SAM benötigt, das entweder neue Versionen vorhandener Schlüssel oder zusätzliche Schlüssel braucht. Diese Schlüssel werden mit dem SAM Kommando LOAD KEY auf das SAM geladen (Siehe [KA_SPEC_SAM_1107], [KA_SPEC_SAM_1300] Kapitel 6.2.2).

Damit eine Organisation Schlüssel mit ihrer Org-ID einbringen kann, wird dazu ein entsprechendes Zertifikat mit einem CHA von ‘56 44 56 5F 4B 41 1A‘ (Beispiel) benötigt. Dieses Zertifikat kann über die Schnittstelle „Get CV Certificate List“ abgeholt werden.

Der Empfang der Liste muss durch „Erhalt einer Nachricht bestätigen“ bestätigt werden.

HTTP-Request-Methode

GET

Parameter

- terminalMngtID
  Identifiziert eindeutig ein externes Terminal Management System
- messageID
  Nachricht-ID der Schlüsselliste. Siehe Manifest-Datei (Kapitel 3.2).

Rückgabewert

Als Rückgabe wird eine ZIP-Datei (MessageServlet.zip) geschickt.

Die ZIP-Datei enthält eine Datei mit dem Namen TXSYMKEYL.XML. Der Inhalt der Datei hat das Format TXSYMKEYL (siehe Abschnitt 4.3.2).

Ausnahmen

Sollten bei einer Anfrage Probleme auftreten und der Request wird nicht sauber bearbeitet, so wird ein entsprechender HTTP CODE zurückgegeben.

- CODE 404: terminalMngtID oder messageID existiert nicht. Siehe http-Content für Details. Falls die angegebene Nachricht-ID nicht existiert, kann über einen erneuten Abruf der Manifest-Datei überprüft werden, ob die richtige Nachricht-ID verwendet wurde.

Beispiel

Aufruf:
https://vhgs.rmv.de/tl/MessageServlet?DeviceId=35159-015-00001&MessageId=381

Rückgabe: ZIP-Datei mit der Datei TXSYMKEYL.XML

3.6 CV-Zertifikatsliste herunterladen

Get CV Certificate List

https://..../MessageServlet?DeviceId=<terminalMngtID>&MessageId=<messageID>

Beschreibung

Diese Schnittstelle liefert die angeforderte Liste von CV Zertifikaten (Card Verifiable Certificates) für den Aufrufer zurück. Die zu verwendende Nachricht-ID für die Liste ist in der Manifest-Datei abzulesen.

CV Zertifikate werden unter anderem für folgendes verwendet:

- Zertifizierung von öffentlichen Schlüsseln
- Autorisierung über den CHA-Inhalt. Z.B. Autorisierung zum Verkauf von Tickets einer anderen Organisation (Siehe [KA_SPEC_SAM] Kapitel 4.3.1.3.1). Das SAM gibt sich durch ein Zertifikat als eine andere Org-ID gegenüber dem NM aus.

Der Empfang der Liste muss durch „Erhalt einer Nachricht bestätigen“ bestätigt werden.

HTTP-Request-Methode

GET

Parameter

- terminalMngtID
  Identifiziert eindeutig ein externes Terminal Management System
- messageID
  Nachricht-ID der Zertifikatsliste. Siehe Manifest-Datei (Kapitel 3.2).

Rückgabewert

Als Rückgabe wird eine ZIP-Datei (MessageServlet.zip) geschickt.

Die ZIP-Datei enthält eine Datei mit dem Namen TXCVCERTL.XML. Der Inhalt der Datei hat das Format TXCVCERTL (siehe Abschnitt 4.7).

Ausnahmen

Sollten bei einer Anfrage Probleme auftreten und der Request wird nicht sauber bearbeitet, so wird ein entsprechender HTTP CODE zurückgegeben.

- CODE 404: terminalMngtID oder messageID existiert nicht. Siehe http-Content für Details. Falls die angegebene Nachricht-ID nicht existiert, kann über einen erneuten Abruf der Manifest-Datei überprüft werden, ob die richtige Nachricht-ID verwendet wurde.

Beispiel

Aufruf:

https://vhgs.rmv.de/tl/MessageServlet?DeviceId=10003-000-00001&MessageId=22

- Rückgabe: ZIP-Datei mit der Datei TXCVCERTL.XML

3.7 Tarifmodul (Kontrollmodul) herunterladen

Hinweis: RMV-seitig wurde entschieden, dass die Funktionalität zur Bereitstellung des RMV-Tarifmoduls ab der Schnittstellenversion KA 1.3.0 eingestellt wird.

Der Mechanismus zur Verteilung des Tarifmoduls wird stattdessen zur Verteilung von weiterhin tariflich relevanten Konfigurationsdateien wie z. B. der Multiberechtigungs-Konfiguration verwendet – vgl. hierzu auch Dokument [RMV KA 1.3.0 MBER].

Get Tariff Module

https://..../MessageServlet?DeviceId=<terminalMngtID>&MessageId=<messageID>

Beschreibung

Diese Schnittstelle liefert die angeforderte Version des RMV-Kontrollmoduls für den Aufrufer zurück. Die zu verwendende Nachricht-ID für die aktuelle Version des RMV-Kontrollmoduls ist in der Manifest-Datei abzulesen.

HTTP-Request-Methode

GET

Parameter

- terminalMngtID
  Identifiziert eindeutig ein externes Terminal Management System
- messageID
  Nachricht-ID des Kontrollmoduls. Siehe Manifest-Datei (Kapitel 3.2).

Rückgabewert

Als Rückgabe wird eine ZIP-Datei (MessageServlet.zip) geschickt.

Ausnahmen

Sollten bei einer Anfrage Probleme auftreten und der Request wird nicht sauber bearbeitet, so wird ein entsprechender HTTP CODE zurückgegeben.

- CODE 404: terminalMngtID oder messageID existiert nicht. Siehe http-Content für Details. Falls die angegebene Nachricht-ID nicht existiert, kann über einen erneuten Abruf der Manifest-Datei überprüft werden, ob die richtige Nachricht-ID verwendet wurde.

Beispiel

Aufruf:

https://vhgs.rmv.de/tl/MessageServlet?DeviceId=35159-015-00001&MessageId=334

Rückgabe: ZIP-Datei.

Der Inhalt der ZIP-Datei wird vom RMV bzw. dem Lieferanten des Kontrollmoduls festgelegt.

3.8 KA-Transaktionen hochladen

Post KA Transaction List

https://..../FileRecipient?DeviceId=<terminalMngtID>&File=<filename>

Beschreibung

Diese Schnittstelle nimmt VDV KA Transaktionen entgegen, die sich aus Kontrollnachweisen, Ofline-Ausgaben, TXTRANSABBRUCH, Sperrungen und/oder Ergebnissen der Aktionsliste zusammensetzen.

Je nach konfigurierter KA Version sind die relevanten Transaktionstypen in [KA_SPEC_SST_1107] oder [KA_SPEC_SST_1300] definiert.

Darüber hinaus werden auch die proprietären Transaktionen TXSYMKEYACK über diese Schnittstelle entgegengenommen.

Als Content wird eine ZIP-Datei oder eine TGZ-Datei hochgeladen. Die ZIP-Datei enthält pro Transaktion eine XML-Datei. Die TGZ-Datei enthält eine TAR-Datei, die pro Transaktion eine XML-Datei enthält.

Der Dateiname sollte wie folgt formatiert sein:

<terminalMngtID>_<lfd. Nr.>.ZIP oder

<terminalMngtID>_<lfd. Nr.>.TGZ

Die enthaltenen Transaktionsdateien sollten wie folgt formatiert sein:

```
SSSSS_RRR_ZZZZZZZZZZ_EEEEE_RRR_TTT_JJJJMMTTHHMMSS.xml
```

Erläuterungen:

SSSSS	5-stellige dezimale OrgID des Senders
RRR	3-stelliger dezimaler Rollen_CODE des Senders (…SSS_RRR…) bzw. des Empfängers (…EEE_RRR…)
ZZZ…	10-stellige dezimale TransSequenznummer des Senders
EEEEE	5-stellige dezimale OrgID des Empfängers
TTT	3-stelliger dezimaler IONTransaktionsTyp_CODE
JJJJ…	transTransaktionsZeitpunkt

Beispiel:

```
39060_001_45_39059_002_002_20111201054242.XML
```

Die in den Dateinamen einzusetzenden Werte sind dem TX_BASE des in der Datei enthaltenen Transaktionsdatensatzes zu entnehmen.

Der Inhalt der Datei ist im Format der jeweiligen Transaktion, siehe Kap. 4.

Das vHGS prüft die Eindeutigkeit der hochgeladenen Transaktionsdatensätze, siehe Kap. 5.3.

Das vHGS prüft beim Import der Transaktionsdatensätze neben der Eindeutigkeit auch weitere Eigenschaften auf Konsistenz und Plausibilität und erzeugt Antwortdatensätze ERR (als nicht verarbeitbar auf Ebene der Kommunikationsschicht abgelehnt), TXA (fachlich abgelehnt) bzw. TXB (bestätigt).

KA Transaktionen:

Siehe [KA_SPEC_SST_1107] bzw. [KA_SPEC_SST_1300] und ergänzende Festlegungen in Kap. 4.

TXSYMKEYACK:

Diese Transaktion ist eine Rückmeldung, dass ein Kryptogramm auf ein SAM geladen wurde.

Über die Schnittstelle “Get Symmetric Key List“ wurden für bestimmte SAMs Kryptogramme heruntergeladen, die mit dem LOAD KEY Kommando in die SAMs geladen wurden. Nachdem diese Kryptogramme in die jeweiligen SAMs geladen wurden, muss dies jeweils durch die Transaktion TXSYMKEYACK mitgeteilt werden.

Siehe Kap. 4.9.

Hinweis:

Da die Integration des vHGS mit fremden PV nicht Bestandteil des aktuell beauftragten Lieferumfangs ist, können Transaktionen auf Berechtigungen fremder PV nicht im vHGS verarbeitet werden und werden daher abgewiesen (TXA an Terminalmanagementsystem).

In späteren Ausbaustufen werden auch derartige Transaktionen auf Berechtigungen fremder PV verarbeitet und an die zuständigen Systeme weitergeleitet werden.

HTTP-Request-Methode

POST

Parameter

- terminalMngtID
  Identifiziert eindeutig ein externes Terminal Management System
- filename
  Eindeutiger Dateiname der hochgeladenen ZIP-Datei
- file
  ZIP-Datei mit VDV KATransaktionen als POST Content.

Rückgabewert

Der Wert der Antwort ist eine Paketnummer, die später als Referenznummer zur Zuordnung der Paket-Quittungen benötigt wird.

Der Mimetype des HTTP Inhalts ist „text/plain“.

Der zurückgegebene HTTP CODE ist 200 (OK).

Ausnahmen

Sollten bei einer Anfrage Probleme auftreten und der Request wird nicht sauber bearbeitet, so wird ein entsprechender HTTP CODE zurückgegeben.

- CODE 404: terminalMngtID existiert nicht.

Beispiel

Aufruf: https://vhgs.rmv.de/tl/FileRecipient?DeviceId=35159-015-00001&File=43456.zip

POST Content: ZIP-Datei mit den Dateien
39060_001_45_39059_001_002_20111201054242.XML,
39060_001_45_39059_001_002_20111206104233.XML,
35158_002_46_39059_001_253_20101018221551.XML

39060_001_45_39059_001_059_20111201054242.XML:

3.9 Paket-Quittung herunterladen

Get Package Acknowledgment

https://..../MessageServlet?DeviceId=<terminalMngtID>&MessageId=<messageID>

Beschreibung

Diese Schnittstelle liefert das Ergebnis (die Paket-Quittung) des Imports aller Transaktionen eines Paketes, das über die Schnittstelle „KA-Transaktionen hochladen“ (siehe Kapitel 3.8) übergeben wurde. Die Zuordnung zu dem Paket erfolgt über die im Attribut ‚packagenumber‘ der Paket-Quittung enthaltene Referenznummer, die das TMS auch als Rückgabewert beim Hochladen der KA-Transaktionen erhalten hat (siehe Kapitel 3.8).

Die zur Verfügung stehenden Paket-Quittungen werden in der Manifest-Datei angezeigt (message-name = „PACKAGEACK“). Zu beachten ist, dass die im Manifest angezeigte Message-ID nicht die Paketnummer ist.

Um zu bestätigen, dass dieses Ergebnis gelesen wurde und in der Manifest-Datei nicht mehr angezeigt werden muss, muss die Paket-Quittung über die Schnittstelle „Erhalt einer Nachricht bestätigen“ (siehe Kapitel 3.10) bestätigt werden.

HTTP-Request-Methode

GET

Parameter

- terminalMngtID
  Identifiziert eindeutig ein externes Terminal Management System
- messageID
  Nachricht-ID der Quittung. Siehe Manifest-Datei.

Rückgabewert

Als Rückgabe wird eine ZIP-Datei (MessageServlet.zip) oder eine TGZ-Datei (MessageServlet.tgz) geschickt. Es wird das Dateiformat (zip oder tgz bzw. tar.gz) verwendet, in dem das Paket hochgeladen wurde.

Die zurückgegebene ZIP-Datei bzw. die TAR-Datei enthält in jedem Fall die Datei

PACKAGEACK.XML,

welche Informationen über das Paket enthält.

Sollten eine oder mehrere Transaktionen abgelehnt worden sein, so enthält die ZIP-Datei bzw. die TAR-Datei die dazugehörigen TXA Transaktionen jeweils in einer Datei. Der Dateiname hat das Format:

TXA_SSSSS_RRR_ZZZZZZZZZZ.xml

Erläuterungen:

SSSSS = 5-stellige dezimale OrgID des Senders

RRR = 3-stelliger dezimaler Rollen_CODE des Senders

ZZZ… = 10-stellige dezimale TransSequenznummer des Senders

Für akzeptierte Transaktionen enthält die ZIP-Datei bzw. die TAR-Datei die dazugehörigen TXB Transaktionen jeweils in einer Datei. Der Dateiname hat das Format:

TXB_SSSSS_RRR_ZZZZZZZZZZ.xml

Erläuterungen: siehe TXA.

Für Transaktionsdateien, die gänzlich nicht verarbeitbar waren und auch kein TXA erzeugt werden konnte, enthält die ZIP-Datei bzw. die TAR-Datei jeweils eine Fehlerdatei mit dem Dateinamen

ERR_<Dateiname>.txt,

wobei für <Dateiname> der Dateiname der nicht verarbeitbaren Transaktionsdatei eingesetzt wird. Die Datei ERR_<Dateiname>.txt enthält die Fehlermeldung aus dem Importprozess des vHGS.

Ausnahmen

Sollten bei einer Anfrage Probleme auftreten und der Request wird nicht sauber bearbeitet, so wird ein entsprechender HTTP CODE zurückgegeben.

- CODE 404: terminalMngtID oder messageID existiert nicht. Siehe HTTP-Content für Details. Falls die angegebene Nachricht-ID nicht existiert, kann über einen erneuten Abruf der Manifest-Datei überprüft werden, ob die richtige Version verwendet wurde.

Beispiel

Aufruf:

https://vhgs.rmv.de/tl/MessageServlet?DeviceId=35159-015-00001&MessageId=354

Rückgabe: ZIP-Datei (MessageServlet.zip) mit den Dateien PACKAGEACK.XML, TXA_35059_001_4025634566.XML

PACKAGEACK.XML:

```
<?xml version="1.0" encoding="utf-8"?>
<PACKAGEACK created="2011-06-01T13:20:34" terminalMngtId="TMNGT12345" MajorVersion="2"
MinorVersion="7">
   <packagenumber>5</packagenumber>
   <packageerrorcode>0</packageerrorcode>
   <rejectedsize>1</rejectedsize>
   <acceptedsize>1034</acceptedsize>
</PACKAGEACK>
```

TXA_35059_001_4025634566.XML

3.10 Erhalt einer Nachricht bestätigen

Confirm Message

https://..../AcknowledgeMessageServlet?DeviceId=<terminalMngtID>&MessageId=<messageID>

Beschreibung

Über diese Schnittstelle wird vom Terminalmanagementsystem der Empfang von Nachrichten bestätigt. Folgende Nachrichten müssen bestätigen werden:

- Paket-Quittung (siehe Kapitel 3.9)
- Liste der Zertifikate (siehe Kapitel 3.6)

- Liste der symmetrischen Schlüssel (siehe Kapitel 3.5)

Nach dem Erhalt der Bestätigung stehen die bestätigten Nachrichten nicht mehr in der Manifest-Datei.

HTTP-Request-Methode

GET

Parameter

- terminalMngtID
  Identifiziert eindeutig ein externes Terminal Management System
- messageID
  Nachricht-ID der empfangenen Nachricht.

Rückgabewert

Es gibt keinen Rückgabewert. Der zurückgegebene HTTP CODE ist 200 (OK).

Ausnahmen

Sollten bei einer Anfrage Probleme auftreten und der Request wird nicht sauber bearbeitet, so wird ein entsprechender HTTP CODE zurückgegeben.

- CODE 404: terminalMngtID oder messageID existiert nicht. Siehe HTTP-Content für Details. Falls die angegebene Nachricht-ID nicht existiert, kann über einen erneuten Abruf der Manifest-Datei überprüft werden, ob die richtige Nachricht-ID verwendet wurde.

Beispiel

Aufruf:

https://vhgs.rmv.de/tl/AcknowledgeMessageServlet?DeviceId=35159-015-00001&MessageId=354

4 Datenstrukturen

Im Folgenden werden alle verwendeten Strukturen vorgestellt. Für die proprietären Datenstrukturen wird eine Schema-Definition (XSD) erstellt. Für die aus den KA spezifischen Elemente und Datenstrukturen wird die jeweilige KA-XSD (1.107K) bzw. KA XSDs (1.3.0) herangezogen.

4.1 Manifest

Die Manifest-Datei beschreibt alle aktuellen Nachrichten, die das Terminalmanagementsystem beim vHGS abrufen kann. Damit kann der jeweilige Aufrufer überprüfen, ob bei ihm die aktuellen Daten (insbesondere Sperr- und Aktionslisten) vorliegen. Im folgenden eine Kurzbeschreibung der einzelnen Elemente innerhalb der Manifest-Datei.

Element	Beschreibung
OpNTCIPManifestCollection	Liste von Manifestdaten (OpNTCIPManifest). Für TMS hat die Liste genau ein Element (OpNTCIPManifest).
OpNTCIPManifest	Die Manifestdaten für ein Terminalmanagementsystem
config-id	Nicht relevant. Wird mit dem Wert ‚0' (Null) belegt.
device-id	Identifier (ID) des Systems, dass das Manifest erstellt hat.
location-id	Nicht relevant. Wird mit dem Wert ‚0' (Null) belegt.
message-list	Liste aller zur Verfügung stehenden Nachrichten (OpNTCIP-Manifest_message)

Element	Beschreibung
OpNTCIPManifest_message	Definition einer Nachricht
message-name	Typ der Nachricht z.B.: – TXSLNM, TXSLNMRESP – TXSLOS, TXSLORGRESP, TXSLSAMRESP – TXSLK, TXSLKASYMRESP, TXSLKSYMRESP – TXAML – TXTRANSABBRUCH (ab KA SST 1.3.0) – TXSYMKEYL – TXCVCERTL – RMVKontrollmodul (ab KA SST 1.3.0 nicht mehr für die KIM-Tarifdaten, sondern für die neue Konfigurationsdatei [RMV_KA130_MBER] verwendet) – PACKAGEACK
major-version	Strukturversion der Nachricht, Hauptversion (für eine Version „2.1" wäre dies die „2")
minor-version	Strukturversion der Nachricht, Detailversion (für eine Version „2.1" wäre dies die „1")
message-id	Nachricht-ID, eindeutige ID der Nachricht

Element	Beschreibung
created-date	Erstellungsdatum der Nachricht

4.2 Sperrlisten, Sperrnachweise und Kontrollnachweise

4.2.1 Sperrlisten

Die VDV KA Strukturen TXSLNM, TXLOS und TXSLK sind aus [KA_SPEC_SST_1107] zu entnehmen.

Festlegung zum TX_BASE Teil der Nachricht: siehe Kapitel 4.10.

Ergänzungen / Änderungen mit Einführung KA 1.3.0

Die VDV KA Strukturen TXSLNMRESP, TXSLKASYMRESP, TXSLKSYMRESP, TXSLORGRESP, TXSLSAMRESP sind aus [KA_SPEC_SST_1300] zu entnehmen.

4.2.2 Sperrnachweise

Die VDV KA Strukturen TXSNAWA und TXSNAWB sind aus [KA_SPEC_SST_1107] bzw. [KA_SPEC_SST_1300] zu entnehmen.

Festlegung zum TX_BASE Teil der Nachricht: siehe Kapitel 4.10.

4.2.3 Kontrollnachweise

Die VDV KA Struktur TXEBER, TXEMBER, TXKNAWDM, TXKNAWA, TXKNAWB sind aus [KA_SPEC_SST_1107] bzw. [KA_SPEC_SST_1300] zu entnehmen.

Festlegung zum TX_BASE Teil der Nachricht: siehe Kapitel 4.10.

4.3 Aktionsliste und Transaktionsnachweise

4.3.1 Aktionsliste TXAML

Die VDV KA Struktur TXAML ist aus [KA_SPEC_AktM] zu entnehmen.

Festlegung zum TX_BASE Teil der Nachricht: siehe Kapitel 4.10.

4.3.2 Transaktionsnachweise aus Aktionsausführung

Die VDV KA Strukturen TXABER, TXRBER, TXSNAWB sind aus [KA_SPEC_SST_1107] bzw. [KA_SPEC_SST_1300] zu entnehmen. Zusätzlich ist die [KA_SPEC_AktM_1107] bzw. [KA_SPEC_AktM_1300] zu beachten.

Festlegung zum TX_BASE Teil der Nachricht: siehe Kapitel 4.10.

Festlegung zum fachlichen Teil des TXABER: siehe PH05-A1 „RMV-EFS“.

Insbesondere ist auch zu beachten, dass die TXABER immer die Datenstruktur berechtigung-TarifbereichZusatz gemäß den Vorgaben des PH05-A1 enthalten.

Ergänzungen / Änderungen mit Einführung KA 1.3.0

Neben den bisher ausgetauschten Transaktionen können nach der Umstellung auf KA 1.3.0 auch die Transaktionen bzgl. Multiberechtigungen (siehe [KA_SPEC_MULTIBER_1300]) übermittelt werden:

- TXAMBER, TXRMBER

4.4 Verkauf (Berechtigungsausgabe, Applikationsausgabe)

4.4.1 Ausgabenachweise TXABER und TXAA aus Verkauf

Die VDV KA Strukturen TXABER, TXAA sind aus [KA_SPEC_SST_1107] bzw. [KA_SPEC_SST_1300] zu entnehmen.

Festlegung zum TX_BASE Teil der Nachricht: siehe Kapitel 4.10.

Festlegung zum fachlichen Teil des TXABER: siehe PH05-A1 „RMV-EFS“.

Ergänzungen / Änderungen mit Einführung KA 1.3.0

Neben den bisher ausgetauschten Transaktionen können nach der Umstellung auf KA 1.3.0 auch die Transaktionen bzgl. Multiberechtigungen (siehe [KA_SPEC_MULTIBER_1300]) übermittelt werden:

- TXAMBER

4.5 Nachweise über abgebrochene Transaktionen TXTRANSABBRUCH

Mit der Einführung der Schnittstellenversion KA 1.3.0 sollen auch die Daten bzgl. Transaktionsabbrüchen an das vHGS übermittelt werden.

Die VDV KA Struktur TXTRANSABBRUCH ist aus [KA_SPEC_SST_1300] zu entnehmen.

Festlegung zum TX_BASE Teil der Nachricht: siehe Kapitel 4.10.

4.6 Symmetrische Schlüsselliste TXSYMKEYL

Die TXSYMKEYL-Struktur enthält eine Liste von symmetrischen Schlüsseln (Kryptogramme), die in SAMs zu laden sind.

Element	Beschreibung
txbase	Siehe [KA_SPEC_SST_1107] bzw. [KA_SPEC_SST_1300] ION-Transaktionen – TX_Base. IONTransaktionsTyp_CODE: 252
symmetrickeylist	Liste von symmetrickey Elementen. Wurzelelement.

Element	Beschreibung
symmetrickey	Beschreibt einen symmetrischen Schlüssel für ein SAM
cryptogram	Der eigentliche Schlüssel, verschlüsselt so, dass nur das SAM, für den der Schlüssel bestimmt ist, das Kryptogramm entschlüsseln kann. Das Verschlüsselungsverfahren ist in [KA_SPEC_SAM_1107] bzw. [KA_SPEC_SAM_1300] in den Kapiteln zum Schlüsselmanagement und zum Kommando LOAD KEY (6.2, 9.6) beschrieben.
samid	Die ID des SAM, für das dieser Schlüssel bestimmt ist. Als ID wird hier die eindeutige SAM Nummer angegeben.
sequencenumber	Eindeutige Sequenznummer bezüglich des durch die übergebene *samid* referenzierten SAMs. Die Nummer legt die Reihenfolge der auszuführenden Kryptogramme für dieses SAM fest (siehe dazu das Kapitel 9.6 LOAD KEY in [KA_SPEC_SAM_1107] bzw. [KA_SPEC_SAM_1300]).
chr	Certificate Holder Reference (CHR) des Organisations-Signatur-Zertifikats, mit dem das Kryptogramm signiert ist (Siehe [KA_SPEC_SAM] 4.3.1.3.5 CHR für Zertifikate zur Verwaltung der Schlüssel im SAM). Format: HexString Representation des CHRs.

4.7 Zertifikatsliste TXCVCERTL

Die TXCVCERTL Struktur enthält eine Liste von CV Zertifikaten.

Element	Beschreibung
txbase	Siehe [KA_SPEC_SST_1107] bzw. [KA_SPEC_SST_1300] IONTransaktionen – TX_Base. IONTransaktionsTyp_CODE: 254
cvcertificatelist	Liste von cvcertificate Elementen. Wurzelelement.

Element	Beschreibung
cvcertificate	Beschreibt ein CV Zertifikat.
keytype	Bedeutung des Schlüssels innerhalb des Zertifikats: 1 - NM und SAM Autorisierungsschlüssel für PKCS#1 Signatur 2 - SAM Autorisierungsschlüssel für ISO-9796-2 Signatur 3 - SAM Encryption-Schlüssel 4 - SAM Signature-Schlüssel 5 - Keymanagement Aktivierungsschlüssel 6 - Keymanagement und Organisation Signaturschlüssel 7 - Zertifikat einer CA
data	Das Zertifikat als TLV Struktur. Zum Aufbau eines CV Zertifikats mit Tags und Values siehe [KA_SPEC_SAM] Kapitel 4.3.3.

	Format: HexString Representation des CHRs.

XML-Strukturdefinition:

Siehe Anlagen KA-vHGS-Schnittstellen-1.107K20120104.zip und KA-vHGS-Schnittstellen-1.3.0.zip.

4.8 Paket-Quittung PACKAGEACK

Die Struktur PACKAGEACK beschreibt die Quittung für ein Paket.

Element	Beschreibung
packagenumber	Paketnummer, für die diese Quittung gilt.
packageerrorcode	Fehlercode für das Paket. Signalisiert Fehler, die das gesamte Paket (hochgeladene ZIP-Datei) betreffen. Werte: 0 = ok, 1 = ZIP-Datei lässt sich nicht öffnen, 2 = ZIP-Datei enthält unerwarteten Inhalt
rejectedsize	Anzahl der abgelehnten Transaktionen. Die ZIP-Datei, die die Paket-Quittung enthält, enthält eine entsprechende Anzahl TXA- und ERR-Dateien.
acceptedsize	Anzahl der bestätigten und angenommenen Transaktionen. Die ZIP-Datei, die die Paket-Quittung enthält, enthält eine entsprechende Anzahl TXB-Dateien.

XML-Strukturdefinition:

Siehe Anlagen KA-vHGS-Schnittstellen-1.107K20120104.zip und KA-vHGS-Schnittstellen-1.3.0.zip.

4.9 Symmetrische Schlüssel Bestätigung TXSYMKEYACK

Die Struktur TXSYMKEYACK beschreibt eine Bestätigung, dass ein Kryptogramm in ein SAM geladen wurde.

Element	Beschreibung
txbase	Siehe [KA_SPEC_SST_1107] bzw. [KA_SPEC_SST_1300] IONTrans-aktionen – TX_Base. IONTransaktionsTyp_CODE: 253
symmetrickey	Beschreibt einen symmetrischen Schlüssel, der in ein SAM geladen wurde.
samid	Die ID des SAM, in den dieser Schlüssel geladen wurde. Als ID wird hier die eindeutige SAM Nummer angegeben.
sequencenumber	Eindeutige Sequenznummer bezüglich des in samid angegebenen

	SAMs. Die Nummer legte die Reihenfolge der auszuführenden Kryptogramme für dieses SAM fest.

XML-Strukturdefinition:

Siehe Anlagen KA-vHGS-Schnittstellen-1.107K20120104.zip und KA-vHGS-Schnittstellen-1.3.0.zip.

4.10 Übersicht über die in TX_BASE verwendeten KA-Rollencodes und Org-IDs

Wie in Kapitel 1 dargestellt ist die Kommunikation zwischen Terminalmanagementsystem und vHGS eine interne Kommunikation innerhalb des jeweiligen KVP bzw. DL. Je nach Sichtweise und technischer Gestaltung kann dies als Kommunikation zwischen zwei Komponenten des KVPS (bzw. DLS) oder als Kommunikation zwischen KVPT (bzw. DLT) und KVPS (bzw. DLS) eingeordnet werden. Der Praxis in anderen Implementierungen der KA folgend wird bei der Kommunikation zwischen KVPT bzw. DLT und KVPS bzw. DLS das KVPS bzw. DLS als transparente Durchgangsstation behandelt. D.h. Sender und Empfänger sind Organisationen/Rollen wie sie im KA-Rollenmodell für die vorangegangenen (Nachrichten vom Hintergrundsystem an das Terminal) bzw. nachfolgenden (Nachrichten vom Terminal an das Hintergrundsystem) Kommunikationsvorgänge des Hintergrundsystems mit anderen Organisationen/Rollen (KVP/DL und PV, KOSE, AH) verwendet werden.

Weiterhin wird in den Sender- bzw. Empfängerattributen des TX_BASE die Org-ID des Mandanten (bzw. eine der Org-IDs des Mandanten, wenn dieser über mehrere Org-IDs verfügt) verwendet.

Die nachfolgende Tabelle zeigt die verwendeten Org-IDs und Rollencodes für alle Anwendungsfälle der Schnittstelle. Die Darstellung unterscheidet zwischen „RMV“ und „RMV KVP/DL-Agentur“. Konzeptionell sind dies zwei verschiedene Organisationen. Aus praktischen Erwägungen haben sich die Verkehrsunternehmen und der RMV darauf verständigt, den RMV als Repräsentanten der „RMV KVP/DL-Agentur“ (in anderen Dokumenten auch als „eTicket RheinMain KVP/DL-Agentur“ bezeichnet) zu betrachten und dessen KA Org-ID auch für die RMV KVP/DL-Agentur zu verwenden.

Anwendungsfall	**transSender**	**transEmpfänger**
Manifest herunterladen	*kein TX_BASE*	*kein TX_BASE*
Sperrlisten herunterladen	RMV KOSE (5)	Org-ID des Unternehmens, dem das anfragende TMS im vHGS zugeordnet ist. Abhängig von der Rolle des Verkehrsunternehmens (VU): • VU ist DL aber nicht KVP: DL (2) • VU ist KVP aber nicht DL: KVP (1) • VU ist DL und KVP: KVP (1)

Anwendungsfall	transSender	transEmpfänger
Aktionsliste herunterladen	RMV PV (3)	Org-ID des Unternehmens, dem das anfragende TMS im vHGS zugeordnet ist. KVP (1)
Kryptogrammliste (symmetrische Schlüssel) herunterladen	RMV KVP/DL-Agentur Rolle wie transEmpfänger Siehe Anmerkung [4]	Org-ID des Unternehmens, dem das anfragende TMS im vHGS zugeordnet ist. Rolle abhängig von der Rolle des Unternehmens , s. „Sperrliste herunterladen“
CV-Zertifikatsliste herunterladen	RMV KVP/DL-Agentur Rolle wie transEmpfänger Siehe Anmerkung [5]	Org-ID des Unternehmens, dem das anfragende TMS im vHGS zugeordnet ist. Rolle abhängig von der Rolle des Unternehmens , s. „Sperrliste herunterladen“
Tarifmodul (Kontrollmodul) herunterladen	*kein TX_BASE*	*kein TX_BASE*

[4] Bislang sind für die Anforderung und den Transport von Kryptogrammen vom Key Management System zum Schlüsselverwender in der KA keine Schnittstellen analog der Spec-SST spezifiziert. In einer solchen Spezifikation könnte der Betreiber des Key Management Systems als Sender auftreten. In Ermangelung einer solchen KA Schnittstellenspezifikation wird hier die RMV KVP/DL-Agentur als Sender eingesetzt.

[5] Analog Anmerkung in Fußnote 4.

Anwendungsfall	transSender	transEmpfänger
KA-Transaktionen hochladen	Org-ID des Unternehmens Die Rolle ist abhängig von der Art der Transaktion. TXAA: KVP (1) TXABER: KVP (1) TXAMBER: KVP (1) TXEBER: DL (2) TXEMBER: DL (2) TXKNAWDM: KVP (1) oder DL (2), abhängig von der Rolle des Terminals, das das defekte Medium erfasst hat TXKNAWA, TXKNAWB: DL (2) TXSNAWA, TXSNAWB (Sperrnachweis): KVP (1) oder DL (2), abhängig von der Rolle des Terminals, das die Sperrung ausgeführt hat. TXABER, TXAMBER, TXRBER, TXRMBER, TXSNAWB (Entsperrnachweis) aus Aktionsausführung: KVP (1). TXSYMKEYACK: KVP (1) oder DL (2), abhängig von der Rolle des Terminals, das den Schlüssel installiert hat. TXTRANSABBRUCH: KVP (1)	Abhängig von der Art der Transaktion: TXAA: KA KG / AH (4) TXABER: RMV / PV (3) TXAMBER: RMV / PV (3) TXEBER: RMV / PV (3) TXEMBER: RMV / PV (3) TXKNAWDM: KA KG / AH (4) TXKNAWA, TXKNAWB: RMV / PV (3) TXSNAWA, TXSNAWB (Sperrnachweis): RMV / KOSE (5) TXABER, TXAMBER, TXRBER, TXRMBER, TXSNAWB (Entsperrnachweis) aus Aktionsausführung: RMV / PV (3) Siehe Anmerkung[6] TXSYMKEYACK: RMV KVP/DL-Agentur / Rolle wie transSender TXTRANSABBRUCH: RMV / PV(3), AH(5) abhängig vom Anwendungsfall (Ausgabe Applikation oder Ausgabe Berechtigung) und Fortschritt der Ausgabe.
Paket-Quittung herunterladen	PACKAGEACK hat kein TX_BASE. Die ggf. enthaltenen TXA verwenden die Werte aus transEmpfänger der abgelehnten Transaktion.	PACKAGEACK hat kein TX_BASE. Die ggf. enthaltenen TXA verwenden die Werte aus transSender der abgelehnten Transaktion.
Erhalt einer Nachricht bestätigen	*kein TX_BASE*	*kein TX_BASE*

[6] In der Schnittstellenversion KA 1.1.07 wurde alternativ auch der Rollen-Code 31 (ALISE) akzeptiert. Ab der Spezifikation KA 1.3.0 ist der Rollen-Code 31 (ALISE) seitens der VDV ETS "für einen aus dem PVS ausgelagerten eigenständigen zentralen ALISE-Server reserviert" und stattdessen ist, wenn ALISE in das PVS integriert ist, die Rolle 3 zu verwenden. Dementsprechend ist in der TMS-Schnittstellenversion KA 1.3.0. zwingend der Rollen-Code 3 für TX* aus Aktionsausführungen zu verwenden.

5 Hinweise zur technischen Umsetzung

5.1 Durchführung der Kontrolltransaktion (TXEBER, TXEMBER)

5.1.1 Abbruch der der Kontroll-Transaktion nach Excecute Transaction

Laut z.B. VDV-KA Spec SYSLH_RTDL_V1107 bzw. SYSLH_DLRT_V130.pdf im Kapitel 1.3.2.4 (DLT: EFS-Berechtigung kontrollieren (kundenselbstbedient)) kann während der Kontroll-Transaktion nach Excecute Transaction aus Performencegründen abgebrochen werden.

Dies ist auch im eTicket RheinMain zulässig. Die Optimierung darf aber nur genau so weit gehen, wie im SysLH beschrieben: der MAC muss erzeugt werden. Zusätzlich muss darauf geachtet werden, dass die Transaktionsdaten (inkl. der erzeugten Kontroll-MACs) auch auf dem Nutzermedium persistiert werden. Dies erreicht man durch die Beendigung der Transaktion nach Ausführung des EXECUTE TRANSACTION Kommando durch Setzen des Parameters P1 = x1. Im Fall eines einfachen Abbruchs (d.h. die Kommandosequenz würde durch ein SEND RECEIPT bestätigt werden, wird es aber aufgrund des Abbruchs nicht) würden die im Laufe der Transaktion entstandenen Daten auf dem NM nicht persistiert werden und somit würden z.B. die Werte der Transaktionszähler bei der nachfolgenden Transaktion dieselben sein.

5.1.2 Datenschutz

Aus der Begutachtung des vHGS durch den Datenschutz des Land Hessen im November 2016 resultierte die Vorgabe, dass die Kontrollnachweise ohne Fahrtnummer und Linieninformation gespeichert werden sollten. Konkret:

In den Transaktionsnachweisen vom Typ TXEBER (aus Kontrolle, IONTransaktionsTyp_CODE = 059, logTransaktionsTyp.code = 27) sollen unter „AllgemeineFahrttransaktionsdaten“ folgende drei Attribute mit „0“ gefüllt werden:

- berLogFahrt_ID.fahrtNummer,
- berLogLinieVarianteID.linie_ID.linienNummer,
- berLogLinieVarianteID.variantenNummer.

Dies soll vorzugsweise bereits durch das Terminal so geschehen.

Da eine kurzfristige flächendeckende Umsetzung in den Terminals nicht realistisch ist, werden bei der Verarbeitung der besagten Transaktionen im vHGS die besagten Attribute mit „0“ überschrieben. Die besagten Attribute sind Teil der Daten über die die MACs gebildet wurden. Das vHGS kennzeichnet daher die so behandelten Transaktionen, die dann von einer späteren MAC-Validierung ausgenommen werden.

Zu beachten: Dies bezieht sich nur auf TXEBER-Kontrollnachweise, nicht generell auf die Attribute Fahrtnummer und Linievariante (insbesondere dürfen diese in einem TXABER nicht überschrieben werden).

5.2 Kodierung von Nullwerten in Bytestrings in KA-Transaktionsdaten

Bei der Codierung der Bytestrings in den KA-Transaktionsdaten ist zu berücksichtigen, dass die „Nullwerte“ bzw. „keine Angabe“-Werte nicht immer durch den Wert ‚0‘ des einzelnen Bytes dargestellt werden.

Zum Beispiel entspricht „Nullwert“ für den PrintableString(5) des Attributs berTarifversion einem String mit 5 Leerzeichen. Das Leerzeichen wird im Bytestring jedoch mit dem Wert ‚20‘ dargestellt.

Für die OrtsTyp_Codes, z.B. in den Attributen efsStartort_ID und efsZielort_ID, ist in der KA der dezimale Wert 255 (hexadezimal ‚FF‘) als „keine Angabe“ spezifiziert.

5.3 Duplikate und wiederholtes Senden

Das vHGS prüft die von den TMS hochgeladenen Transaktionsdaten (siehe Kap. 3.8) nicht auf eindeutige Dateinamen.

Das vHGS prüft den Inhalt der Dateien, also die Transaktionsdatensätze auf Eindeutigkeit.

Transaktionsdaten können auf zweierlei Weise ein Duplikat sein.

1. Die Transaktions-ID und Wiederholungszähler der XML-Transaktion (transTransaktion_ID und transWiederholungsZaehler aus TX_BASE) sind identisch zu einer bereits im vHGS vorhandenen Transaktion.
2. Die ID einer in einer XML-Transaktion enthaltenen NM-Transaktion (in TLV Form) ist identisch zu einer bereits im vHGS vorhandenen NM-Transaktion.

Wenn vom vHGS ein Duplikat erkannt wird, wird der Transaktionsdatensatz abgelehnt und mit einem TXA beantwortet. Um den Ablehnungsgrund differenziert an den Verursacher zu transportieren, müsste die Codeliste AblehnungsTyp_CODE entsprechend erweitert werden, so dass sowohl „XML-Tx-ID-Duplikat“ als auch „NM-Tx-ID-Duplikat“ signalisiert werden können. Hierfür sind entsprechende zusätzliche Codes bei der VDV KA noch zu beantragen.

Bei der Duplikatsprüfung wird auch das in der KA-Spezifikation beschriebene „wiederholte Senden“ berücksichtigt. Sofern das vHGS eine Transaktion TX-2 erhält und im vHGS bereits eine Transaktion TX-1 mit gleicher Transaktions-ID aber anderem Wiederholungszähler vorhanden ist, antwortet das vHGS mit einer Kopie des TXA bzw. TXB, mit der der bereits vorhandene Transaktionsdatensatz TX-1 beantwortet wurde, wobei in das Attribut transWiederholungsZaehler der Kopie der entsprechende Wert aus TX-2 eingesetzt wird.

Das Attribut TX_BASE.transTransaktion_ID enthält die Datenstruktur IONTransaktion_ID. Die IONTransaktion_ID besteht aus transSender_ID (Org-ID) + transSenderRolle (Rollen-Code) + transSequenznummer (SequenceNumberFour).

Für die Betreiber der TMS resultiert aus der Anforderung, dass Transaktions-IDs eindeutig sein müssen, die Pflicht, dies ggf. auch über mehrere technische Systeme hinweg sicherzustellen. Daraus folgt insbesondere, dass für die transSequenznummer Nummernkreise gebildet werden müssen, wenn ein transSender (Verkehrsunternehmen) mehrere Systeme (Terminalmanagementsysteme) betreibt, die transSequenznummern vergeben.

Der jeweils zulässige Nummernkreis zur Verwendung der transSequenznummern wird im eTicket RheinMain durch die Übergeordnete Fachliche Betriebsführung vHGS zugewiesen.

5.4 Optionale Attribute in TX_BASE ab KA 1.3.0

Mit der Einführung der ZVM und der Aufteilung der Schnittstellendefinitionen (XSDs) wurden einige Attribute in TX_BASE als optional (minOccurs="0" maxOccurs="1") deklariert. Dazu gehören:

Attribut	**Handhabung im RMV**
transAuftrag	nicht optional

transStatus	nicht optional
transTransaktionsTyp	nicht optional
transVersion	nicht optional
transWiederholungsZaehler	nicht optional
transSignaturTyp	optional
transSignaturZertifikat	optional
transSignatur	optional

6 Verwendung der SST durch SCG Ticketinfo Mobil Kontrollgeräte

6.1 SCG Ticketinfo Mobil Kontrollgeräte

Die SCG Ticketinfo Mobil Kontrollgeräte sind Smartphones mit NFC-Schnittstelle (z.B. Samsung Galaxy Nexus) mit der von Soellner Consult GmbH (SCG) entwickelten Anwendung (Android App) zum Einlesen und Anzeigen von KA Berechtigungen (RMV-EFS).

Die SCG Ticketinfo Mobil Kontrollgeräte werden als kostengünstige Lösung dort eingesetzt, wo der Einsatz eines vollwertigen mobilen Kontrollterminals wirtschaftlich nicht sinnvoll ist.

Die Kontrolle erfolgt als reine Sichtkontrolle mit automatischer Auswertung ausgewählter EFS-Attribute (z.B. zeitliche Gültigkeit).

Da das Smartphone nicht über ein SAM verfügt, erfolgen keine kryptographischen Prüfungen des KA Nutzermediums und der KA Berechtigungen und es können keine Transaktionen mit dem Nutzermedium durchgeführt werden.

Die SCG Ticketinfo Mobil Kontrollgeräte sollen die nutzermediumbezogene Sperrliste (TXSLNM) vom vHGS beziehen und auswerten.

6.2 Verwendung der TMS-Schnittstelle

Der Datenaustausch zwischen SCG Ticketinfo Mobil Kontrollgeräten und dem vHGS beschränkt sich auf das Herunterladen der nutzermediumbezogenen Sperrliste (TXSLNM). Der Kommunikationsablauf (vgl. Kap. 3.1)beschränkt sich daher auf

1. Manifest herunterladen, siehe Kapitel 3.2
2. Anhand der aus dem Manifest abgelesenen Nachricht-ID (message-id) der nutzermediumbezogenen Sperrliste (message-name = TXSLNM) gegen die im Gerät gespeicherte Nachricht-ID der zuletzt heruntergeladenen Sperrliste prüfen, ob eine neue Sperrliste herunterzuladen ist. Falls keine neue Sperrliste vorliegt, kann der Vorgang an dieser Stelle beendet werden.
3. Sperrliste für Berechtigungen und Applikationen herunterladen, siehe Kapitel 3.3

Für die SCG Ticketinfo Mobil Kontrollgeräte wird im vHGS ein neuer Gerätetyp „Ticketinfo Mobil Kontrollgerät“ mit eigenem Typcode eingerichtet.

Für einen Gerätetyp können im vHGS beliebig viele Geräte mit individueller Gerät-ID (Device-ID) angelegt werden. Die Gerät-ID setzt sich zusammen aus Org-ID des Unternehmens + Gerätetypcode + Nummer.

Bis auf weiteres sollen alle SCG Ticketinfo Mobil Kontrollgeräte über eine Gerät-ID geführt werden. Als Org-ID dieser gemeinsam genutzten Gerät-ID wird die Org-ID des RMV verwendet.

Für den Gerätetyp „Ticketinfo Mobil Kontrollgerät“ Gerät wird vom vHGS bei der Manifesterzeugung nur die nutzermediumbezogenen Sperrliste (TXSLNM) berücksichtigt. Dies kann ggf. später erweitert werden, falls weitere Nachrichtentypen für die SCG Ticketinfo Mobil Kontrollgeräte relevant werden.

Für den technischen Ablauf der Kommunikation zwischen SCG Ticketinfo Mobil Kontrollgerät und vHGS gelten die Festlegungen in Kapitel 2.2.

Die Authentifizierung an der Schnittstelle erfolgt per http Basic Authentication, wobei als Benutzername die Gerät-ID (Device-ID) verwendet wird, vgl. Kapitel 2.2.5. Das Passwort wird in der SCG Ticketinfo Mobil App gespeichert und ist dem Anwender nicht zugänglich. Die Speiche-

rung in der App muss nach dem Stand der Technik angemessen gegen Ausspähung geschützt sein. Es ist durch den Hersteller der App ein Mechanismus vorzusehen, der den Austausch des Passworts in allen im Einsatz befindlichen Apps erlaubt.

Alle vom vHGS an der TMS-Schnittstelle angebotenen Webservices verlangen die Angabe des Parameters „DeviceId“. Dort ist die an die SCG Ticketinfo Mobil Kontrollgeräte vergebene Gerät-ID einzusetzen.

Es ist davon auszugehen, dass mittelfristig eine Vielzahl von SCG Ticketinfo Mobil Kontrollgeräten (Größenordnung 500 Geräte) im Einsatz sein werden, die täglich Sperrlisten herunterladen werden. Es ist daher erforderlich, dass der Zeitpunkt des automatischen Herunterladens der Sperrliste durch die Geräte so gesteuert wird, dass die resultierende Last für den vHGS-Server verteilt wird.

Die Zeitpunkte des automatischen Herunterladens sollen auf ein vorgegebenes Zeitfenster verteilt werden. Die Verteilung soll zufällig und gleichverteilt sein. Jedes Gerät berechnet zu Beginn des Zeitfensters eine gleichverteilte Zufallszahl Z auf der Dauer des Zeitfensters in Sekunden und startet die Kommunikation mit dem vHGS zum Zeitpunkt Beginn-des-Zeitfensters + Z.

Sofern die Kommunikation nicht zustande kommt oder abbricht, werden von der App maximal drei Wiederholungsversuche unternommen. Die Wiederholungsversuche erfolgen im Abstand von drei Minuten + X Sekunden, wobei X eine gleichverteilte Zufallszahl aus [0 .. 180 Sekunden] ist.

7 Anhang

7.1 XSD

Die Datenstrukturen an der Schnittstelle für Terminalmanagementsysteme werden in folgenden XSD-Dateien spezifiziert

- OpNTCIPManifest.xsd

  XSD des Manifests (siehe Abschnitt 4.1)

  Siehe Anlage vHGS-TMS-Schemata.zip.

- [KA_XSD_1107]

  XSD der KA 1.107K Datenstrukturen (siehe Abschnitte 4.2 bis 4.4) und der vHGS-spezifischen, auf KA 1.107K Transaktionen basierenden Datenstrukturen (siehe Abschnitte 4.5 bis 4.9).

  Siehe Anlage KA-vHGS-Schnittstellen-1.107K20120104.zip.

- [KA_XSD_1300]

  XSD der KA 1.3.0 Datenstrukturen (siehe Abschnitte 4.2 bis 4.4) und der vHGS-spezifischen, auf KA 1.3.0 Transaktionen basierenden Datenstrukturen (siehe Abschnitte 4.5 bis 4.9).

  Siehe Anlage KA-vHGS-Schnittstellen-1.3.0.zip.

7.2 Offene Punkte

keine