Anlage 2
Technische Funktionsbeschreibung

EVU-Schnittstelle Bestellsystem

Version 4.4.2

Historie / Änderungen

Version	Bearbeitet/ geändert von	Beschreibung der Änderungen/Bemerkungen	Datum
4.0.0	DB Netz AG Wolfgang Kuzaj	Neukonzeption der EVU-Schnittstelle auf Grund der Herstellung der TAF/TAP TSI-Konformität und der Anbindung an das Bestellsystem der DB Netz (Initialfassung)	16.03.2015
4.1.0	DB Netz AG Konstantin Pussep	Überarbeitung auf der Grundlage internationaler Abstimmungen in den TelematicExpertGroups (TEG) der RailNetEurope (RNE), der Anpassungen des Sector-Handbook der RNE und der xsd V. 2.2.3	23.07.2019
4.1.1	DB Netz AG Wolfgang Kuzaj	Überarbeitung auf Basis xsd Version 2.2.4 Kapitel 3.5., 4. Absatz wurde ersetzt durch: „Die Integrität der Nachrichten wird über den Standard-TLS Mechanismus (MAC - Message Authentication Codes) sichergestellt.“	25.02.2020
4.2.0	DB Netz AG Konstantin Pussep, Alexander Petioky	Kapitel 2.1, 2. Absatz: Ergänzung des Hinweises auf die neue Anlage 5 „WSDL-Austausch-TAF-TAP-TSI-Nachrichten-und-Heartbeat.zip“. Kapitel 2.3: Ausführliche Beschreibung der technischen Validierung von eingehenden Nachrichten. Kapitel 3.2.2, 1. Absatz: Ergänzung des Verweises auf die neue Anlage 5. Kapitel 3.2.2, letzter Absatz: Die Befüllungsregel für das Element „messageIdentifier“ wurde korrigiert. Kapitel 3.3: Ergänzung der Verweise auf die in den Anlagen 5 bis 7 bereitgestellten XSD und WSDL.	26.02.2021
4.3.0	DB Netz AG Alexander Petioky	Kapitel 2.3, neuer Absatz 5: Detailierung der Validierung von eingehenden Nachrichten und der Fehlermeldungen Kapitel 3.4: Verwendung der Zertifikate von RNE CA und Abhängigkeit zum CompanyCode der Nachrichten	16.08.2021
4.4.0	DB Netz AG Alexander Petioky	Kapitel 2.3: Die inhaltliche Validierung der eingehenden Nachrichten erfolgt zum Großteil asynchron	28.02.2022
4.4.1	DB Netz AG Alexander Petioky	Keine Anpassungen	22.08.2022
4.4.2	DB Netz AG Aleander Petioky	Kapitel 2.2: Anpassung der CI-InstanceNumber auf einen Integerwert „1“	10.05.2023

Inhaltsverzeichnis

1 Einleitung

Zum Verständnis der Kommunikation zwischen EVU und DB Netz sind insbesondere folgende Dokumente relevant:

- Hauptdokument zur Dokumentation der Schnittstelle des Bestellsystems der DB Netz für EVU-Systeme: Fachliche Beschreibung der Schnittstelle (u. a. Objekte, Nachrichten und deren Abfolgen, zu beachtende Geschäftsregeln)
- Anlage 1 der Dokumentation zur Schnittstelle des Bestellsystems: Struktur und Datenfeldbeschreibungen; Fachliche Beschreibung der Datenstrukturen in den Nachrichten
- Technisches Dokument der ERA zum Common Interface (Annex D.2: Appendix E, siehe [1]). In diesem Dokument sind die Kapitel (4 „COMMUNICATION LAYER BETWEEN COMMON INTERFACE"); **5** „WEB SERVICE" und **6** „WEB SERVICE FOR REMOTE LI HEARTBEAT CHECK" die Basis für die Implementierung der Schnittstellen beider Schnittstellen-Partner.
- Anlage 2 der Dokumentation zur Schnittstelle des Bestellsystems: Technische Funktionsbeschreibung; Technische Aspekte der Kommunikation als ergänzende Beschreibung zum führenden technischen Dokument der ERA (Appendix E, siehe [1]). Hier werden optionale Funktionalitäten fixiert, Rahmenbedingungen definiert.

Schärfung unterschiedlicher existierender Begriffe, Sichten und Ausprägungen:

Die DB Netz implementiert eine technische Schnittstelle in Form eines SOAP WebService („CI_Planning_DBNetz" genannt) zum Austausch von Nachrichten zwischen dem EVU-System und dem Bestellsystem der DB Netz.

In Abgrenzung dazu existiert das Common-Interface der RNE, welches von der RNE spezifiziert und veröffentlicht wird sowie Teil des Common Components Systems ist. Das Common Components System besteht neben dem Common Interface der RNE aus weiteren Komponenten u.a. „Central Reference File Database" (CRD) sowie „Certificate Authority" (CA). Informationen sind über den Link http://ccs.rne.eu/common-interface/ abrufbar.

Beim Common Interface muss zwischen der Spezifikation als solche und einer spezifischen Implementierung in einer Software unterschieden werden. Die RNE lizensiert in diesem Zusammenhang eine Software, welche die Spezifikation des Common-Interface implementiert. Die DB Netz hat sich entschlossen, eine eigene, kompatible Software zu implementieren. Die zukünftige EVU-SST für das neue Bestellsystem der DB Netz bildet die Spezifikation des Common Interface der ERA ab, welche eine technische Definition für den TAF/TAP-TSI konformen Nachrichtenaustausch zwischen den beteiligten Bahngesellschaften (EVU und EIU) ist.

Zum Verständnis gilt es zwischen folgenden Begrifflichkeiten zu unterscheiden:

i) Spezifikation des Common-Interface („CI-Spec"). Die Spezifikation beschreibt u.a. die Funktionsweise des technischen Nachrichtenaustauschs; der Umgang mit Zertifikaten etc.

ii) Lizenzpflichtige CI-Software, welche die RNE entwickelt hat („*CI-SW-RNE*"). In der Dokumentation der RNE wird nicht unterschieden zwischen dieser Software und der Spezifikation. Die Begriffe „Common Interface", „CI", „CI Tool", „CI Reference Implementation" u.a. werden synonym verwendet.

iii) CI-Instanz, welche die RNE zentral betreibt und über diese die EVU und EIU ebenfalls Nachrichten austauschen können („CI der RNE").

iv) EVU-Schnittstelle des Bestellsystems der DB Netz ab Version 4.0.0, welche den zukünftigen TAF/TAP-TSI konformen Nachrichtenaustausch zwischen den beteiligten Bahngesellschaften realisiert. Dieser SOAP WebService („***CI_Planning_DBNetz***") bildet ebenfalls die CI-Spec [1] ab.

v) Eine beliebige Instanz einer Common-Interface konformen Schnittstelle wird im Text mit „*CI*" benannt.

vi) Im allgemeinen, unspezifischen Sinn ist in diesem Dokument vom „Common Interface" die Rede.

2 Kommunikation mit CI_Planning_DBNetz

2.1 Allgemeine Hinweise zur Kommunikation

Grundlage für die Kommunikation zwischen den EVU und der DB Netz ist die XSD-Version, die der aktuell gültigen EVU-SST-Dokumentation der DB Netz zugrunde liegt. Im Detail erfolgt die technische Kommunikation

- grundsätzlich auf Basis der CI-Spec, siehe [1] Kapitel 4 und 5.
- „peer to peer“, d.h. durch separate 1:1 („one-to-one“ oder „point-to-point“) Verbindungen, über die jeweils 2 Partner miteinander kommunizieren.
- über HTTPS (die Daten werden mit SSL verschlüsselt), das Protokoll auf dem Application-Layer ist SOAP, die Struktur der Nachrichten (des payload) ist XML.

Mit dem Hintergrund, dass sowohl EVU als auch EIU Nachrichten an den jeweils anderen Partner senden, müssen beide Instanzen eine SOAP Schnittstelle (WebService) betreiben, den die Partner aufrufen können. Die öffentliche WSDL der ERA wird als Anlage 5„WSDL-Austausch-TAF-TAP-TSI-Nachrichten-und-Heartbeat.zip“ bereitgestellt.

Das neue Bestellsystem der DB Netz kann nur die für den Trassenbestell- und Zuweisungsprozess erforderlichen TAF/TAP-TSI Nachrichten verarbeiten, siehe Hauptdokument der EVU-SST-Dokumentation, Kapitel 2.2. Konkret sind dies folgende Nachrichten, die vom EVU an DB Netz gesendet werden können:

- PathRequestMessage
- PathConfirmedMessage
- PathDetailsRefusedMessage
- PathCanceledMessage
- ReceiptConfirmationMessage
- ErrorMessage
- ObjectInfoMessage
- UpdateLinkMessage

Umgekehrt erfordert eine peer-to-peer Kommunikation per WebService, dass jedes EVU, welches über CI_Planning_DBNetz mit dem Bestellsystem der DB Netz kommunizieren möchte, ebenfalls einen WebService bereitstellt. Dieser WebService muss sich ebenfalls nach der TAF/TAP-TSI Spezifikation richten. Er muss die notwendigen Aspekte der CI-Spec [1] implementieren. Mit der Zielsetzung einer erfolgreichen TAF/TAP-TSI Kommunikation zur Bestellung von Trassen bei der DB Netz, muss der WebService des EVU die im Hauptdokument der EVU-SST-Dokumentation, Kapitel 2.2 beschriebenen und von der DB Netz gesendete Nachrichten verarbeiten können. Die DB Netz sieht eine Versendung der nachfolgenden Nachrichten an die EVU vor:

- PathDetailsMessage
- PathNotAvailableMessage
- ReceiptConfirmationMessage
- ErrorMessage
- ObjectInfoMessage
- UpdateLinkMessage

Den fachlich/funktionalen Teil der Kommunikation regelt das Hauptdokument sowie Anlage 1 der EVU-SST-Dokumentation.

2.2 Bilateral zu vereinbarende Kommunikationsparameter

Wie in [1], Kapitel 5 beschrieben gilt es, die notwendigen Kommunikationsparameter bilateral abzustimmen. Sowohl für die Kommunikation vom EVU zur DB Netz als auch umgekehrt.

Folgende Parameter sind für die Kommunikation mit CI_Planning_DBNetz seitens DB Netz vorab bekannt:

- Receiver Company: *0080*
- CI Instance Number: *1*
- Communication mode: *Web-Service*
- Protocol: *HTTPS*

Die nachfolgenden Parameter seitens DB Netz bekommen Sie nach Antragsstellung mitgeteilt:

- Public host names/IP Address for sending and receiving
- Port
- Informationen zum Client-Zertifikat der DB Netz (siehe Kapitel 3.4)
- URL des Heartbeat Web-Service, (siehe Kapitel 3.8)

Die nachfolgenden Kommunikationsparameter seitens des EVU gilt es an DB Netz im Vorfeld der Kommunikation mitzuteilen

- CompanyCode des EVU (CompanyCode mit welchem Sie mit DB Netz kommunizieren möchten)
- Public host names/IP Address for sending and receiving
- Port
- CI Instance Number (Instanz Ihres Common-Interface); Falls abweichend vom Standard 01. Die CI Instance Number referenziert den Verfahrens-User. Dieser ist eine von DB Netz vergebene Bezeichnung für das IT-Verfahren des EVU, welches für die Kommunikation benutzt wird.
- Informationen zum Client-Zertifikat des EVU (siehe Kapitel 3.4)
- URL Ihres Heartbeat Web-Service, (siehe Kapitel 3.8)
- Bezeichnung der freigegebenen Software/des IT-Verfahrens des EVU (siehe Kapitel 4).

2.3 Funktionsweise der Nachrichtenverarbeitung

Die Validierung eingehender Nachrichten erfolgt in mehreren Schritten und Detailierungstiefen. Die technisch notwendigen Validierungen erfolgen bereits mit Aufruf der Common Interface Schnittstelle und werden synchron beantwortet.

2.3.1 Synchrone Validierung eingehender Nachrichten

Die synchrone Validierung von Nachrichten vom EVU erfolgt in folgenden Schritten und kann folgende Ergebnisse liefern.

1. **Technische Überprüfung der Nachrichtenübertragung**

   Fehlerfall:

   Sind die Anmeldedaten nicht korrekt, wird im HTTP-Header der ErrorCode 403 (not authorized) zurückgegeben. Bei Fehlern auf Protokollebene wird im HTTP-Header der ErrorCode 500 zurückgegeben.

2. **Überprüfung der Autorisierung**

   Es wird die Berechtigung zum Aufruf der Common Interface Schnittstelle überprüft und sichergestellt, dass der aufrufende Partner für den in der TAF/TAP-TSI Nachricht hinterlegten Sender (Element im MessageHeader) berechtigt ist. Details sind dem Abschnitt 3.4 Authentifizierung und Autorisierung zu entnehmen.

   Fehlerfall:

   Ist der Kommunikationspartner unbekannt oder nicht für den Aufruf berechtigt, so erhält der Absender synchron einen SOAP-Response gemäß CI-Spec [1], Kapitel 5.3 mit ResponseStatus = NACK. Die XSD zu der Nachricht (CI_Acknowledgement.xsd) wird im Anhang 5 „WSDL-Austausch-TAF-TAP-TSI-Nachrichten-und-Heartbeat“ bereitgestellt.

3. **Überprüfung der MessageReference bei der übermittelten TAF/TAP-TSI Nachricht**

   Da für die Zuordnung von asynchronen Fehlernachrichten die eindeutige Identifizierung der eingegangenen Nachricht notwendig ist, wird die Existenz einer fachlichen XML-Nachricht nach TAF/TAP-TSI im SOAP-Body unter <UICMessage><message> überprüft.

   In dieser fachlichen Nachricht wird unter <MessageHeader> die <MessageReference> erwartet (Strukturbeschreibung siehe EVU-SST Dokumentation Anlage 1, Kap. 3.2) und überprüft. Diese Daten werden für die Referenzierung bei den asynchronen Fehlernachrichten verwendet.

   Fehlerfall:

   Kann im SOAP-Body keine Message gefunden werden oder sind die Daten in der <MessageReference> nicht vollständig, so wird ein SOAP-Fault mit entsprechendem Fehlertext retourniert, wie zum Beispiel „Missing MessageHeader“ oder „No Message in SOAP-Body“.

   Erfolgsfall:

   Waren diese technischen Validierungen erfolgreich, so erhält das EVU synchron einen SOAP-Response gemäß CI-Spec, [1] Kapitel 5.3 mit ResponseStatus = ACK. Die XSD zu der Nachricht (CI_Acknowledgement.xsd) wird in Anlage 5 „WSDL-Austausch-TAF-TAP-TSI-Nachrichten-und-Heartbeat“ bereitgestellt.

4. **Allgemeiner technischer Fehler bei der synchronen Verarbeitung:**

   Tritt bei der synchronen Verarbeitung des Requests oder der übersendeten Nachricht auf Seiten DB Netz ein technischer Fehler auf, der keinem fachlichen Fehlercode zugeordnet werden

kann, so wird ein SOAP-Fault mit <faultcode> „6000“ und dem Hinweis „Interner technischer Fehler bei der Verarbeitung“ im <faultstring> zurückgegeben.

2.3.2 Asynchrone Validierung eingehender Nachrichten

War die synchrone Validierung erfolgreich, so findet nach dem Versenden des Acknowledgements (mit ResponseStatus „ACK“) eine asynchrone technische und fachliche Validierung der eingehenden TAF-TAP Nachricht statt.

Erkannte Fehler werden mit der TAF/TAP-TSI Nachricht „ErrorMessage“ (Strukturbeschreibung siehe Anlage 1 Kap. 2.2.8 der EVU-SST Dokumentation) übermittelt. Für die Zuordnung der ErrorMessage zur ursprünglichen Nachricht wird unter <ErrorCauseReference> die <MessageReference> der validierten, eingegangenen Nachricht angegeben.

> Die verwendeten ErrorCodes sind der TAF/TAP-TSI Codeliste entnommen. Wenn notwendig wurden von Seiten DB Netz zusätzliche ErrorCodes definiert, diese können der Anlage 9 „Fehlermeldungen der DB Netz“ entnommen werden.

1. **Überprüfung von SOAP-Header**

   Zu Beginn der asynchronen Validierung erfolgt eine Überprüfung des SOAP-Headers entsprechend Kapitel 3.2.2.

   Fehlerfall:

   Schlägt diese Validierung fehl, so wird eine ErrorMessage mit <ErrorCode> 6087 und sprechender Fehlermeldung im <FreeTextField> zurückgeliefert. Der Fehlerfall wird bei DB Netz protokolliert. Der Absender muss in diesem Fall die Nachricht mit korrigierten Daten erneut senden.

   Beispiel für eine ErrorMessage bei unterschiedlichen Message Identifier in SOAP Header und Message Header der eingehenden Nachricht:

2. **Überprüfung der Struktur der übermittelten TAF/TAP-TSI Nachricht**

   Die im SOAP-Body enthaltene TAF/TAP-TSI Nachricht wird gegen die aktuelle TAF/TAP-TSI Schemadefinition validiert (siehe Kapitel 3.3). Zusätzlich werden weitere EIU-spezifische Regeln, entsprechend den Vorgaben im Hauptdokument und der Anlage 1, überprüft. So werden bspw. die NetworkSpecificParameters auf Pflichtangaben, Format und zulässige Werte überprüft.

   Fehlerfall:

   Ist die Nachricht nicht valide, so wird eine ErrorMessage mit den Details zu den Fehlern (in <ErrorCode> und <FreeFieldText>) gesendet.

   Der Fehlerfall wird bei DB Netz protokolliert. Das EVU muss in diesem Fall die Nachricht mit korrigierten Daten erneut senden.

3. **Validierung der Identifiers**

   Ist das Nachrichtenformat valide und konform, so werden <MessageIdentifier> auf Eindeutigkeit und <Identifier>, abhängig von Nachrichtentyp, auf Eindeutigkeit bzw. Bekanntheit überprüft.

   Fehlerfall:

   Schlägt diese Validierung fehl, so wird eine entsprechende ErrorMessage gesendet.

4. **Fachliche Validierung bezogen auf den Geschäftsvorfall**

   Vor der fachlichen Verarbeitung der Nachricht werden fachliche Validierungen des Inhalts durchgeführt. Dies sind beispielhaft die Überprüfung von Anmeldefristen bei Erstanmeldungen

oder der zeitgerechten Zusendung einer PathConfirmedMessage zu einem bereits laufenden Geschäftsvorfall.

Fehlerfall:

Fachliche Fehler in den Daten der Nachricht oder bezogen auf den Geschäftsvorfall werden mit einer TAF/TAP-TSI ErrorMessage und spezifischen ErrorCodes an das EVU gemeldet.

Erfolgsfall:

Konnten die Nachricht erfolgreich verarbeitet und wenn notwendig einem laufenden Geschäftsfall zugeordnet werden, so wird dem EVU eine ReceiptConfirmationMessage übermittelt. Die eingehende Nachricht wird bei DB Netz protokolliert. Die weitere fachliche (asynchrone) Verarbeitung erfolgt gemäß dem Hauptdokument der Schnittstellendokumentation, Kapitel 5.

3 Technische Hinweise und Anforderungen

3.1 WSDL

Die WSDL der DB Netz ist inhaltlich identisch mit der der ERA. Lediglich die Service-URL muss (entsprechend der erhaltenen Zugangsdaten) angepasst werden.

3.2 SOAP über HTTP(s)

SOAP stellt ein Netzwerkprotokoll dar, mit dessen Hilfe Daten zwischen Systemen ausgetauscht und Remote Procedure Calls durchgeführt werden können. SOAP steht für einen industriellen Standard des World Wide Web Consortiums (W3C).

Siehe CI-Spec [1], Kapitel 5.2

3.2.1 SOAP Envelope

Der SOAP-Envelope ist Teil der SOAP-Spezifikation und nicht der WSDL. Aus diesem Grund existieren seitens der CI-Spec [1], Kapitel 5, keine Vorgaben für den Envelope. Nachfolgend finden Sie einen Ausschnitt aus einem Beispiel im Annex 3:

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:uicm="http://uic.cc.org/UICMessage">

Beispiele für SOAP-Requests finden Sie in [1] in Annex 2 und Annex 3.

- Annex 2: SAMPLE MESSAGE-WITH-COMPRESSION-SIGNING-ENCRYPTION
- Annex 3: SAMPLE MESSAGE-WITHOUT-COMPRESSION-SIGNING-ENCRYPTION

3.2.2 SOAP Header

Der SOAP-Header ist beschrieben in der CI-Spec [1], Kapitel 5.2. Die WSDL („CI_WSDL_Messaging.wsdl“) definiert, welche Parameter im SOAP-Header erlaubt sind, und wird in Anlage 5 „WSDL für Austausch von TAF/TAP-TSI Nachrichten und Heartbeat“ bereitgestellt.
Die DB Netz erwartet für die Werte der Parameter ‚compressed‘, ‚encrypted‘ und ‚signed‘ jeweils den Wert „false“.

Nachfolgend finden Sie einen Ausschnitt aus einem Beispiel im Annex 3:

```
<soap:Header>
        <uicmh:signed xmlns:uicmh="http://uic.cc.org/UICMessage/Header">false</uicmh:signed>
        <uicmh:encrypted xmlns:uicmh="http://uic.cc.org/UICMessage/Header">false</uicmh:encrypted>
        <uicmh:compressed xmlns:uicmh="http://uic.cc.org/UICMessage/Header">false </uicmh:compressed>
        <uicmh:messageIdentifier xmlns:uicmh="http://uic.cc.org/UICMessage/Header">796cc4ee-cd51-49c2-a8cf-3bd73b29ddfa </uicmh:messageIdentifier>
        <uicmh:messageLiHost xmlns:uicmh="http://uic.cc.org/UICMessage/Header">122.109.101.100</uicmh:messageLiHost>
</soap:Header>
```

Die CI-Spec [1] sieht nur eine Signatur im SOAP-Header und nicht im HTTP-Header vor. Der messageIdentifier muss identisch mit dem messageIdentifier in der Datenstruktur MessageHeader sein (siehe Anlage 1, Abschnitt 3.2.2 Datenfelder der Struktur „MessageHeader“)

3.3 Schemata (XSD)

Die Strukturen der TAF/TAP-TSI Nachrichten werden anhand von XSD-Dateien spezifiziert. Die erforderlichen XSD-Dateien, die als Beschreibungsvorlage für die Erzeugung der jeweils gewünschten XML-Daten zu verwenden sind, finden Sie in den Anlage 4 der EVU-SST-Dokumentation:

- Anlage 4: „taf_tap_cat_complete_sector.xsd“ Definitionen der Nachrichten (von TAF/TAP-TSI festgelegt)

Die TAF/TAP-Nachrichten werden über ein Webservices ausgetauscht. Die WSDL- und XSD-Dateien des Webservices auf Seiten der DB-Netz finden Sie ebenfalls in den Anlagen:

- Anlage 5: Anl5_WSDL-Austausch-TAF-TAP-TSI-Nachrichten-und-Heartbeat (zip)

Des Weiteren stellt die DB Netz eine jaml-Datei für die Übernahme der im Trassenbestellprozess notwendigen Stammdaten zur Verfügung.

- Anlage 6: Anl6_Technische_Funktionsbeschreibung_Stammdatenbereitstellung_V4.x.x.pdf

- Anlage 7: Anl7_stammdatenEVU.openapi.yaml

Die Tabellenstrukturen der Stammdaten sind in der Anlage 1 der EVU-SST-Dokumentation beschrieben. Der Aktualisierungszyklus der Stammdaten sowie die Plattform zum Download der entsprechenden Dateien wird Ihnen im Zuge der Beantragung des Zugangs zur EVU-Schnittstelle bekanntgegeben.

3.4 Authentifizierung und Autorisierung

Die Authentifizierung in beide Richtungen erfolgt über X.509-Zertifikate. Dies gilt für den WebServer und den Client, die im Rahmen einer TLS (Transport Layer Security) Verbindung (siehe auch Kapitel 3.5 Sicherheit) sich mit Hilfe des von RNE CA ausgestellten Zertifikats authentifizieren. Das von RNE CA ausgestellte Zertifikat wird sowohl als Server-, wie auch als Client-Zertifikat genutzt. Hierfür muss jeder Schnittstellenpartner seinen WebServer sowie SOAP-Client entsprechend konfigurieren.

Als Server-Zertifikat stellt es sicher, dass die von DB Netz aufgerufene Partner-URL authentisch ist. In der Verwendung als Client-Zertifikat stellt es zunächst sicher, dass nur bestimmte Partner die CI-Schnittstelle aufrufen dürfen. In dem ausgestellten Zertifikat wird im CommonName eine eindeutige Kennung (Domänenname des aufrufenden Partners) hinterlegt. Anhand dieser wird durch DB Netz die Berechtigung zur Übermittlung der enthaltenen Nachricht überprüft (siehe Kapitel 0). Die Zuordnung der Nachrichten zu einem Partner erfolgt anhand des CompanyCode im Sender-Element der TAF/TAP-TSI Nachricht. Auf Seiten von DB Netz ist die Berechtigung der Domänennamen (aus dem Zertifikat) für CompanyCodes (aus der übermittelten Nachricht) hinterlegt und wird entsprechend bei jedem Aufruf überprüft. Es besteht eine 1:n-Beziehung: Von einer Domäne können Nachrichten unterschiedlicher CompanyCodes gesendet werden, für einen CompanyCode ist jedoch genau eine sendende Domäne berechtigt.

Die benötigten Zertifikate werden für jeden Partner von RailNetEurope (RNE) Certification Authority (CA) zentral ausgestellt. Für die Verifizierung der Zertifikate muss jeder Partner das Root-Zertifikat des RNE in seinem lokalen Truststore installieren. Die im Rahmen der TLS/SSL-Verbindung ausgetauschten Zertifikate werden anhand des installierten RNE-Zertifikats verifiziert.

Eine Anleitung für die Konfiguration eines WebServers ist z.B. für den Apache Server hier zu finden: https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html.

Das EVU muss sich für die Nutzung eines bereits durch DB Netz getesteten und freigegebenen Verfahrens anmelden und bei jeder Kommunikation erneut verfahrensbezogen authentifizieren. Sofern ein Verfahren durch mehrere unterschiedliche EVU genutzt wird, erfolgt die Freigabe des Verfahrens nur einmal, die Anmeldung zur Nutzung des Verfahrens jedoch EVU-bezogen.

3.5 Sicherheit

Die Security-Aspekte sind beschrieben in [1], Kapitel 2.3, 2.4, 5.2, 5.6, 5.7

Der Nachrichtenaustausch findet verschlüsselt auf Transportebene über SSL/TLS statt. Die Kommunikation mit dem CI_Planning_DBNetz muss über X.509 Zertifikate abgesichert werden. Dadurch werden die Integrität und Vertraulichkeit der Nachrichten sichergestellt.

Die Common Interface Spezifikation erlaubt es, optional die Nachrichten-Inhalte zusätzlich zu verschlüsseln und zu signieren (siehe [1], Kapitel 5.2). Dies erfordert einen gegenseitigen Austausch der Partner-Zertifikate und ist redundant zu den Schutzmechanismen von TLS. Dies wird daher seitens DB Netz aktuell nicht vorgesehen bzw. nicht unterstützt. Alle Nachrichteninhalte der von der DB Netz gesendeten Nachrichten sind ebenfalls nicht verschlüsselt.

Die Integrität der Nachrichten wird über den Standard-TLS Mechanismus (MAC - Message Authentication Codes) sichergestellt

Es werden nur Zertifikate akzeptiert, die von der RNE CA (Certificate Authority) ausgestellt wurden. Diese erhält man vom „RNE CC Service Desk“: http://ccs.rne.eu/service-desk/

Die DB Netz erwartet, dass Sie TLS (Transport Layer Security) Version 1.2, besser Version 1.3 unterstützen.

3.6 Kodierung des Zeichensatzes

Bitte verwenden Sie zur Kodierung der XML-Daten ausschließlich den Unicode Zeichensatz UTF-8 und geben Sie dies entsprechend im XML-Header an. Siehe [1] Kapitel 5.2.2. Die Verwendung abweichender Zeichensätze ist ausgeschlossen und führt zur technischen Zurückweisung der Nachricht.

3.7 Timeout

Bitte setzen Sie das Timeout in Ihrer Schnittstelle auf mindestens 2 Minuten. In der Regel sind die Nachrichten unterhalb einer Sekunde abgearbeitet, bei Hochlastzeiten kann sich jedoch der Zeitbedarf erhöhen.

3.8 Anforderungen an die Verfügbarkeit der Systeme

Die ERA-Spezifikation beschreibt einen zweiten WebService als „Heartbeat Check“, Beschreibung siehe [1], Kapitel 6. DB Netz wird diesen WebService ebenfalls anbieten, die WSDL zu diesem Service (CI_WSDL_Heartbeat.wsdl) ist in der Anlage 5 „WSDL-Austausch-TAF-TAP-TSI-Nachrichten- und-Heartbeat“ abgelegt.

DB Netz fordert seitens der Schnittstellen-Partner bei ihrer TAF/TAP-TSI Schnittstelle diesen Heartbeat Check WebService ebenfalls anzubieten. Hintergrund ist die Anforderung, dass eine Systemüberwachung möglich sein muss, ohne Nutzdaten zu senden. Der gegenseitige Austausch der URL der Heartbeat WebServices erfolgt bei der Beantragung des Zugangs zur EVU-Schnittstelle, siehe Kapitel 2.2.

Die DB Netz strebt eine Schnittstelle mit einer Verfügbarkeit > 99,8% („hochverfügbar“) mit sehr wenigen geplanten Downtimes in vorher angekündigten Wartungsfenstern an. Im ungeplanten Störungsfall soll die Ausfallzeit maximal 4 Stunden dauern. Die gleichen Anforderungen stellt die DB

Netz auch an den Betrieb des CI auf Seiten der Partner-EVU mit einer Verfügbarkeit > 99,8% („hochverfügbar“). Das Senden von Nachrichten sollte grundsätzlich jederzeit möglich sein.

Seitens DB Netz wird erwartet, dass einzelne Nachrichten zwischengespeichert und asynchron verarbeitet werden. Dadurch soll auch bei hoher Anzahl von Nachrichten (insbesondere im Falle des VNP und ENP) eine Überlastung vermieden werden.

4 Testumgebung

Analog zur bisherigen EVU-SST für TPN muss vor der Nutzung der TAF/TAP-TSI konformen EVU-SST sowohl ein fachlicher als auch ein Integrationstest durchgeführt werden. Die DB Netz stellt hierfür eine entsprechende Testumgebung bereit. Die Kontaktdaten zur Abstimmung der durchzuführenden Tests (Testpartner, Abläufe, Testfälle etc.) sowie die Zugangsdaten zur Testumgebung erhalten Sie im Zuge der Anfrage zur Nutzung der TAF/TAP-TSI konformen EVU-SST beim entsprechenden Kundenbetreuer.

Erst nach erfolgreichem Test erfolgt eine Freigabe des IT-Verfahrens des EVU zur Nutzung für die Kommunikation über die EVU-Schnittstelle des Bestellsystems. Sofern ein Verfahren durch mehrere unterschiedliche EVU genutzt wird, erfolgt die Freigabe des Verfahrens nur einmal, die Anmeldung zur Nutzung des Verfahrens jedoch EVU-bezogen.

5 Dokument-Referenzen

[1] European Union Agency for Railways (2017): Interoperability Unit. TAF TSI – Annex D.2 : Appendix E – Common Interface. Reference ERA-TD-104. Document Type: Technical Document. Version 3.0, 15.06.2021. Verfügbar unter: https://www.era.europa.eu/sites/default/files/filesystem/taf/technical_documents/baseline_3.0.0/era_technical_document_taf-td-104_d_2_appendix_e.pdf

Internet-Links

Startseite ERA

https://www.era.europa.eu/

Startseite RNE Common Components System

http://ccs.rne.eu/

Beantragung eines UIC (RICS) CompanyCodes, siehe

http://www.uic.org/rics