EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system
work better for society.

Mr Libor Král
Aplikační Architekt IT
ČD – Informační Systémy, a.s.
Praha 3-Žižkov,
Pernerova 2819/2a,
130 00
Czech Republic

Valenciennes, 16th September 2022

TAF TSI Compliance Resultc – your Oracle Service Bus (OSB) as the TAF TSI Common Interface (CI) alternative implementation

To whom it may concern,

I confirm and certify herewith that the following TAF TSI Common Interface functionality implemented by the company ČD – Informační Systémy, a.s. (Czech Republic), is compliant with the appropriate provisions of the TAF-TSI Regulation 2021/541 and its Technical Documents.

The detailed results of the verification process are concluded as follows:

ČD – Informační Systémy, a.s. has sent to the European Union Agency for Railways on 11 August 2022, for verification, the document “CDIS request for OSB as CI alternative v1.pdf” – see details in Annex.

In addition, ČD Cargo has sent an explanatory note to the European Union Agency for Railways on 15 September 2022 for point g. „ handling the single common access to various databases“of above document.

ERA has verified the compliance of the document and of the explanatory note for the following points:

a. message formatting of outgoing messages according to the metadata,
b. signing and encryption of outgoing messages,
c. addressing of the outgoing messages,
d. authenticity verification of the incoming messages,
e. decryption of incoming messages,
f. conformity checks of incoming messages according to metadata,
g. handling the single common access to various databases.

The applicant has demonstrated, that above functions of the OSB are in line with chapter “4.2.11.5. Common Interface” of the TAF/TAP TSI regulation.

For above point g. it should be mentioned additionally, that the OSB is not used for the time being for connection to any database. The only existing TAF TSI database is CRD. The partners of CD IS have access to CRD via web and this fulfils all their needs. The so-called Rolling Stock Reference Database (RSRD) is distributed - with GCU Broker as connecting central point. The partners of CD IS are connected to the so-called GCU Broker in both ways via web services, tus, no need to use the Common Interface necessairily.
So there is no functional requirement to use the CI for this purpose. On the other hand, CD IS and its partners plan to use CI for several other use-cases (Train Composition Messages, Train Ready Messages, Train running, Path Request) soon.

Mickael VARGA
European Union Agency for Railways
Railway Systems Unit
Project Officer
Email: mickael.varga@era.europa.eu

Annex:

Informační Systémy

Request for Certification of the Oracle Service Bus as the Common Interface alternative implementation

We, ČD-Informační systémy, a.s. are IT provider for our sister company ČD Cargo, a.s (CDC). and as well for České dráhy, a.s (CD) as a parent company. They entrusted us to implement the TAF Common Interface for them using the existing Oracle Service Bus (so not using the Common Interface software from RNE).

One of their data exchange partners (Správa železnic, SZ, Czech IM) requests certification that this CI implementation fulfils the TAF CI requirements. Therefore we issue this request to EUAR and we ask you to kindly evaluate our arguments and issue an TAF CI compliance certificate.

Our implementation uses standard functions and features of the Oracle Service Bus (OSB), which is used for (almost) all internal and external communications of CDC and CD. This system was configured to act as the TAF CI and it was successfuly tested to Exchange TAF messages with the (RNE) CI of Správa železnic. To prove and evident correct functioning, sending of Train Composition Messages was implemented from system PRIS of CDC to system COMPOST of SŽ (via OSB-CI at CDC and RNE-CI at SŽ).

1 EUAR requirements

The requester submits to ERA elements or screen shots demonstrating that your Common Interface is able to handle:

a. *message formatting of outgoing messages according to the metadata,*
b. *signing and encryption of outgoing messages,*
c. *addressing of the outgoing messages,*
d. *authenticity verification of the incoming messages,*
e. *decryption of incoming messages,*
f. *conformity checks of incoming messages according to metadata,*
g. *handling the single common access to various databases.*

Your CI should be able to be configured to exchange TAF compliant messages with your partners / databases according to the specifications in the Technical Document " TAF TSI — Annex A.5: Figures and Sequence Diagrams of the TAF TSI messages".

Please indicate which TAF TSI functions are supported by your CI. Please send for these functions the messages / datasets from your legacy system and the corresponding TAF compliant messages which have been generated by your CI. Please give us some information about the IT solution you use for this CI and the linked IT Systems within ČD.

The other TAF Technical Document "TAF TSI - ANNEX D.2: APPENDIX E - COMMON INTERFACE" gives you further requirements about CI2CI communication too.

Please indicate us which EU funding you have received to realise this project. If this is not the case please indicate that you have not received EU funding.

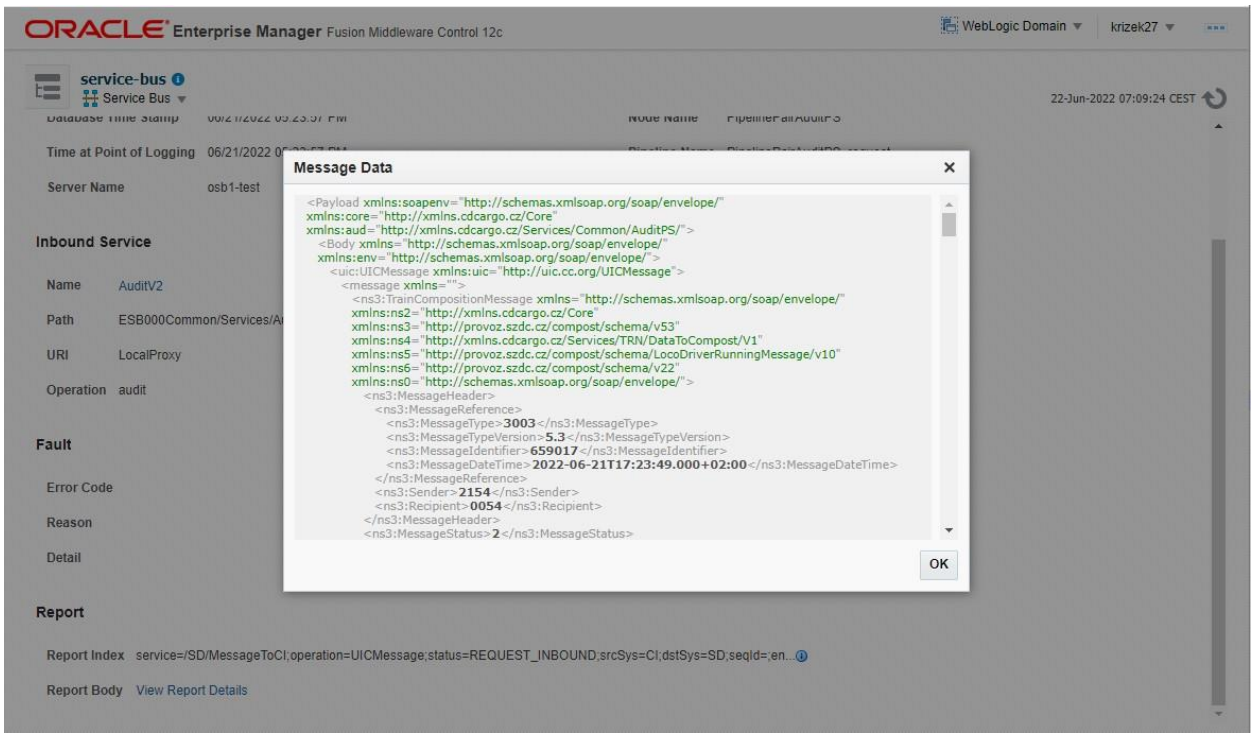
2 Fulfilment of the requirements

a. Message formatting of outgoing messages according to the metadata

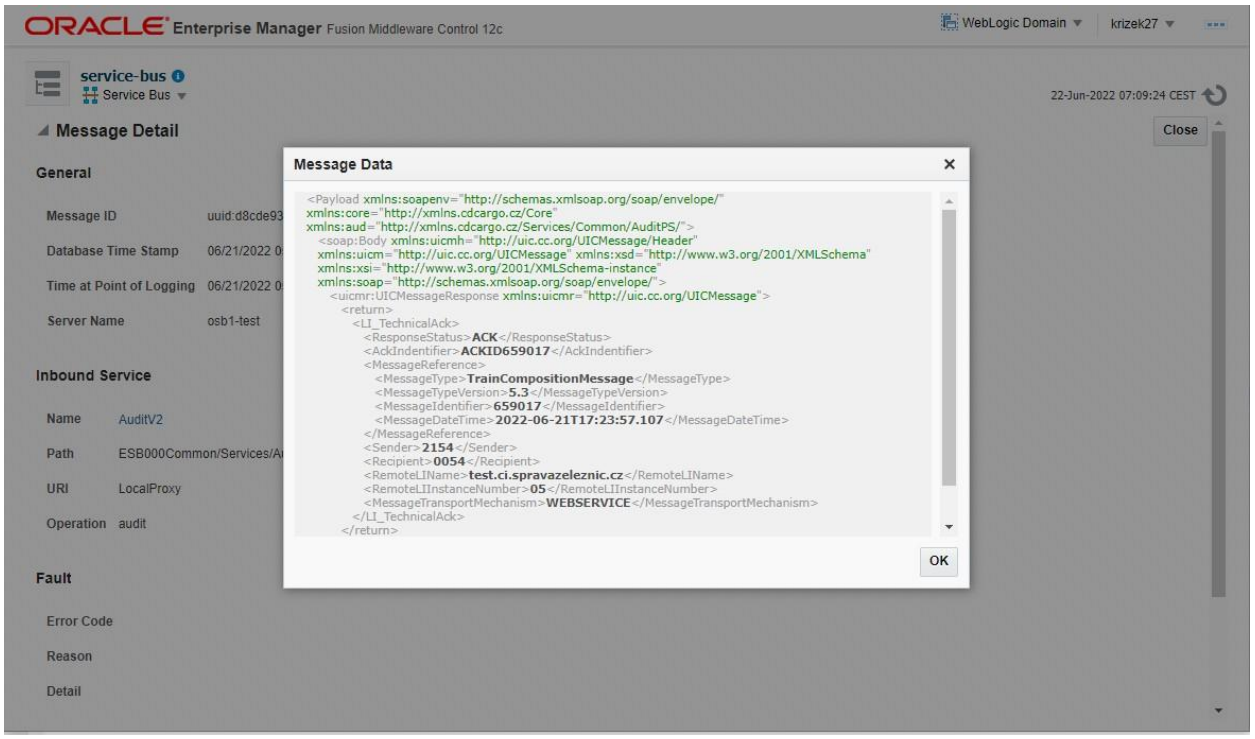
Source information systém of ČD Cargo – PRIS (Production Information Systém) generates Train Composition messages based on the TAF standard and same time fulfils the validation requirements defined on the side of the Common Interface. So created messages are nativly generated in source system in valid format, as requested by the TAF TCM xsd schema.

Message TO CI

Request (example)

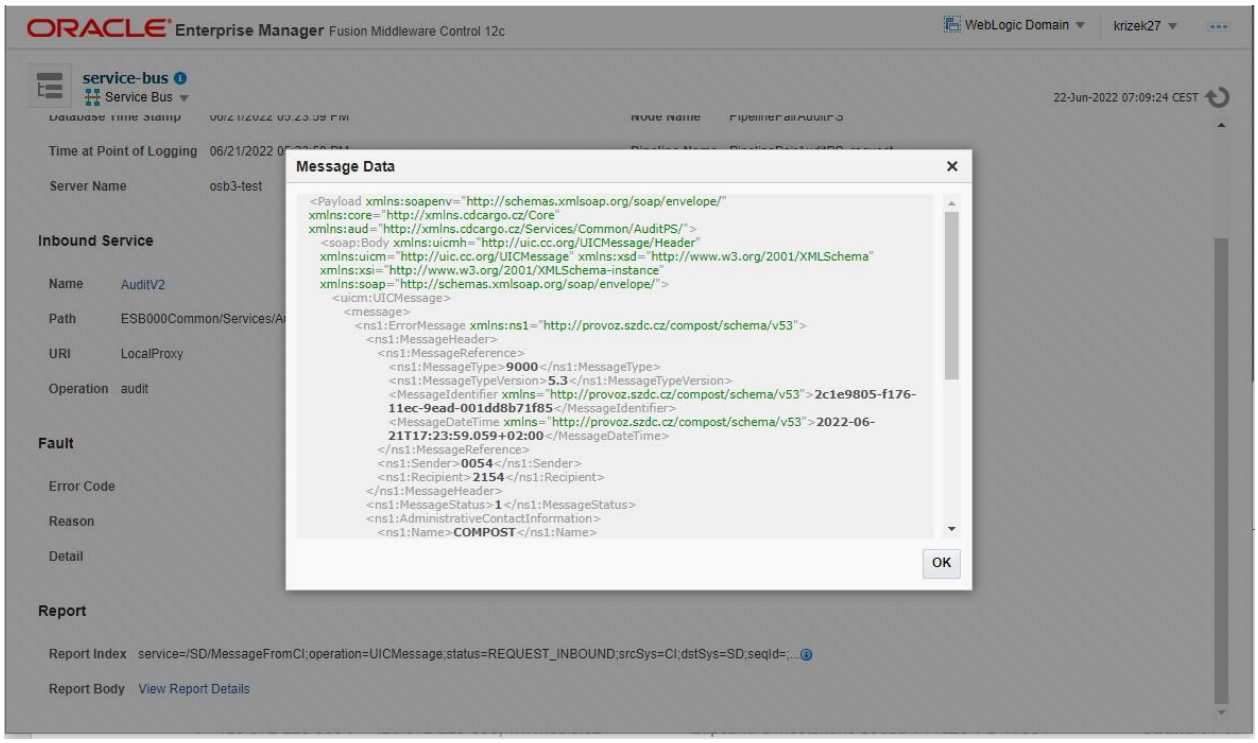


Response (example):

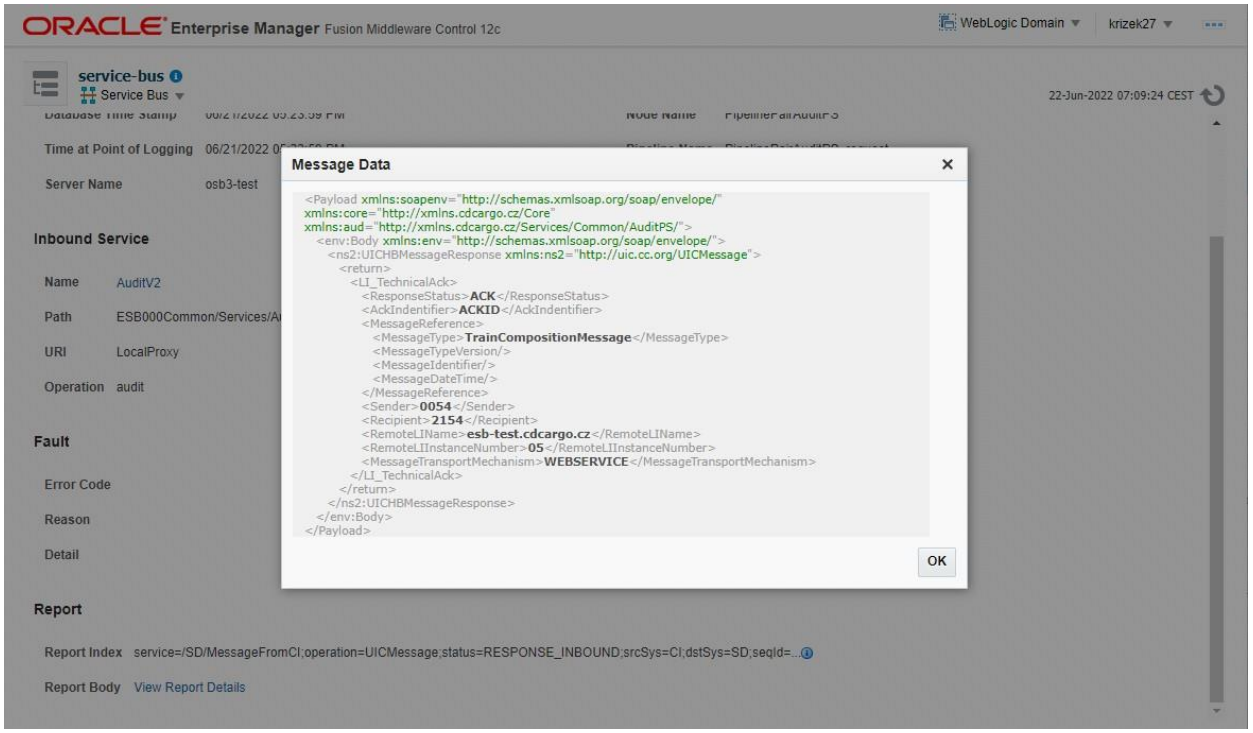


Message From CI

Request



Response



b. Signing and encryption of outgoing messages

Certificate

According to the document „era_technical_document_taf_d_2_appendix_e.pdf“ are both encryption and authentication optional features. Since the communication between CDC and SŽ is performed only in shared intranet, it is accepted and agreed between CDC and SŽ to exchange messages with out these features.

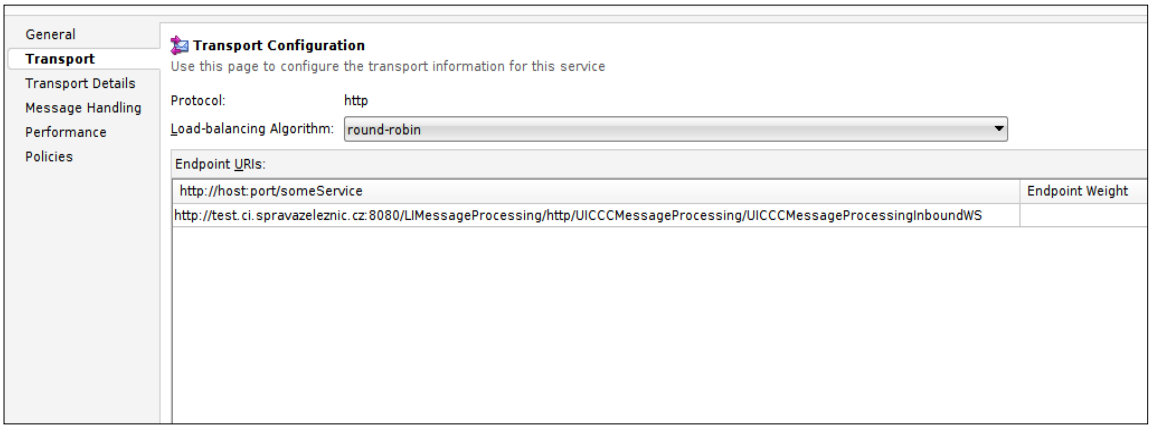
Anyhow, for future purposes (eventual move to Internet) and communication with other partners, CD Cargo, a.s., as well as ČD a.s., concluded CCS Agreement with RNE and purchased and obtained the X.509 security certificate (for non-RNE CI implementation).

Secured communication (using https) will be tested.

It is not currently required by ČD Cargo, a.s., or ČD a.s.

c. Addressing of the outgoing messages

We have recieved needed URL from SŽ for transmission of the Train Compostion messages, which we set into the OSB.


General
Transport
Transport Details
Message Handling
Performance
Policies
Transport Configuration
Use this page to configure the transport information for this service
Protocol:
http
Load-balancing Algorithm:
round-robin
Endpoint URIs:
http://host:port/someService
Endpoint Weight
http://test.ci.spravazeleznic.cz:8080/LIMessageProcessing/http/UICCCMessageProcessing/UICCCMessageProcessingInboundWS

d. Authenticity verification of the incoming messages

For the purpose of communcation and possible setup of signature verification are in OSB imported keys into standardized keystore, it means root certificate. From there is the key used by OSB when communicating with Common Interface – through encrypted https channel.

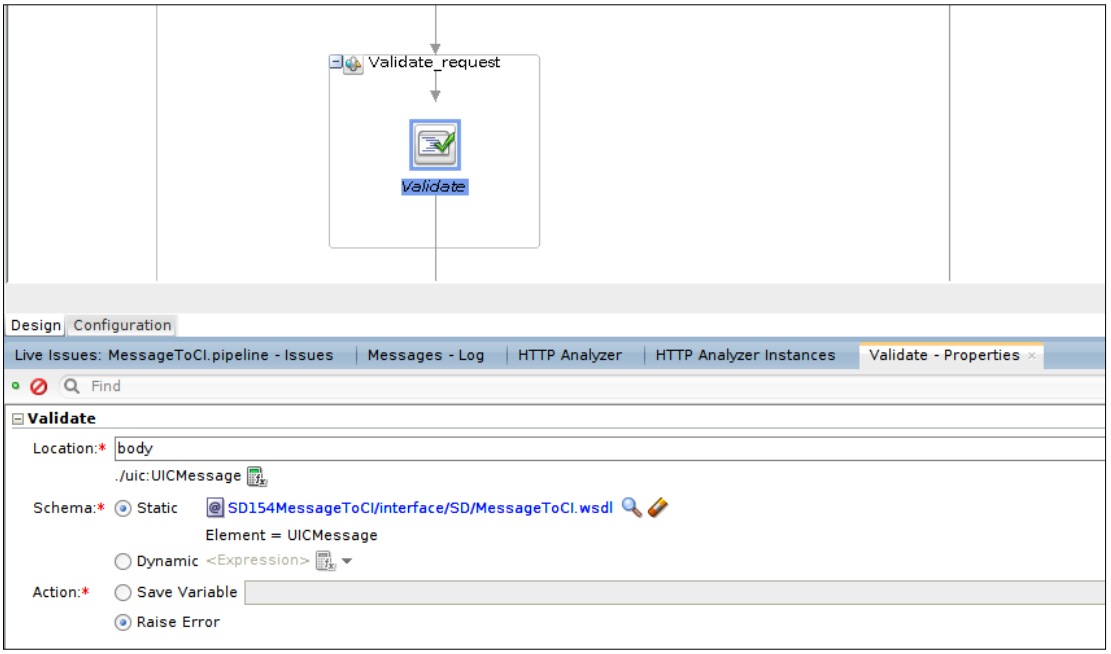
```
[root@osb4-test ~]# /usr/java/latest/bin/keytool -list -v -alias mykey -keystore /usr/java/latest/jre/lib/security/cacerts -st
Alias name: mykey
Creation date: Feb 25, 2022
Entry type: trustedCertEntry

Owner: C=AT, ST=Vienna, L=Vienna, O=RNE, OU=Common Components System, CN=CA CCS 1
Issuer: C=AT, ST=Vienna, L=Vienna, O=RNE, CN=Root CA
Serial number: 4351629bfce8a095
Valid from: Wed Nov 29 11:53:28 CET 2017 until: Tue Nov 29 11:53:28 CET 2022
Certificate fingerprints:
         SHA1: F5:5A:1A:D2:79:03:70:8A:C4:68:F3:75:50:BF:74:D2:5C:FA:8D:F6
         SHA256: 10:7C:3F:BD:D0:64:B1:8F:7C:93:7A:88:C6:93:AD:91:41:D2:E6:C9:9F:D9:9A:81:B5:AA:B3:31:7D:F3:D5:D2
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 4F 6E AE 18 71 95 DE 3F   A0 1D F5 AA 24 E7 99 11  On..q..?....$...
0010: CE BC DA B6                                        ....
]
]

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
     [URIName: http://rootca.rne.eu/publicweb/webdist/certdist?cmd=crl&issuer=CN=Root%20CA,O=RNE,L=Vienna,ST=Vienna,C=AT]
   CRLIssuer:[C=AT, ST=Vienna, L=Vienna, O=RNE, CN=Root CA]
]]

#4: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [1.3.6.1.4.1.50887.1.2]
[]  ]
]

#5: ObjectId: 2.5.29.46 Criticality=false
FreshestCRL [
  [DistributionPoint:
     [URIName: http://rootca.rne.eu/publicweb/webdist/certdist?cmd=deltacrl&issuer=CN=Root%20CA,O=RNE,L=Vienna,ST=Vienna,C=AT]
]]

#6: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#7: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 35 F9 00 2D 44 B1 1C D0   A4 DE AD 33 12 A5 C2 23  5..-D......3...#
0010: E0 4D B0 B0                                        .M..
]
]
```

e. Decryption of incoming messages

Please see the comments in chapter b.

f. Conformity checks of incoming messages according to metadata

Flow for automated validation of messages against defined XSD was used as part of the implementation.



Example of validity check and example of validtion error:

Invalid message (in OSB environnent)

Request Document

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    </soap:Header>
    <soapenv:Body>
        <uic:UICMessage xmlns:uic="http://uic.cc.org/UICMessage1">
            <!--Optional:-->
            <message>anyType</message>
            <!--Optional:-->
            <signature>anyType</signature>
            <!--Optional:-->
            <senderAlias>anyType</senderAlias>
            <!--Optional:-->
            <encoding>anyType</encoding>
        </uic:UICMessage>
    </soapenv:Body>
</soapenv:Envelope>
```

Message validity check and following error alert response

Response Document

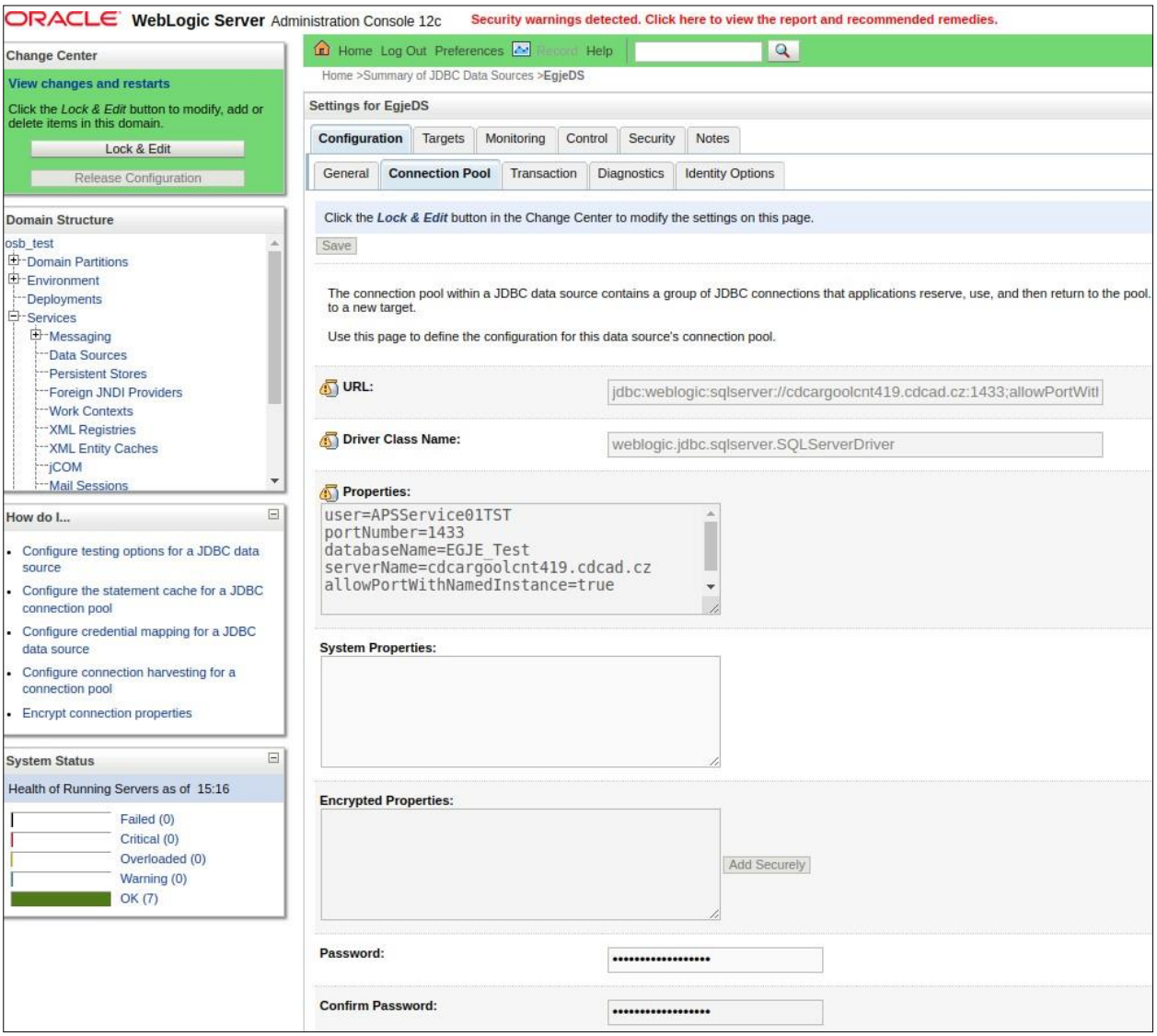
The invocation resulted in an error: .

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Body>
        <soapenv:Fault>
            <faultcode>soapenv:Server</faultcode>
            <faultstring>
                OSB-382505: OSB Validate action failed validation
            </faultstring>
            <detail>
                <con:fault xmlns:con="http://www.bea.com/wli/sb/context">
                    <con:errorCode>OSB-382505</con:errorCode>
                    <con:reason>OSB Validate action failed validation</con:reason>
                    <con:details>
                        <con1:ValidationFailureDetail xmlns:con1="http://www.bea.com/wli/sb/stages/transform/config">
                            <con1:message>
                                XPath statement produced no nodes to validate
                            </con1:message>
                            <con1:xmlLocation/>
                        </con1:ValidationFailureDetail>
                    </con:details>
                    <con:location>
                        <con:node>Pipeline</con:node>
                        <con:pipeline>
                            request-7f000001.Nc0661cd.0.15ba9c1a690.N8000
                        </con:pipeline>
                        <con:stage>Validate_request</con:stage>
                        <con:path>request-pipeline</con:path>
                    </con:location>
                </con:fault>
            </detail>
        </soapenv:Fault>
    </soapenv:Body>
</soapenv:Envelope>
```

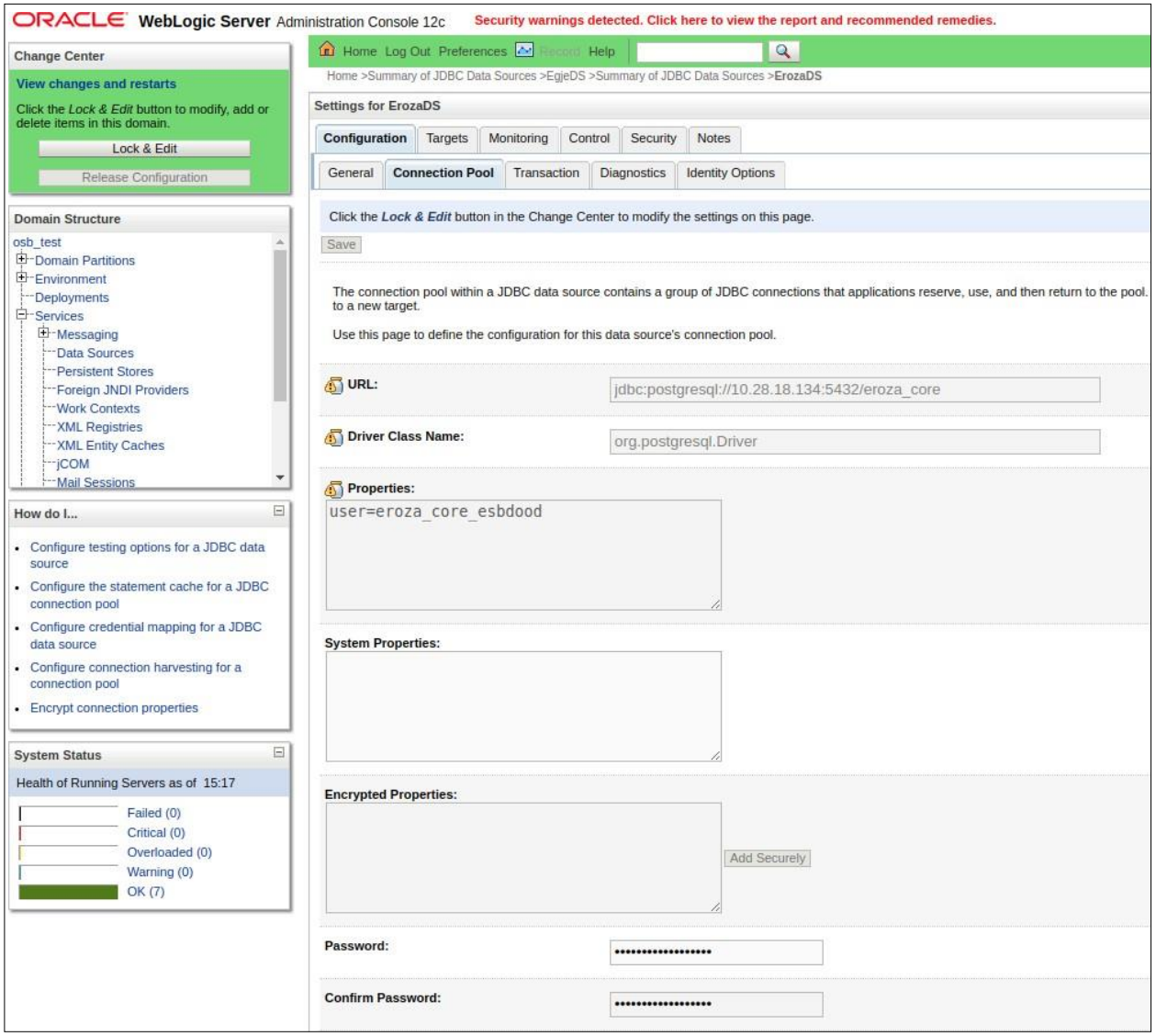
Validation error report

g. Handling the single common access to various databases

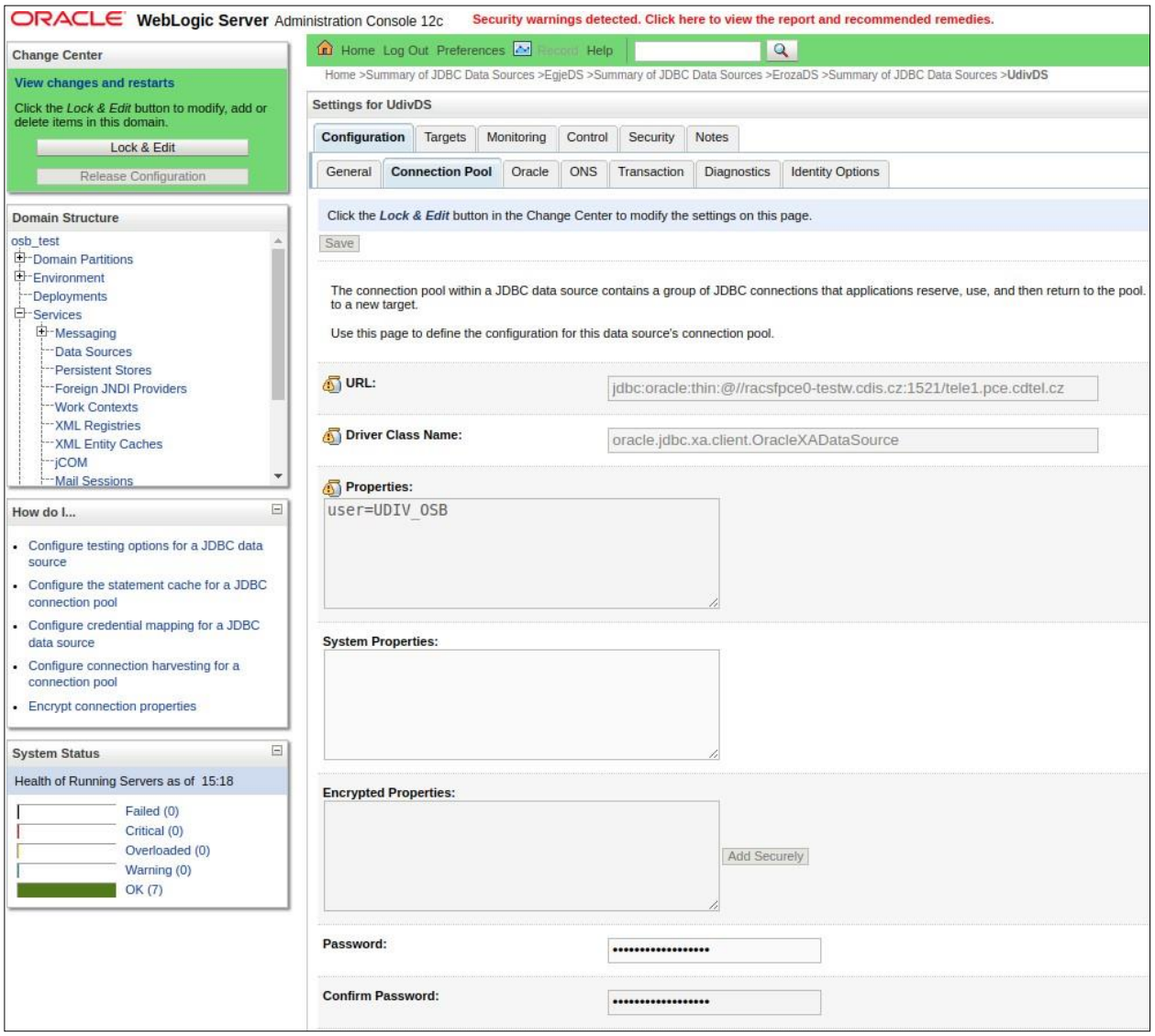
OSB system with its components enables connection to various databases. Examples of connection Oracle SQL, MS SQL a Postgre databses are given below.



MS SQL connect



Postgre connect



Oracle SQL connect

3 Information about our environment

TAF TSI functions supported, exchange of TAF compliant messages

Our OSB-Common Interface is able to transmit TAF compliant messages.

As first TAF function implemented, it supports the Train Preparation function.

It was configured to send TAF Train Composition and Train Ready messages to Správa železnic (SŽ), the Czech IM and to receive confirmation messages from SŽ (both message receipts and processing results messages).

Examples of the TAF Train Composition and Train Ready messages are attached to this Request.

These messages are generated by the source application PRIS as TAF messages so the CI does not need to make any translation of format.

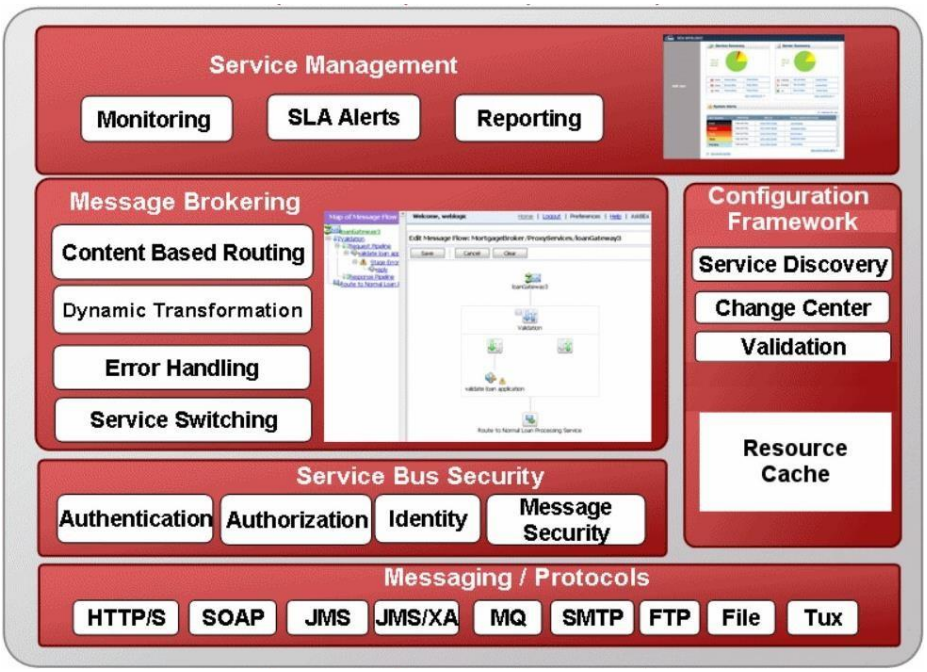
PRIS is the main production system od CDC, where all transported wagons are registered and all train consists are captured.

OSB description

Both ČDC and ČD uses the Oracle service bus (OSB) for communication between its own systems. Both ČDC and ČD also use OSB to communicate with other companies' systems. ČDC and ČD currently operate dozens of integrations on this platform.

OSB is an enterprise integration platform that provides a number of functionalities in the field of Service management, Security, Message brokering, many types of messages and protocols. The functionalities required in a. - g. Are described in the documentation for the specified url.

https://docs.oracle.com/cd/E14571_01/doc.1111/e15020/architecture_overview.htm#OSBCA140

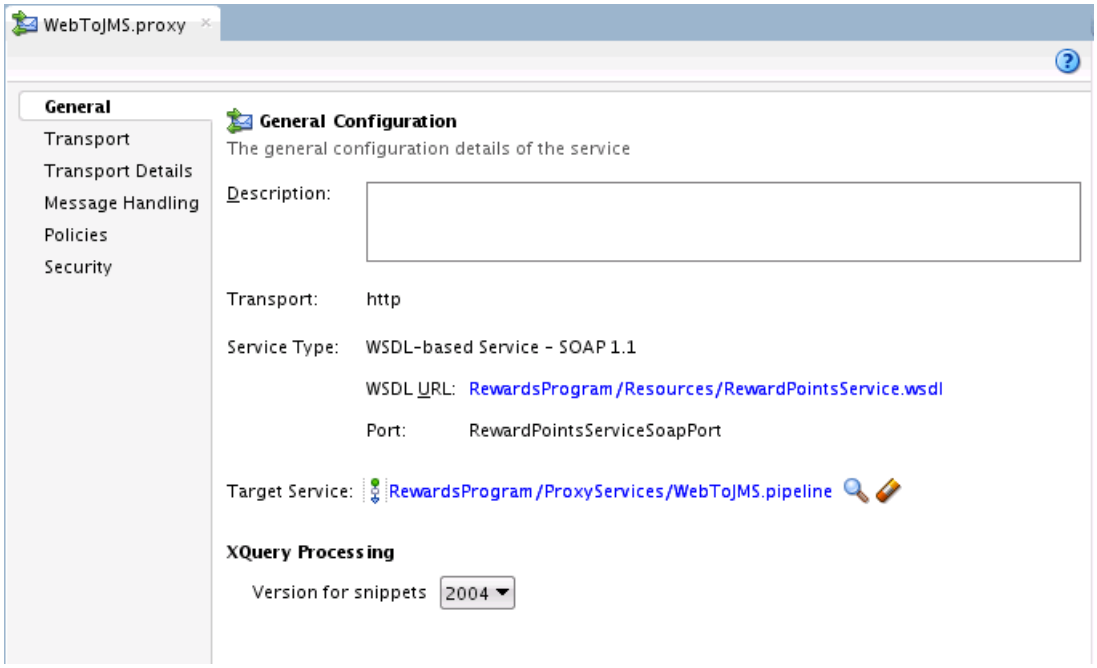


Picture 1 Oracle service bus architecture

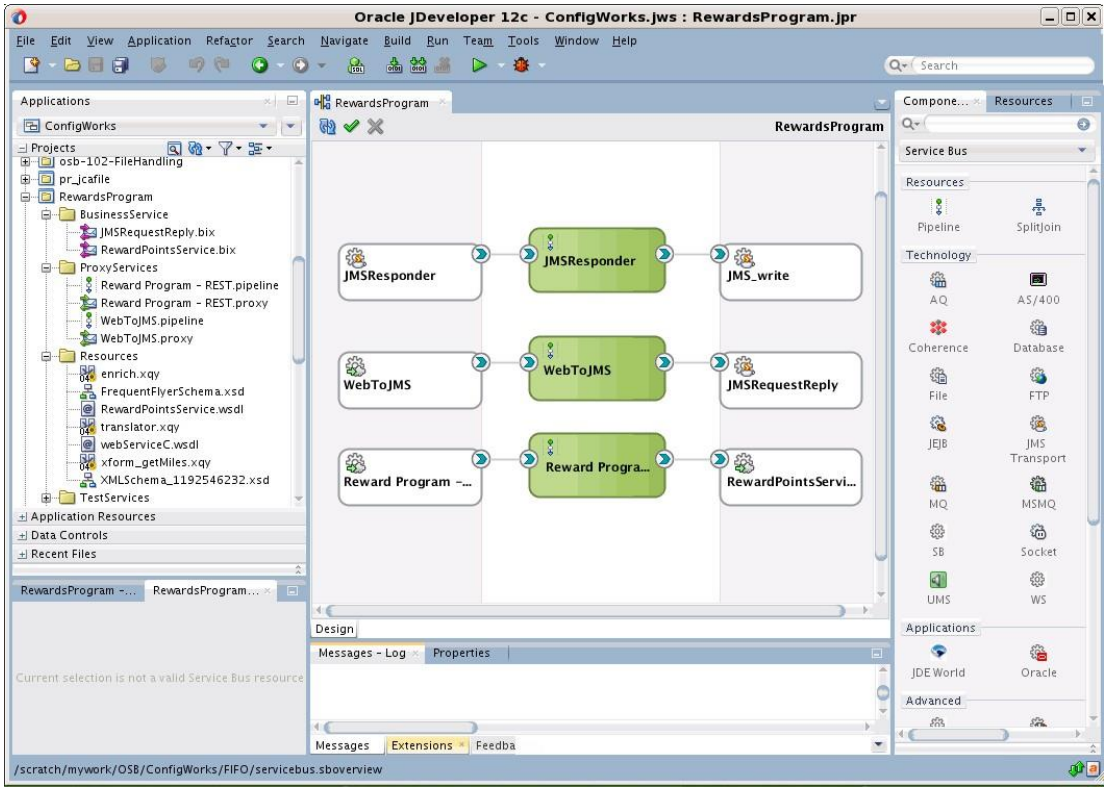
All integrations (including TAF messages) are implemented in the Configuration Framework, which is part of the OSB.

The OSB integration platform is in principle intended for the implementation of communica tion between business services as well as between different communication platforms.

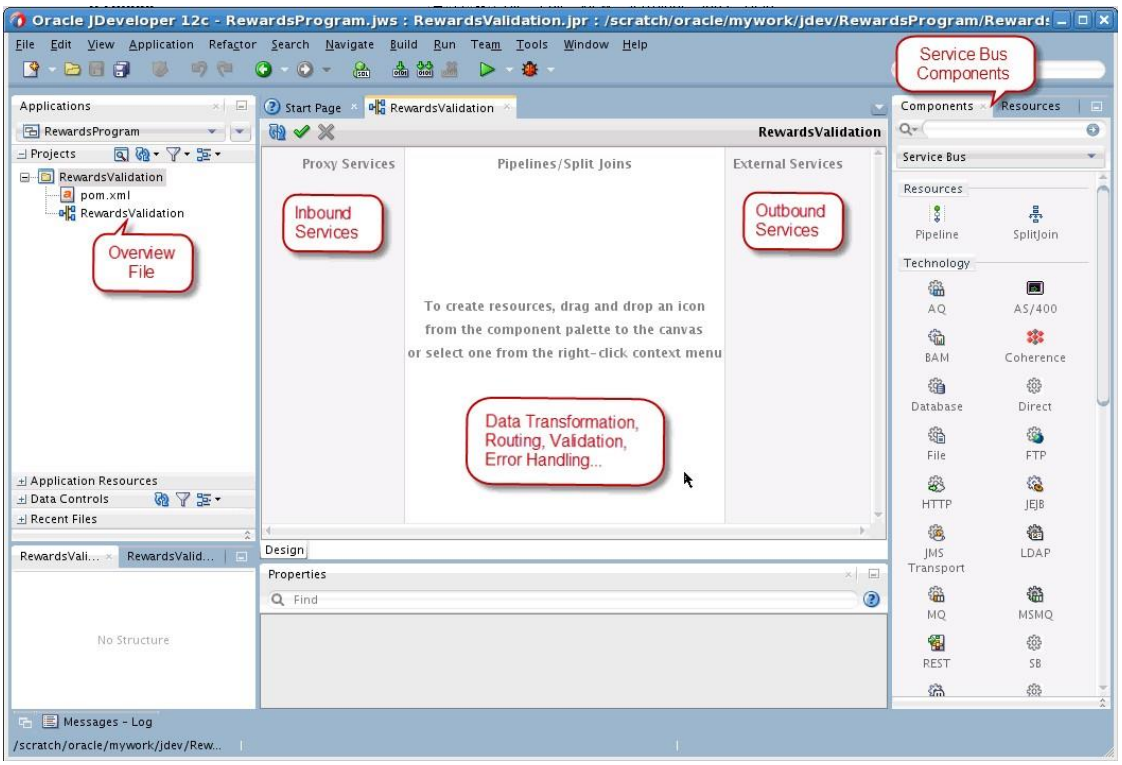
Below are some printscreen development environments for implementing integrations.



Picture 2 Proxy Service Definition Editor in JDeveloper



Picture 3 Oracle Service Bus in JDeveloper



Picture 4 Service Bus Overview Editor

ČD-Informační systémy already operates several OSB instances within the holding. In ČD cargo, TAF already uses messages integrated via OSB for communication between its own systems or for communication with systems of Infrastructure Manager (IM). As an example, we enclose the TAF Train composition message and Train ready message.

EU Funding used

EU funding (through Czech state Ministry of Transport funding program „Operational Programme Transport, Interoperability in rail transport, part Implementation of telematics subsystem – TSI telematic applications in freight transport“) was used in 2014 for implementation of the TAF functions within ČD Cargo. ČD a.s. did not use any funds for their OSB.

3.1 Train composition message:

<Payload xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:aud="http://xmlns.cdcargo.cz/Services/Common/AuditPS/"
xmlns:core="http://xmlns.cdcargo.cz/Core">

<Body xmlns="http://schemas.xmlsoap.org/soap/envelope/" xmlns:soap-
env="http://schemas.xmlsoap.org/soap/envelope/">

<SendMessageV53Request xmlns="http://xmlns.cdcargo.cz/Services/TRN/DataToCompost/V1"
xmlns:ns6="http://provoz.szdc.cz/compost/schema/v22"
xmlns:ns5="http://provoz.szdc.cz/compost/schema/LocoDriverRunningMessage/v10"
xmlns:ns4="http://xmlns.cdcargo.cz/Services/TRN/DataToCompost/V1"
xmlns:ns3="http://provoz.szdc.cz/compost/schema/v53" xmlns:ns2="http://xmlns.cdcargo.cz/Core">

<DMHeader xmlns="http://xmlns.cdcargo.cz/Core">

<IntegrationID>IS015</IntegrationID>

<IntegrationVer>1.01</IntegrationVer>

<SrcSystem>PRIS</SrcSystem>

<DstSystem>COMPOST</DstSystem>

<Timestamp>2020-10-20T13:31:00.000+02:00</Timestamp>

<CorrelationID>OSB_osb2-prod_20201020133100221_XXX</CorrelationID>

</DMHeader>

<Payload xmlns="">

<CZ_CompostMessage xmlns="http://provoz.szdc.cz/compost/schema/v53">

<User>

<Login>priscompost1</Login>

<Password>**********</Password>

</User>

<TrainCompositionMessage>

<MessageHeader>

<MessageReference>

<MessageType>3003</MessageType>

<MessageTypeVersion>5.3</MessageTypeVersion>

<MessageIdentifier>XX</MessageIdentifier>

<MessageDateTime>2020-10-20T13:30:55.000+02:00</MessageDateTime>

</MessageReference>

<Sender>XX</Sender>

<Recipient>XX</Recipient>

</MessageHeader>

<MessageStatus>2</MessageStatus>

<TransportOperationalIdentifiers>
<ObjectType>TR</ObjectType>
<Company>XX</Company>
<Core>DISCO055617C</Core>
<Variant>00</Variant>
<TimetableYear>2020</TimetableYear>
<StartDate>2020-10-20</StartDate>
</TransportOperationalIdentifiers>
<OperationalTrainNumberIdentifier>
<OperationalTrainNumber>05XX</OperationalTrainNumber>
</OperationalTrainNumberIdentifier>
<OperationalTrainNumber>05XX</OperationalTrainNumber>
<TrainCompositionJourneySection>
<JourneySection>
<JourneySectionOrigin>
<CountryCodeISO>CZ</CountryCodeISO>
<LocationPrimaryCode>XX</LocationPrimaryCode>
</JourneySectionOrigin>
<JourneySectionDestination>
<CountryCodeISO>CZ</CountryCodeISO>
<LocationPrimaryCode>XX</LocationPrimaryCode>
</JourneySectionDestination>
<ResponsibilityActualSection>
<ResponsibleRU>XX</ResponsibleRU>
<ResponsibleIM>XX</ResponsibleIM>
</ResponsibilityActualSection>
<ResponsibilityNextSection>
<ResponsibleRU>XX</ResponsibleRU>
<ResponsibleIM>XX</ResponsibleIM>
</ResponsibilityNextSection>
</JourneySection>
<TrainRunningData>
<TrainRunningTechData>
<TrainType>2</TrainType>
<TrainWeight>172</TrainWeight>
<TrainLength>35</TrainLength>
<TrainMaxSpeed>90</TrainMaxSpeed>
<BrakeType>P</BrakeType>
<NumberOfVehicles>2</NumberOfVehicles>

<NumberOfAxles>8</NumberOfAxles>
</TrainRunningTechData>
<ExceptionalGaugingInd>false</ExceptionalGaugingInd>
<DangerousGoodsIndicator>false</DangerousGoodsIndicator>
<Activities>
<TrainActivityType>0012</TrainActivityType>
<ActivityLocationIdent>
<CountryCodeISO>CZ</CountryCodeISO>
<LocationPrimaryCode>XX</LocationPrimaryCode>
</ActivityLocationIdent>
</Activities>
</TrainRunningData>
<LocoIdent>
<TractionType>91</TractionType>
<LocoTypeNumber>XX</LocoTypeNumber>
<TractionMode>11</TractionMode>
</LocoIdent>
<LocoIdent>
<TractionType>91</TractionType>
<LocoTypeNumber>XX</LocoTypeNumber>
<TractionMode>31</TractionMode>
</LocoIdent>
<LivestockOrPeopleIndicator>0</LivestockOrPeopleIndicator>
</TrainCompositionJourneySection>
</TrainCompositionMessage>
</CZ_CompostMessage>
</Payload>
</SendMessageV53Request>
</Body>
</Payload>

3.2 Train ready message.:

<Payload xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:aud="http://xmlns.cdcargo.cz/Services/Common/AuditPS/"
xmlns:core="http://xmlns.cdcargo.cz/Core">

<Body xmlns="http://schemas.xmlsoap.org/soap/envelope/" xmlns:soap-
env="http://schemas.xmlsoap.org/soap/envelope/">

<SendMessageV53Request xmlns="http://xmlns.cdcargo.cz/Services/TRN/DataToCompost/V1"
xmlns:ns0="http://xmlns.cdcargo.cz/Services/TRN/DataToCompost/V1">

<DMHeader xmlns="http://xmlns.cdcargo.cz/Core">

<IntegrationID>IS016</IntegrationID>

<SrcSystem>DISCOR</SrcSystem>

<DstSystem/>

<Timestamp>2020-10-20T12:56:00</Timestamp>

<CorrelationID>OSB_osb1-prod_20201020125651841_459017535</CorrelationID>

</DMHeader>

<Payload xmlns="">

<CZ_CompostMessage xmlns="http://provoz.szdc.cz/compost/schema/v53"
xmlns:ns1="http://provoz.szdc.cz/compost/schema/v53">

<User>

<Login>discor1</Login>

<Password>**********</Password>

</User>

<TrainReadyMessage>

<MessageHeader>

<MessageReference>

<MessageType>3006</MessageType>

<MessageTypeVersion>5.3</MessageTypeVersion>

<MessageIdentifier>0a5e5b2d-a583-XX-312bc0204f67</MessageIdentifier>

<MessageDateTime>2020-10-20T12:56:50+02:00</MessageDateTime>

</MessageReference>

<SenderReference>0a5e5b2d-a583-4500-XX</SenderReference>

<Sender>2154</Sender>

<Recipient>0054</Recipient>

</MessageHeader>

<MessageStatus>2</MessageStatus>

<TransportOperationalIdentifiers>

<ObjectType>TR</ObjectType>

<Company>XX</Company>

<Core> --- 0061032A</Core>

<Variant>00</Variant>
<TimetableYear>2020</TimetableYear>
<StartDate>2020-10-20</StartDate>
</TransportOperationalIdentifiers>
<OperationalTrainNumberIdentifier>
<OperationalTrainNumber>XX</OperationalTrainNumber>
</OperationalTrainNumberIdentifier>
<ResponsibleRU>XX</ResponsibleRU>
<TrainContactDetails>GSM-R; TRS; TESLA; +XX</TrainContactDetails>
<TrainLocation>
<CountryCodeISO>CZ</CountryCodeISO>
<LocationPrimaryCode>35575</LocationPrimaryCode>
<PrimaryLocationName>Otrokovice</PrimaryLocationName>
</TrainLocation>
<TrainReadyStatus>
<TrainReady>1</TrainReady>
</TrainReadyStatus>
<TrainStartTime>2020-10-20T12:56:50+02:00</TrainStartTime>
<TrainReadyTime>2020-10-20T12:56:50+02:00</TrainReadyTime>
</TrainReadyMessage>
</CZ_CompostMessage>
</Payload>
</SendMessageV53Request>
</Body>
</Payload>