D3.4

FENIX Integration & Verification

Deployment of FENIX infrastructure in Pilots and validation report V1.0

Version number:	0.9
Main authors:	T-Systems, ATOS, PTV
Dissemination level:	PU
Lead contractor:	ATOS
Due date:	31/08/2021
Delivery date:	31/08/2021
Delivery date updated document:	31/03/2022

Co-financed by the European Union
Connecting Europe Facility

CONTROL SHEET

Version history			
Version	**Date**	**Main author**	**Summary of changes**
0.1	01/02/2021	T-Systems	D3.4 First version
0.2	08/02/2021	T-Systems	First revision
0.3	10/02/2021	all	Partner Contributions
0.4	25/03/2021	T-Systems	Revision
0.51	01/04/2021	T-Systems	Final Pre-Deployment version
0.6	20/04/2021	all	Glossary of terms
0.7	16/07/2021	ATOS	Update
0.8	17/08/2021	T-Systems	Version for core team review
0.9	20/08/2021	T-Systems	Version for peer review
1.0	30/08/2021	T-Systems	Review Comments
1.1			

	Name		**Date**
Prepared	T-Systems	Ralf Grigutsch	23/08/2021
Reviewed	ERTICO	Peter Schmitting	27/08/2021
Authorised	FENIX Consortium	-	

Circulation			
Recipient	**Date of submission**		
Project partners			**17.08.2021**
FENIX Management Committee			**22.08.2021**
INEA			**30.08.2021**

Deliverable is public?

TABLE OF CONTENT

FIGURES

TABLES

LIST OF ABBREVIATIONS & ACRONYMS

Act.	Activity
API	Application Program Interface
CA	Certification Authority
CEF	Connecting Europe Facility
DG MOVE	Directorate-General Mobility Transport, MOVE
DMZ	Demilitarized Zone
DTLF	Digital Transport and Logistic Forum
DXC	Data Exchange
EC	European Commission
EDI	Electronic Data Interchange
ETA	Estimated Time of Arrival
EU	European Union
FENIX	A European FEderated Network of Information eXchange in Logistics
GA	Grant Agreement
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IDM	Identity Management
IDM	Identification Module
IDS	Industrial Data Spaces
INEA	Innovation and Networks Executive Agency
iPaaS	Integration Platform as a Service
ISO	International Organization for Standardization

IT	Information Technology
ITS	Intelligent Transport Systems
JSON	JavaScript Object Notation
kb	kilobyte
PS	Pilot Site
Q&A	Questions and Answers
REST	Representational State Transfer
secs	Seconds
SELIS	Shared European Logistics Intelligent Information Space
SLA	Service Level Agreement
SME	Small and Medium-Sized Enterprise
TEN-T	Trans-European Transport Network
TEN-Tec	Trans-European Transport Network
TLS	Transport Layer Security
TMS	Transport Management System
TSI	T-Systems International GmbH
UC	Use Case
URL	Unified Resource Locator
XML	eXtensible Markup Language

Table 1: Abbreviations & Acronyms

1. INTRODUCTION

1.1 Purpose of the document

The present document provides the approach and the performance on sub-activity 3.4 during the related project phases of FENIX. Based on the committed overall methodology the document summarizes the technical and organizational background of sub-activity 3.4.

Contractual references are followed by the objectives, milestones and the relations to other project activities or deliverables. The FENIX architecture and relevant roles are leading to the methodology of sub-activity 3.4. The methodology itself covers the project phases of pre-deployment, deployment and operation (V1.1 of the deliverable) concerning the FENIX infrastructure and how supporting, monitoring and reporting of the activities of the Pilots Sites has been setup. Finally, a so-called support journal will document all relevant information and actions defined, analyzed and processed until end of the project lifetime. This document will finally be available in two versions, V1.0 corresponding to milestone 'end of Pilot site deployment of the FENIX infrastructure' and V1.1 corresponding to the 'end of the project' milestone.

Commented [PS1]: Milestones with these names do not exist. Specify which milestone (with number) is targeted.

1.2 Contractual references

FENIX stands for "A European FEderated Network of Information eXchange in Logistics". FENIX is an action 2018-EU-TM-0077-S under the Grant Agreement number INEA/CEF/TRAN/M2018/1793401 and the project duration is 35 months, effective from 01 April 2019 until 31 March 2022. It is a contract with the Innovation and Networks Executive Agency (INEA) under the powers delegated by the European Commission.

Communication details of the Agency:

Any communication addressed to the Agency by post or e-mail shall be sent to the following address:

Innovation and Networks Executive Agency (INEA)

Department C – Connecting Europe Facility (CEF)

Unit C2 Transport

B - 1049 Brussels

Fax:+32 (0)2 297 37 27

E-mail addresses:

General communication: inea@ec.europa.eu

For submission of requests for payment, reports (except ASRs) and financial statements: INEA-C2@ec.europa.eu

Any communication addressed to the Agency by registered mail, courier service or hand-delivery shall be sent to the following address:

Innovation and Networks Executive Agency (INEA)
Avenue du Bourget, 1
B-1140 Brussels (Evere)
Belgium

TEN-Tec shall be accessed via the following URL:
https://webgate.ec.europa.eu/tentec/

Any communication details of the beneficiaries

Any communication from the Agency to the beneficiaries shall be sent to the following addresses:
For European Road Transport Telematics Implementation Coordination Organisation – Intelligent Transport Systems & Services Europe:
Eusebiu Catana
Senior Project Manager
Avenue Louise 326, 1050 Brussels
E-mail address: e.catana @mail.ertico.com

1.3 Objectives, Milestones and Relations

The Grant Agreement (GA) and the description of work for the FENIX project define the following background of sub-activity 3.4 (see chapter 1.2).

Overall, this sub-activity is related to the

- Integration of action's infrastructure in Pilot Sites
- Pre-deployment and deployment
- Application of verification processes defined in Activity 2

Commented [PS2]: ?

Derived from these, the objectives and tasks for the sub-activity are defined as:

- Support the deployment of the FENIX infrastructure in the Pilot Sites (PS)
- Monitor and analyze the verification processes of the PS to perform refinements

To clarify the above objectives, keywords and terminology need to be analyzed to set them into relation to other activities in the project, and to define the following determinations:

- The process of checking software is divided into;
  - Verification: The process of determining the conformity of the software product with its specification. -> Act 3
  - Validation: The process of accepting a software product. -> Act 5
- Test & Verification to be done by the federated platforms themselves.
- Detailed information, requirements and the planned setup of the PS are defined in Activity 2.
- The verification aspects of federated platforms and the FENIX Connector are defined in deliverable D2.5 and are part of the certification process of the FENIX facilitator.
- The technical specification given by Activity 3 is defined in deliverable D3.2 for the so-called FENIX Infrastructure. Therefore, the objects to be monitored and supported by task 3.4 are the components defined in D3.2; FENIX Connector and the logging process.

Commented [PS3]: Is this what you want to say?

- The relevant phases of task 3.4 are:
  - Pre-deployment (began before the start date of task 3.4),
  - Deployment (see milestones 33, 35 and 36) of the FENIX infrastructure and
  - Operation of the FENIX infrastructure (see milestone 34)

    see also Table 3: Task 3.4 reporting phases.

Commented [PS4]: "task" or "Task". Use consistently. Same for A(a)ctivity etc.

- FENIX Activity 4 covers the effort of the PS and their technical setup on federated platforms and use cases (Integration of Action Infrastructure in Pilot Sites).

- The support of the pre-deployment and deployment until milestone 33 in the Pilot Sites is defined as technical consultancy, answering questions and organizing workshops with the technical staff of the federated platforms of the PS.
- For online workshops or interactive consultancy, the timeslot of 09:00 to 12:00 CET on Friday is foreseen (this slot is defined by the overall project methodology as reserved for interactive project web meetings) – alignment with other FENIX activities is assumed.
- These workshops and the specified checklists of the relevant topics to verify technical functionality of the FENIX Connector and the logging deployment cover the monitoring task.
- All sub-activity 3.4 actions are not considered active involvement in PS planning, neither implementation actions nor deployment of PS results.

# Milestone	Milestone title	Due date	Related deliverable
33	Pre-deployment and deployment of the FENIX infrastructure: FENIX Connector and Logging	31/08/2021	Deployment of FENIX infrastructure in Pilots and validation report V1.0
34	Deployment of the FENIX infrastructure overall: Operation of the FENIX Connector at the platforms (01/09/2021 – 31/03/2022)	31/03/2022	Deployment of FENIX infrastructure in Pilots and validation report V1.1
35	Monitor validation process	31/08/2021	Deployment of FENIX infrastructure in Pilots and validation report V1.0
36	Perform refinements	31/03/2022	Deployment of FENIX infrastructure in Pilots and validation report V1.1

Table 2: Milestones Sub-activity 3.4

- Concerning the two versions required for this deliverable (V1.0 and V1.1), it is important to note that chapter 4 'SUPPORT & REPORT JOURNAL' documents the different phases under which the FENIX infrastructure is in use at the PS.

Phase	Chapter
Pre-deployment	4.1 Pre-Deployment phase
Deployment	0 Deployment phase
Operation	0 Operational phase

Table 3: Task 3.4 reporting phases

- All relations to the overall relevant activities are listed in the references, check there for the valid versions of D2.3, D2.4, D2.5, D6.1, D3.1, and D3.2.

Commented [PS5]: Please phrase a bit clearer e.g. "All relevant deliverables from the FENIX activities are listed in the references section."

2. FENIX architecture & Roles

Within the FENIX project, Activity 3 is in charge of providing a secure framework to share information between the members of the FENIX federation following the governance rules defined by Activity 2. The FENIX Federation has been defined following four main strategic principles:

- All members must constitute a **federation** where every member must follow a set of governance rules for the exchange of data between the members.
- The FENIX federation follows a **decentralized approach** where no central component is deployed. Every certified platform is a node of the federation and keeps its internal control and operation.
- The FENIX federation is composed of different platforms sharing data between each other forming an **ecosystem of data and services**.
- The FENIX federation is an environment of **trustworthiness** between the logistic actors where **Data Sovereignty** is ensured by each actor. Each member is the owner of its data.

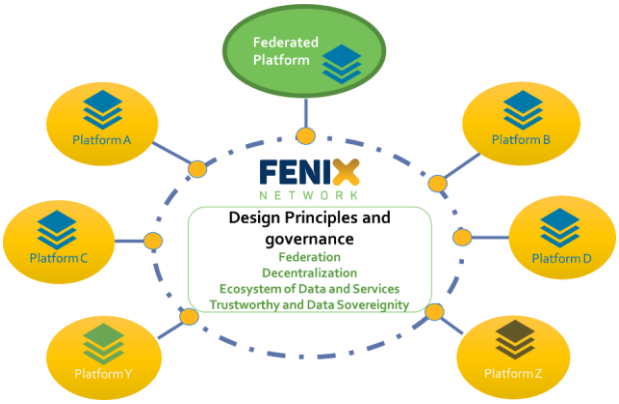


Figure 1: FENIX architecture concept based on design principles

The FENIX Connector was designed after the definition of these four pillars.

The FENIX Connector is the main component through which every member of the FENIX federation can access all the resources available from other members' platforms. Every member that wants to be part of the FENIX federation must deploy its own FENIX Connector to start exchanging data through FENIX.

As explained in D3.2 – FENIX Connector Specification, the FENIX Connector is a software component that must be deployed in every platform that is aiming to exchange data within the FENIX federation. The FENIX Connector has three different modules that need to be deployed:

- Identity Manager; To ensure the identities of the participants of the federation, authentication of identities.
- Data Exchange: To enable data sharing between different FENIX Connectors.
- Broker; To search services of a distributed catalogue of services and data available in each node of the federation.

The structure of the FENIX Connector is shown in Figure 2:

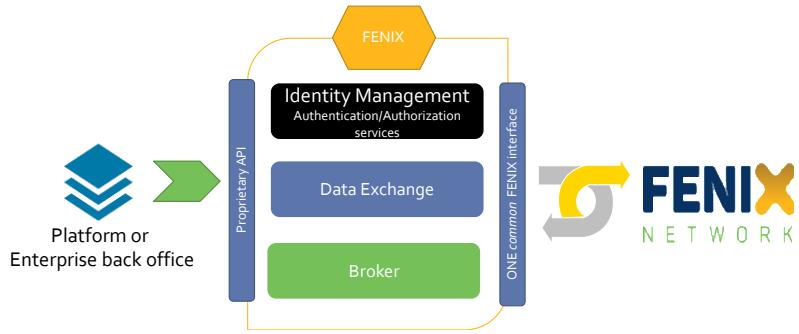


Figure 2: FENIX Connector architecture

During the execution of sub-activity 3.2, a detailed technical specification of the different modules of the FENIX Connector was done. The FENIX Connectors will exchange information between each other, having a machine-to-machine communication and, therefore, several processes need to be identified for each module.

D3.2 identifies the user stories and use cases for two modules. For the Identity Manager it contains definitions for the identification process for a FENIX Connector that wants to access any operation provided by the FENIX Connector itself. It deals with the authorization and authentication framework using OAuth 2.0 standards.

Commented [PS6]: another?

For the Broker, it is specified how the exposition of resources from a member must be done and how other FENIX members can access that information through the Broker capabilities. Finally, different communication patterns are described that can be used to exchange information between two FENIX Connectors using the Data Exchange component.

The document contains comprehensive technical details such as the security mechanisms to be implemented, the message structure to exchange information, the structure of the catalogue of resources, and the description of the API for the different modules.

Finally, the logging concept that must be implemented for the support phase that is taking place under the current sub-activity 3.4 is described.

Due to the agile character of the FENIX Connector specification, all required changes and updates of the specified modules will become part of deliverable D3.4 (see Annex).

Commented [PS7]: Which one? There are several.

3. METHODOLOGY

Due to the very special situation during the Covid-19 pandemic, a revised overall methodology has been discussed and agreed by the project consortium. This methodology is based mainly on online workshops within defined PS groups and online reports by the Federated Platforms of the PS. All relevant information will be added into the present deliverable to a 'support journal', which will document the task T3.4 phases and the related activities.

For the FENIX project, the concept of a support journal started with online workshops in the pre-deployment phase with PS groups. The workshops led to refinements to support the deployment phase and the monitoring process, which are results from the workshops with the PS groups and the reporting from the Federated Platforms. All information was collected and added to the present deliverable as a collection of data, and as a journal of the deployment phase leading to version V1.0 of deliverable D3.4.

The reporting by Federated Platforms during the final operational phase will be collected and added to the deliverable as a collection of data, and as a journal of the deployment phase for version V 1.1 of deliverable D3.4. All activities and actions based on this will be stopped with this final deliverable.

Commented [PS8]: What?

3.1 Pilot Site Groups

As defined in the methodology, the following groups of PS and their federated platforms have been setup and defined to organize the online workshops.

- Group #1: PS Germany (Rhine- Alpine), PS Spain, PS France
- Group #2: PS Italy 1 & PS Italy 2, PS Austria
- Group #3: PS Belgium 1 & PS Belgium 2, PS Slovakia
- Group #4: PS Greece, PS Netherlands

3.2 Online Workshops

During the Pilot Site phases (pre-deployment (until end of March 2021), deployment (until end of August 2021) and operation (until end of the project, planned for end of March 2022)), two 'Online Workshops' for each PS group took place:

- Workshop #1 within the pre-deployment phase in months February and March 2021, and
- Workshop #2 within the deployment phase in months April to beginning of August 2021

In order to reflect the overall objectives and the derived tasks to support the PS, and to monitor the technical verification, the workshops have been structured equally.

The main topics and actions are defined as follows:

- Check platform reporting (see chapter 3.3 Reporting by checklist)
- Check and discuss questions on deliverable D3.2 (based on reports interactively)
- Add agreements, actions and refinements to workshop minutes (all minutes have been added to the chapter 4 (SUPPORT & REPORT JOURNAL)

3.3 Reporting by checklists

During the deployment and the operational phases of the PS activity, all federated platforms within each PS need to report the weekly status by providing information within a defined checklist.

The provided information is used as input for the versions of this deliverable. With relation to the defined milestones of sub-activity 3.4, the checklist topic A is in line with the milestones MS 33, 35 and 36, and the checklist topics B & C with milestone MS 34.

The technical staff of the federated platforms was asked to store the reports on the project SharePoint by the following nomenclature for the file name:

FENIX_year/month/day_Report_PS#_PlatformName.docx

(year = xxxx, month = xx, day = xx)

The structure for storing all relevant information is defined as:

- FENIX
  - Deliverables & Working Documents
    - ACT 3 Technology Integration
      - D3.4
        - D3.4 Pilot Sites Reports
          - Reports
            - (Platform_Name), e.g. AEOLIX
            - etc.

Figure 3: Structure of reports filing

For each Federated Platform, the reports are checked and processed weekly by the T3.4 sub-activity team, where they are used as input for D3.4 V1.0, based on checklist topics A & B, and as input for D3.4 V1.1, based on checklist topic C.

The content of the reports and the checklist topics are structured as shown in the following overview (see also Appendix):

Commented [PS9]: There is no appendix!

Metadata:

Name of platform (mandatory):	
Used by Pilot Site(s) (mandatory): minimum one Pilot Site or more to be listed	
Phase of reporting (mandatory): pre-deployment, deployment, operation (see PS planning)	
Owner of platform (mandatory):	
Date of report (mandatory):	
Free text space for comments on reporting week (optional)	

Table 4: Reporting topics: Meta Data

Content data:

Part A:

This is related to the FENIX infrastructure defined in D3.2 and to be reported during the implementation/deployment phase per each federated platform.

DXC - Status per each phase in %:

Implementation/deployment (mandatory) 0-100%.	
Test (mandatory) 0- 100%.	
Operational (mandatory) 0- 100%.	
Free text space for comment.	
Free text space for question.	

Table 5: Reporting topics: DXC Data

IDM - Status per phase in %:

Implementation/deployment (mandatory) 0-100%.	
Test (mandatory) 0-100%.	

Operational (mandatory) 0- 100%.	
Free text space for comments.	
Free text space for questions.	

Table 6: Reporting topics: IDM Data

BROKER - Status per phase in %:

Implementation/deployment (mandatory) 0-100%.	
Test (mandatory) 0- 100%.	
Operational (mandatory) 0- 100%.	
Free text space for comments.	
Free text space for questions.	
Free text space on status of latest versions of broker lists, e.g. logging extracts	

Table 7: Reporting topics: Broker Data

Logging - Status per phase in %:

Implementation/deployment (mandatory) 0-100%.	
Test (mandatory) 0- 100%.	
Operational (mandatory) 0- 100%.	
Free text space for comments.	
Free text space for questions.	

Table 8: Reporting topics: Logging Data

Part B:

This part of the reporting is related to the verification aspects derived by Activity 2 on governance and the broker catalogue.

Status of certification of the FENIX connector:

Not planned	
Planned in …	
Approved since … until …	
Recertification needed (optional)	
Free text space for questions	

Table 9: Reporting topics: Certification Data

Topics on Broker Catalogue:

How many data services are you currently offering via the Broker catalogue?	
How many other services are you currently offering via the Broker catalogue?	
How often your broker catalogue is updated? Frequency: once, weekly, monthly …	

Table 10: Reporting topics: Broker Catalogue Data

Part C:

This part is related to the technical KPIs defined in deliverable D6.1 FENIX service quality (self-) certification methodologies and it is mandatory to report weekly for each federated platform during the operational phase.

Are logging parameter available (Yes/No)	Yes / No
If yes, fill the table below	If no, provide a comment
Comment (free text space):	

Table 11: Reporting topics: Logging Meta Data

General comments on logging at Pilot level	
Free text space:	
Questions raised during reporting period	
Free text space:	
What is the avg. end - to - end duration for a request response (secs)?	
What is the avg. request size (kb)?	
How many requests were sent (#)?	
What is the avg. response size (kb)?	
How many response messages were generated (#)?	
Which of the following http error codes (400, 401, 403 – 409, 415, 429, 500, 501- 505) are implemented and how often? (e.g. 400 / # of error code)	
Derived # per error code available? yes/no	
Long-run	
Short-run	
What is the peak hour request size (max, avg, min)?	
What is the peak hour request number (#)?	

What is the avg. peak hour response size ?	
How many responses were sent within the peak hour (#)?	
What is the total number of transmissions vs. number of successful transmissions (#)?	

Table 12: Reporting topics: Logging Operational Data

4. SUPPORT & REPORT JOURNAL

The following describes the support & report journal. This is a journal based on single events like workshops with PS or platform owners, bilateral discussions with technical staff and the monitoring by weekly reports (see chapter 4.4).

4.1 Pre-Deployment phase

During the pre-deployment phase of the project and in relation with the final version of D3.2, Workshop #1 took place with the defined PS groups. Furthermore, on-demand bilateral calls with the sub-activity 3.4 core team and single PS were organized to discuss and clarify questions on pre-final versions of D3.2.

Technical WS 02.02.2021

Format: Web Call

Participants: T-Systems. PTV, ATOS, Mondelez

Agenda/Purpose: Questions & Answers see attachment

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
Questions #1 to #21 answered see Annex for Q&A	all	closed	na

Interactive Q&A 02.02.2021

Format: EMail

Participants: ATOS, Indra

Agenda/Purpose: Questions & Answers see attachment

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
Answers provided #23 - #26 see Annex for Q&A	all	closed	-

WS #1 with Group #1: 26.02.2021

PS Germany (Rhine- Alpine), PS Spain, PS France

Format: Web Call

Participants: T-Systems, PTV, ATOS, Poliba, eBos, CERTH/HIT, NeoGIs, Indra, Port of Bilbao

Agenda:

- Short introduction
- Presentation on T3.4 approach
- Future PS/Platforms reporting
- Q&A on D3.2
- Next Steps

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
Action: Provide draft version of D3.4 on ERTICO Sharepoint.	T-Systems	done	-
Action: Provide WS slides on ERTICO Sharepoint.	T-Systems	done	-
Information: No further technical questions discussed today, current available Q&A attached in the draft D3.4 version	T-Systems	done	-
Information: Further information, e.g. 'How to get certificate for project purpose' available on ERTICO SharePoint.	T-Systems	done	09.03.2021

WS #1 with Group #2: 05.03.2021

Group #2 PS Italy 1 & PS Italy 2, PS Austria

Format: Web Call

Participants: T-Systems, PTV, ATOS, Poliba and PS Group 2 partners

Agenda:

- Short introduction
- Presentation on 3.4 approach
- Future PS/Platforms reporting
- Q&A on D3.2
- Next Steps

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
Action: Provide draft version of D3.4 on ERTICO SharePoint.	T-Systems	done	-
Action: Provide WS slides on ERTICO SharePoint.	T-Systems	done	-
Information: No further technical questions discussed today, current available Q&A attached in the draft D3.4 version	T-Systems	done	-
Information: Further information, e.g. 'How to get certificate for project purpose' available on ERTICO SharePoint.	T-Systems	done	09.03.2021

WS #1 with Group #3: 12.03.2021

PS Belgium 1 & PS Belgium 2, PS Slovakia

Format: Web Call

Participants: T-Systems, PTV, ATOS, Poliba and PS Group 3 partners

Agenda:

- Short introduction
- Presentation on 3.4 approach
- Future PS/Platforms reporting
- Q&A on D3.2
- Next Steps

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
Action: Provide draft version of D3.4 on ERTICO SharePoint.	T-Systems	done	
Action: Provide WS slides on ERTICO SharePoint.	T-Systems	done	-

Interactive Q&A: 23.03.2021

Format: EMail

Participants: ATOS, Mondelez

Agenda/Purpose: Questions & Answers see attachment

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
Answers provided see Annex Q&A	Atos	closed	-

WS #1 with Group #4: 26.03.2021

PS Greece & PS Netherlands

Format: Web Call

Participants: T-Systems, PTV, ATOS, Poliba and PS Group 4 partners

Agenda:

- Short introduction
- Presentation on 3.4 approach
- Future PS/Platforms reporting
- Q&A on D3.2
- Next Steps

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
Action: Provide draft version of D3.4 on ERTICO SharePoint.	T-Systems	done	-
Action: Provide WS slides on ERTICO SharePoint.	T-Systems	done	-

4.2 Deployment phase

During the deployment phase of the project and in relation with the final version of D3.2, Workshop #2 took place with the defined PS groups. Furthermore, on-demand bilateral calls with the sub-activity 3.4 core team and single PS were organized to discuss and clarify questions on task 3.4 and D3.2.

Technical WS with PS Belgium 2: 27.05.2021

Format: Web Call

Participants: T-Systems, Procter and Gamble, Logit One

Agenda:

- Separate instructions on reporting, Q&A and refinements of D3.2
-

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
No actions defined	all		

Technical WS with Mondelez: 04.06.2021

Format: Web Call

Participants: T-Systems. PTV, ATOS, Mondelez

Agenda:

- Example of the overall architecture of PS Rhine-Alpine incl. the use of the FENIX Connector
- Overall draft architecture of PS SK incl. the foreseen use of the FENIX Connector
-

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
Action: Federated Platforms: Reports are needed only for platforms who will deploy and run a FENIX Connector within their IT infrastructure. Platforms who will only connected to a Federated platform using different interfaces than the FENIX connector	all		

are not asked to report.			

During the deployment phase of the project until MS 33, 34 and 36, with relation to the final version of D3.2, Workshop #2 took place within the defined PS Groups #1 to #4.

WS #2 with Group #1: 11.06.2021

PS Germany (Rhine-Alpine), PS Spain, PS France

Format: Web Call

Participants: T-Systems, PTV, ATOS, Poliba, eBos, Certh, NeoGls, Indra, Port of Bilbao

Agenda:

- Status of reporting
- Status of Q&A
- Status on derived refinements of D3.2

Minutes:

Topic agreements, actions or refinements	Owner	Status	Next step, until
No topics defined			-

WS #2 with Group #2: 18.06.2021

PS Italy 1 & PS Italy 2, PS Austria

Format: Web Call

Participants: T-Systems, PTV, ATOS, Poliba and PS Group 2 partners

Agenda:

- Status of reporting
- Status of Q&A
- Status on derived refinements of D3.2

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
Action: Federated Platforms: Reports are needed only for platforms who will deploy and run a FENIX	All		-

Connector within their IT infrastructure. Platforms who will only connected to a Federated platform using different interfaces than the FENIX connector are not asked to report.			

WS #2 with Group #3: 01.07.2021

PS Belgium 1 & PS Belgium 2, PS Slovakia

Format: Web Call

Participants: T-Systems, PTV, ATOS, Poliba and PS Group 3 partners

Agenda:

- Status of reporting
- Status of Q&A
- Status on derived refinements of D3.2

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
Action: Federated Platforms: Reports are needed only for platforms who will deploy and run a FENIX Connector within their IT infrastructure. Platforms who will only connected to a Federated platform using different interfaces than the FENIX connector are not asked to report.	All		-

WS #2 with Group #4: 30.06.2021

PS Greece & PS Netherlands

Format: Web Call

Participants: T-Systems, PTV, ATOS, Poliba and PS Group 4 partners

Agenda:

- Status of reporting
- Status of Q&A
- Status on derived refinements of D3.2

Minutes:

Topic Agreements, actions or refinements	Owner	Status	Next step, until
Action: Federated Platforms: Reports are needed only for platforms who will deploy and run a FENIX Connector within their IT infrastructure. Platforms who will only connected to a Federated platform using different interfaces than the FENIX connector are not asked to report.	All		-
NL: 2 Federated platforms (TransFollow, Xynaps)	NL		-
Greece: 2 Federated Platforms (Yellow Pages, HPCS)	GR		-

4.3 Operational phase

This chapter will be edited during the operational phase. All information will be available in version V1.1 of this deliverable.

4.4 Monitoring of reports

The following chapter is a journal of the reports that each federated platform delivers weekly.

- The weekly report is looking for information of last week and should be available for analysis to the support and monitoring team Monday noon of the subsequent week.
- A weekly reminder to PS Platforms is sent by the task team each Friday noon asking for reports until Monday noon.
- The reports should be stored by each federated platform, latest Monday noon, at the ERTICO SharePoint (see chapter 3.3).
- A formal check and an analysis concerning questions is done by the T3.4 team each Monday afternoon.
- Collected questions are added to the Q&A list and distributed to the technical core team for discussion and answers.
- Each identified required refinement with relevance to D3.2 is published and provided as a separate document (see Annex) in relation to the questions in the Q&A excel file.
- A short summary and relevant numbers of each week are available in chapter 5.1.
- All reports of the federated platforms related to the different reporting phases are stored and will be made accessible for the project reviewers on demand only. These reports are not planned to be made public.

Commented [PS10]: I find T3.4 team, sub activity team, core team, etc. Please use only one of those terms.

4.4.1 Federated Platforms

During the pre-deployment and the deployment phase until milestone MS 34, the following federated platforms have finally identified to be relevant for technical support of task 3.4.

During this process, the number of federated platforms increased during the first weeks of reporting. See Table 14: Overview weekly reports.

The requirements for becoming a federated platform within the federation of FENIX are defined by Activity 2 as follows:

- A FENIX federated platform within the eco-system of FENIX needs to pass the certification process to become a certified member of the federation.
- Each FENIX member needs to pass the technical certification for each of its FENIX connector to operate these connectors.
- After the technical certification, the FENIX facilitator will provide the certificate needed to connect to other federated platforms to the FENIX member.
  (For project use, T-Systems will provide the needed certificates.[1])

Name of platform	Used by FENIX project Pilot site(s)	Operator / Platform owner[2]	FENIX Project Partner
AEOLIX	PS France, Greece, Italy, Spain	ATOS	yes
BRUcloud	PS Belgium 1	Procter&Gamble	yes
CARGO2RAIL & DRY PORT GATE	PS Spain	INDRA	yes
CO2Monitoring	PS France	NeoGLS	yes
DIH	PS Rhine-Alpine Germany, PS Austria	T-Systems	yes
eCMR PLATFORM	PS Italy 1	CODOGNOTTO	?
ePuertoBilbao (PCS)	PS Spain	Port of Bilbao	yes
HPCS	PS Greece	PCT	yes

Commented [GR11]: Carlo?

[1] Status Aug. 17th 2021: 11 certificates distributed

[2] During project runtime it is agreed that project partner platforms or linked platforms have passed first certification level by default.

Name of platform	Used by FENIX project Pilot site(s)	Operator / Platform owner[2]	FENIX Project Partner
INTERNATIONAL FEDERATIVE MODULE	PS Italy 1	Circle/Milos	?
Logit One	PS Belgium 2	?	?
Mondelez TMS	PS1 Slovakia	Mondelez	yes
MxP - SmartCitydelleMerci	PS Italy 2	?	?
MYCICERO	PS Italy 1	Pluservice	?
OIA Connect	PS Belgium 2	OAI GLOBAL	?
PCS SINFOMAR	PS Italy 2	PNAEAS and Info.Era	?
SINFOMODAL	PS Italy 1	ALPE ADRIA	?
TM2.0 Service Centre	PS Italy 1	Swarco	yes
Noscifel	PS France	Nosifel	yes
Yellow Pages	PS Greece	CERTH/HIT (on behalf of the Greek MIT)	yes
YOU TRUCK ME	PS Italy 1	Matras	?
Xynaps	PS NL	Pionira	?
Wolf	PS Italy	CROSSTEC SRL	?
Milos Federative Services	PS Italy 2	Circle	?
Mondelez ERP	PS SK	Mondelez	yes
TransFollow	PS NL	VivaServices	?

Table 13: Federated platforms

Commented [GR12]: @All: Please check for operators and status of project partner
Be aware that this list is not consistent what have stated in Act 2 !!!!!!!

4.4.2 Weekly Reports for MS 33, 35, 36

The following table summarizes numbers related to the deployment reporting phase of task 3.4 focusing on identified platforms, available reports, raised question & answers and derived refinements. All reports are available for project internal purpose at the defined SharePoint by ERTICO.

#Week	Number of identified federated platforms	Number of reports accessible	Total number of Q&A (incremental)	Total number of refinements (incremental)
< 14	-	-	38	-
14	5	5	-	-
15	5	5	39	-
16	20	8	44	2
17	23	8	-	-
18	23	11	44	-
19	23	11	47	5
20	23	11	70	11
21	23	10	75	-
22	23	12	78	-
23	25	12	86	12
24	25	8	90	13
25	25	11	-	-
26	25	15	-	-
27	25	15	95	14
28	25	10	-	-
29	25	7	-	-
30	25	7	99	16
31	25	7	108	17
32	25		8	
33[3]	25			
34	25			

Table 14: Overview weekly reports

[3] Week 33 – 34 will be reported within deliverable D3.4 V 1.1

It is obvious that due to several aspects the reporting level was not constant. Reasons were the pandemic situation and the different time planning of the platform owners. However, all workshops, discussions and available reports state a fruitful and useful update on knowledge and edited specification of the FENIX Connector. Finally, all derived refinements will make deliverable D3.2 version 1.3.1 better and more detailed for use by the developers of the federated platforms.

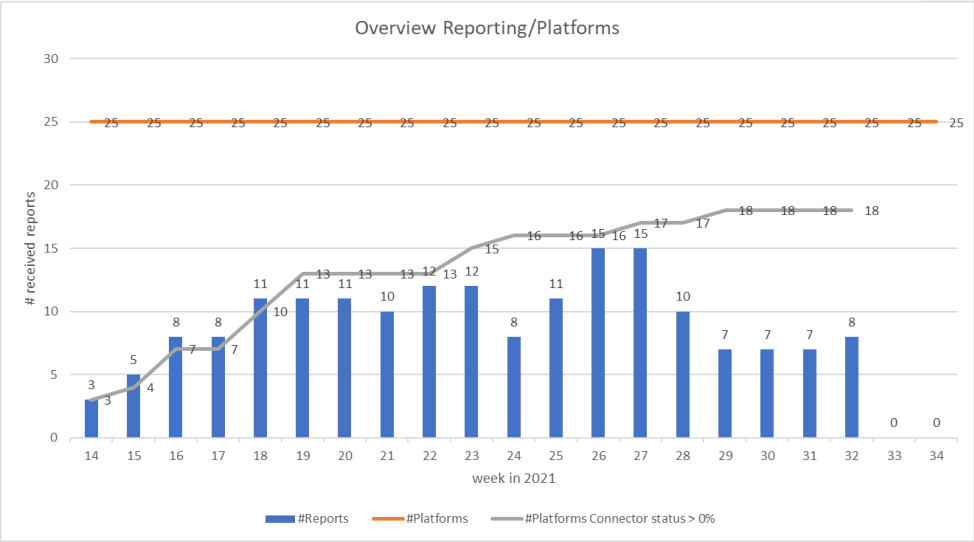


Figure 4: Status by platforms end of week 32

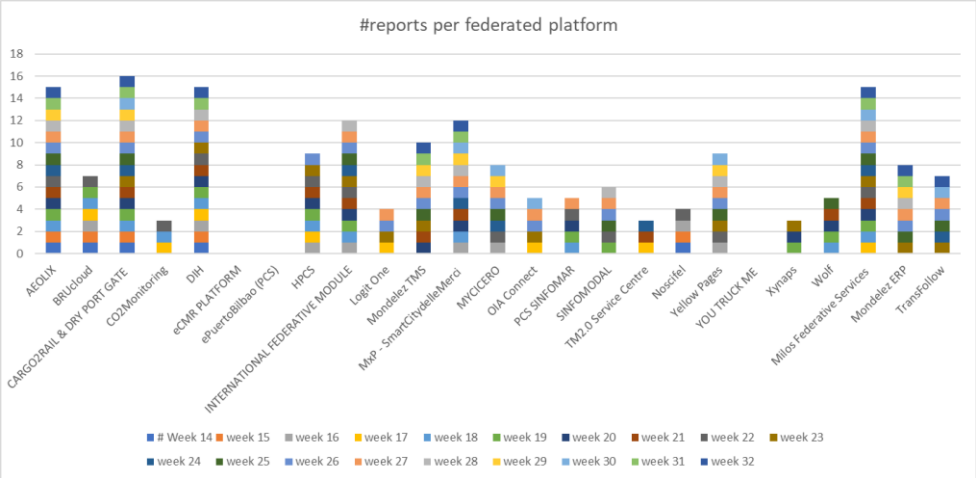


Figure 5: Reports per federated platforms

The following diagram shows the status of FENIX Connector components per federated platform incl. reports of week 32 2021.

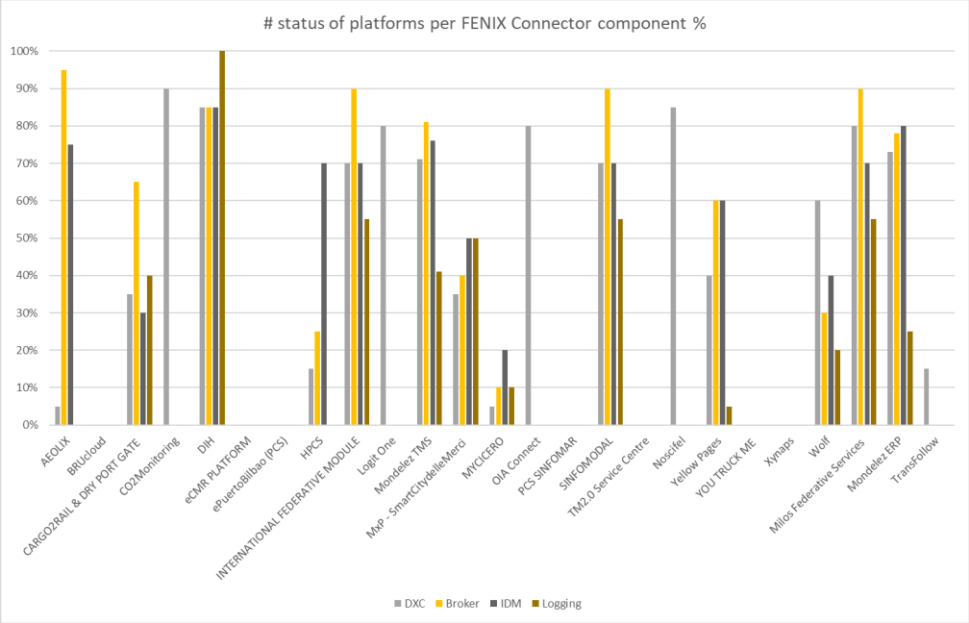


Figure 6: Status of FENIX Connector components until end of week 32

4.4.3 Weekly reports until MS 34

This chapter is related to the operational phase of FENIX and the defined milestone MS 34.

Update of the chapter will become available with version D3.4 V1.1.

Annex

Template Checklist:

D3.4

FENIX Integration & Verification

Weekly Report Pilot Site

Version 1.0 / April. 1st 2021

Co-financed by the European Union
Connecting Europe Facility

Purpose:

During the deployment and the operational phases of the PS all federated platforms within each PS need to report the weekly status by providing information within a defined checklist.

The provided information will be used as input for the two versions of this deliverable. With relation to the defined milestones of Sub-activity 3.4 the checklist topic A is in line with the milestones MS 33, 35, 36 and the checklist topics of B & C with milestone MS 34.

The technical staff of the federated platforms is asked to store the reports on the project SharePoint of FENIX by the following nomenclature for the file name:

FENIX_year/month/day_Report_PS#_PlatformName.docx

(year = xxxx, month = xx, day = xx)

The structure for storing all relevant information is defined as:

- FENIX
  - Deliverables & Working Documents
    - ACT 3 Technology Integration
      - D3.4
        - D3.4 Pilot Sites Reports
          - Reports
            - PS 1 xx (PS_Name)
            - PS 2 xx
            - etc.

Figure: Structure of reports filing

Platform Data:

Name of platform (mandatory):	
Used by Pilot Site(s) (mandatory): *e.g. PS 3 Belgium 1*	PS
Current phase of reporting (mandatory): pre-deployment, deployment, operation *e.g.: PD, D or O*	PD
Operator of platform (mandatory): *e.g. Company name*	
Date of report (mandatory): *MM/DD/YYYY*	dd/mm/yyyy
Free text space for comments on reporting week *(optional)*	

Status Implementation (Mandatory during deployment phase):

DXC - Status in %:

Implementation/deployment (mandatory) 0- 100%:	0
Test (mandatory) 0- 100%:	0
Operational (mandatory) 0- 100%:	0
Free text space for comments:	
Free text space for questions:	

IDM - Status in %:

Implementation/deployment (mandatory) 0- 100%:	0
Test (mandatory) 0- 100%:	0
Operational (mandatory) 0- 100%:	0
Free text space for comments:	
Free text space for questions:	

BROKER - Status in %:

Implementation/deployment (mandatory) 0- 100%:	0
Test (mandatory) 0- 100%:	0
Operational (mandatory) 0- 100%:	0
Free text space for comments	
Free text space for questions	
Free text space on status of latest versions of broker lists, e.g. logging extracts:	

Logging - Status in %:

Implementation/deployment (mandatory) 0- 100%:	0
Test (mandatory) 0- 100%:	0
Operational (mandatory) 0- 100%:	0
Free text space for comments:	
Free text space for questions:	

Status Governance (mandatory during operational phase)

Status of certification of the FENIX connector:

Not planned	
Planned in …	
Approved since … until …	
Recertification needed (optional)	
Free text space for questions:	

Topics on Broker Catalogue:

How many data services are you currently offering via the Broker catalogue?	
How many other services are you currently offering via the Broker catalogue?	
How often your broker catalogue is updated. Frequency: once, weekly, monthly …	

Status Operation (mandatory during operational phase):

Technical KPIs defined in D6.1, (for operational phase mandatory, others optional)

Are logging parameter available (Yes/No)	Yes / No
If yes, fill the table below	If no, provide a comment
Comment (free text space):	

General comments on logging at Pilot level	
Free text space:	
Questions raised during reporting period	
Free text space:	
What is the avg. end - to - end duration for a request response (secs)?	
What is the avg. request size (kb)?	
How many requests were sent? (#)	
What is the avg. response size (kb)?	
How many response messages were generated (#)	
Which of the following http error codes (400, 401, 403 – 409, 415, 429, 500, 501- 505) are implemented and how often? (e.g. 400 / # of error code)	
Derived # per error code available? yes/no	
Long-run	
Short-run	
What is the peak hour request size (max, avg, min)?	
What is the peak hour request number?	
What is the avg. peak hour response size ?	
How many responses were sent within the peak hour? (#)	
What is the total number of sending's vs. number of successful sending's (#)?	

Q&A

#	Question	Answer
1	At MDLZ we are thinking to use any of the Existing iPaaS Vendor to build our connectors and then connect to our back end via secure connection . As it is a iPaaS Solution there will be IP ranges allocated – Can such a platform be registered ?	iPaaS solution can be used, up to you to deploy the connector, API(s) specified in D3.2
2	What kind of Network & Platform isolation expected between two FENIX Member connectors? Ex : should they be on Member's own Cloud subscriptions or In DMZ etc	one platform will get one certificate
3	Resource Catalogue – Please share Technical implementation guidelines of this Module or Service Registry	FENIX BROKER: Metadata data model is defined in D3.2, content will be provided by each platform
4	What is the recommendation for platforms running on TLS 1.2 and lower w.r.t data encryption as the document considers HTTPS implementation using TLS 1.3	TLS 1.3 requested for communication between FENIX connectors, TLS 1.2 use needs to be checked
5	API Endpoints: Documentation of Endpoints is needed: Currently there is only the URL and some basic information given, but more detailed information such as field names etc. is absolutely required. An optimal case would be swagger a documentation, however ATOS mentioned that this will not happen soon. Example: message_id: "Description", String, required	Message fields are explained in subsection 4.6.2. Also related to the different content-types (your connector can support xml/json…)
6	Granting of access to our Platform: How should it be possible for us to evaluate if an access request to our resource should be granted and following also if an access token should be generated? How can we ensure that only the needed and valid suppliers in our system request access or how can we identify if it's really them. --> In my opinion this can't be done automatically for us ATM.	Since you are part of a federation, all the members will be able to ask you for your services. In the description of the service catalogue (in the broker), you can describe them as public or restricted, which would imply to have separated (private) conversations with the requestor party (see subsection 4.4.1)

#	Question	Answer
7	Authentication & access token generation: Is it possible to use bearer tokens for authentication? (and generate an access token afterwards) Is it possible to only use bearer tokens instead of experiencing access tokens and therefore skip the access token generation?	see D3.2 Sec. 4.3 , bearer tokens are access tokens, up to platform
8	Establishing the Certificate chain The document describes that a certificate chain has to get established. However it does not describe what steps need to be done in order to establish the chain. We would need at least some more information on how we have to generate our certificate based on the root certificate from FENIX and how the certificate has to get maintained (process in case certificate has to get changed, etc.).	for the FENIX project TSI will provide needed certificates, overall, the question is related to Act. 2/6
9	Version handling of the API's In case there will be new additions or changes on the Fenix API Endpoints, what is the concept to establish them? Do we have to adapt our Endpoints or will there be a new version of the endpoints which we then won't support?	within D3.2 not foreseen during project lifetime to have more than one
10	Please elaborate what kind of Network / Platform integration expected to register on FENIX Federation from a cloud environment ?	see D2.5 for onboarding process
11	Is the FENIX Connector expected to be in DMZ or what kind of Network separation expected between Companies Middleware platform and the FENIX Connector?	The technical set up is up to each platform provider. The only requirement is that the API is reachable from the outside world to other connectors that wants to make use of it.
12	What is the Role of AEOLIX & SELIS Services in the Pilot Testing sites?	Some pilots are using AEOLIX as data sharing platform (Italy, France, Spain). Using FENIX Connector they are FEDERATED platforms.
13	Could you give us a reference Architecture dig that shows hardware / data sharing in the FENIX Federated Network	Act. 3 will NOT provide a reference architecture. Every platform implementing the connector should think on their own architecture because the underlying platforms will be different, and it is up to each vendor to take the decision on how to make their implementation.
14	Governance Model Activity 2 , 2.5 referenced in the Deliverables document need to be shared to understand the details of the Access request	see project sharepoint

#	Question	Answer
	process .	
15	What is the recommendation for platforms running on TLS 1.2 and lower w.r.t data encryption as the document considers HTTPS implementation using TLS 1.3	Your platform can communicate with your connector using TLS 1.2, since you are building the connector. Then, the interface to communicate the FENIX connector with other FENIX connector can be built using TLS 1.3.
16	Please provide reference link or access to the open source IDM (Keycloak) solutions to the FENIX Platform members	www.keycloak.org
17	Certificate Specification: Who is in charge to produce and validate certificate of the Fenix connectors?	In the future the Fenix Facilitator will be responsible for this, for the demonstration purposes of the Fenix project we can provide a root certificate and issue platform certificates
18	Certificate Specification: It is the Fenix project or each Connector can create by itself?	In the future the Fenix Facilitator will be responsible for this, for the demonstration purposes of the Fenix project we can provide a root certificate and issue platform certificates
19	Certificate Specification: The document describes that a certificate chain has to get established. However it does not describe what steps need to be done in order to establish the chain. We would need at least some more information on how we have to generate our certificate based on the root certificate from FENIX and how the certificate has to get maintained (process in case certificate has to get changed, etc.).	see D3.2 p. 44, Is there any information missing?
20	Certificate Specification: Section 4.2 of FENIX D3.2 V1 document talks about Authentication using Oauth using X.509 certificates during message exchange. Will FENIX Governance body act as certification Signing Authority for the certificates?	In the future yes, during the project there will be no governance entity
21	Issue token by local platform • Is it possible to use bearer tokens for authentication? (and generate an access token afterwards) • Is it possible to only use bearer tokens instead of experiencing access tokens and therefore skip the access token generation?	o A Bearer token is a form of an access token, I guess there is a confusion with the OAuth Authorization Code flow. o We plan to use the 'Client Credentials Grant' flow (https://tools.ietf.org/html/rfc6749#section-4.4), which means to present a certificate to get an bearer access token and that's it.
22	One catalogue substitutes another or it's an incremental update?	When updating the Broker catalogue, the whole catalogue must be sent again and replace the existing one

#	Question	Answer
23	Catalogue of resources: How and from whom do we get the catalogue of resources?	Once the connector is deployed and operational, it must ask, through the Broker API, to other connectors to provide their catalogue of resources. API described in section 4.7 of D3.2.
24	Which is the Broker functionality?	Provide a catalogue of resources available in a platform to the other members of the FENIX federation. Also, it provides the access requests to those resources.
25	How do we know when a Member has an update on his/her catalogue?	The Broker works with an hybrid approach in which every certain time (1 day, 1 week, 1 month…) it must ask for other members' catalogue and update it on its local version. Explained in section 4.5.1 of D3.2.
26	Certificates: how to deal with them and who provides them? Is there any CA?	During FENIX there will not be a CA perse. For demo purposes, T-SYSTEMS will provide the root certificate that can be used.
27	The Broker will use a catalogue to be implemented on the data platform at the backend side of the connector?	yes
28	The catalogue will hold concise information about services or data offered by the resource.	Yes, the Broker meta table provides a structured format to list and describe each resource.
29	In figure 21 and 22 for the FenixResourceCatalogue are 14 items mentioned and in figure 27 there are 11 items. o Is the structure of the Catalogue of Resources already final? o Who will manage this structure in case changes are proposed during the implementation of the connector by the pilot sites? o In par. 4.5.2 (GetAccessToResource) is described that parties will first contact each other about using the resource regarding a service or data.	Figure 21 +22 is the resource catalogue. Figure 27 is similar the figure 22 but provides an expanded view for the parameters: data, contact, samples. No changes are planned. Changes, if any must pass the Fenix Federation Governance instance. The current set provides the minimum required information set. You need to request use and or access right first.
30	In par 4.5.3 classification categories as part of the metadata are mentioned. o Will this list be managed by the FENIX community or can categories be freely chosen? o Could categories as "road transport", "rail transport", "transport monitoring", etc. be a valid category?	Classification was done in course of Activity 4. Could be included as other. transport monitoring would perhaps fit to “track & trace”

#	Question	Answer
31	Will the Broker functionality focus on the visibility of resources for services and data? o What is the role of the Broker in the operational situation when resources are used? o The token is the mechanism to control the eligible and valid access to resources?	yes, It will provide a list of services, description and contact information. none, yes.
32	• For the Dutch pilot site I look at the supply chain communications for "door-to-door" transport of goods. o Actors offer transport services and cargo handling services (prepare the moving of goods) o Contracted actors will report about their performance (execute the moving of goods) • For a fully automated data exchange parties need to agree on at least data structures (semantic/syntactic interoperability aspects) which will be part of the message in the payload. o I think there are still many small companies who are limited in deploying sophisticated IT-systems. o For instance in large ports a PCS is deployed as a service platform for terminals behind the PCS. § For such a case there will be a variety of resources (behind the PCS) which may not all be able to connect fully automated. § Do they need to be mentioned anyhow? Par. 4.4.1 § Does a PCS expose all these resources and are expected to handle all the communications? § Is it to be expected that they serve a data hub for the other resources? § Does only the PCS become a FENIX member?	It depends on how the use cases are designed. The PCS can become a FENIX member and then, it will be its responsibility to distribute the data obtained from the federation to the relevant actors. This step would be out of the FENIX scope. The other option is that, if any actor wants to become a FENIX member, they must deploy their own FENIX connector.
33	Building such a connector is certainly possible and already exists for specific use cases within the Nallian platform for connections with other platforms. However, building a connector is always done in the context of a specific use case. The document does not contain specific use cases and assumes that all resources and data available in a platform can be offered by the Fenix connector. Making such a general connector to make all	The specification is built as generic as possible but covering all the needs that may appear in each specific use case. It is not mandatory to make available all the resources of the platforms but the ones that want to be shared. Each Pilot Site must define which are these resources to showcase their specific use cases.

#	Question	Answer
	possible resources and data available is not really realistic. What could be more realistic, however, is to build such a connector according to the specifications in the document, based on some specific use cases where data has to be shared between different platforms in order to solve a specific problem.	
34	Assuming CSV file received during on-boarding (ProcessConnectorCSV) is the full list of all available connectors. When do we get it? Can we make our own CSV for the pilot?	This is part of the governance part of the project (Activity 2.5) and is still pending. The FENIX Facilitator will share this list when a new member passes the on-boarding process of the FENIX federation. We are assuming that this will be a kind of CSV or json file. I guess you can do it and maybe, one day, you would have to adapt it a bit (I don't see a big change here).
35	How often should we refresh the resource catalogue? Will we get updated versions of the CSV file?	The catalogue of resources of every member should not change a lot. We designed the process to work with local versions of the resource catalogue to increase performance avoiding unnecessary network latency. There is not a fixed interval. You can add a parameter there and adjust if necessary.
36	There is passing mention of resource versioning, what is the preferred approach when managing resource consumers who use different versions?	This is on the resource owner side. If they consider they have made an update on their resource, they must increment the version and, therefore, update its catalogue of resources. But I cannot tell you how each provider manages their versioning.
37	" When describing the resource in the FENIX catalogue, it must be also indicated which is the communication pattern that is being used to share this resource" Expectation is to provide pattern of communication – API / EDI in the resource catalogue , meta data definition of the resource catalogue given Fig 27 does not mention about pattern , please clarify	Yes, we are adding an additional field for that. If your connector works using REST, it will not be possible to use a resource which is shared using Pub/Sub, for example. To communicate properly between connectors, both must use the same communication pattern. And this must be indicated in the resource catalogue.
38	Clarification required , MIC code could be generated using any random number generator function or is there any discretion from Federation ? if so please clarify	You can use generate a checksum using MD5 hash. We will add it to the doc
39	DCX: Does it mean "Data Consumer Exchange"?	DCX is the Connector component for the data exchange, = DXC (Typo)

#	Question	Answer
40	D3.2 leaves the content type of a data source open, but wraps everything in JSON. Several common used data formats are rather incompatible to JSON, e.g. csv. How to prevent conversion issues? Would it be better to move any meta information to http headers (e.g. x-message-id: msgid123) and use the HTTP content-type mechanics?	The specification was thought to share information in a form of messages, not files. That's why everything can be sent string field inside the json field original_msg. Regarding the metadata, it was agreed in several meetings to keep it like that also for logging purposes of the message.
41	Every connector should have its own URL, why do we to add the destination connector id in the request, wouldn't that information be redundant?	It can be redundant, but also will help to the logging.
42	MIC TLS already integrates message integrity, why do we need to add it manually? The MIC chapter does not define whether its generated using the whole message or only the original_msg field, that should be clarified to avoid misunderstandings	It is determined in the table describing the fields of the message. Initially, it was defined for non-repudiation of the messages applied to the original_msg field. If the TLS protocol provides de functionality, then maybe we should remove it, since it didn't apply to all the messages.
43	Why is Getting data is done via a POST request?	Since every message must contain the context information, the operation must be a POST.
44	The OAuth2 Bearer token is usually transmitted in the Authorization HTTP Header, why doing it differently?	As far as I know (I could be wrong), the Oauth returns the token in the body too
45	What's the purpose of the sent_at field? Client timestamps cannot be trusted and the server should transmit his timestamp in the Date HTTP header.	see below
46	OAuth2 is a well-defined standard, however D3.2 alters that standard to incorporate the FENIX message format. That requires reimplementation of OAuth Endpoints and is not anticipated.	This was also presented and agreed before the submission of the document: Discussed and agreed to refine the use. Therefore refinement #001 have been provided. see same folder as Q&A.
47	D3.2 only defines a single request to be used when communicating with services. As most service have multiple methods it would a lot of additional effort to project that on a single request. We are proposing more flexible approach, described in new FENIX_Connector_Specification_Refinement_Services_v0.1.docx	Sounds good. There can be calls for services that don't have a fixed URL. In any case, this information about how to consume the services must be properly shown in the documentation that the broker retrieves with regard to service. Document amended with the suggested changes

#	Question	Answer
48	We need to distinguish between services and data sources in the Catalogue of resources. It is needed to add an additional field in the Broker catalogue. It can be named, for example, resource_type, and can get the values: DataSource or Service. It is needed to use the DXC endpoints.	It is needed to modify the Broker section and images. Also add this field to the FENIX message table description.
49	In the resource catalogue, it will be very useful to add the Company providing the resource. Now it is foreseen to have the imprint, but it is very difficult to access and extract automatically this information.	Images sent by PTV. ATOS to add them the new refinement and modify the table with the new parameter.
50	The D3.2 document states that the primary focus of the FENIX connector is a M2M communication. As such the use of the OAuth2.0 Client Credentials grant is proposed as the flow to obtain access tokens from the Connector IDM. This implies that the Connector IDM will need to maintain and issue client credentials for the other FENIX Connector that want to request an access token. Wouldn't it be better to implement the OAuth 2.0 Mutual-TLS Client Authentication flow (https://datatracker.ietf.org/doc/html/rfc8705)? This would mean that the connectors can use their certificates instead of Client Credentials to authenticate	Exactly, MTLS based OAuth authentication has advantages with regard to M2M communication. Although not mentioned in chapter 4.3.1.1, use of MTLS OAuth is explicitly recommend on p. 22 (UC-001) and p. 45 (Security) with FENIX certificates. Use of these mechanisms for authentication can be decided based on intended use of connector.
51	Most of the flows are driven by a specific user of the platform such as UserA , UserB etc. Fenix Connector is not responsible to hold any details of the platform user Identity nor authenticate them? Please confirm	That's right. A FENIX Connector is only responsible of authenticating Connectors.
52	Need detail on Use case by Use case what are the different Data source & Services required in each Connector such as MDLZ TMS , 3PL etc?	Data Source is any piece of information that you want to share with other platform. e.g., Cargo information, container info, etc. Service is any IT service that you are using or offering. E.g., PTV provides an ETA service to be used. You provide location information (among other) and you get the ETA

#	Question	Answer
53	The FENIX message in Figure39 is not a valid Json structure : "resource_type" :["dataSource" :{ "ds_id" : "Ds ID", "ds_name": "Ds Name" } "status" :["Registered","Denied"]], "mic" : "mic" where as in Acess Response example,the data is a Json object { "context": { "message_id":”35236574”, "conn_origin_id":”006”, "conn_dest_id":”001”, "usr_origin":"user@destination.com", "usr_dest":"javier.garcia@atos.net", "sent_at":"Thursday 14-Jan-21 12:15:34 UTC”, "msg_type":"resource_grant_response", "resource_type":{ "service": { "srvc_id":”006_ES123456_37ab3198c8331654”, "srvc_name":"Service Name" } } }, "mic":“437295827052375465349813560956358”, "original_msg":{ "msg_standard":"” “standard_used_by_the_service”", "msg_body":"response with the access granted or not (coming from the platform)." } }	The image only shows all the possible values that the fields can get. The table below explains in detail how the fields must be used, the parameters and in which operations are mandatory or not.

#	Question	Answer
54	When the resource owner grants access to the resource requested by data user. How long is this access valid? F-US-003 & F-US-004. The resource access grant also will get expired if token expired?	Once you give access to the resource, you should be able to reject it whenever you want. A separate thing is, if you need to provide an expiration token for usage, then it is up to you to choose how long does it take. The one consuming the resource would have to refresh the token or not, but the access grant would remain until the resource owner rejects the access grant
55	UC-002 – Authenticate Access Token steps are not very clear. Need further clarification. Page 22 & Page 48 page no. 24, Is UC-002 mainly talks about Authenticating Access Token Request and not Access Token generated by target IDM. Can we this be corrected in the specification since it is leading to confusion In page no. 24, under Steps section, "Finally, if required, the access token will be checked for user authorization towards the resident IDM." Are we considering the user authorization with resident IDM? If so, what will be the endpoints used to connect with resident IDM for user authorization?	yes, will be revised
56	As per Oauth 2.0 standards, each IDM endpoint had a defined request/response parameters. In that case sample request provided in Page 84 does not hold good.(https://tools.ietf.org/html/rfc6749#section-4.4.1)	This question has already been asked (and answered) in #46.
57	In resource access request the resource_id and user_id are of target or origin?	no
58	In resource access response the resource_id is of target or origin?	When you request access to a resource, you have the ID. When you give this access, the resource_id is the same resource_id. Is to be able to track the request and the response on the grants for a resource. E.g., We are granting access to the resource with the ID that you asked for.

#	Question	Answer
59	What does getPlatformEndpoint method(Broker access request and access response) do?	This method must get the FENIX Connector destination URL. Without the URL of the connector at destination, you will not be able to request anything. For demo purposes, each connector will manage a file with all the available FENIX Connectors in the Federation, containing an ID, and the URL where they are deployed.
60	what information does the BrokerMetaData contain?	The chapter 4.5.3 contains a more detailed description of the different parameters
61	Why does the accessResponse i.e Fenix Message has mic and original_msg section? { "context":{ "message_id":”35236574”, "conn_origin_id":”006”, "conn_dest_id":”001”, "usr_origin":"user@destination.com", "usr_dest":"javier.garcia@atos.net", "sent_at":"Thursday 14-Jan-21 12:15:34 UTC”, "msg_type":"resource_grant_response", "resource_type":{ "service":{ "srvc_id":”006_ES123456_37ab3198c8331654”, "srvc_name":"Service Name" } } }, "mic":“437295827052375465349813560956358”, "original_msg":{ "msg_standard":"” “standard_used_by_the_service”", "msg_body":"response with the access granted or not (coming from the platform)." } }	MIC will be removed from all the messages. An update on the specification will come with these changes
62	What are possible Values of each field in the Fenix Catalgoue?What is eta in tags? - Section catalogue/find	eta => "Estimated Time of Arrival". eta is used as example of a possible tag. The service provider assigns TAGs as search values for the service
63	What is the sigificance of ownOrAll= true/false - Section 4.4.2.2. GetBrokerMetaData	The parameter "ownOrAll" is mentioned in an older version of the document. Please refer to 4.4.2.2 in the latest version of the document
64	What is the difference between Classification and classifications in FenixMetaBroker? (Figure 22)	This picture wrong and will be replaced soon. "classifications" is not a valid parameter.
65	Will platform details(Ex: INET or ERP) be a part of processConnector CSV For example Platform destination Endpoint?	The parameter "shortDescription" is a possible place for such details.

#	Question	Answer
66	How do we get the Message_Id mentioned in Fenixmessage? Is it sequentially generated value of a table?	The message_id needs to be a UUID and should be generated by the sender of the message.
67	How does the getPayload() method mentioned in Request Access and Access Response sequence diagram will get the Fenixmessage when the Fenixmessage is not passed a part of requestAccess and sendGrantsAccess method?(Broker sections Request Access and Response diagram)	Every operation must have the FENIX message except the ones related to the IDM, which are related to oauth (see last amendment of the specification). The getPayload is to retreive the original_msg field. If this field is not in the FENIX message, then it does not apply.
68	What is FenixData and what does it contain and will this Data be a part of ConnectorCSV file?(Figure 27)	Not part of the csv file. It contains a description of the provided service data, e.g. weather, ETA etc..
69	Page no: 48 and figure 17. From the sequence diagram, we can see a request from Service B goes to IDM B for getting signing key. Is the flow correct? From the rest of the document all the communications with IDM happens within the FENIX connector components. So, this type of requesting signingkey and verifying the token generated by FENIX Connector's IDM by Platform and its service is valid?	Referred sequence shows the procedure to get the signing key of platform B's IDM to verify the access tokens. In general, we do not use FENIX data format to communicate with the IDM, instead we stick to OAuth 2.0 standard (see answer 67). So, it is right, that Service B communicates with IDM B without any connector.
70	Access Token Lifetime -> Do we have any recommendation? Ideally token lifetime bydefault is set to 1 hour but its configurable & can be changed.	Lifetime of access token is not specified in FENIX Connector and may vary. 1 hour (as recommend in RFC 6479) can be a good starting point. In scenarios with higher security requirements can be reduced. Also depends on the intended use of the token. JWT claims offer an opportunity to contain fine granular access rights, especially when there is an option to revoke then shorter token lifetimes might be anticipated.
71	The documentation mentions different types of Tokens (Access Token, User Token, possibly other). Please explain how each of them are used.	User Token is a misleading terminology, in Fenix there is no such “user”, communication happens on technical (machine) level between services. This point is already addressed for the next refinement of D3.2.

#	Question	Answer
72	The documentation mentions different types of Certificates (Service Certificate, Connector Certificate, possibly other): Please explain how each of them are used.	There are three types of certificates: a. Fenix Root Certificate à Fenix CA certificate for verification of the others, is used to create connector certificates b. Connector Certificate à issued for every connector, should be used to create service certificates by the connector maintainer. Can be used for authorization between connectors e.g. for retrieving a broker catalogue c. Service Certificate à main authentication/authorization certificate which should be used to retrieve access tokens for data communication
73	1. See https://datatracker.ietf.org/doc/html/rfc6749#section-4.4, listing following key parameters: § Access Token Request: • Grant-type = "password" • Username • Password § Access Token Response: • Access_token 2. See https://auth0.com/blog/using-m2m-authorization/, listing following key parameters: § Access Token Request: • Grant-type = "client_credentials" • Client_id • Client_secret § Access Token Response: • Access_token 3. The spec (FENIX D3.2_v1.3.1.pdf) on pages 88+, listing following key parameters, does not prescribe the use of such a 'secret': § Access Token Request: • Message_id • Conn_origin_id • Conn_dest_id § Access Token Response: • Access_token 4. The figure 4 (UC-001 'Request Access Token') and figure 5 (UC-002 'Authenticate Access Token') on page 23-25 mention:	Grant-type=password was a mistake and will be replaced by grant-type=client-credentials Client_secret is just needed for a confidential client. Every connection in Fenix is secured by mutual tls (please refer to D3.2 chapter 4.2), therefore public clients without client_secret can be used The Access Token Request has been updated to fit to the oauth standard à e.g. POST https://{connector_url}/idm/protocol/openid-connect/token Content-Type: application/x-www-form-urlencoded grant_type=client_credentials&client_id=fenix-idm Refinement Document for D3.2 containing this changes has been provided here: https://erticobe.sharepoint.com/:w:/r/sites/FENIX/_layouts/15/Doc.aspx?sourcedoc=%7BC683024E-E7C8-4554-9B0E-E5211D78E808%7D&file=FENIX_Connector_Specification_Refinement_v0.1-05052021.docx&action=default&mobileredirect=true

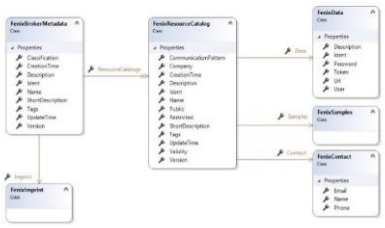
#	Question	Answer
	§ Access Token Request: • Connector certificate • Resource ID • User token § Access Token Response: • Access_token 5. The above seems to be inconsistent, and item (3) in particular seems to be incomplete. 27.5.21: 1. Re. #73: Authentification of client: In case mutual TLS (mTLS) applies, how is this visible in the message specs? Re. #73: As far as I can see, the mentioned inconsistency still applies (re. authentification of client + identification of resource), where can I find consistent updates on A3.2 in the refinement note?	

#	Question	Answer
74	1. Since the client must always hold the client secret, this grant is only meant to be used in trusted clients. In other words, clients that hold the client secret must always be used in places where there is no risk of that secret being misused. 2. The client and his secret will be preconfigured on beforehand within the resource server so that he can be recognized as a trusted client. How does that relate to the Fenix objective of providing a decentralized mechanism where the client can discover – through the resources catalogue – which resources are available? It seems to be that he already has knowledge of a particular resource on beforehand and has made certain that his identity and his secret is known within that resource server. 27.05.2021: Re. #74: How can restricted use be implemented (i.e. granting access to a resource to a specific client only): By linking the connector certificate to a known client? Identification of resource: Is the access token provided to have access to a specific resource?	General remark: There is no centralized resource catalogue available at any time. Any platform is free to provide via the FENIX connector (Broker) his resource catalogue to other Fenix connectors (Brocker). The summary of all received catalogues is up to each single platform. If a platform owner has idetiefied an interssting source within such catalogue the Broker component with the FENIX connector can communicatze a request on it to the source provider. The resource owner platfrom will manage the the potential access rights. 01.06.2021 The certificate will contain the necessary information about the requesting client (service) and therefore to provide an access token for that client. Our recommendation is to use ppk signed JWT tokens containing the certificate hash as access token. Restricting the access to resources can be done in two ways afterwards: 1. Adding the rights to the token, + calling the idm component upon every request is unnecessary as only the token integrity has to be verified - access rights are bound to token lifetime, i.e shorter periods should be chosen 2. The token only contains the identity and access rights are evaluated on every request + Suitable for highly dynamic revokal/granting of rights - likely to introduce additional overhead
75	We have some questions about the structure of service catalogues. We are asking for an example from Mr juergen.stolz@ptvgroup.com	We (FK) replied to the email asking for additional information. We are waiting for the answer. If needed, we could share an OpenApi yaml.
76	What is the format for Broker Metadata Ident field	The type ist a string and the format is a UUID
77	Can you provide reference values of "Communication Pattern" field in resource catalog	The values can be ['rest','webhooks','pubsub']. They can be checked in the FENIX Message in sections 4.6.2.1 in the Refinement #2 document. It is in the image and the table below.

#	Question	Answer
78	Sample Connector CSV file, Sample Resource Catalog and sample Broker Metadata	check chapter 4.7.3 example for the broker resource catalogue sample Connector list can be found here: https://erticobe.sharepoint.com/sites/FENIX/Deliverables%20%20Working%20Documents/Forms/AllItems.aspx?viewid=faefad1c%2Dc923%2D4d9d%2D8a80%2D1b68443d3016&id=%2Fsites%2FFENIX%2FDeliverables%20%20Working%20Documents%2FACT%203%20Technology%20integration%2FD3%2E4%2FConnector%20List
79	Specification Refinement Document, Section 4.7.6 1) will it be a POST/GET method 2) Where will we get the information of route_id in the endpoint url	It's either GET, PUT, POST or DELETE. The path behind the service/{resource_id}/ is up to the service being called and the route_id is only an example how it could look like.
80	Can you share the signed certificate?	see #8, for project certificate please ask T-Systems via mail
81	Need details on interfaces to integrate with T-System	The 'interface to T-Systems is the DIH Fenix Connector for PS Rhine Alpine. Communication will work as defined for the FENIX Connector. Allignment on Data to be exchanged is likely part of Sub-Act. 3.3.
82	ValidateAccessToken - is it required to do this step in every broker and data exchange flow?	ValidateAccessToken needs to be validated every time performing a FENIX operation between FENIX Connectors.
83	In Section Technical Broker overview, Figure 2 of FENIX ConnectorSpecification_Task 3.4_Refinements, what is Broker Url and Connector Url? Do they hold different values?	Obsolete, due repalced chapter and figures.
84	In Fenix Message table,there is 'name' under catalog section, which is the name of the catalog provider, and there is resource_name under resource as well . In Figure 3,of refinement document (catalogue of resources structure) the name refers to resource name. Should the name in the catalogue in the Fenix message be the resource name itself? why do we need catalog provider name here?	You are right. There is a typo in the table. Under the Catalogue section: Name: Is the name of the resource. This is used when you request the catalogue of resources. Under the Resource section: resource_name: Is the name of the resource but this is used for other purposes, as explained in the table
85	Need T-System Connector's Client certificate. This Client certificate is needed to register "T-System connector" as a client in TMS and ERP Connector.IDM	For Project use only certificates for the connector can be requested from T-Systems via EMail. These certificates are only for demonstartion use during project lifetime. The FENIX facilitator is in charge to provide official certificates at any time.
86	What is the endpoint to get BrokerMetaData of	GET /broker/

#	Question	Answer
	other connectors?	
87	Need sample Broker MetaData CSV	No csv available, perhaps the connector_list.xlsx meant? Ertico sharepoint (von T-Systems an alle: 12:24 PM https://erticobe.sharepoint.com/:x:/r/sites/FENIX/Deliverables%20%20Working%20Documents/ACT%203%20Technology%20integration/D3.4/Connector%20List/connector_list.xlsx?d=wc2f44d9d48774e73a17695a64c5cb65b&csf=1&web=1&e=uCwKLx)
88	Is Ident in the BrokerMetaData same as Connector Id?	Yes
89	When DXC of Connector.A sends data (or) request for data to Connector.B's DXC , as per specification - Connector.A DXC will send request to get access token to Connector.B IDM --> Connector.B IDM will validate the Client certificate of Connector.A and generate access token and return the access token as a response to Connector.A DXC. How are we authorizing Platform A has access to Platform B resource in this flow?	Our recommendation is to use ppk signed JWT tokens containing the certificate hash as access token. Restricting the access to resources can be done in two ways afterwards: 1. Adding the rights to the token, + calling the idm component upon every request is unnecessary as only the token integrity has to be verified - access rights are bound to token lifetime, i.e shorter periods should be chosen 2. The token only contains the identity and access rights are evaluated on every request + Suitable for highly dynamic revokal/granting of rights - likely to introduce additional overhead
90	when DXC of Connector.A sends data (or) request for data to Connector.B's DXC the process is as follows- [Authentication] 1) Connector.A DXC will send request to get access token to Connector.B IDM --> Connector.B IDM will validate the Client certificate of Connector.A and generate access token and return the access token as a response to Connector.A DXC [Authorization] 2) Connector.A DXC, with the access token will sends a request to Connector.B DXC. Connector.B DXC will send the access token to Connector.B IDM to validate the access token and if the access token is valid, Connector.B DXC will get the resource id requested and send a "validateaccess" request to Platform.B's IDM to	yes, this looks like a valid approach

#	Question	Answer
	check if Connector.A have access to the requested resource id in connector.B [Authorization] 3) Platform.B IDM will validate the access and sends back the response as either "200 OK" (valid access) or "403 Forbidden" (not has access) to Connector.B DXC. Based on the response, Connector.B DXC will take the further steps Here, Authorization will happen from Connector.DXC component and Authentication at Connector.IDM. For the rest of all calls where resourceid is not to be passed, only Authentication to be applied at the Connector.IDM level but not authorization Can this approach be followed?	
91	JWT Token is self contained & they cannot be revoked. Hence /idm/protocol/openid-connect/revoke API in Fenix Connector IDM is not relevant. Please confirm.	yes, it is not relevant
92	Is the Federated Identity Provider (Connector IDM) responsible to issue access token or Platform(Mondelez TMS IDM)?	Primary subject in Fenix is the connector IDM, therefore it is responsible for issuing the Fenix token.
93	Can you share the document the onboarding process document which contains the process to request certificate?	https://erticobe.sharepoint.com/:p:/r/sites/FENIX/_layouts/15/Doc.aspx?sourcedoc=%7B8D175621-B1EC-489C-B9A1-79BBF4E129B8%7D&file=FENIX_Approach_3.4_howto_Certificate.pptx&action=edit&mobileredirect=true

#	Question	Answer
94	1.Imprint is needed on broker level but also on resource level 2. A Catalog as in FenixResourceCatalog implies it covers multiple entries, just FenixResource would be better 3. The multiplicity could be stated explicitly 4. The fields on FenixData need some description (in particular Password and Token, do you expect plain text passwords here?!) 5. Samples should be a List and FenixSamples should be FenixSample i.e. singular 6. Fields for FenixSample ? 7. BrokerMetadata Classification = list? 8. Classification for resource? (Here just a single entry) 9. How to differentiate between Datasources and Services	1. Done 2.-> Agree. Every resource must have all the fields. 3. => 2 arrows refer to a list, legend needed 4. => removed 5. Done 6. Done 7. Done 8. Done 9.Done -> We suggested to add a field “resource_type” with those two values to identify the resource. In the Q&A doc, is the #48. 
95	1. Will there be a separate BrokerMetaData csv provided or	There is neither a brokerMetaData csv nor a resourceCatalogue csv. Meta Data and the catalog has to be retrieved from every broker using the described endpoints.
	2. Is the BrokerMetaData supposed to have values from the resourceCatalogue csv? If yes, then what will be the value of version in BrokerMetaData? Version is resource specific	
96	Endpoint to get BrokerMetaData is a GET or POST call ? In QA tracker and in refinement specification document section 4.5.3 it is mentioned GET , but in section 4.4.2.1 it is mentioned as POST	GET
97	When we get BrokerMetaData from other connector ,	1. no
	1. Is the response returned in Fenix Message format?	2. See 1.
	2. If Fenix message format, what is the msg_type? Currently we do not have any msg_type for	3. See 1.

#	Question	Answer
	BrokerMetaData	
	3. Fenix Message table structure currently does not have any section for BrokerMetaData	4. no
	4. Access token to be passed in the call for BrokerMetaData?	
98	Is Imprint & Resources to be included in the response when returning the BrokerMetaData?	Imprint: yes, Resources: no
99	1. Classifications in BrokerMetaData is a list of enums or string?	1. List
	2. Is it to be picked from the resource list or has default list ?	2. It is up to you what classifies your broker the best, however extracting it from the resource list is a valid approach
100	The indications reported on page 97 of the document FENIX D3.2_v1.3.1.pdf provide for a fairly clear handling of errors ("All the methods of the API must provide an error handling" in which err_code corresponds to the HTTP status) meanwhile the page 84 of the same document, in the description of the error field it is written "If any error happens in the FENIX Connector, and it is not a HTTP error, this must be informed as an error". Should we transform each error status according to the specified standard (value of the error field in the FENIX message) or not? If the error field of the message must be filled in, which HTTP Status must be returned by the call, the original one (i.e.: HTTP Status 500 + FENIX message) or the response becomes an HTTP OK (HTTP Status 200 + FENIX message)? In the case of client-side errors (i.e.: timeout of the call to the external endpoint), should they be treated as a server-side error? (i.e.: timeout error for calling the service, the application will have the FENIX message as a response with the error field valued as error 500)	1. The differentiation lies in http transport errors and application errors. Any request directly answered by a fenix connector component (idm, dxc, broker) should usually be ansered by a fenix specific message. If standard components in between like proxies, firewalls, etc. produce an error it would be unresonable effort to transform that error into a FenixError. 2. The http status should not be altered, the fenix error code not necessarily represents the http error code, it could also be application specific. 3. No, client-side errors should be answered with a 4xx

#	Question	Answer
101	On page 18 of the document FENIX_Connector_Specification_Refinements_#3-21062021.pdf, very specific endpoints have been defined: it is absolutely necessary that they respect that signature (/idm/protocol/openid-connect/XXX) or it can be changed (/idm/connect/XXX), as the same endpoints are easily recoverable from the configuration? (endpoint GET /idm/.well-known/openid-configuration)	Yes, please stick to that specification, it is not required to have discovery implemented and therefore cannot be guaranteed for every platform
102	The broker endpoints mentioned in page 54 of the document FENIX D3.2_v1.3.1.pdf remap in the following way: GetBrokerMetadata à Get/broker GetBrokerResourceCatalog -> POST /broker/catalogue/find FENIX_Connector_Specification_Refinements_#3-21062021.pdf, page 19: defined as both POST and GET à POST is assumed because there is a body, is that correct?	Corrected in refinement #4 GET /broker/catalogue is the correct endpoint
103	Endpoint GET/broker: since the response is not a FENIX message FENIX_D3.4_QA_11072021.pdf, question 97), is it possible to have an example of the respond?	The broker meta data is a fenix message (message_type=broker_meta_data) GET https://dih-connector.caritc.de/broker?includeExternal=false { "context": { "message_id": "c67c5ba6-00af-4fee-b7e6-02c8b84ff568", "conn_origin_id": "7b1f271b-1f1b-4436-9494-edc1dd5c08a4", "sent_at": 2021-08-02T09:41:38+02:00, "msg_type": "broker_meta_data" }, "brokerMetaData": [{ "classifications": ["Track & trace / Event handling", "Cargo monitoring",

#	Question	Answer
		"Traffic management", "Trip & Capacity planning & matching"], "creationTime": 2021-07-06T11:31:46+02:00, "description": "Fenix Connector for Data Intelligence Hub.", "ident": "7b1f271b-1f1b-4436-9494-edc1dd5c08a4", "name": "DIH-Connector", "shortDescription": "Fenix Connector ", "tags": ["dih"], "updateTime": 2021-07-06T11:33:29+02:00, "version": "v0.8", "imprint": { "address": "Hahnstraße 43D 60528 Frankfurt am Main", "email": "info@t-systems.com", "legal": "Connected Mobility", "owner": "T-Systems", "phone": "069 / 200 600" } }] }
104	Endpoint GET /broker -> FENIX_Connector_Specification_Refinements#4, pg. 10 fig. 3, pg. 12 fig. 4: the class FenixBrokerMetadata has a field resourceCatalogs, but in the example provided it is not valued/present, must be removed?	example must be revised (figure)
105	Endpoint GET /broker/catalogue -> does it return only the resources (data and services) that the connector offers by itself?	yes, only the resources of the connector itself
106	FENIX_Connector_Specification_Refinements#4, pg.18, is reported that “In every operation performed by the API, there must be the authorization token (JWT)”, but in the document FENIX_D3.4_Q&A_29072021.pdf, the answer to	-Broker Meta Data (GET /broker) does not need a token as the information is available to any FENIX member (just the certificate needs to be checked) '- GET /broker/catalogue should only return non-public resources when an authorized token has been provided,

#	Question	Answer
	Q#97.4 is “no”: are there any endpoints that do not need to have JWT token authentication? If so, which ones?	but does not necessarily need a token (e.g. if you do not have non-public resources in the Fenix network)
107	GET /broker, Q#106: “just the certificate needs to be checked” -> how do we check the certificate? Do we simply verify who issued it or other verifications?	The requester should provide his service (client) certificate + his platform (intermediate) certificate. Afterwards you can verify the chain, i.e. intermediate against root ca and client against intermediate Here is an example how to combine them both in a pfx file: openssl pkcs12 -export -inkey service-lcmm.key -in service-lcmm.crt -certfile fenix-connector.crt -out service-lcmm.pfx
108	Access to the resources: The call must be done POST /broker/datasource/{id}/access (o POST /broker/service/{id}/access) also for the public resources? § Call GET /broker/catalogue also without the JWT token, but POST /broker/{resource}/{id}/access with JWT token -> do you confirm?	There is a distinction between the fields public and restricted: Public : Regulates the visibility of a service/datasource in the catalogoue. If a resource is non-public details like data, documentation and samples should only be visible with a existing agreement, i.e. granted access. As access rights are potentially encoded into the jwt token it should be presented when these information are required. A non-public resource should also be restricted. GET /broker/catalogue without JWT à only public information GET /broker/catalogue with JWT à public information + non-public information of authorized resources Restricted: Indicates access to a resource has to be requested first but has no influence on the visibility inside the catalogue.

FENIX Connector Specification

Task 3.4

Refinements

The following refinements are an update of the FENIX Connector specification based on D3.2 V1.3. These refinements have been identified and agreed by the technical core team of Act. 3. The use of the refinements is mandatory for all federated platforms.

TABLE OF CONTENT in relation to D3.2 Chapters

Table of Figures

Table of Tables

Commented [PS13]: Table and figure numbers?

Table of Changes

Section	Description of the Change	D3.2 Page
4.4.1	Add “Company” field structure of the catalogue of resources	53
4.5.3	Add “Company” field structure of the catalogue of resources	62
4.6.2	Add “Company” field structure of the catalogue of resources and Remove MIC field	80-82
4.6.2	FENIX Message Image updated	79
4.6.2.4	This section is discontinued. Explanation provided there.	87
4.7.X	Updates on the examples of API introducing the abovementioned changes	87 - 97
4.5.3	resource_type added to the catalogue of resource.	62
4.5.3	New Images by PTV.	62
4.5.3	Under the Catalogue section: Name: Is the name of the resource. This is used when you request the catalogue of resources. Under the Resource section: resource_name: Is the name of the resource but this is used for other purposes, as explained in the table	62
4.4.2.1	New figure	
4.7.3	New section Get BrokerMetadata	
4.5.3	Catalogue of Resources structure	
4.6.2.1.	New figure 4 Fenix Message	
4.7.1	Added broker meta data endpoint	
4.7.2	Updated broker catalogue endpoint	

Section	Description of the Change	D3.2 Page
4.5.3 & 4.6.2.1	Updated figures 3 & 4	

4.5.3 Scope of the Resources

Once the resources categorization is clear, it is necessary to dig into the different scopes that these resources may have. Certainly, many datasets or information pieces can be made available worldwide inside the FENIX Federation without having any specific price or private restriction. On the other hand, there may exist some data that, due to its nature, must be treated in a more confidential way (maybe some business agreements are required between parties). The FENIX Federation will also support these parties so they can improve their business by using the FENIX Connector in a unified way.

For more clarity, it is necessary to say that every resource that is shared through the FENIX Federation must be listed in the FENIX resources catalogue.

4.4.2.1 Public Resources

If a resource is considered "public", all its information (resource ID, description, content message structure, contact, etc) will be available in the resource description of the FENIX catalogue. This will facilitate to request access to the resource from one FENIX member to the resource owner (also a FENIX member). Once evaluated and granted access, the member who made the request, will be able to receive information from that resource.

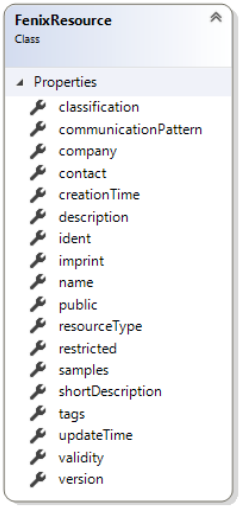


Figure: FenixResource catalog

4.4.2.2 Restricted Resources

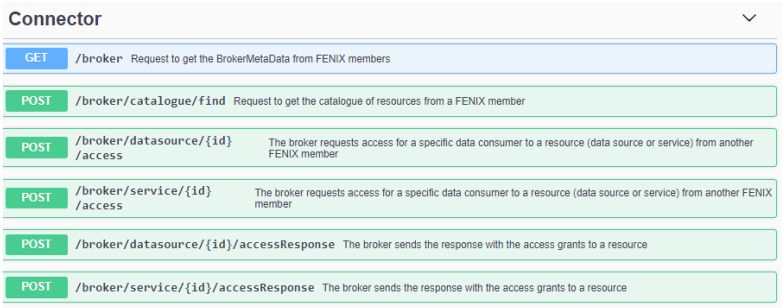
As explained before, a resource, owned by a FENIX member, can contain information that is not directly shareable within the FENIX Federation. There can exist specific conditions (business constraints, for example) that do not allow to show which is the available information (message structure) for a resource. In these cases, the resource may be listed in the FENIX catalogue with the minimum required information (see subchapter 4.5.1), including the member's contact information, and both members will have to communicate to get the remaining information and to make the proper agreements to start sharing information through the resource.

If everything is ok, then the flow will remain the same: the interested party will make the request access to the resource and the resource owner would grant access to it, so they establish the information sharing process using their FENIX Connectors for that.

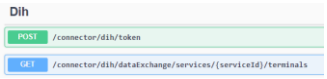
4.5.3 Technical Broker overview

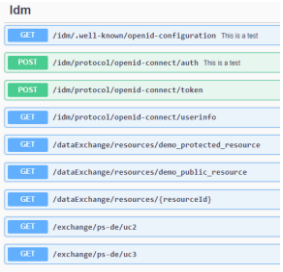
The following images are examples, how a Fenix member can implement "its" Fenix environment. The screenshots are taken from an OpenAPI description.

The endpoints of the connector section



The other sections
These sections are examples depending on the needs of the implementing member





4.4.2.1 Get broker metadata

The endpoint “/broker” (POST) is used to query the Broker basic data. The Broker API and the Connector API run in the platform environment of a Fenix member. Users of a Fenix member (TX, PTV, ...) can use the method “/broker” to get the metadata of themselves (their own broker) and of external brokers whose connectors are known after onboarding.
The return value of the method is a list of metadata.
Examples:

- A user wants to get the metadata of "his" broker => Parameter "includeExternal=false". The implementation returns a list of metadata with exactly one entry, namely the own metadata.
- A user wants to display the metadata of all brokers (including his own) => Parameter "includeExternal=true". The (own) implementation of this method now calls all known connectors BUT with "includeExternal=false" and collects the results of all connectors. After all results are available the resulting list with metadata is returned to the user (for details see section 4.7.3).

4.4.2.2 Get the broker resources

After receiving the list of “FenixBrokerMetadata”, this method is used to query detailed information (a list FenixResource) of a specified broker (for details see section 4.7.4)

4.5.3 Structure of the Catalogue of Resources

The structure of the catalogue of resources follows a meta model which contains detailed information of the resources of the catalogue (FenixResource class). The meta structure comprises several elements to identify the resource and its purpose. In total 19 entries are to be filled.

1. Ident: A FENIX-wide unique identifier for this catalogue. These identifiers must be generated when the catalogue is generated. The Identifier follows a 3-block structure:

Block 1	Block 2	Block 3

Connector ID	VAT number of the resource owner	Object number

- Connector_ID: During the On-Boarding Process, each FENIX_Connector receives an ID to be identified within the FENIX Federation.
- VAT: VAT number of the company (Resource owner).
- Object Number: ID that the resource may have within its operational platform.

All these three fields together make a unique identifier for each of the resources.
Example: 006_ES123456_37ab3198c8334d24

2. Name: A given name from the catalogue provider. This can be the product name or any other name which is provided for the resource by the resource owner.
3. Classification[4]: Fenix classified object types of the provided resources. The classification will support spotting resources, since product names are often ambiguous, e.g. "blue banana service".

   Classification categories are:

   - Track & trace / Event handling
   - Cargo monitoring
   - Traffic management
   - Parking services
   - Slot management / reservation & booking
   - Dangerous goods management
   - Trip & Capacity planning & matching
   - Optimization of customs services
   - Gate management
   - Emissions
   - Catalogues
   - Transport & cargo e-documentation
   - Other

4. Short Description of the resource: A shorter description of the provider, catalogue and provided resources); e.g. "blue banana" is an ETA service by company XYZ.
5. Description: A more detailed description of the resource.
6. Tags: Values to describe content (like "eta") to ease a search.
7. Contact: The main contact for the resource can be given here, e.g. responsible product owner or customer service can be given here.
8. Imprint: Contains the imprint of the resource owner. This represents the legal view towards the resource owner.

[4] The FENIX classification has been discussed in cross collaboration between Activity 3 and Activity 4. This classification can be also found in *"D4.1.1 – Collaborative Business Environment"*.

9. Data & Documentation: Links to further resource documentation.
10. Samples: Links to samples.
11. Public: This entry sets the resource to be publicly visible or visible only after request.
12. Restricted: This entry defines the restriction level of the resource. It is a Boolean type.
13. Creation Time: Timestamp of the creation.
14. Update Time: Timestamp of the last update.
15. Validity: Sets a certain date for the validity of the resource or can set unlimited validity for the resource entry.
16. Version: Version number, increases after update.
17. Communication Pattern: e.g. WebHooks
18. Company: The company owning the resource
19. Resource Type: Enum used to distinguish between Data and Service

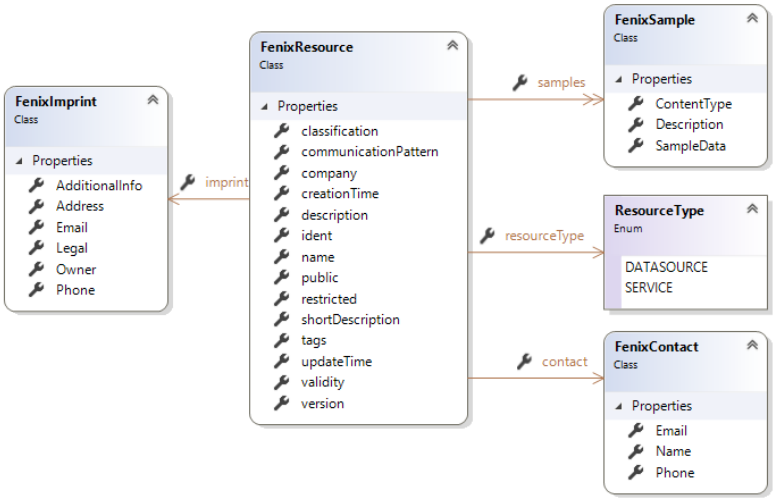


Figure: Catalogue of Resources structure

4.6.2 FENIX Message

The FENIX Connector is the main module to perform the information exchange process between the FENIX Federation members. As explained in previous chapters, every member needs to deploy a FENIX Connector to exchange information with others.

In section 3.4 (See D3.2 V1.3.1) it is explained how FENIX provides technical interoperability between

data platforms by implementing the FENIX Connector. One of the key elements needed to provide this level of interoperability is that the FENIX Connectors must understand each other.

To do so, it is necessary to talk about a common FENIX message structure that will contain all the necessary information to identify how the communication between connectors is being performed. Also, the different types of messages that the connector will exchange must be described. The FENIX messages must be used as main body of every API operation, either if it is a request, a response (if available) or an error. Further examples are provided in section 4.7.

As described in the sections above, there are many messages that need to be exchange between the modules of the FENIX Connectors, therefore, these kinds of messages have been identified and described below.

Finally, it is necessary to describe which is the message technical format (json, xml, etc.) that will be supported by the FENIX Connector. This content is available in the next subsections.

4.6.2.1 Structure

The FENIX Connectors will exchange information by using a common message structure that will make these components interoperable between them.

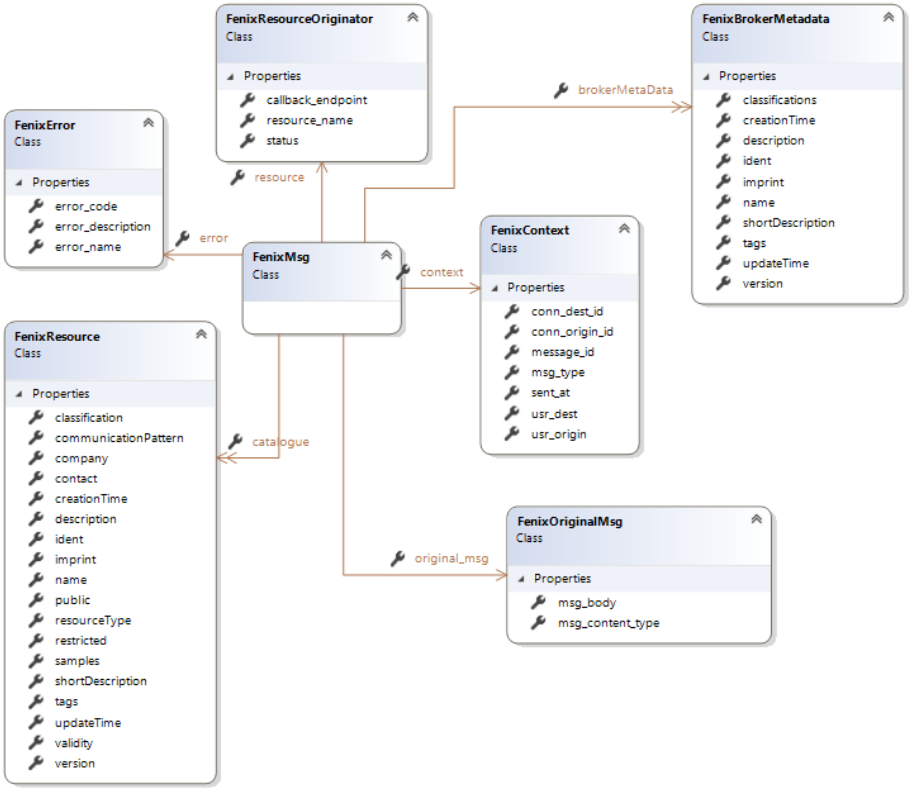


Figure: FENIX Message

The table below explains each of the fields described in the FENIX message. For the root elements, they may appear as Optional but, if they are informed, some of its nested elements may be required and others may be Optional.

Field	Parent Field	Required	Field Type	Description	To be included when
context	*root*	*Required*			In every message body, either body or response.
message_id	context	Required	Text	ID generated for the message	In every message body, either body or response.
conn_origin_id	context	Required	Text	ID of the sender FENIX Connector	In every message body, either body or response.
conn_dest_id	context	Required	Text	ID of the receiver FENIX Connector	In every message body, either body or response.
usr_origin	context	Optional	Text	ID of the user sending the original message	If the underlying platform needs to work with users, it must be included either in the body or response.
usr_dest	context	Optional	Text	ID of the user receiving the original message	If the underlying platform needs to work with users, it must be included either in the body or response.
sent_at	context	Required	Timestamp	Current date & time when sending the message. Timestamp must be indicated in ISO 8601 standard, UTC time:	In every message body, either body or response.

				- YYYY-MM-DDThh:mm:ss+00:00	
msg_type	context	Required	Enum	Defines the type of message that is being sent. It can take the following values: - access_request - access_response - user_info - data_request - data_record - service_request - service_response - resource_catalogue - resource_grant_request - resource_grant_response - subscription_request - subscription_response - error - broker_meta_data	In every message body, either body or response, except for the access operations, where oauth 2.0 is used.
user_info	root	Optional	Object	Contains the user information to whom a token belongs in the resident IDM	It must be specified in the next situations: - User Info (sect. 4.7.1.1)
sub	user_info	Required	Text	ID of the user	

name	user_info	Required	Text	Name of the user	
updated_at	user_info	Required	Timestamp	Last update of the user information. Timestamp must be indicated in ISO 8601 standard, UTC time: - YYYY-MM-DDThh:mm:ss+00:00	
resource	root	Optional	Object	Identifies the resource sending information	The resource (data source or service) is described by its own URL. If additional information wants to be provided, like the resource name, it can be done using this Object.
resource_name	resource	Optional	Text	Name of the resource addressing the request or sending the response	It must be specified in the next situations: - If asking for information to a resource - If a resource sends information as a response - When requesting access to a resource - When granting access to a resource

status	resource	Optional	Enum	When trying to subscribe to a resource using webhooks, the access grants must have been done in advance. Therefore, if there is no grant, the status must be Denied. If it was already granted, the process will make the subscription and return a Registered. It can take the following values: - Registered - Denied	To be used ONLY if webhooks pattern is being used. Whenever a subscription operation to a resource takes place.
callback_endpoint	resource	Optional	Text	When using the webhooks pattern, the data consumer must provide an endpoint where to post data when available.	To be included in the next operations using the Webhooks pattern: - Subscribe to a datasource - Subscribe to a service
original_msg	root	Optional	Object		To be included in the next operations: - Get Access to a Resource (sect. 4.7.3) (Optional) - Get Message from a Data Source (sect. 4.7.4) - Get Data from a Service (sect. 4.7.5) - Publish Data Record to a resource
msg_content_type	original-_msg	Optional	Text	If the original message is formatted following any standard, it can be indicated here.	
msg_body	original-_msg	Required	Text	Original message sent from the underlying platform. It must be stringified.	

					(sect. 4.7.6)
catalogue	root	Optional	Array of Catalogue Items	Contains the information specified in section 0. Every resource must be described with each of the fields described below.	To be included in the next operation: - Get Catalogue of resources (sect. 4.7.2)
ident	catalogue	Required	Catalogue Item - Text	A Fenix wide unique identifier for this resource	
name	catalogue	Required	Catalogue Item - Text	Name of the resource	
classification	catalogue	Required	Catalogue Item - Enum	Fenix classified object types of the provided resources. It can take the following values: - Track&trace/EventHandling - cargoMonitoring - trafficManagement - parkingServices - slotManagement (slot management, reservation, booking) - dgManagement (Dangerous goods management) - trip&CapacityPlanning - optimizationCustomsServices (optimization of	

				customs services) - gateManagement - emissions - catalogues - transport&cargoDocumentation - other	
shortDescription	catalogue	Required	Catalogue Item - Text	A short description of the resource.	
description	catalogue	Optional	Catalogue Item - Text	A more detailed description of the resource.	
tags	catalogue	Optional	Catalogue Item - Array	Values to describe the content to ease the search.	
contact	catalogue	Required	Catalogue Item - Object	Contact for the resource: e.g., responsible product/resource owner	
imprint	catalogue	Required	Catalogue Item - Object	Imprint of the resource owner. This represents the legal view towards the resource owner.	
doc	catalogue	Required	Catalogue Item - Text	Link to resource documentation	
samples	catalogue	Optional	Catalogue Item	Link to resource’s samples	

			- Text		
public	catalogue	Required	Catalogue Item - Bool	Sets the resource to visible to public or visible only after request	
restricted	catalogue	Required	Catalogue Item - Bool	Defines the restriction level of the resource.	
creationTime	catalogue	Required	Catalogue Item - Timestamp	Timestamp of the creation. Timestamp must be indicated in ISO 8601 standard, UTC time: - YYYY-MM-DDThh:mm:ss+00:00	
updateTime	catalogue	Required	Catalogue Item - Timestamp	Timestamp of the last update of the resource. Timestamp must be indicated in ISO 8601 standard, UTC time: - YYYY-MM-DDThh:mm:ss+00:00	
validity	catalogue	Required	Catalogue Item - Timestamp	Sets a certain date for the validity of the resource or can set unlimited validity for the resource entry. Timestamp must be indicated in ISO 8601 standard, UTC time: - YYYY-MM-DDThh:mm:ss+00:00	
version	catalogue	Required	Catalogue Item - Text	Version number of the resource. Increases after update.	
communicationPattern	catalogue	Required	Catalogue Item	Indicates the type of communication pattern	

			- Text	implemented by the FENIX Connector that exposes the resource.	
company	catalogue	Required	Catalogue Item - Text	Name of the company that is owner of the resource.	
resourceType	catalogue	Required	Catalogue Item – Enum (DATASOURCE, SERVICE)	It can be named, for example, resource_type, and it can get the values: - DataSource - Service. It is needed to use the DxC endpoints.	
error	root	Optional	Object	Application Error	If any error happens in the FENIX Connector, and it is not a HTTP error, this must be informed as an error.
error_name	error	Required	Text	Error Name	If there is a specific error name, it can be indicated here
error_description	error	Required	Text	Error Description	Description for the error to understand what is happening
error_code	error	Optional	Text	Error Code	If there is any code that want to be sent. Usually, there would be internal platform codes which are meaningless.

4.6.2.4 Message Integrity

Due to the fact that the TLS protocol already provides MIC codes perse, it does not make sense to have it as part of the FENIX messages. Hence, this has been discontinued.

4.7 API – External Communication

The FENIX Connector communicates *w*ith other FENIX Connectors to exchange information. Based on this concept that has been explained along this document it is necessary to expose an API to enable this communication.
The current subchapter describes the operations that can be used to communicate with other FENIX Connectors.

The API operations will have a root domain followed by one of the main modules that are part of the FENIX Connector. It would be like this:

https://connector_url:connector_port

Where Connector_URL is the target FENIX Connector and Connector_Port is the target connector's port.

The three modules are: idm, dataExchange and broker. Therefore, the API can be grouped like this:

https://connector_url:connector_port/idm/...

https://connector_url:connector_port/broker/...

https://connector_url:connector_port/dataExchange/...

Note that for the examples provided in the next subsections, JSON format has been chosen, but the Content-Type of the messages can be any of those described in 4.6.2.3.

4.7.1 Headers

In every operation performed by the API, there must be the authorization token (JWT). This token will be gotten through the "token" operation explained in subsection 4.6.2.3. The operation to get the access token is the only operation that does not require it.

HEADERS	Required	Description
Authorization	X	Include the JWT generated to perform operations
Content-Type	X	Application/json. Specifies the content type of the FENIX message.

Table : API Headers

4.7.2 Identification & Authentication

Based on overarching API endpoint structure of FENIX Connector specification, IDM endpoints must be reachable via **/idm/** subdirectory of a platform. For example, the token endpoint of a FENIX platform has to be reachable via *https://connector_url:connector_port/idm/protocol/openid-connect/token* uniform resource identifier.

FENIX IDM connector will be built on industry standard authentication and authorization protocols OAuth 2.0 and OpenID Connect.

Endpoint	Required	Methods	Description
/idm/.well-known/openid-configuration	X	GET	OpenID configuration discovery endpoint
/idm/protocol/openid-connect/auth		POST	Optional authentication endpoint, only used in cases of end-user auth
/idm/protocol/openid-connect/logout	X	POST	Invalidation of all user access tokens
/idm/protocol/openid-connect/userinfo	X	POST	Validate and retrieve details about access token
/idm/protocol/openid-connect/revoke	X	POST	Revocation of issued OAuth 2.0 token (as described in RFC7009)
/idm/protocol/openid-connect/token	X	POST	Obtain access token for FENIX usage.

Table: Access API

Example: Access Request	
POSt	https://{connector_url}:{connector_port}/idm/protocol/openid-connect/token
Body	grant_type=client_credentials&client_id=fenix-idm

Example: User Info	
POST	https://{connector_url}:{connector_port}/idm/protocol/openid-connect/userInfo
Header	Authorization: Bearer *access_token*
Body	*none*
Response	{ "sub": "110248495921238986420", "name": "Pepe Moreno", "updated_at": "2020-08-01T11:52:25+0000" }

4.7.1 Get Broker Meta Data

Endpoint	Required	Methods	Description
/broker?includeExternal=<true|false>		GET	Request to get the internal (includeExternal=false) or internal + external (includeExternal=true) broker meta data from a

			FENIX member

Table: Catalogue of Resources API

Example: Get Catalogue of Resources	
GET	https://{connector_url}:{connector_port}/broker?includeExternal=false
Response	{ "context": { "message_id": "c67c5ba6-00af-4fee-b7e6-02c8b84ff568", "conn_origin_id": "7b1f271b-1f1b-4436-9494-edc1dd5c08a4", "sent_at": 2021-08-02T09:41:38+02:00, "msg_type": "broker_meta_data" }, "brokerMetaData": [{ "classifications": ["Track & trace / Event handling", "Cargo monitoring", "Traffic management", "Trip & Capacity planning & matching"], "creationTime": 2021-07-06T11:31:46+02:00, "description": "Fenix Connector for Data Intelligence Hub.", "ident": "7b1f271b-1f1b-4436-9494-edc1dd5c08a4", "name": "DIH-Connector", "shortDescription": "Fenix Connector ", "tags": ["dih"], "updateTime": 2021-07-06T11:33:29+02:00, "version": "v0.8",

	"imprint": { "address": "Hahnstraße 43D 60528 Frankfurt am Main", "email": "info@t-systems.com", "legal": "Connected Mobility", "owner": "T-Systems", "phone": "069 / 200 600" } }] }

4.7.2 Get Catalogue of Resources

Endpoint	Required	Methods	Description
/broker/catalogue		GET	Request to get the catalogue of resources from a FENIX member

Table: Catalogue of Resources API

Example: Get Catalogue of Resources	
GET	https://{connector_url}:{connector_port}/broker/catalogue
Response	{ "context":{ "message_id":”35236574”, "conn_origin_id":”006”, "conn_dest_id":”001”, "sent_at":"2021-01-14T12:15:25+0000", "msg_type":"resource_catalogue" },

	“catalogue”:[{ "ident":"006_ES123456_37ab3198c8334d24", "name":"ETA_calculator", "classification":"Track & Trace", "shortDescription":"The service provides real time track & trace capabilities", "description":"The service provides real time track & trace capabilities ...", "tags":["eta", "track&trace"], "contact": { "email": "joe.doe@mail.com", "name": "Joe Doe", "phone": " +49 1245 1411-159" }, "imprint": { "address": "Hahnstraße 43D 60528 Frankfurt am Main", "email": "info@t-systems.com", "legal": "Connected Mobility", "owner": "T-Systems", "phone": "069 / 200 600" }, "doc":"URL_with_available_doc", "samples":"URL_with_samples", "public":"true/false", "restricted":"true/false", “creationTime”: “2018-03-05T16:55:25+0000", "updateTime":"2021-01-14T12:15:34+0000", “validity”: “2022-01-14T09:25:00+0000”,

	"version":"1.1”, “communicationPattern”: “webhooks”, “company”: “PTV group” }] }

4.7.3 Get Access to Resource

Endpoint	Required	Methods	Description
/broker/datasource/{id}/access		POST	The broker requests access for a specific data consumer to a resource (data source or service) from another FENIX member
/broker/service/{id}/access		POST	The broker requests access for a specific data consumer to a resource (data source or service) from another FENIX member
/broker/datasource/{id}/accessResponse		POST	The broker sends the response with the access grants to a resource
/broker/service/{id}/accessResponse		POST	The broker sends the response with the access grants to a resource

Table: Get Access to Resource API

Example: Access Request to a Data Source	
POST	https://{connector_url}:{connector_port}/broker/datasource/{id}/access
Body	{ "context":{ "message_id":”35236574”, "conn_origin_id":”001”, "conn_dest_id":”006”, "usr_origin":"javier.garcia@atos.net", "usr_dest":"user@destination.com", "sent_at":”2021-01-14T12:15:25+0000”, "msg_type":"resource_grant_request", }, "resource": { "resource_name":" Data Source Name" } } }
Response	HTTP Response

Example: Access Response from a Data Source	
POST	https://{connector_url}:{connector_port}/broker/datasource/{id}/accessResponse
Body	{ "context":{ "message_id":”35236574”, "conn_origin_id":”006”, "conn_dest_id":”001”, "usr_origin":"user@destination.com", "usr_dest":"javier.garcia@atos.net", "sent_at":"2021-01-14T12:15:25+0000”, "msg_type":"resource_grant_response" }, "resource": { "resource_name":"Data Source Name" }, "original_msg": { "msg_content_type ": "application/xml", "msg_body":"response with the access granted or not (coming from the platform)." } }
Response	HTTP Response

Example: Access Request to a Service	
POST	**https://{connector_url}:{connector_port}/broker/service/{id}/access**
Body	**{** **"context":{** **"message_id":"35236574",** **"conn_origin_id":"001",** **"conn_dest_id":"006",** **"usr_origin":"javier.garcia@atos.net",** **"usr_dest":"user@destination.com",** **"sent_at":"2021-01-14T12:15:25+0000",** **"msg_type":"resource_grant_request",** **},** **"resource": {** **"resource_name":"Service Name"** **}** **}** **}**
Response	**HTTP Response**

Example: Access Response from a Service	
POST	https://{connector_url}:{connector_port}/broker/service/{id}/accessResponse

Body	{ "context":{ "message_id":”35236574”, "conn_origin_id":”006”, "conn_dest_id":”001”, "usr_origin":"user@destination.com", "usr_dest":"javier.garcia@atos.net", "sent_at":"2021-01-14T12:15:25+0000”, "msg_type":"resource_grant_response" }, "resource": { "resource_name":"Service Name" }, "original_msg": { "msg_content_type ": "application/xml", "msg_body":"response with the access granted or not (coming from the platform)." } }
Response	HTTP Response

4.7.4 Get Message from a Data Source

Endpoint	Required	Methods	Description
/dataExchange/datasource/{resource_id}		POST	This method will retrieve a data set from a resource

Table: Get Data from a Data Source API

Example: Get data from Data Source	
POST	https://{connector_url}:{connector_port}/dataExchange/datasource/006_ES123456_37ab3198c8334d24
Body	{ "context":{ "message_id":”35236574”, "conn_origin_id":”006”, "conn_dest_id":”001”, "usr_origin":"user@destination.com", "usr_dest":"javier.garcia@atos.net", "sent_at":"2021-01-14T12:15:25+0000”, "msg_type":" data_request" } }
Response	{ "context": { "message_id":”33424662”, "conn_origin_id":”006”, "conn_dest_id":”001”, "usr_origin":"user@destination.com", "usr_dest":"javier.garcia@atos.net", "sent_at":"2021-01-14T12:15:34+0000”, "msg_type":"data_record" }, "resource": { "resource_name":"Data source Name"

	}, "original_msg": { "msg_content_type ": “application/edifact”, "msg_body": "your_original_message_to_be_sent" } }

4.7.5 Get Data from a Service

Endpoint	Required	Methods	Description
/dataExchange/service/{resource_id}/…		GET, PUT, POST, DELETE (OPTIONS?)	Methods to exchange data with a service. The shown part of the url is fixed, while the remainder depends on the service to be accessed.

Example: Get data from a Service	
GET	https://{connector_url}:{connector_port}/dataExchange/service/006_ES123456_37ab3198c8331654/routes/<route_id>

Body	{ "context":{ "message_id":”33424664”, "conn_origin_id":”001”, "conn_dest_id":”006”, "usr_origin":"javier.garcia@atos.net", "usr_dest":"user@destination.com", "sent_at":"2021-01-14T10:15:34+0000”, "msg_type":"service_request" }, "resource": { "resource_name":"Service Name" }, "original_msg":{ " msg_content_type ":"", "msg_body":"\{\"id\":\"<route id>\",\r\"startDate\":\"2021-05-10T-09:50+00\",\r\"endDate\":\"2021-05-10T-10:50+00\",\r\"waypoints\":\[…\]\r\}" } }
Respo nse	{ "context":{ "message_id":”33424665”, "conn_origin_id":”006”, "conn_dest_id":”001”, "usr_origin":"user@destination.com", "usr_dest":"javier.garcia@atos.net", "sent_at":”2021-01-14T10:15:45+0000”, "msg_type":"service_response" }, "resource": { "resource_name":"Service Name" }, "original_msg":{

	"msg_content_type ":" application/json", "msg_body":"original response from the service execution" } }

4.7.6 Webhooks pattern

These operations must be implemented if the communication pattern to be used is based on webhooks. When subscribing to a resource, the data consumer that makes the request must provide an endpoint to which, the data owner must post the data records when available. On the one hand, the data consumer must make available that endpoint to be reachable by the data owner when a data record is ready. On the other hand, the data owner, if accepts the subscription, must keep a list of the data consumers' endpoints to know who must be notified when a data record is ready.

Endpoint	Required	Methods	Description
/dataExchange/datasource/{resource_id}/subscribe		POST	This method provides an endpoint generated to receive information from a data owner when available. To be used to subscribe to a Data Source

/dataExchange/service/{resource_id}/subscribe		POST	This method provides an endpoint generated to receive information from a data owner when available. To be used to subscribe to a Service
/dataExchange/datasource/{resource_id}/{received_endpoint}		POST	This method sends any data record to the proper receiver. To be used to subscribe to a Data Source
/dataExchange/service/{resource_id}/{received_endpoint}		POST	This method sends any

			data record to the proper receiver. To be used to subscribe to a Service

Example: Subscribe to a Data Source	
POST	https://{connector_url}:{connector_port}/dataExchange/datasource/006_ES123456_37ab3198c8331654/subscribe

Body	{ "context":{ "message_id":”33424664”, "conn_origin_id":”001”, "conn_dest_id":”006”, "usr_origin":"javier.garcia@atos.net", "usr_dest":"user@destination.com", "sent_at":"2021-01-14T10:15:34+0000”, "msg_type":"subscription_request" }, "resource": { "resource_name":"Data Source Name" }, "callback_endpoint":"/dataExchange/resources/endpoint_for_Service_Inputs” }
Respo nse	{ "context":{ "message_id":”33424665”, "conn_origin_id":”006”, "conn_dest_id":”001”, "usr_origin":"user@destination.com", "usr_dest":"javier.garcia@atos.net", "sent_at":"2021-01-14T10:15:45+0000”, "msg_type":"subscription_response" }, "resource": { "resource_name":"Data Source Name" } }

Example: Publish Data Record to a resource	

POST	https://{connector_url}:{connector_port}/dataExchange/ datasource /endpoint_for_Service_Inputs
Body	{ "context": { "message_id":”33424665”, "conn_origin_id":”006”, "conn_dest_id":”001”, "usr_origin":"user@destination.com", "usr_dest":"javier.garcia@atos.net", "sent_at":"2021-01-14T10:15:34+0000”, "msg_type":"data_record" }, "resource": { "resource_name":"Data Source Name" }, "original_msg":{ "msg_content_type ":" application/xml", "msg_body":"original response from the data source execution" } }
Response	HTTP Response

Example: Subscribe to a Service	
POST	https://{connector_url}:{connector_port}/dataExchange/service/006_ES123456_37ab3198c8331654/subscribe

Body	{ "context":{ "message_id":”33424664”, "conn_origin_id":”001”, "conn_dest_id":”006”, "usr_origin":"javier.garcia@atos.net", "usr_dest":"user@destination.com", "sent_at":"2021-01-14T10:15:34+0000”, "msg_type":"subscription_request" }, "resource": { "resource_name":"Service Name", "callback_endpoint":"/dataExchange/resources/endpoint_for_Service_Inputs” } }
Respon se	{ "context":{ "message_id":”33424665”, "conn_origin_id":”006”, "conn_dest_id":”001”, "usr_origin":"user@destination.com", "usr_dest":"javier.garcia@atos.net", "sent_at":"2021-01-14T10:15:34+0000”, "msg_type":"subscription_response" }, "resource": { "resource_name":"Service Name" } }

Example: Publish Data Record to a resource	
POST	https://{connector_url}:{connector_port}/dataExchange/service/endpoint_for_Service_Inputs
Body	{ "context": { "message_id":”33424665”, "conn_origin_id":”006”, "conn_dest_id":”001”, "usr_origin":"user@destination.com", "usr_dest":"javier.garcia@atos.net", "sent_at":"2021-01-14T10:15:34+0000”, "msg_type":"data_record" }, "resource": { "resource_name":"Service Name" }, "original_msg":{ "msg_content_type ":" application/xml", "msg_body":"original response from the service execution" } }
Response	HTTP Response

References

FENIX Grant Agreement

FENIX Grant Agreement Supporting Document

FENIX Activity 2,3 and 6 deliverables:

D2.2.2 Common requirements for the federated architecture of platforms, 30/04/2020, Version 2.0

D2.5 Governance model for collaboration, still under construction

D3.1 FENIX Architectural design specification, 30/04/2020, Version 1.0

D3.2 FENIX Connector Specification, 03/04/2021, Version 1.3.1

D6.1 FENIX service quality (self-) certification methodologies due 30/11/2021, Version 1.0

Commented [GR14]: Carlo: planned date , Version