D3.1

FENIX Architectural Design Specification

Version number:	1.0
Main author:	ATOS
Dissemination level:	PU
Lead contractor:	ATOS
Due date:	31/03/2020
Delivery date:	30/04/2020
Delivery date updated document:	

Co-financed by the European Union
Connecting Europe Facility

CONTROL SHEET

Version history			
Version	**Date**	**Main author**	**Summary of changes**
0.1	01/03/2020	ATOS	D3.1 First version
0.2	19/03/2020	ATOS	D3.1 Section 3, 4 and 5 inputs
0.3	24/03/2020	ATOS, CLMS, INLECOM, PTV, T-SYSTEMS, POLIBA, GS1	Business cases and Use cases descriptions in section 5
0.4	27/03/2020	ATOS, GS1	Section 1, Section 2, update on section 5
0.5	30/03/2020	ATOS	Section 3 update, Section 5 updates and roadmap input
V0.6	31/03/2020	ATOS	Glossary of terms
V1.0	17/04/2020	ATOS	Executive Summary & Comments from Peer Reviewers
	Name		**Date**
Prepared	ATOS	-	31/03/2020
Reviewed	T-SYSTEMS eBOS	-	14/04/2020 16/04/2020
Authorised	FENIX Consortium	-	23/04/2020
Circulation			
Recipient	**Date of submission**		
Project partners			**27/04/2020**
FENIX Management Committee			**28/04/2020**
INEA			**30/04/2020**

TABLE OF CONTENT

Contents

FIGURES....5

TABLES....6

LIST OF ABBREVIATIONS....8

1. INTRODUCTION....10

1.1 Purpose of the document....10

1.2 Glossary of Terms....10

1.3 Contractual references....11

2. EXECUTIVE SUMMARY....13

3. CONTEXTUAL DRIVERS....14

3.1 Business Drivers....14

3.2 Technological Drivers....15

3.3 Policy Drivers....19

4. FENIX Network design principles....22

5. FENIX IT Architecture vision....27

5.1 Logical view of FENIX Federation....28

5.2 FENIX Roles....29

6. FENIX Network of platforms....32

6.1 User stories....32

6.1.1 Business User Stories....32

6.1.2 FENIX User Stories....35

6.2 Use cases....40

6.3 Traceability Matrix....52

6.4 FENIX Connector 53
6.4.1 Modules functionality 54
6.4.2 FENIX connector and roles interaction 55
6.4.3 Technical specifications 56
7. Conclusions and Way Ahead 57
REFERENCES 60

FIGURES

Figure 1. FENIX work packages distribution 13
Figure 2: FENIX Contextual drivers in the concept design 14
Figure 3. Industrial Data Space. Core Principles. Source: Fraunhofer & Industrial Data Space 16
Figure 4. CEF Building Blocks Source: CEF Digital 17
Figure 5. Commodity for data sharing in supply and logistics Source: DTLF 21
Figure 6: FENIX network design principles 23
Figure 7: FENIX architecture concept based on design principles 26
Figure 8. FENIX Federated Network 29
Figure 9. F-US-001 On Boarding 36
Figure 10. F-US-002 Search Available Resources in the FENIX Federation 37
Figure 11. F-US-003 Request Access to Resource in the FENIX Federation 38
Figure 12. F-US-004 Send/Receive Data through FENIX Federation 39
Figure 13. F-US-005 Grant/Revoke Access to Resource in the FENIX Federation 40
Figure 14: FENIX Connector architecture 54
Figure 15 FENIX Connector roles 55
Figure 16. Activity 3 tasks interactions 59

TABLES

Table 1. F-BUS-01 *Partner accesses data service to GET data from the service* 34
Table 2. F-BUS-02 *Partner accesses data service to WRITE data into the service database* 35
Table 3. F-US-001 On Boarding 35
Table 4. F-US-002 Search Available Resources in the FENIX Federation 36
Table 5. F-US-003 Request Access to Resource in the FENIX Platform 37
Table 6. F-US-004 Send/Receive Data through FENIX Federation 38
Table 7. F-US-005 Grant/Revoke Access to Resource in the FENIX Federation 39
Table 8. UC-001 Request Access to FENIX Federation 41
Table 9. UC-002 Evaluate New Joining Request 41
Table 10. UC-003 Provide Platform Minimum Requirements 41
Table 11. UC-004 Adapt Platform to Requirements 42
Table 12. UC-005 Send Connector Specification 42
Table 13. UC-006 Implement Connector 42
Table 14. UC-007 Evaluate Connector Implementation 43
Table 15. UC-008 Generate Certificate for Platform 43
Table 16. UC-009 Publish New Platform URL 43
Table 17. UC-010 Request Available Resources 44
Table 18. UC-011 Receive Catalogue Request 44
Table 19. UC-012 Add Platform Certificate 44
Table 20. UC-013 Validate Platform Certificate 45
Table 21. UC-014 Broadcast Request to Federation 45
Table 22. UC-015 Get Endpoints of Federation Connectors 46
Table 23. UC-016 Send Resources Catalogue 46
Table 24. UC-017 Compose Message with Resources Catalogue 46
Table 25. UC-018 Send Resources Catalogue to Platform X 47
Table 26. UC-019 Request Access to Resource 47
Table 27. UC-020 Receive Request to Access Resource 47
Table 28. UC-021 Accept/Reject Access Request to Resource 48
Table 29. UC-022 Send Response to Platform X 48
Table 30. UC-023 Send Data 48
Table 31. UC-024 Receive Data 49
Table 32. UC-025 Adapt Message to FENIX Specification 49
Table 33. UC-026 Get Destination Connector URL 49

Table 34. UC-027 Send Message to DXC Platform 50
Table 35. UC-028 Receive Message from DXC Platform X 50
Table 36. UC-029 Forward Message to Platform X URL 50
Table 37. UC-030 Reject Message 51
Table 38. UC-031 Revoke Access to Resource to Platform 51
Table 39. UC-032 Send Notification 51
Table 40. UC-033 Receive Notifications 52
Table 41. Traceability Matrix. User Stories - Use Cases 53
Table 42: FENIX Network architecture roadmap plan 58

LIST OF ABBREVIATIONS

ACL	Access Control List
AEO	Authorised Economic Operator
AIS	Automatic identification system
API	Application Program Interface
B2A	Business to Administration
B2B	Business to Business
CE	Connectivity Engine
CEF	Connecting Europe Facility
CRUD	Create, Retrieve, Update, and Delete
COTS	Commercial Off The Shelve
DG MOVE	Directorate-General Mobility Transport, MOVE
DTLF	Digital Transport and Logistic Forum
e-CMR	Electronic Convention des Merchandises par Route
EC	European Commission
EDI	Electronic Data Interchange
ERTMS	European Rail Traffic Management System
EU	European Union
ETA	Estimated Time of Arrival
ETL	Extraction, Transformation, & Loading
ETD	Estimated Time of Departure
FENIX	A European FEderated Network of Information eXchange in Logistics
GDPR	General Data Protection RegulationO
GE	Germany
GHG	Greenhouse Gas
HTTP	Hypertext Transfer Protocol
INEA	Innovation and Networks Executive Agency
ID	Identifier

IDM	Identity Management
IDS	Industrial Data Spaces
IoT	Internet of Things
ISO	International Organisation of Standardisation
IT	Information Technology
ITS	Intelligent Transport Systems
JSON	JavaScript Object Notation
LSP	Logistics Service Provider
M&P	Maritime & Ports
MQTT	Message Queue Telemetry Transport
REST	Representational State Transfer
SELIS	Shared European Logistics Intelligent Information Space
SLA	Service Level Agreement
SSL	Secure Sockets Layer
SSO	Single Sign On
SLA	Service Level Agreement
SME	Small and Medium-Sised Enterprise
SSL	Secure Sockets Layer
TAF/TAP TSI	Technical Specification for Interoperability relating to Telematics Applications for Freight/Passenger Services
TCT	Trimodal Container Terminal
TEN-T	Trans-European Transport Network
T&L	Transport and Logistics
TLS	Transport Layer Security
TMS	Transport Management System
UBL	Universal Business Language
UC	Use Case
UML	Unified Modeling Language
UDP	User Datagram Protocol
VPN	Virtual Private Network

VTS	Vessel Traffic Services
WCO	World Customs Organisation
WSS	Web Service Security
XML	eXtensible Markup Language
4PL	Fourth Party Logistics

1. INTRODUCTION

1.1 Purpose of the document

The present document intends to provide a first approach to what the FENIX Network of Platforms looks like and which are the business, technical and policy drivers that lead to specify a solution as such. Besides, the document explains which is the framework under the FENIX Federation, how it is designed and how it will be applied in the context of the FENIX Project.

As a second point, the current deliverable starts dealing with the definition of the actors of the FENIX Federation and the roles that can appear. The specifications that the FENIX Federation will provide to the different platform providers will also be explained. The present documents analyses some of the current business user stories to deep dive into the Federation User stories specification, which will lead to the identification of the different use cases to be covered by the FENIX architecture.

Finally, the document focusses on the FENIX connector, which is the component to communicate between the members of the FENIX Federation. This section explains how the connector is designed at a high level, its three building blocks and the operations that will perform within the federation. As it is still in a design phase, the present document does not provide an implementation, nor very deep specification details of the FENIX connector. This information will be covered in D3.2.

1.2 Glossary of Terms

A short list description of the four terms used in this document is included below. This small glossary of terms tries to put in context to the reader of what it is understood for each of the terms and has been used definitions from business and software engineering dictionaries and documents. These four terms are:

- *Federation* > a body formed by a number of organisations, platforms, entities, unions, etc., that works to bring attention to issues that are of importance to all of its members, who retain control of their own internal affairs[1].
- *Digital Ecosystem* > A digital ecosystem is defined as a distributed adaptive open socio-technical system with properties of self-organisation, scalability and sustainability[2].
- *Platform* > a major piece of software, such as an operating system, an operating environment, or a database, under which various smaller application programs can be designed to run[3]. In the context of FENIX, the platforms are those software systems and environments used in the logistics business to share data and/or to offer added value services.
- *Connector* > software connectors perform transfer of control and data among components. Connectors can also provide services, such as persistence, invocation, messaging, and transactions, that are largely independent of the interacting components' functionalities. These services are usually considered to be "facilities components"[4].

1.3 Contractual references

FENIX stands for “A European **FE**derated **N**etwork of **I**nformation e**X**change 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

[1] http://www.businessdictionary.com/definition/federation.html

[2] G. Briscoe and P. De Wilde. Digital ecosystems: evolving service-orientated architectures. In Proceedings of the 1st international conference on Bio inspired models of network, information and computing systems, page 17.
ACM, 2006.

[3] https://www.dictionary.com/browse/software-platform

[4] https://www.oreilly.com/library/view/software-architecture-foundations/9780470167748/ch05.html

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

2. EXECUTIVE SUMMARY

According to the GA, one of the three main objectives of the FENIX project is to *"establish a federated network of transport and logistics actors across Europe, enabling sharing of information and services needed to optimise TEN-T corridors from economic, environmental and societal perspective."* [5]

Mainly, this objective is covered by Activity 2, and Activity 3. Activity 2 analyses the pilot sites' needs and provides common requirements for the FENIX federation of platforms, while Activity 3 designs the framework under which all these IT platforms will share information among them.

The figure below shows the relation between the different project activities and how the results of each one must serve as input to others. In the case of Activity 3, and more concretely sub-activity 3.1, this has taken much information from sub-activities 2.1 and 2.2, which describe the current situation of the pilot sites and their configuration. Such description starts the definition of the concepts that are mentioned in the current deliverable.

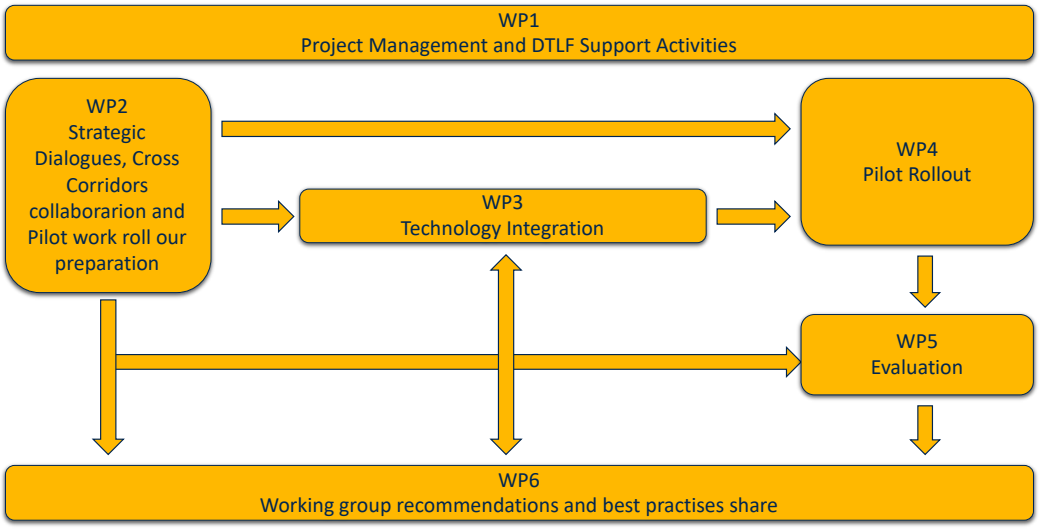

Figure 1. FENIX work packages distribution

This deliverable elaborates the first stage of the definition of the FENIX federation and describes which is the approach to be followed to establish the relations of trust and security between the participant platforms, as well as which will be the mechanisms to execute the information sharing processes between them.

The result of Sub-activity 3.1 will serve as input for sub-activity 3.2, in which all the concepts explained will be further elaborated and specified. Also, this report intends to give a first overview about how the FENIX federation will look like to all the pilots participating in the project and give their first steps in Activity 4.

[5] [FENIX] [Grant Agreement number INEA/CEF/TRAN/M2018/1793401 - CALL 18-EU-TM007-S – ARTICLE 1.3] [Page 24]

3. CONTEXTUAL DRIVERS

Each of project decisions are made in every context, and the description of the technological concept of a federated network of platforms cannot avoid its own context. Based on this, the definition of the FENIX Federated network has to be based on some of the current trends and drivers that are impacting its application domain, and on three different levels: business, digital and policy.

This document just collects a short summary of the high-level concepts that act as context on each of the specified levels. These are not all the exclusive context drivers, but are the ones that may be taken into account when identifying the design principles of the architectures, as well as identifying current best practices and patters regarding concepts like data sovereignty, data sharing at digital level. Other contexts can be the inputs coming from the DTLF and more specifically on the subgroup 2, focussed on Corridor Information Systems. This Group aims to create a common understanding and common solutions for data sharing in supply and logistics that are a basis for innovation and cost reduction, and contribute to societal challenges like safety, security, and sustainability.

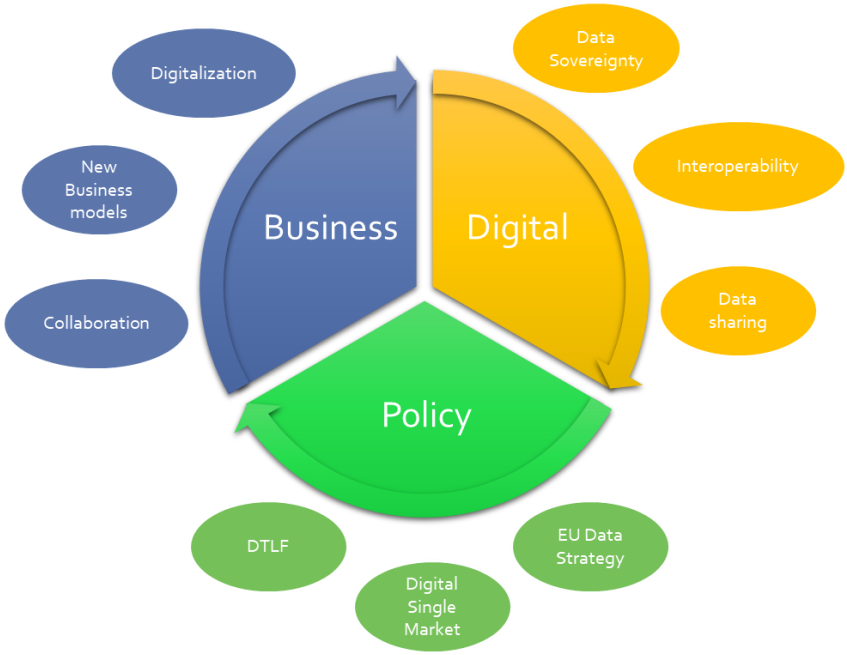

Figure 2: FENIX Contextual drivers in the concept design

3.1 Business Drivers

The following subsection provides an overview of the key business drivers identified in the Supply Chain market.

Digitalisation

Digitalisation or Digital Transformation is considered a key business driver. As stated by the World

Economic Forum "responsible, accelerated and affordable digitisation can facilitated global trade and sustainably reduce poverty"[6]. In addition, according to a McKinsey article, " Smart algorithms may be able to generate faster, more accurate demand forecasts, for example, but executing against those forecasts **requires the combined effort and alignment of hundreds of individuals across the organisation**, each with their own preconceptions, incentives, biases, motivations, and limitations" [7] . It is stated that Digital transformation approaches enhance the access to information, favour the decision making and are more successful than those don't adopt them. The FENIX approach, with the connection of the entire actors of the supply chain, will leverage boost these approaches.

Flourishing ecosystems and new business models

The creation of new business services will support the increase of market share and will promote innovation in the whole ecosystem. A platform federation allows participants to increase their visibility and the visibility of their new services, being available for the rest of the ecosystem in a short period of time and favouring the innovation adoption. According to a report from ARC Advisory Group[8] SCCN market produces " a new market known as SCCN Supply Chain Collaboration Networks has arisen and this produces over $3 billion in annual revenues and is growing at a double-digit rate" according to market research from the ARC Advisory Group.

Enhance security and Trustworthiness

Companies are interconnected and have to do business together. However, security is not anymore a matter of one organisation, as the whole components of the ecosystem should be involved and collaborate on it. The Federation approach followed in FENIX will build trustworthiness among the organisations implementing security and certifications tools that will increase the trustworthiness among the companies, boosting the development of new business.

3.2 Technological Drivers

This section provides an overview of some architectural concepts that are the base of the FENIX concept and explains and differentiates some concepts that are commonly mixed or confused.

---

[6] 5 ways to digitalise logistics and boost trade. (2020). Retrieved 19 March 2020, from https://www.weforum.org/agenda/2020/02/how-the-global-logistics-industry-can-collaborate-to-increase-trade-and-reduce-poverty/

[7] Digital supply-chain transformation with a human face. (2020). Retrieved 19 March 2020, from https://www.mckinsey.com/business-functions/operations/our-insights/digital-supply-chain-transformation-with-a-human-face

[8] Supply Chain Collaboration Networks | ARC Advisory Group. (2020). Retrieved 19 March 2020, from https://www.arcweb.com/market-studies/supply-chain-collaboration-networks

Data Sharing

In a fragmented and collaborative ecosystem like logistics, data is a key element that can be used to increase efficiency in the shipping process. As in other industrial domains (i.e. Industry 4.0, health, etc.) a new design pattern on data sharing or data marketplace has been evolving, including an analysis of roles in data exchange, interactions or flows, data exchange technical protocols, data governance model pattern and more. A short summary of the key current approaches that have been analysed in the context of FENIX network can be found below.

1. **Industrial data space + IDSA reference model version 3**

   "The industrial data space is a virtual space leveraging existing standards and technologies, as well as accepted governance models for the data economy, to facilitate the secure and standardised exchange and easy linkage of data in a trusted business ecosystem."[9] This model was boosted by Fraunhofer-Gesellschaft and it is supported by the German Government with the aim to develop a secure data sharing architecture to foster the creation of new services that facilitate the innovation. Furthermore, the ultimate goal is to obtain the internationalisation of the architecture. Industrial data space is involved at the design and continuous development of the core principles of the IDS Reference Architecture Model (IDS-RAM) for the creation of a secure "network of trusted data". In the picture below, the main strategic requirements and capabilities, that are basis of the reference architecture, can be identified.

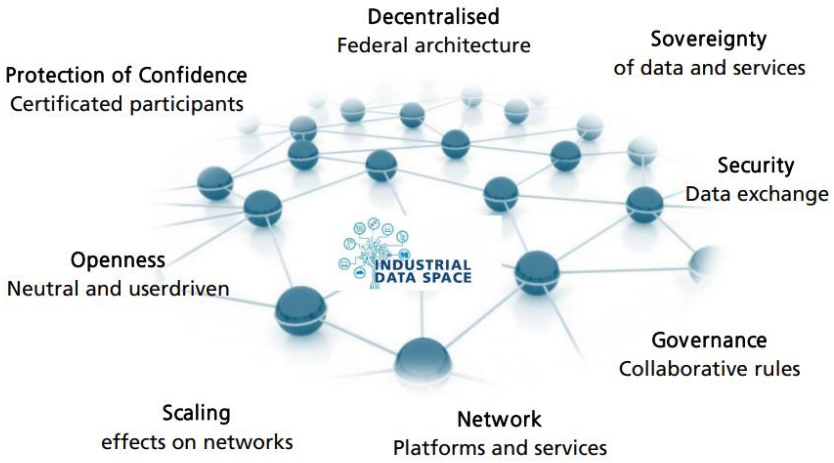

Figure 3. Industrial Data Space. Core Principles. Source: Fraunhofer & Industrial Data Space

[9] *Ids Reference Architecture Model Industrial Data Space*. (2018). Retrieved from https://www.fraunhofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/IDS_Referenz_Architecture.pdf

2. CEF building blocks

The Connecting Europe Facility program CEF was created to support the Digital Single Market to this end. CEF funds reusable Digital Service Infrastructures (DSI) known as Building Blocks. [10] The current building blocks are shown in the figure below:

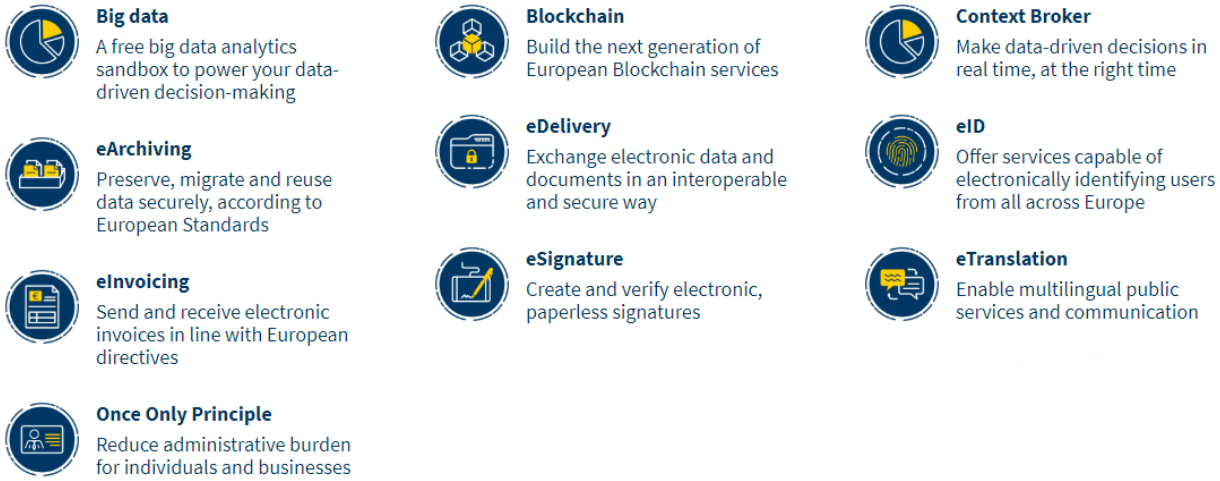

Figure 4. CEF Building Blocks Source: CEF Digital [11]

Among the CEF building blocks, eDelivery is the special interest for the FENIX project. "eDelivery helps public administrations to exchange electronic data and documents with other public administrations, businesses and citisens, in an interoperable, secure, reliable and trusted way" [12]. CEF eDelivery provides the tools to organisations to set up a message exchange solution.

Moreover, one of the uses of eDelivery has been analysed is PEPPOL. OpenPEPPOL's mission is stated as follows: "To enable businesses to communicate electronically with any European government institution in the procurement process, increasing efficiencies and reducing costs"[13]. PEPPOL is a set of tools that allows organisations' cross-border eProcurement. It is governed by OpenPEPPOL. PEPPOL uses the eDelivery Network (CEF Building block) to connect the eProcurement systems.

---

[10] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/The+Vision

[11] **CEF Building Blocks presented at Releasing the Power of Procurement. (2020). Retrieved 25 March 2020, from https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/05/07/CEF+Building+Blocks+presented+at+Releasing+the+Power+of+Procurement**

[12] The Vision. (2020). Retrieved 25 March 2020, from https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/The+Vision

[13] About OpenPEPPOL - Peppol. Retrieved 25 March 2020, from https://peppol.eu/about-openpeppol/

3. From Cloud to Federation of platforms

The concept of federation of clouds and sharing resources has been analysed, however not as a data sharing pattern. In this context, a distinction should be made between Hybrid Cloud, Inter-Cloud and Cloud federation:

- Hybrid Cloud: a cloud architecture that allows a private cloud to form a partnership with a public cloud;
- Inter-Cloud: technical solutions that permit different clouds to be interconnected (as a cloud of clouds);
- Cloud federation: "a geographically dispersed community, where several heterogeneous and autonomous clouds cooperate **sharing computer resources** to achieve a common goal described in a contract."[14] [15]

In a cloud federation two or more networks/solutions/platforms are connected to inter-operate. In a cloud federation hardware resources and data and services can be shared. FENIX is looking to setup a federation of the pan-EU cloud solutions / platforms available in the logistics corridors as follows:

- More focused on data and services (at SaaS level);
- It is expected to support cooperation/interoperability in a trusted and secure environment;
- Not a federation to share IaaS/PaaS resources.

Data Sovereignty

As in most of the business sectors, digitalisation and data is at the heart of this transformation, notably thanks to the mobile & IoT revolutions that enable to connect people and things with business. EU business and SMEs are using or sharing data to develop new services or applications to maintain their leadership and competitiveness. However, they want to increase the control over the data as well as define its usage policies. Based on this, EU policies rely increasingly on data: how data is stored, shared and processed are at the core of the current digital business ecosystems, and concepts like data sovereignty have appeared. In general terms, data sovereignty is used to make

[14] Manno, G., Smari, W. W., & Spalazzi, L. (2012). FCFA: A semantic-based federated cloud framework architecture. *Proceedings of the International Conference on High Performance Computing & Simulation (HPCS)*, Madrid, Spain (p. 42–52). IEEE Computer Society. 10.1109/HPCSim.2012.6266889

[15] Celesti, A., Tusa, F., Villari, M., & Puliafito, A. (2010). Security and cloud computing: Intercloud identity management infrastructure. In Reddy, S. (Ed.), *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE)* (pp. 263–265). IEEE Computer Society. doi:10.1109/WETICE.2010.49

digital information subject to the laws of the country in which such data is shared, processed and stored.

Remove Interoperability barriers

The high fragmentation of the supply chain and the fact that a wide range of SMEs participate in it, turn the lack of interoperability into a main barrier that makes the connection of companies and their services difficult, resulting in the lock-in effect and the increasing the cost for enterprises. The FENIX federation will support organisations to overcome this barrier by interconnecting them and providing tools to seamlessly use the services they offer.

3.3 Policy Drivers

Policy makers are supporting the FENIX concept directly or indirectly. This subsection attempts to show a brief summary of some of these policies and how they support the FENIX concept.

Digital Single Market Policy

The European Commission has promoted the access to an online world for individuals and business. Several initiatives have been promoted, including the **Digitalisation of transport**. In the European Council's conclusions on the digitalisation of transport, the EU proposes the elimination of the obstacles to acquiring a seamless and more effective multimodal transport system in Europe: "BUILDING on the vision of the secure and free movement of data that fosters innovation and reduces the barriers to the seamless functioning of the Single Market and therefore could be considered as a 'fifth freedom' of the European Union " [16].

This is fully aligned with the FENIX federated platform's concept that provides "an European federated architecture for data sharing serving the European logistics community of shippers, logistics service providers, mobility infrastructure providers, cities, and authorities in order to offer interoperability between any individual existing and future platforms" [17].

EU Data strategy

Data is considered the new-oil and it is placed in the centre of the transformation. The EU Commission considers that "The EU can become a leading role model for a society **empowered by data to make better decisions** – in business and the public sector". In the communicated "A

[16]Council conclusions on the digitalisation of transport. (2020). Retrieved 19 March 2020, from http://data.consilium.europa.eu/doc/document/ST-15431-2017-INIT/en/pdf

[17] https://FENIX-network.eu/

European strategy for data"[18], the Commission bases the strategy on four pillars:

- *A cross-sectoral governance framework for data access and use*: one of the key actions planned is the analysis of the importance of data in the digital economy. FENIX' outcomes will serve as inputs for this analysis.
- *Enablers*: investments in data, strengthening Europe's capabilities and infrastructures for hosting, processing and using data, interoperability. The FENIX platform provides both capabilities and infrastructures to reach the expected outcomes of hosting, processing and using data.
- *Competences*: empowering individuals, investing in skills and in SMEs. The FENIX platform will support the innovation in SMEs by building business ecosystems and fostering the creation of new services.
- *Common European data spaces in strategic sectors and domains of public interest*: The European Commission will support the establishment of several common European data spaces. FENIX can clearly contribute to the construction of two of them:
    (1) A Common European mobility data space;
    (2) Common European data spaces for public administrations.

Digital Transport and Logistic Forum (DTLF)

A group of experts in transport and logistics, "DTLF supports the EU strategy for an internal market for transport". DTLF was established by DG MOVE and places its policy context in the following European Commission's initiatives and policies:

- White Paper on Transport, 2011;
- Digital Single Market Strategy, 2015;
- ICT Standardisation Priorities for the Digital Single Market, 2016;
- eGovernment Action plan, 2016-2020;
- European Interoperability Framework Strategy, 2017;
- European Parliament Resolutions, Jan & May 2017;
- Tallinn Digital Transport Days, Nov 2017;
- Conclusions on the digitalisation of transport, EU Council of Ministers, Dec 2017;
- Commission Decision C (2018) 5921 of 13 September 2018;

[18]A European strategy for data. (2020). Retrieved 19 March 2020, from https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

- Horizontal rules on the creation and operation of Commission expert groups C (2016) 3301 of 30 June 2016.

The DTLF recommended that, since the logistic sector is highly fragmented and composed by a wide range of SMEs, public institutions should take the initiative in boosting the creation of the logistic federative platform. This DTLF recommendation is the foundation of the FENIX Project.

The DTLF establishes the objetive of using data sharing as a commodity, based on the following principles:

- *Plug and Play* : each end user can connect to his/her platform and the federative platform provides the required services.
- *Technology independent infrastructure services*: The services provided for the commodity platform are technology independent.
- *Trusted*, *safe and secure* : The federated platform should be trusted, safe and secure and accesable only by authorised users. Furthermore, data integrity is properly assured.
- *Federation*: network of platforms and peer to peer solutions. The federation connects different platforms , which are able to use inter-connected services and share data.

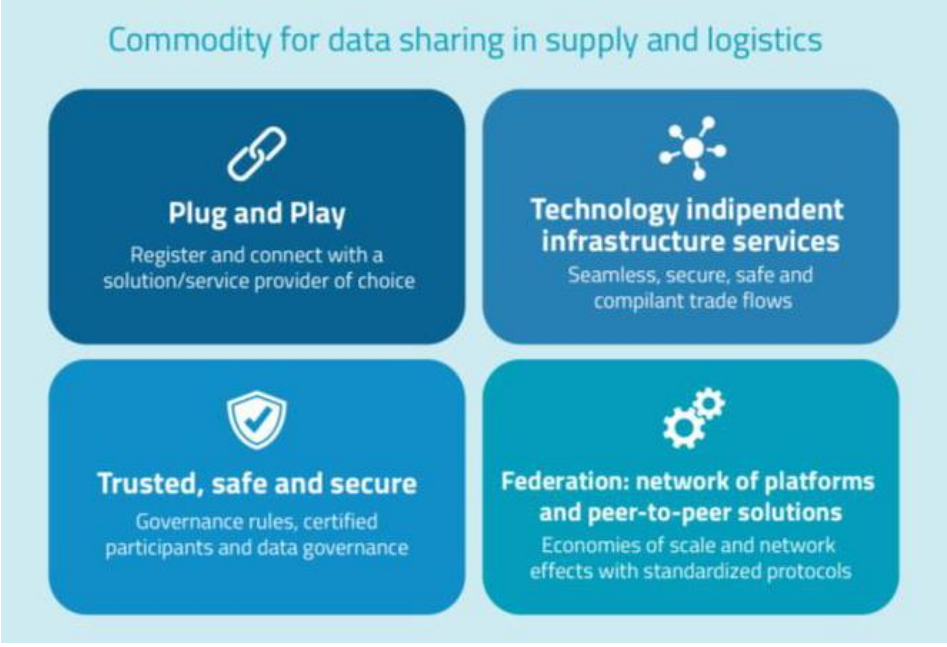

Figure 5. Commodity for data sharing in supply and logistics Source: DTLF

4. FENIX Network design principles

Federation stems from the Latin words *foedus* and *foederis*, which both mean treaty, agreement, and contract. In most cases, if the term federation is used, it refers to combining autonomously operating objects. For example, States can be federated to form one Country, or companies can operate as a federation. According to businessdictionary.com[19], a federation is an organisation that consists of a group of smaller organisations or companies that works to bring attention to issues that are of importance to all of its members. Each organisation that comprises the federation maintains control over its own operations.

In logistics, its own configuration for the physical movement of the goods, implies that at organisational level it is implemented by many different actors due the highly fragmented market. This means that at technological or IT infrastructure level, these actors deploy different types of solutions, such as Transport Management Systems, Terminal Operation Systems, Booking systems, Port Community Systems, Forwarding IT systems, etc., according to its role (authorities, PCS, freight forwarders, warehouse terminal, shippers, etc.). These systems generate or consume different types of information (automated of manual information), and following the business processes, they need to interact between themselves to exchange information. This collaboration and information exchange has been either difficult or slow to achieve, but in the latest years, service providers and actors in the chain have been collaborating to deploy their own data platforms or information systems to support these type of activities, facilitating the integration with external systems. This enables the data sharing between partners and addresses different interoperability issues. In fact, different approaches in logistics have derived either in the deployment of bilateral agreements or in interfaces to share data. Others have derived to join a community ecosystem, which is the case of the with Port Community System (PCS) or Business Community Systems (BCS), or, finally, to join a proprietary information system or platform owned by a dominant player. Some of them, such as PCS or BCS, have addressed some data sharing aspects in concrete stages of the supply chain, or in other cases, has been based on access points or service oriented architectures using standards to address the integration of systems. However, there is lack of interoperability among them at different levels (semantic, business, technical, etc.), which adds complexity (and cost) to the ecosystem when visibility is needed for the complete movement of the goods along a corridor.

[19] http://www.businessdictionary.com/definition/federation.html

Considering the analysis of the pilot needs described in FENIX Activity 2 reports (like D2.2.2) together with the proposition of the DTLF for a federation of decentralised information exchange platforms and peer-to-peer solutions (where organisations and authorities implement functionality of their systems themselves[20]), FENIX activity 3 proposes an ecosystem in form of a federation of platforms to address data sharing between them in the supply chain.

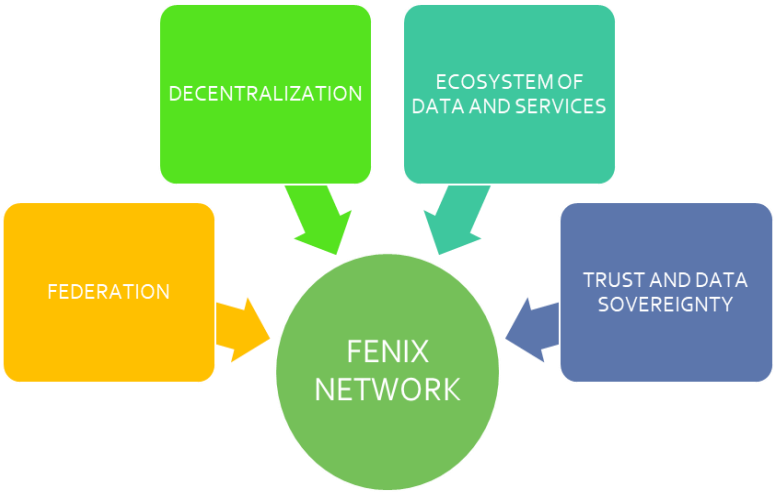

Figure 6: FENIX network design principles

The approach followed in the development of the FENIX Network Architecture considers federation and the following strategic features and requirements of its core framework, as depicted in figure 4 and in alignment with the DTLF design pattern and industrial reference architecture state of art.

Decentralised approach. The design of the FENIX architecture does not rely on a centralised platform or software approach supporting central data storage or management, which is currently a constraint for platforms and logistics stakeholders. All the platforms that are part of the federation are considered nodes of the network and always retain their internal control. This means that all data remains in its stakeholder platform of choice, and the FENIX network should focus on providing governance mechanisms (technological, legal and business) to enable a federation of trusted platforms and services to support their engagement, monitoring and allowing decentralised access control and exchange to data or services provided by each platform. This decentralisation approach

[20] Enabling organisations to reap the benefits of data sharing in logistics and supply chain Executive summary of the final report https://sharepoint.dtlf.eu/SG2%20Meetings/1.%20SG2%20Meeting%20-%2012%20April/3.%20Supporting%20documents_%20DTLF_%20SG2%20Final%20Report%20Executive%20summary.pdf

supports the re-use and connection of the current platforms, solutions and services provided by the parties, enabling the exchange of information through a service layer without any intention to replacement of the existing system functionality.

Trust & Data Sovereignty. Trust is essential for digital services. Logistics actors will not embrace digital services if they don't trust that their data will be protected. Data sovereignty means maintaining authority and control of data within jurisdictional boundaries. Trust is the at the basis of the FENIX IT Framework, which should provide guidelines to ensure the trustworthiness between the federated platforms and support data sovereignty. Together with other security aspects, such as secure communication between nodes of the network, data sovereignty is essential for data security. FENIX provides specifications and governance to federated platforms, without granting access to them.

Ecosystem of Data and Services: FENIX is composed of platforms, data assets and services. The data and services are made available for secured consumption or sharing via the federated network. As appointed in one of the principles, FENIX network is in form of a federation, where the main common functionality is to enable data sharing between individual platforms, which will be created by means of common (platform interoperability) protocols to support data sharing services. Stakeholders can communicate with their platform provider of choice. This provider is held to relevant trust, security, and performance standards by the authorities and FENIX specifications, coordinating with the rest of the network. In this area, data usage policies should be taken into account by the networked platforms functionalities and its link to the protocol supporting the data sharing.

FENIX Federation network is a secure data sharing framework in the form of a federation, where there is not a centralised entity owning the ecosystem, and where all the participants of the federation have the same rights and obligations and follows the federation governance.

Based on the definition provided above, the federation governance is key to stablishing the federation goal, the governance model, the regulation and rules of the ecosystem that all participants of the federation must accept. The governance must include the definition of roles and responsibilities in the federation network. One of the aspects to be considered is how to support the involvement of a new platform into the federation. This on-boarding process should be guided and aligned with the governance model and must include an authentication mechanism where the new

platform must get a digital certificate to participate in the network. Such certificate must come from a certified authority , following the rules and regulations specified in the governance model, which will be detailed in activity 2.5.

Moreover, based also on these design principles, the FENIX network should support the federation requirements depicted in Activity 2. From the analysis of existing platforms, the following expected requirements can be extrapolated:

- The platform must support multiple and heterogeneous data sources.
- The platform should enable communication among the different services.
- Data privacy and user pseudonymisation must be respected.
- To use the data, the consumer must fully accept the data owner's usage policy.
- Based on the decentralisation principle, it requires a comprehensive description of each data source and the value and usability of data for other companies, which needs to be complemented with a broker functionality to provide services for real-time data or discovery of services.

Based on these previous principles and aligned with the depicted requirements on D2.2.2, the design of the FENIX Network architecture is focussed on the provision of a specification of a connector, following reference architecture data sharing concepts which respect the decentralisation of the ecosystems of platforms. These concepts should also focus on the description of the technical roles and specification of a few functionalities that are needed to be federated and must respect the following design principles:

- **Identity Management** – to ensure the identities of the participants of the federation and the authentication of identities. The objective of this feature is to allow the exchange of identities between the nodes of the platform to guarantee the access to the right service or data asset.
- **Broker** – search and discovery service of a distributed catalogue of services and data available in each of the federated platforms in the network. The functionality should allow federated entities to discover which logistics services or data are offered by each of the platforms and providers, based on a harmonised data and service description metadata model.
- **Data exchange** – as the degree of global collaboration grows, and multi-tiered nature of today's supply chain, the supply chains become increasingly complex. Data sharing between

stakeholders is a key activity for each of them. There is the challenge to achieve the ability to connect and share information between the different logistics data platforms with the rest of the business federated ecosystem.

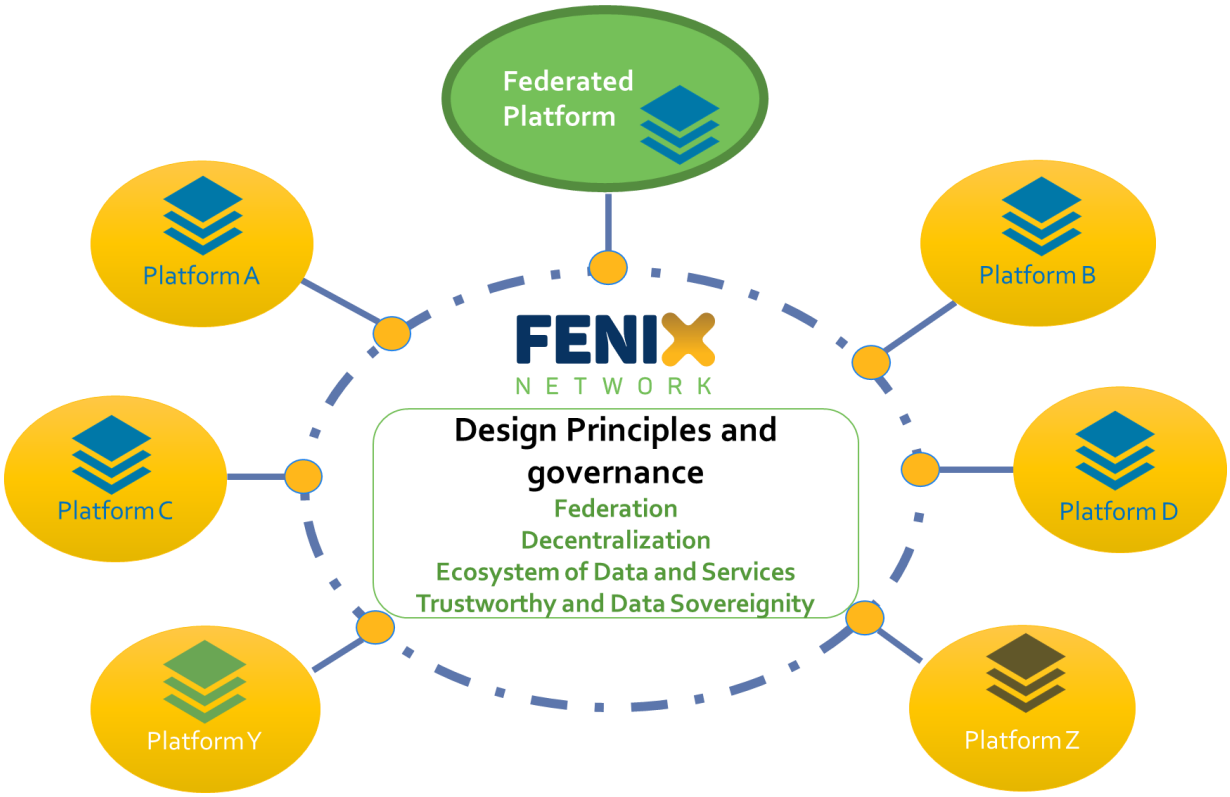

Figure 7: FENIX architecture concept based on design principles

Figure 7 provides an overview of the FENIX Federation network of platforms. It depicts the main federation design principles in the middle of the picture, and the different platforms (different circles) that share data with each other following the principles. Each of these platforms has as well its own datasets or services (i.e. ETA service, planning service, CO2 footprint, IT services, etc.) and the federated services specified in FENIX (identity management, broker and data exchange) are represented as the small circles linked to each platform of the federation.

The following chapters provide a vision of how these framework principles and functionalities are considered to identify the main technical roles involved in the architecture concept design for the FENIX Network.

5. FENIX IT Architecture vision

In a world where data is one of the most valuable existing assets, there are plenty of different systems and platforms that generate, share and move huge amounts of this data. Despite the rapid flow of data, there are many inconveniences that do not allow to access it to improve business, in this case, in the logistics domain. Data is stored in many servers and with its own format. Much of it can be standardised or not. Many of the actors involved in the logistic business could benefit from the access to specific data.

The main vision of FENIX is to be able to create a federated network of platforms through which all the actors involved can discover already existing data or services that may help them to improve their daily operations and business while keeping their data under their own control. From a technical point of view, the objective of the FENIX Federation is to put into touch to all those platform providers that are interested in sharing information and having to make very large integrations within their operational systems. The aim is to access other information that, commonly, would be very difficult to get otherwise.

The idea of such a federation sounds like the solution of all the problems. Nevertheless, experience shows that there have been and there will still be some barriers that need to be overcome for this concept to work.

At a first stage, it is important to stress that not all the platforms are technically aligned. This means that all the platforms are different, not only in the functionalities that they provide to their users, but also in their implementation and design. For instance, platform A can be accessed through a perfectly structured identity management system, with a very well-defined hierarchy of users and roles, while platform B cannot even have a user management system due to its specific requirements.

Another example can be the case in which one platform already shares information among its members, having a good and defined data governance process. However, it is possible to have a platform that only generates information, without sharing it among others. These concepts are not technically aligned because the needs to be covered by these platforms are not the same.

Security mechanisms, data management, and a quite long list of other reasons are enough to know that, if a Federation of Platforms wants to be created, some guidelines must be provided to reach

the minimum technical requirements to join the federation and benefit from it.
The FENIX Federation network is being designed taking into account all the needs from the different systems and platforms. The union to the federation must be a process achievable by all kinds of parties. This union shall be possible with small efforts, technically and economically speaking. This being said, the expansion of the federation will be ensured.

Having all these premises in mind, it is possible to find in the next subchapters how the conceptual design of the FENIX Federation is being elaborated. The following chapters explain the concept and the way that its implementation is being thought. In this chapter, the reader will see which will be the main roles for the federation participants, the operations that will be covered and a technical proposal to succeed in this task.

5.1 Logical view of FENIX Federation

FENIX represents a virtual network formed by different platforms aiming to share information between them. To be part of this community, all the players must participate under the same conditions, in terms of technical infrastructure (providing some minimum capabilities to join the federation), security, privacy policies and data sovereignty.

Each platform in the market is built differently. Platforms can provide similar or the same functionalities, data exchange or services provision but, in their core, they will be different. This is what the FENIX Federation tries to achieve. This is a common way to put all these platforms together and allowing the information to be exchanged among members in a common way and with a common language.
To succeed in this purpose, FENIX must provide guidelines that every member must follow to become part of the federation: this will allow the platform to be comprehensible and understandable. Every platform must implement a communication mechanism dealing with the rest of the platforms in the Federation.

That is what is described in the Figure below. Each platform becomes a node in the FENIX Federation. To access to the Federation resources, every node must implement a Connector, which will provide the needed mechanisms to access those resources provided by the rest of the members, and must be able to provide its own to the Federation.

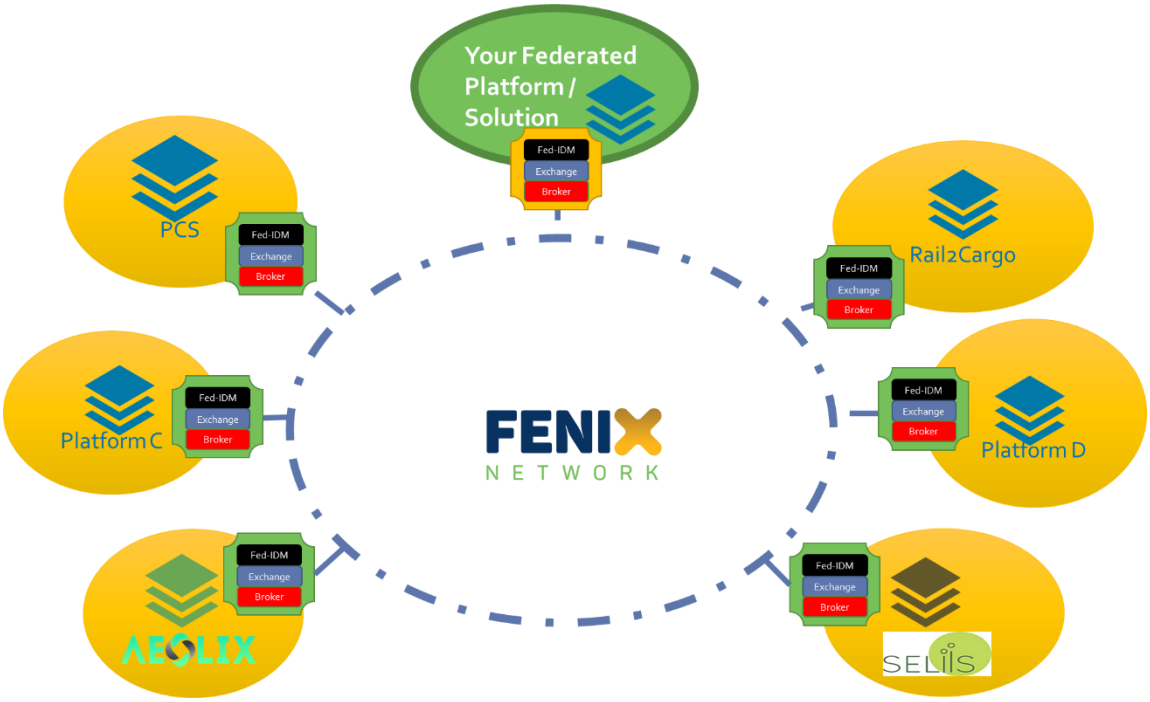

Figure 8. FENIX Federated Network

The FENIX Connector, which will be deeply explained in subsection 6.4, will deal with all the functionalities requested to a federation like FENIX: Identity Management and validation of each of the FENIX members, provision of resources information along the network through different operations and data exchange capabilities to interact and share information between participant platforms.

5.2 FENIX Roles

A starting point for the specification of the FENIX Network is to identify the different actors and roles involved in the interactions and functionalities around the ecosystem of the federated network of platforms. Together and aligned with activity A2.5 FENIX Governance, the identification of all actors (user roles), which are expected to interact within the FENIX Federation and are therefore requesting functionality, will provide the needed input for the user stories and use cases. For the definition and implementation purposes of FENIX, the list below outlines the different users and roles, as well as the relations that exist between them. These can be classified in three different categories:

1. General roles: These roles are the ones related to the actors involved in the data exchange.

- **Data Owner**: the legal organisation or individual that creates the data, has control over it and is responsible for its accuracy, integrity, and timeliness. The Data Owner

can setup data usage policies and conditions to its datasets. The Data Owner has control to grant or revoke access to its datasets to the interested entities.

- **Data User**: the legal organisation or individual that has been granted the use of the data provided by the data owner according to the agreed data usage policies.
- **Data Provider/Service Provider**: serves as information intermediary in the data exchange operations for the data owner. Provides functionalities to the data owner to facilitate the data exchange with the interested entities and monitors the different exchange transactions. Data Owners can combine their role with the role of the data provider.
- **Data Consumer**: as in the previous role, serves as information intermediary at the consumption side of the data exchange to facilitate the information to the data user. He/she also provides functionalities to the data user to monitor the transactions and may offer data services to extract value from the data received according to the data usage policies. The Data User can combine its role with the role of the Data Consumer.

2. Platform roles: In the context of FENIX, the platforms identified in the project may act usually as Data Provider and Data Consumer roles. These roles have as well some specific related roles to specific functionalities that may be assumed by the platform itself or by related trusted organisations. These platform roles are:

- **Identity Manager**: is an identity broker that is responsible for asserting digital identities with claims for service providers to consume. He/she is in charge of managing all the access rights to the resources of the platform and provide a secure and valid access token to the different resources, data, services or users that will be part of the platform. The Identity Manager can grant or revoke access to every kind of users, services or applications within the security environment. Two differentiations to be considered in the context of FENIX:
  - A **resident identity provider**[21] is defined with respect to a digital identity. The identity provider is responsible for asserting the digital identities within its trust domain. Sometimes this is also referred to as local identity provider or incumbent identity provider.
  - A **federated identity provider**[20] is defined with respect to a trust domain and is responsible to assert digital identities that belong to another

[21] https://wso2.com/articles/2018/06/what-is-federated-identity-management/

particular trust domain. A trust relationship is established between the two identity providers.

- **Broker Manager**: is responsible for advertising a catalogue of service or data offerings and service plans from the data owners and service providers, providing metadata information regarding the resources available. Its main functions is to allow data owners or service providers to register and describe their resources (data or services) in a catalogue based on a common metadata description model. Other functions allow the data user and consumers to be offered a discovery service of these resources according to the common metadata description model.
- **Monitor Manager**: Is in charge of offering logging services that allow the storage of data regarding operations, such as data exchange transactions. Personal information and personal data are never transmitted. The Monitor Manager is in charge of gathering usage information for different purposes (clearing, maintenance, audit and billing) and to maintain the platform in an optimal operational way.
- **SW**, **Tools & Service Provider**: this role is assigned to the entities that offer services, applications or tools to the participants of the platform, and who take advantage of the data or services available and offered in the platform.

3. FENIX Governance roles:

- **FENIX Federation provider** is an organisation which specifies the governance rules of the eco system. This role is one of the main contributions of FENIX to the data sharing ecosystem, as it is in charge of establishing the rules and regulations of the federation network of platforms. Full specific details of the rules and regulations of the federation will be defined in the governance model at Activity 2.5.
- **Certification Authority**: is a trusted entity that issues Digital Certificates and public-private key pairs. One of its missions is to guarantee that the individual who owns and granted the unique certificate is who he or she claims to be. A Certificate Authority can be a trusted third party which is responsible for physically verifying the legitimacy of the identity of an individual or organisation before issuing a digital certificate. It is a critical security element in a network as it is in charge of verify the identities, issue digital certificates, validate them and maintain a revocation list.
- **Evaluator/Auditor:** Is in charge of providing evaluation facilities to monitor that platforms of the FENIX network are compliant with the technical, legal and business terms and conditions of the trusted FENIX network of platforms.

6. FENIX Network of platforms

As stated in the previous chapters, the FENIX Network of platforms will provide a specification that allows each of the interested platforms to connect between them. It is very important to understand the needs and requirements of the platform providers, understand which is the current situation and how they need to make use of the FENIX Federation. Most of this information comes from Activity 2 of the project but, in order to align both business and the technical views, some business user stories have been described in the current document. Such stories will take place in some of the pilot sites and explain how the FENIX Federation will be used. Besides, and from the FENIX Federation point of view, all the User Stories have been defined to fully understand the behaviour that the Federation must have. The methodology requires to start from these user stories and get gradually more in detail in the analysis and design by extracting all the necessary use cases that may be part of each user story.

After the identification of all the use cases, they will be described in detail to have a whole overview of the functionalities that must be enabled through the FENIX Federation and its connector.

6.1 User stories

The current subchapter describes, on the one hand, some user stories related to business cases that shows how the FENIX Federation is needed and how it will be used to cover these business needs, and on the other hand, the user stories that have been identified to be covered by the federation. This will lead to a better understanding on the operations that will be enabled through the FENIX Federation.

6.1.1 Business User Stories

The Business User Stories below describe examples of processes that will occur in across several of the FENIX pilot sites and use cases. They are included here merely for the purposes of clarification of the impact from business user stories on the technical requirements for a federative network as implemented within the FENIX project. The idea behind specifying these business use cases is to identify the need of being part of a federation of networks like FENIX to get or share the missing information that can be helpful to improve stakeholder's daily operations. Both business use cases show how these operations would look like by being part of FENIX.

During the project, implementation of aspects from the Business User stories may differ from the exact details, as described below.

User Story: F-BUS-01 ***Title:*** *Partner accesses data service to* ***GET*** *data from the service (e.g. ETA for single mode of transport / transport movement)*

Description

> Logistics Context

- Stakeholder wants to receive ETA (Estimated Time of Arrival).
- In this Use Case a truck executing a specified trip plan for a specific shipper.
- The estimated time of arrival is calculated according to the given transport plan. During the transport execution, the truck OBU (On-Board Unit) or transport unit device ("smart container") will continuously provide geo-position information to the ETA Data Service Provider (DSP).
- The ETA service uses this information to (re)calculate the ETA.
- The ETA service (or shipper) may share this ETA information with other authorised stakeholders.
- When the transport movement finishes, the ETA calculation/s will stop.

>Preparations:

- A shipper wants to transport goods in a container from A to B.
  The shipper requests the LSP (e.g. Jan de Rijk)) to perform the transport.
- The LSP provides the shipper with the transport plan (trip).
- The shipper agrees to transport plan suggestion and reference id is created.

> Pre-requisites:

- Data Service Provider (DSP) and Data Service User (DSU) have exchanged relevant data (reference ID and trip information such as starting location and destination location; preferable using unambiguous global data standard ID Keys) before the request for ETA calculation is sent from DSU to DSP.

> Operations:

1. Truck departs from starting location and sends departure confirmation to ETA DSP using the FENIX network (and FENIX connectors).
   Must use the relevant Reference ID Key for the trip plan.
   In effect, the first *Request* to calculate the ETA for this transport movement.
   Format agreed between ETA DSP and ETA DSU.
2. ETA DSP calculates first Estimated Time of Arrival (ETA) based on starting location and route to destination location.
3. ETA DSP returns the calculated ETA to the ETA DSU in *Response* to the *Request* using the FENIX network (and FENIX connectors).
   Must use the relevant Reference ID Key for the trip plan (may use Request ID also).
   Format agreed between DSP and DSU.
4. ETA DSP or DSU (e.g. Shipper) may choose to also notify other relevant stakeholders.
   They may use the FENIX network (or choose other means for that information exchange).
5. During the actual movement along the route planned for this transport movement,

the truck (or transport unit) sends multiple requests to recalculate the ETA to the ETA DSP based on the actual geo-position transmitted in the Request.
This and the following steps (up to and including step 10) iterate for each of the recalculation requests sent to the ETA DSP.

6. The truck sends the recalculation request using the FENIX network (and FENIX connectors).
   Must use the trip plan Reference ID Key and geo-position (preferably using global data standards). Request format agreed between the DSP and DSU.
7. The ETA DSP recalculates the ETA based on the actual geo-position and the destination location (taking trip plan details into consideration).
8. The ETA DSP may change the route to be followed based on various conditions (e.g. traffic, weather and road works). TO BE CONFFIRMED.
9. The ETA DSP will send a new ETA to DSU in response to the Request for recalculation.
   Must use trip plan ID Key (and may use Request ID).
   QUESTION: How does one deal with a change in the ROUTE?
10. The ETA DSP or DSU (Shipper) may choose to share the new ETA with other stakeholders.
    They may use the FENIX network (or choose other means for that information exchange).
11. When the truck arrives at the destination, the truck (or transport unit) will send the confirmation of Arrival to the ETA DSP using the FENIX network (and FENIX connectors)
    Must use trip plan ID Key.
12. The ETA DSP will cease to calculate new ETA for the trip / transport movement.
    May respond to further request to recalculate with appropriate (error) message.

Table 1. F-BUS-01 ***Partner accesses data service to GET data from the service***

User Story: F-BUS-02 ***Title:*** *Partner accesses data service to* ***WRITE*** *data into the service database*
Description **> Logistics Context** • Two logistic operational sites aim to exchange data/information between them within the FENIX context. • Among others, they will transport intermodal containers (identified with BIC codes) coming from a multi modal hub to a maritime port or vice versa. • These containers are moved under Customs bond (pre-cleared in the multi modal facility if shipped out of Europe from the port; the clearance is postponed until a multi modal hub for containers imported into Europe via the port). • The two sites will exchange information using the FENIX connectors that each will develop as part of the FENIX project. • For this User Story we will look at the Use Case where an intermodal container is loaded in the multi modal facility (under Customs bond) on a train taking the container to a port.

> Pre-requisites:

- Both, the multi modal hub and the port have a platform to manage their data.
- Both platforms are validated in the FENIX Governance provider.
- User from the multi modal hub already has the data service information he wants access to.

> Operations:

1. The Multi Modal Hub's IT system provider decides to use the FENIX network (using the FENIX connector).
2. The Multi Modal Hub's IT system will retrieve the service description though the broker.
3. The Multi Modal Hub's IT system will invoke the service through the FENIX connector for the relevant data service from the Port's platform to inform that the system of the fact the container has been loaded.

4. The FENIX connector of the Multi Modal Hub's platform will establish the link with the FENIX connector of the port's platform.
   The two sites may already be linked (e.g. as a result from a previous data exchange).
5. The port's FENIX connector will then process the API invocation further to determine the exact data service that this API needs to be routed to.
6. The data service invoked then receives the API invocation through the port's FENIX Connector. The FENIX connector will be able to identify the incoming request and check if the requestor is allowed to make use of this service or not.
7. Assuming the Multi Modal Hub's IT system is authorised to invoke the service, the data service from the port will process the request and ensure the data transmitted is securely stored in the relevant port's IT system/s.

Table 2. F-BUS-02 ***Partner accesses data service to WRITE data into the service database***

6.1.2 FENIX User Stories

This chapter collects the FENIX User Stories around the FENIX Network of platforms. The user stories are focused from the platform perspective which, in the end, will be the one interacting with the federation of platforms.

Once the user stories are defined, they will be translated into several use cases, which will lead to the identification of more detailed needs, not only from a business point of view but also from a technical one.

User Story: F-US-001 ***Title:*** On Boarding
Description
A new platform provider wants to join the FENIX Federation. This user story defines how the on boarding process must be both, from the new platform provider perspective and from the FENIX Federation perspective.

Table 3. F-US-001 On Boarding

In the scenario of the current user story, the involvement of three different actors has been identified:

- Platform X: The platform provider that wants to join the FENIX Federation.
- Platform Governance Provider: The FENIX governance body in charge to decide if it is possible for the new platform to join the federation and provide the mechanisms.
- Certification Provider: The body in charge of generating the Certificates for the new platform.

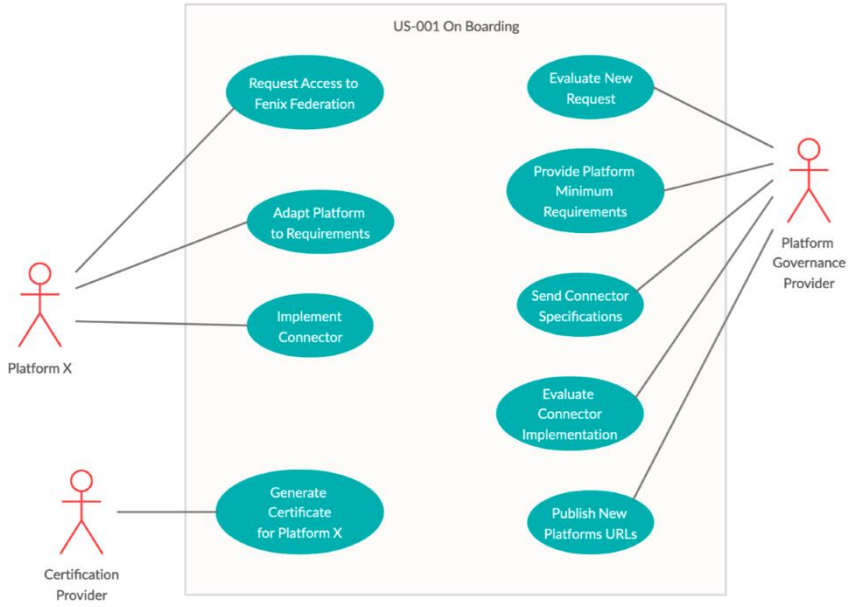

Figure 9. F-US-001 On Boarding

User Story: F-US-002 ***Title:*** Search Available Resources in the FENIX Federation
Description One of the advantages to join the FENIX Federation is that every partner belonging to any platform that is part of the federation can access to all the available resources. To be able to access or share information through the FENIX Federation, it is necessary to know which are all the available resources from all the Federation Members. In this case, the platform will request the catalogue of resources and, through its platform connector, it will receive all the information available along the federation.

Table 4. F-US-002 Search Available Resources in the FENIX Federation

In the scenario of the current user story, the involvement of many different actors has been identified:

- Platform X: Wants to know available resources in the FENIX Federation.
- IDM Platform X: Is in charge of managing the identity of the platform X.
- Broker Platform X: Is in charge of making the resources discovery in the Federation.
- Platform Y…N: Sends its available resources.
- IDM Platform Y…N: Verifies the request of resources from the origin and provides the identity of each platform with their certificates.
- Broker Platform Y…N: Receive the resource request and sends it back to the requestor platform.

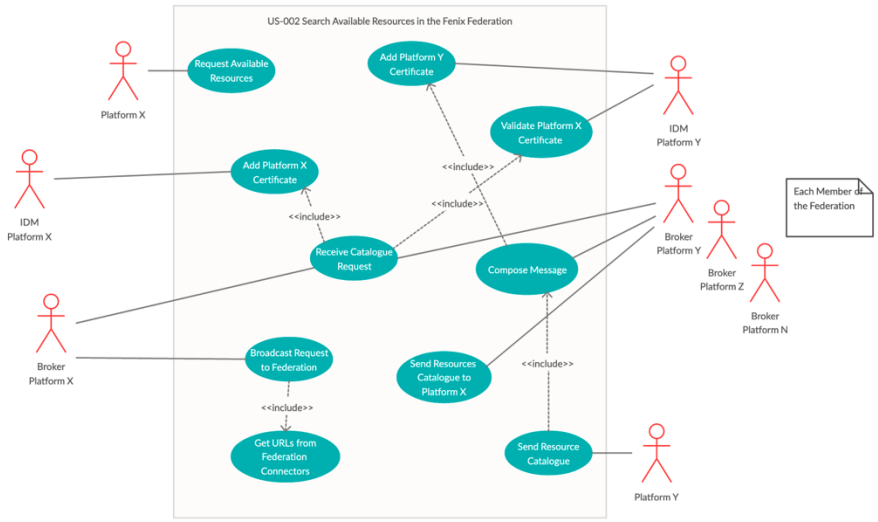

Figure 10. F-US-002 Search Available Resources in the FENIX Federation

User Story: F-US-003 ***Title:*** Request Access to Resource in the FENIX Federation
Description
This user story describes how a member of a platform X that belongs to the FENIX Federation can request access to make use of a resource from another platform Y that is also part of the FENIX Federation. In this case, Platform X has already received the list of available resources in the Federation. It has chosen those that can help to develop its business and now, the platform member must request access to use the resource. On the other side, the resource owner must receive, through the Connector, the platform X's request, evaluate it and accept or reject it accordingly.

Table 5. F-US-003 Request Access to Resource in the FENIX Platform

In the scenario of the current user story, the involvement of many different actors has been defined:

- Platform X: Wants to access to some resources in the FENIX Federation.
- IDM Platform X: Is in charge of managing the identity of the platform X.
- Broker Platform X: Is in charge of requesting access to resources in the Federation.
- Platform Y: Receives and accepts/rejects the access to its resources.
- IDM Platform Y: Verifies the request of resources from the origin and provides the identity of the platform with its certificates.
- Broker Platform Y: Receives the resource request and sends it back to the requestor platform.

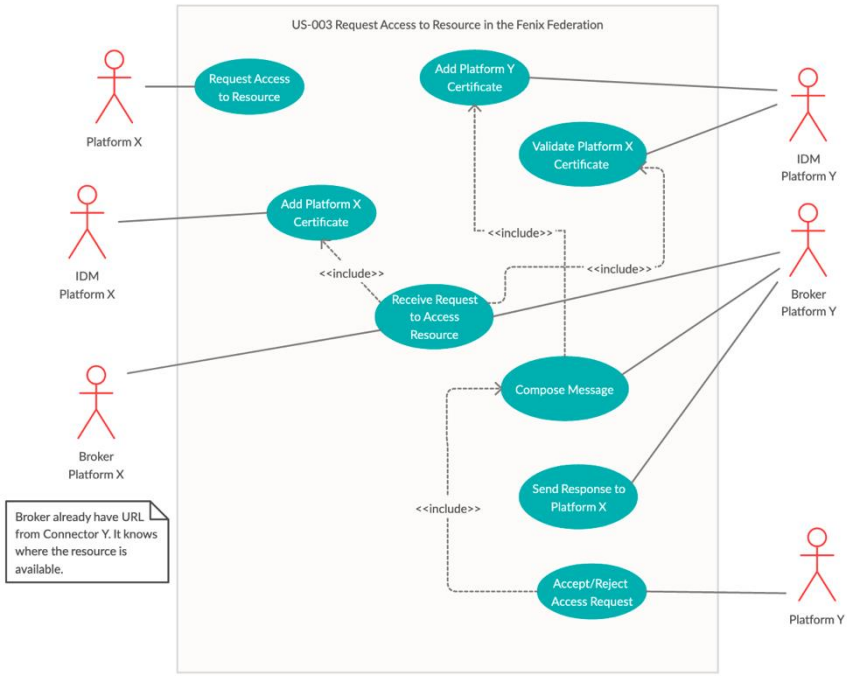

Figure 11. F-US-003 Request Access to Resource in the FENIX Federation

User Story: F-US-004 ***Title:*** Send/Receive Data through FENIX Federation
Description
In this User Story, the member in Platform X has already received permission to access a resource from platform Y. In this case, there are two main operations that the member from Platform X can perform: publish data or receive it, depending on the type of service for which access has been requested. Therefore, the user story will cover both of the cases, the one that publishes data to a resource and the one that the platform member subscribes to a resource to receive data.

Table 6. F-US-004 Send/Receive Data through FENIX Federation

In the scenario of the current user story, the involvement of many different actors has been defined:

- Platform X: Wants to send and/or receive information through some resources from the Federation.
- IDM Platform X: Is in charge of managing the identity of the platform X.
- DXC Platform X: Connects with other Data Exchanges so information can be sent and received through it.

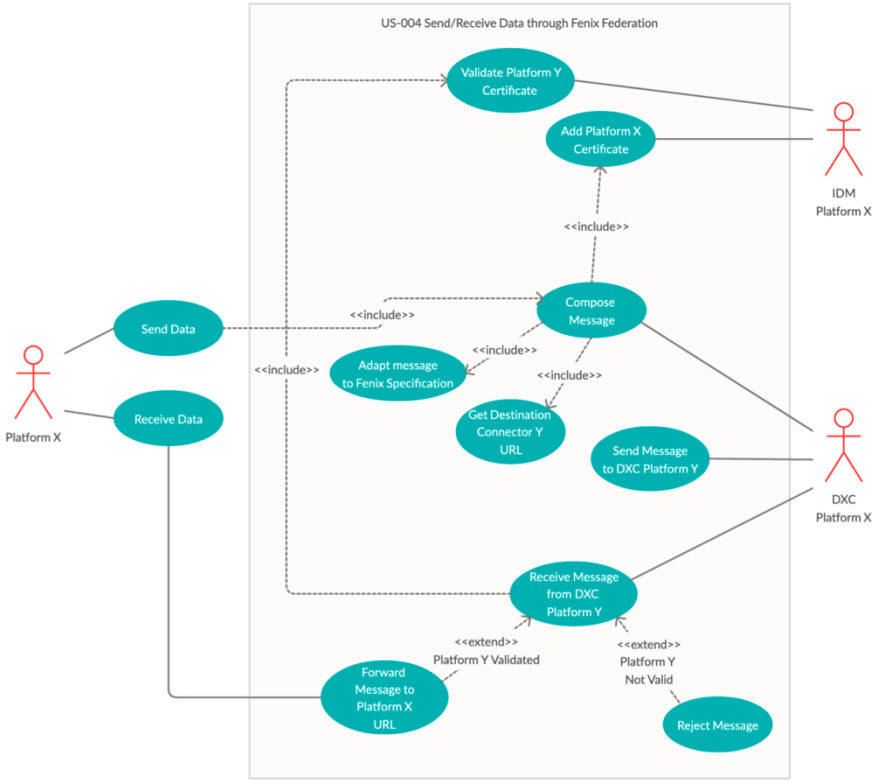

Figure 12. F-US-004 Send/Receive Data through FENIX Federation

User Story: F-US-05 ***Title:*** Grant/Revoke Access to Resource in the FENIX Federation
Description
The current user story explains the case in which a platform member wants to grant access to one of its resources or, in case the resource is already granted, the platform member wants to revoke the access for whatever reason.

Table 7. F-US-005 Grant/Revoke Access to Resource in the FENIX Federation

In the scenario of the current user story, the involvement of many different actors has been defined:

- Platform X: Wants to revoke access to one of its resources from another platform Y.
- Broker Platform X: Is in charge of notifying the revoke operation to platform Y.

- Broker Platform Y: Is in charge of getting the notification that access to a resource has been revoked by platform X.
- Platform Y: Receives the notification that access to a resource has been revoked.

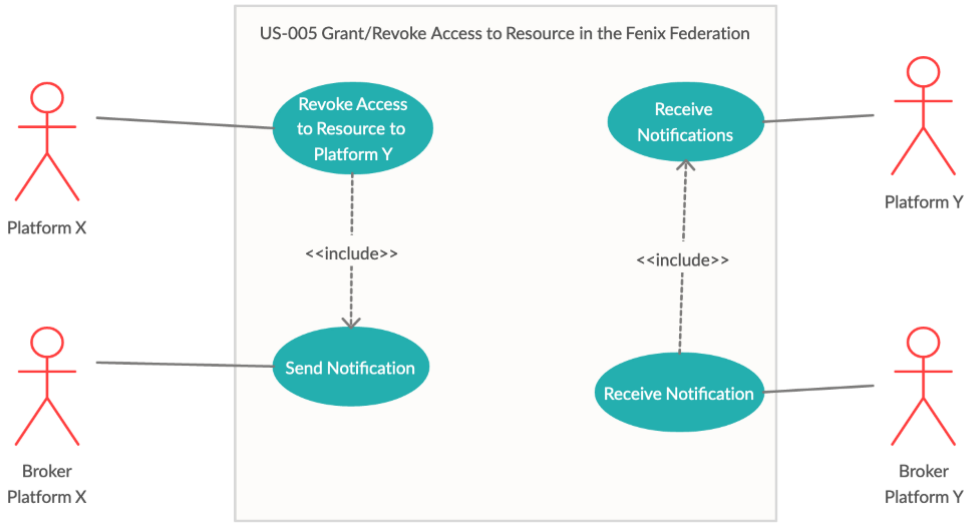

Figure 13. F-US-005 Grant/Revoke Access to Resource in the FENIX Federation

6.2 Use cases

In relation with the previous chapter, this section focuses on the description of each of the use cases identified in the different User Stories. These use cases correspond with the functionality that must be covered by the FENIX Connector specification and that are different from the use cases described by the pilot sites. The use cases are identified as tables containing the following information:

- **Related US**: Defines in which User Story diagram the use case has been identified. This does not mean that each use case is unique for one US. The use cases are unique and can appear in several User Stories but they will be described just once.
- **Description**: Describes the purpose and behaviour of the use case.
- **Actors**: Describers which are the actors involved in the operation of that specific use case.
- **Pre-conditions**: The requirements that need to be completed for the use case to take action.
- **Steps**: Describes the sequence of operations that will be performed during the execution of the use case.

UC-001 Request Access to FENIX Federation
Related US: Table 3. F-US-001 On Boarding
Description: A platform provider wants to join the FENIX Federation.
Actors: Platform Provider

Pre-conditions: N/A

Steps:

- The platform provider accesses the FENIX Network web page;
- The platform provider looks for the application form to join the FENIX Federation and compliments it.

Table 8. UC-001 Request Access to FENIX Federation

UC-002 Evaluate New Joining Request
Related US: Table 3. F-US-001 On Boarding
Description: How to validate and accept a platform as part of the network (according to governance rules) The FENIX Governance Provider receives a request access from a Platform in order to be part of the federation and make its services available to the interested parties. The request is evaluated on the basis of the criteria identified by Platform Governance Provider. After the evaluation process has completed, the request can be accepted if the criteria are fulfilled or rejected otherwise. An acceptance/rejection notification is sent back to the Platform X from the Governance Provider.
Actors: IDM Platform X, Platform Governance Provider
Pre-conditions: • The Platform X has requested access to FENIX Federation.
Steps: • Receive Request Access to FENIX Federation from Platform X; • Evaluate request according to governance rules; • The request can be in accepted or rejected status; • FENIX Governance Provider notifies Platform X about the status with a message; • Platform Governance provides platform minimum requirements (in case of positive validation).

Table 9. UC-002 Evaluate New Joining Request

UC-003 Provide Platform Minimum Requirements
Related US: Table 3. F-US-001 On Boarding
Description: To join the FENIX Federation of platforms, each platform must be compliant with a minimum set of technical requirements before joining the FENIX Federation.
Actors: Platform Governance Provider
Pre-conditions: The Platform provider must have requested to join the FENIX Federation.
Steps: • To get the Platform Minimum Requirements document and send it to the platform provider.

Table 10. UC-003 Provide Platform Minimum Requirements

UC-004 Adapt Platform to Requirements
Related US: Table 3. F-US-001 On Boarding
Description: The platform that wants to join the FENIX Federation needs to comply with the minimum requirements needed to join the Federation. Therefore, some adaptions may be done.
Actors: Platform Provider
Pre-conditions: • The Platform provider has received the Minimum Platform Requirements document from the FENIX Governance Provider.
Steps: • The Platform provider reviews the minimum requirements that the platform must have; • It evaluates each requirement and implements them in the platform so it can be prepared to integrate within the FENIX Federation.

Table 11. UC-004 Adapt Platform to Requirements

UC-005 Send Connector Specification
Related US: Table 3. F-US-001 On Boarding
Description: The FENIX Governance provider sends the new Platform Provider a document with the FENIX Connector specification that must be implemented in the Platform side.
Actors: FENIX Governance Provider, Platform Provider
Pre-conditions: • The platform provider has implemented the minimum requirements to join the FENIX Federation.
Steps: • The FENIX governance provider sends over email the FENIX Connector Specification to to the Platform provider.

Table 12. UC-005 Send Connector Specification

UC-006 Implement Connector
Related US: Table 3. F-US-001 On Boarding
Description: The Platform provider implements the FENIX Connector in its platform so they can join the FENIX Federation.
Actors: Platform Provider
Pre-conditions: • The FENIX Governance provider has sent the document with the FENIX Connector Specification.
Steps: • To follow the FENIX Connector Specification and implement each of the requested modules to be able to connect to the FENIX Federation.

Table 13. UC-006 Implement Connector

UC-007 Evaluate Connector Implementation
Related US: Table 3. F-US-001 On Boarding
Description: Once the Platform provider has developed the Connector to join the federation, it must be evaluated by the FENIX Governance provider to see if it covers all the requirements provided by the FENIX Federation.
Actors: FENIX Governance Provider / Evaluator
Pre-conditions: • The Platform Provider has given access to its connector implementation documentation.
Steps: • To follow the technical and non-technical validation process to be specified by the FENIX Governance rules and regulation.

Table 14. UC-007 Evaluate Connector Implementation

UC-008 Generate Certificate for Platform
Related US: Table 3. F-US-001 On Boarding
Description: Platform X wants to become member in FENIX eco system.
Actors: Platform Provider, Certification Provider, Evaluator/Auditor
Pre-conditions: • FENIX Governance Provider has defined certification governance rules • Platform X generates CSR (Certificate signing request) • Evaluator/Auditor has confirmed governance compliance • Platform X has successfully implemented the FENIX Connector
Steps: • The certification provider signs CSR; • Platform X gets signed CSR

Table 15. UC-008 Generate Certificate for Platform

UC-009 Publish New Platform URL
Related US: Table 3. F-US-001 On Boarding
Description: The FENIX Governance provider must make available the new Platform Connector information to allow the rest of the members to access to its resources.
Actors: Platform Governance Provider
Pre-conditions: • The Platform Provider has received an OK to its connector implementation from the Platform Governance Provider, and it has been given a Certificate.
Steps: • The Platform Governance Provider broadcasts the URL of the new Platform Connector to the rest of the FENIX Federation members.

Table 16. UC-009 Publish New Platform URL

UC-010 Request Available Resources
Related US: Table 4. F-US-002 Search Available Resources in the FENIX Federation**.**
Description: A user from platform X requests the list of available resources in the FENIX Federation.
Actors: Data consumers, Service consumers, Platform X and Broker Platform X.
Pre-conditions: • Platform X belong to the FENIX Federation and has the list of platforms federated.
Steps: • The user request the list of available resources; • Platform X sends the request to the Broker Platform X; • The Broker Platform X sends a catalogue request to each Broker Platform in the federated list.

Table 17. UC-010 Request Available Resources

UC-011 Receive Catalogue Request
Related US: Table 4. F-US-002 Search Available Resources in the FENIX Federation**.**
Description: The FENIX connector receives a request from a Platform to receive the Resources Catalogue. The Broker must compose a request message following the FENIX Specification format and adding the Platform Certificate to make the broadcast of the request to all the Connectors in the Federation.
Actors: Broker Platform X and IDM Platform X.
Pre-conditions: • The Platform X has made a request to its connector to receive the catalogue of resources.
Steps: • To receive the Request Catalogue Message from Platform X; • To get Platform X Certificate from IDM Platform X; • To compose the Request Catalogue Message following the FENIX Specification and adding the Platform Certificate.

Table 18. UC-011 Receive Catalogue Request

UC-012 Add Platform Certificate
Related US: Table 4. F-US-002 Search Available Resources in the FENIX Federation**.**
Description: The identity manager includes the platform certificate in an outcoming message
Actors: IDM Platform X
Pre-conditions: • Platform X is a trusted platform in the FENIX Federation and has an identity certificate
Steps: • The IDM Platform X receives a message to be signed; • The IDM Platform X includes the certificate in the message; • The IDM Platform X sends the message to the next step.

Table 19. UC-012 Add Platform Certificate

UC-013 Validate Platform Certificate
Related US: Table 4. F-US-002 Search Available Resources in the FENIX Federation**.**
Description: When any message arrives to a platform connector, the platform certificates from the sender must be validated before forwarding the message to the recipient platform.
Actors: The IDM Platform
Pre-conditions: • A message has arrived to the Broker or de Data Exchange module
Steps: • The IDM from the destination connector must check if the certificate from the connector at origin is trusted and is part of the federation; • It sends the Ok depending whether it is a trusted platform or not.

Table 20. UC-013 Validate Platform Certificate

UC-014 Broadcast Request to Federation
Related US: Table 4. F-US-002 Search Available Resources in the FENIX Federation**.**
Description: Broker Platform X needs to ask all the connectors in the Federation for their Resources Catalogue. This is accomplished by using a Request Catalogue message that is specified in the FENIX Specification. The message is broadcasted to all connectors of the Federation, which in return must respond with their Resources catalogue.
Actors: Platform X, Broker Platform X, Broker Platform Y, Broker Platform Z, … and the Broker Platform *n.*
Pre-conditions: • The platform X is part of the FENIX Federation; • The Broker Platform X has composed a Request Catalogue Message and added the Platform Certificate.
Steps: • A list of all the connectors of the Federation is retrieved as described in UC-015; • The Broker Platform X then sends the composed Request Catalogue Message and the Platform Certificate to each and every connector in the list (Y, Z, …, n); • Finally, the Broker Platform X will consolidate all the information and return to Platform X a list of available Resources from all the connectors that replied, in the form of a Resources Catalogue message following the FENIX Specification.

Table 21. UC-014 Broadcast Request to Federation

UC-015 Get Endpoints of Federation Connectors
Related US: Table 4. F-US-002 Search Available Resources in the FENIX Federation**.**
Description: In order to interact with the FENIX Federation, a connector needs to know the Endpoints of the other connectors. The Broker Platform X must request the list of the connectors from the *FENIX Federation provider*.
Actors: Broker Platform X and the FENIX Federation Provider.
Pre-conditions: • Platform X is part of the Federation.

Steps:

- Broker Platform X creates a *Connector Listing Request* Message as per the FENIX Specification adding the Platform Certificate;
- To request a list of all the connectors from the FENIX Federation Provider using the *Connector Listing Request* message;
- To retrieve the response: A *Connector Listing* message, as per the FENIX Specification.

Table 22. UC-015 Get Endpoints of Federation Connectors

UC-016 Send Resources Catalogue
Related US: Table 4. F-US-002 Search Available Resources in the FENIX Federation**.**
Description: When a Broker receives a request for its Resources Catalogue, it must validate the caller using the provided certificate and then retrieve the Resources Catalogue from its underlying Platform.
Actors: Platform Y and Broker Platform Y.
Pre-conditions: • Platform Y is part of the Federation; • Platform X has initiated a request for the Resources Catalogue; • A request for the Resources Catalogue has been received by Broker Platform Y.
Steps: • Broker Platform Y requests the Resources Catalogue from Platform Y; • Platform Y returns the catalogue with all the Resources that are available to the Federation.

Table 23. UC-016 Send Resources Catalogue

UC-017 Compose Message
Related US: Table 4. F-US-002 Search Available Resources in the FENIX Federation**.**
Description: The FENIX connector has received a request from a Platform to return its Resources Catalogue. The Broker Platform Y retrieved the catalogue from the underlying platform and now needs to compose the response message following the FENIX Specification format and adding the Platform Certificate.
Actors: Broker Platform Y and IDM Platform Y.
Pre-conditions: • Platform Y is part of the Federation; • Platform X has initiated a request for the Resources Catalogue; • The Resources catalogue has been retrieved from the Platform Y.
Steps: • To get Platform Y a Certificate from IDM Platform Y; • To compose *Resources Catalogue* message following the FENIX Specification; • To add the Platform Y Certificate to the response message.

Table 24. UC-017 Compose Message with Resources Catalogue

UC-018 Send Resources Catalogue to Platform X
Related US: Table 4. F-US-002 Search Available Resources in the FENIX Federation**.**
Description: The FENIX connector has received a request from a Platform to return its Resources Catalogue. The Broker has composed the Resources Catalogue response message and then returns it to the requesting Platform, which in return consolidates the catalogue with the responses from the other connectors.
Actors: Broker Platform Y and Broker Platform X.
Pre-conditions: • Platform X and Platform Y are part of the Federation; • Platform X has initiated a request for the Resources Catalogue; • The Resources Catalogue message has been composed by Broker Platform Y.
Steps: • Broker Platform Y returns the Resources Catalogue message to Broker Platform X; • Broker Platform X receives the message and validates the included certificate of Platform Y.

Table 25. UC-018 Send Resources Catalogue to Platform X

UC-019 Request Access to Resource
Related US: Table 5. F-US-003 Request Access to Resource in the FENIX Platform
Description: A user in platform X requests access to a resource in platform Y.
Actors: Data Consumer, Data Owner
Pre-conditions: • Platform X and Platform Y are trusted and part of the FENIX Federation. • Resource is listed in a catalogue response coming from Broker Platform Y of the FENIX Federation.
Steps: • The user sends a request via Broker Platform X linked to the FENIX Federation to the resource owner in Platform Y.

Table 26. UC-019 Request Access to Resource

UC-020 Receive Request to Access Resource
Related US: Table 5. F-US-003 Request Access to Resource in the FENIX Platform**.**
Description: The data owner receives a request of a data user to grant access to data resource.
Actors: Data Owner and Data Consumer.
Pre-conditions: • Platform X and Platform Y are trusted and part of the FENIX Federation; • The resource is listed in a catalogue response coming from Broker Platform Y of the FENIX Federation; • The data Consumer has the user right, in his platform, to send requests to resource in Platform ; • The data Consumer has sent a request to access resource in Platform Y.
Steps: • The data owner in Platform Y, receives the request to grant access to an owned resource.

Table 27. UC-020 Receive Request to Access Resource

UC-021 Accept/Reject Access Request to Resource
Related US: Table 5. F-US-003 Request Access to Resource in the FENIX Platform
Description: Data owner accepts/rejects the request of a data user to access a resource.
Actors: Data Owner, Data Consumer
Pre-conditions: • The resources' acceptance request message comes from a trusted Platform in the FENIX Federation
Steps: • The Data owner reviews the access request to its resource; • The Data owner reviews the requesting data user; • The Data owner accepts/rejects the request of a data user to access a resource.

Table 28. UC-021 Accept/Reject Access Request to Resource

UC-022 Send Response to Platform X
Related US: Table 5. F-US-003 Request Access to Resource in the FENIX Platform**.**
Description: When a platform accepts or rejects the usage of one of its resource, this decision must be communicated to the requestor.
Actors: Broker Platform Y and Broker Platform X.
Pre-conditions: • The platform provider Y, at destination, has accepted/rejected the usage of one of its resources. The message has been composed by the Broker Platform Y to be sent to the platform at origin.
Steps: • To get the composed message with the response; • To send it to the Broker Platform X in the Platform X Connector, at origin.

Table 29. UC-022 Send Response to Platform X

UC-023 Send Data
Related US: Table 6. F-US-004 Send/Receive Data through FENIX Federation**.**
Description: A Data Provider from a Platform wants to send information to a Data Consumer from a different platform.
Actors: Platform Provider.
Pre-conditions: • The platform is part of the FENIX Federation.
Steps: • The Data Provider sends a piece of data information through its own mechanisms.

Table 30. UC-023 Send Data

UC-024 Receive Data
Related US: Table 6. F-US-004 Send/Receive Data through FENIX Federation**.**
Description: A Data Consumer from a platform receives a message coming from a resource that is connected to through the FENIX Federation.

Actors: **The** Platform Provider and the DXC Platform.

Pre-conditions:

- The Broker in the platform of destination has identified a message as valid. The platform of origin is trusted. Therefore, the message is forwarded to the platform at destination.

Steps:

- The platform at destination has implemented a method to received incoming messages;
- The platform at destination gets the message, extracts its body and manages the message as needed.

Table 31. UC-024 Receive Data

UC-025 Adapt Message to FENIX Specification
Related US: Table 6. F-US-004 Send/Receive Data through FENIX Federation**.**
Description: An outgoing message needs to be adapted to the FENIX Data specification before being forwarded to another platform.
Actors: DXC Platform X
Pre-conditions:
• Platform X has been successfully identified and validated in the FENIX Network. The destination URL of connector is known and used to forward the message.
Steps:
• Platform X issues a request or replies to a request from another platform; • The identification has occurred and certificates are validated; • The outgoing message is composed and is sent to the DXC for further forwarding; • DXC encapsulates message in the FENIX specification.

Table 32. UC-025 Adapt Message to FENIX Specification

UC-026 Get Destination Connector URL
Related US: Table 6. F-US-004 Send/Receive Data through FENIX Federation**,** Table 3. F-US-001 On Boarding**.**
Description: Platform X needs to send a message to Platform Y. In order to do so, the Platform Y connector URL is required.
Actors: Broker Platform X
Pre-conditions:
• Broker Platform X has run the discovery functions in order to populate the Platform with information about available platforms in the FENIX Federation.
Steps:
• Both connecting platforms have passed the certification process; • Platform X has discovered Platform Y through the Broker Platform X's discovery functions; • Platform X composes the request for a specific resource on Platform Y according to FENIX specifications and forwards it to DXC Platform X; • DXC Platform X retrieves the Platform Y connector's URL for platform Y to be used for the request.

Table 33. UC-026 Get Destination Connector URL

UC-027 Send Message to DXC Platform
Related US: Table 6. F-US-004 Send/Receive Data through FENIX Federation**.**
Description: DXC Platform X sends a message to Platform DXC Y. Platform Y has already granted access to the requested resource.
Actors: DXC Platform X and DXC Platform Y.
Pre-conditions: • A certification process has already been completed, the identification has been validated and the access has been granted for the relevant resource; • Platform X has discovered the required Platform Y service; • Platform X has composed the message to be sen.t
Steps: • Platform X forwards the message to the DXC Platform X; • DXC Platform X encapsulates/transforms the message according to FENIX specifications; • DXC Platform X gets the DXC Platform Y URL; • DXC Platform X forwards the message to the DXC Platform Y.

Table 34. UC-027 Send Message to DXC Platform

UC-028 Receive Message from DXC Platform X
Related US: Table 6. F-US-004 Send/Receive Data through FENIX Federation**.**
Description: Platform DXC receives a message from DXC Platform X. Platform X has already requested & granted access to a requested resource.
Actors: DXC Platform X, IDM Platform X and DXC Platform Y.
Pre-conditions: • A certification process has already been completed, the identification has been validated and the access has been granted for the relevant resource.
Steps: • DXC Platform Y receives a message from DXC Platform X; • DXC Platform Y validates access using IDM Platform Y; • DXC Platform Y decomposes message; • DXC Platform Y forwards message to relevant resource in Platform Y.

Table 35. UC-028 Receive Message from DXC Platform X

UC-029 Forward Message to Platform X URL
Related US: Table 6. F-US-004 Send/Receive Data through FENIX Federation**.**
Description: DXC Platform Y forwards a message to request a Platform resource via its corresponding URL.
Actors: DXC Platform Y and DXC Platform X.
Pre-conditions: • Certification and identification have been completed and access has been granted to the corresponding resource; • DXC Platform Y has received a message from an external platform.
Steps: • The message is stripped by DXC Platform Y's metadata; • The message is forwarded to DXC Platform X' URL.

Table 36. UC-029 Forward Message to Platform X URL

UC-030 Reject Message
Related US: Table 6. F-US-004 Send/Receive Data through FENIX Federation
Description: A message is received by the Platform and is rejected either because it is invalid, because no access has been granted or the sending platform is not member of the FENIX Federation
Actors: DXC Platform Y, IDM Platform Y
Pre-conditions: • Certification and identification processes have been completed.
Steps: • A message is received by the DXC Platform Y from DXC platform X. • If the certificates are not valid, the message is rejected. • If the certificate is valid, the message is decomposed. • The message is then forwarded to the requested resource with relevant metadata • If there are any errors in the decomposition process the message is rejected. • If the data provider has revoked access, the requesting platform/service does not have success, or message is mal formatted, the message is revoked.

Table 37. UC-030 Reject Message

UC-031 Revoke Access to Resource to Platform
Related US: Table 7. F-US-005 Grant/Revoke Access to Resource in the FENIX Federation**.**
Description: To revoke access on specific platform resource (data source, service).
Actors: platform X and IDM platform Y**.**
Pre-conditions: • Previous access has been granted to Platform X on specific resource from Platform Y
Steps: • Platform Y decides to revoke the access; • Platform Y rejects any further requests of platform X.

Table 38. UC-031 Revoke Access to Resource to Platform

UC-032 Send Notification
Related US: Table 7. F-US-005 Grant/Revoke Access to Resource in the FENIX Federation**.**
Description: A user of platform X executes an action that requires to notify platform Y**.** Platform X sends a notification to Platform Y. This notification may be a grant access response, a reject access response or any other async information.
Actors: Broker Platform X, the Service Provider and the Data owner.
Pre-conditions: • Platform X and platform Y are part of the FENIX federation; • Platform X knows Platform Y's Connector URL.
Steps: • User A executes an action in Platform X that requires to notify user B in Platform Y; • Platform X sends the notification to its connector; • Broker Platform X builds the message and sends it to the Broker Platform Y.

Table 39. UC-032 Send Notification

UC-033 Receive Notifications
Related US: Table 7. F-US-005 Grant/Revoke Access to Resource in the FENIX Federation
Description: platform Y receives a notification from platform X and redirects it to the destination user
Actors: Broker Platform Y, Service Consumer, Data Consumer
Pre-conditions: User B from platform Y has requested an action from platform X that requires any async response.
Steps: • Broker Platform Y receives a notification message. • Broker Platform Y validates the origin of the message. • If the origin is validated, redirect the message to the platform Y. • The platform Y redirects the message to the user.

Table 40. UC-033 Receive Notifications

6.3 Traceability Matrix

The present table represents a traceability matrix in which the link between User Stories and Use Cases can be found. As some of the use cases can appear in different use cases, this is the way to identify them.

UCs/USs	F-US-001	F-US-002	F-US-003	F-US-004	F-US-005
UC-001	X				
UC-002	X				
UC-003	X				
UC-004	X				
UC-005	X				
UC-006	X				
UC-007	X				
UC-008	X				
UC-009	X				
UC-010		X			
UC-011		X			
UC-012		X	X	X	
UC-013		X	X	X	
UC-014		X			
UC-015		X			

UC-016		X			
UC-017		X	X	X	
UC-018		X			
UC-019			X		
UC-020			X		
UC-021			X		
UC-022			X		
UC-023				X	
UC-024				X	
UC-025				X	
UC-026				X	
UC-027				X	
UC-028				X	
UC-029				X	
UC-030				X	
UC-031					X
UC-032					X
UC-033					X

Table 41. Traceability Matrix. User Stories - Use Cases

6.4 FENIX Connector

As introduced in section 4.1, the federation of platforms is achieved through the implementation of connectors and implementations of the FENIX Connector, that will provide the necessary mechanisms of identification, validation, discovery, and communication to ensure a secure exchange of information in a trusted environment.

The user stories and the use cases defined in the previous section together with the design patterns by DTLF guided the identification of the main functionalities that the FENIX Connector must provide in form of services for the federation.

Federated services will be implemented with three main pillars which fits in the business processes based on:

- ***Federated Identity Registry*** **-** to ensure the identities of the participants of the federation, authentication of identities;

- ***Data Exchange Federated Services*** **-** data exchange connector to enable the data sharing;
- ***Broker*** **-** Search and discovery service of a distributed catalogue of services and data available in each node of the federation.

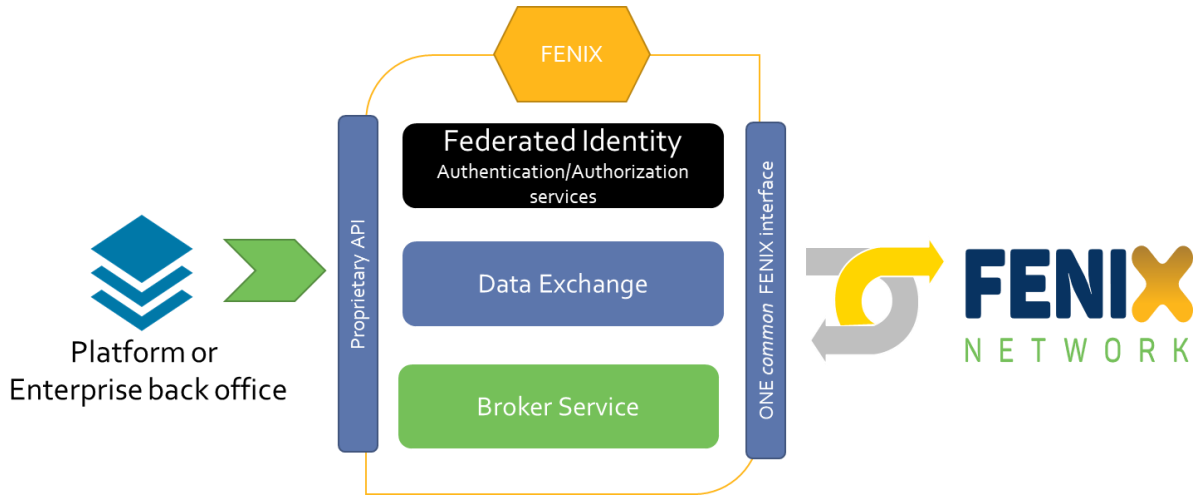

Figure 14: FENIX Connector architecture

These three main functional blocks are surrounded by two interfaces, one common FENIX interface that must be deployed following the FENIX requirements, and a proprietary API that interacts with the platform. The FENIX interface is the communication point between FENIX Connectors and the final enabler of the federation.

The implementation of each connector is unique for each platform and must be achieved by the platform provider, so the implementation of the modules is out of the scope of this activity.

6.4.1 Modules functionality

Federated Identity

- Is aligned with technical requirements and standards for the identification and authentication services;
- Interact with certification authorities to validate digital certificates in FENIX operations with other connectors/platforms.

Data exchange

- Is a service in charge of the data Exchange operation (get/write data from/into services) between two organisations via the connector. It ensures the secure communication between both connectors;
- It interacts with the authorisation and usage policies modules of the platform to perform the operation;
- It notifies the monitoring module to log each transaction executed via the connector.

Broker Service

- Discover service to search and discover resources (data and services) available in brokers of the networked platform. The discovery service may support the search for resources using wildcards, similarity and multiple criteria, so that one can easily find new resources without knowing the exact details;
- It allows data owners to register, modify or remove metadata information of the resources. A common service description metadata model must be used.
- It allows data users to request Access to a specific resource found via the broker, by pushing the request to the resource owner.

Together with the main three functional modules, there are several blocks that complement the functionality of the connector and must be considered within the platform specification. Further versions of the specification will detail modules for metering, monitoring, notification, etc.

6.4.2 FENIX connector and roles interaction

The figure below represents the basic interaction between two platforms in a data exchange process with a platform at each side, and the FENIX Connectors enabling the communication between users from each platform. Each box represents a role in the federated ecosystem and the lines interaction between them.

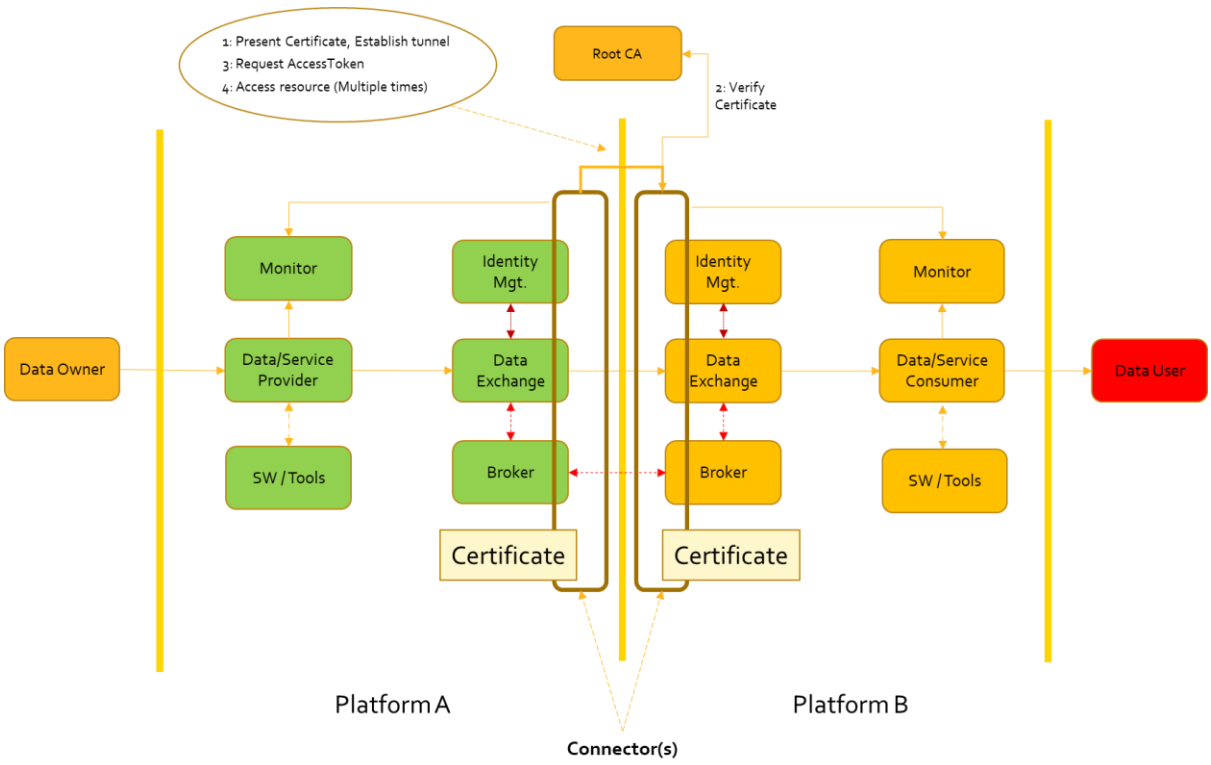

Figure 15 FENIX Connector roles

At each extreme, the users use different services from their platform and the services communicate in a transparent way via the modules of the connectors.

Before the data exchange action, the brokers have enabled the data/services discovery and have made the access request easier. The data exchange module allows the flow of information from platform A to platform B via the federated ecosystem. All these actions are secured by the identity manager that manages and validates the certificates of the platforms.

The activity will be monitored by the monitoring modules at the platform sides and used by the software tools of the platform after validating the access and usage policies.

6.4.3 Technical specifications

The functional specification of the FENIX Connector's components must be extended with the technical specification for each subcomponent, the protocols definition, and the metadata specification. All this information together will build the Connector specification that will be provided to the platform providers.

In the next open discussions, the activity will face the specification of:

- IdM certificate validation process;
- Data Exchange protocols;
- Broker metadata specification;
- Broker Discovery pattern;
- Platform boarding and revocation broadcast;
- Access request process;
- Metering and monitoring process.

7. Conclusions and next steps

The FENIX network of platform is focussed on the specification of an open and trusted architecture for data sharing between platforms. This federation ecosystem that enables the data exchange between platforms will support the efficiency of the shipping processes and the cooperative management of end-to-end intermodal freight transport chains across the logistics corridors. FENIX' network architecture is built on the assumption of four main design principles: a federation, a decentralised approach, an ecosystem of trustworthy data and services and data sovereignty.

This final part of the report will define a detailed and final version of the roadmap plan, which illustrates the definition of the FENIX Network Infrastructure and the FENIX Connector functionalities to be fully specified and later developed for the implementation of the early and full prototypes by each platform in the network from the FENIX Pilots. The initial infrastructure prototype will allow demonstrating authentication and identification on a federated manner between platforms, establishing initial data sharing among them following the FENIX specifications and governance rules and protocols. This shall ensure an early validation of the key ecosystem functionalities (trust and data sharing) while the rest of features and functionalities will be added following an incremental approach. The following table summarises the plan for the components and sub-activities during the period 2 (M13-M24) of the project:

Time	Actions	Related sub-activities
M13-M15 FENIX Connector and ecosystem	• To setup of a Data Providers working group including the platform providers in the pilot specifications on activity 2. This action shall monitor and share the FENIX connector specifications and create a communication channel to share practices, patterns and support the later implementation of the connector by each data/platform provider. • To identify minimum functions of role FENIX Federation provider; • To identify and consolidate the FENIX connector requirements fixing the open issues and details	Sub-activity T3.2, T3.3 and T3.4

	specified in section 5.4.3 of this document. • By the end of M15, the outcome will be a first version of the FENIX connector specifications.	
M13-M18 Platform providers use cases	• To identify business cases and platforms providers from Pilots in Activity 4 to be involved in the first loop of building FENIX Infrastructure. • To work on identifying specific technical requirements of the broker subcomponent • To identify a common metadata service description model for the available services registered in each broker component. • To identify services available in platforms to populate the respective connector • To follow-up on technical meetings with the platform providers' group to monitor the support of the specification of the connector and to establish an implementation work plan.	Sub-activity T3.2, T3.3
M18-M24 FENIX Initial testing	• [M18-M22]: To test with selected Pilot Site Use Cases and perform refinements. • [M22-M24]: To eelease the Pilot Site solution development.	Sub-activity T3.2, T3.4

Table 42: FENIX Network architecture roadmap plan

All the interactions between the sub-activities in activity 3 can be also seen in the figure below, which also contains information related to the inputs received from other activities (Activity 2) and the outputs provided by Activity 6 and more.

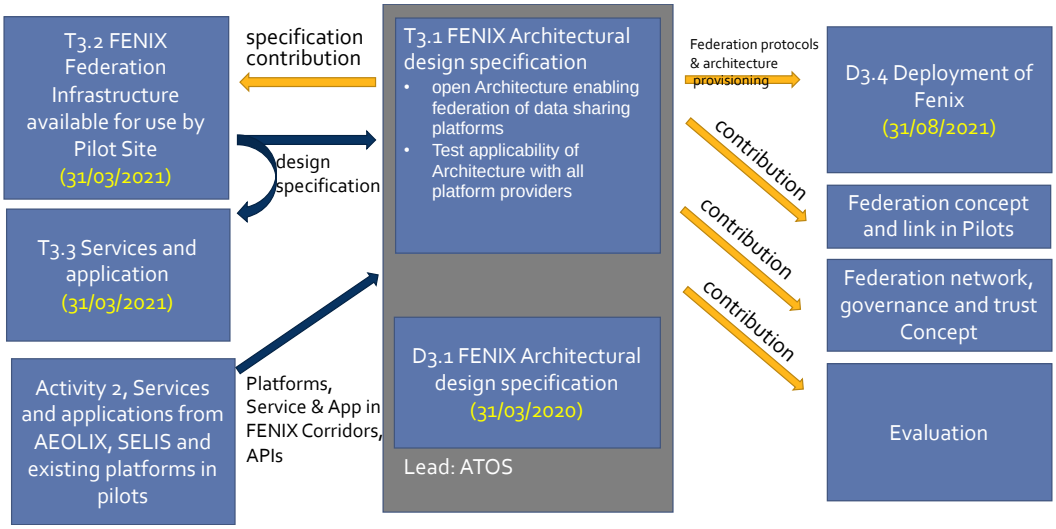

Figure 16. Activity 3 tasks interactions

REFERENCES

FENIX PARTNERS' CONTRIBUTIONS

FENIX Grant Agreement

FENIX Grant Agreement Supporting Document

FENIX Activity 2 documents (D2.1.1, D2.1.2, D2.2.1, D2.2.2)