FENIX

A European Federated Network of Information exchange in Future Logistics

Virtual ITS European Congress
9-10 November 2020

Dr. Eusebiu Catana
ERTICO-ITS Europe
#STAYHOME

Contents

- What is FENIX?
- Strategic principles and features
- FENIX Architecture & Connector Overview
- FENIX Connector Specifics:
  - Identified User Stories & Use Cases
  - The FENIX Connector specification
- Technical Interoperability
- DTLF contribution

FENIX NETWORK

What is FENIX?

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.

Main FENIX federation governance aspects:

- Rules and regulations for the federation: On-Boarding Process to become Member of the FENIX Federation
  - Rules, Legal Issues, Certification, Interoperability
- Rules and regulations for data exchange within the federation:
  - Technical Implementation of the FENIX Connector according to the specification

FENIX NETWORK

OVERVIEW

Project overview:

- FENIX aims to interconnect the different digital platforms and harmonise the services they offer
- Interoperability: common protocols for supporting data sharing services
- Data sharing in the form of digital corridor information systems serving the European logistics community
- Cloud-based will facilitate horizontal collaboration within the LSC
- Overcome today's fragmentation and lack of connectivity around ICT-based systems for logistics decision making
- Open-solution and not "privately owned" and technological neutral

FENIX NETWORK

OBJECTIVES

Main project objectives:

- Establish a federated network of transport and logistics actors across Europe, enabling sharing of information and services needed to optimise TEN-T (A2&A3)
- Demonstrate the operational feasibility and benefits through the organised national pilots –focus on testing the achieved interoperability capabilities (A4)
- Set up the EU corridor community building programme and to promote the benefits to the participants in terms of reduced costs and GHG emissions (A5&A6)

FENIX NETWORK

ACTIVITIES

- A1: Project management =8 milestones
- A2: Strategic dialogue, cross-corridors collaboration and pilot roll out preparation=15
- A3: Technology integration=13 milestones
- A4: Pilots roll out=22 milestones
- A5: Evaluation=19 milestones
- A6: Working groups, recommendations and sharing of best practices=24 milestones

6 activities/101 milestones
for:

- Pilot sites 11: AT, BE, FR, DE, GR, IT, NL, SP, SK
- 3 years: 1st April 2019-31st March 2022
- 36months
- 60.6MEuro
- 43 partners, +50 implementating bodies
- 2 Member States

FENIX NETWORK

FENIX Test sites

H: Smart **door-to-door** multimodal T&L services across TEN-T

SL: **Mondelez** T&L multimodal services across TEN-T corridors

B1: **AirCargo** pilot site(Be)-implement/pre-deploy/deploy specific use cases for the air cargo community linked to the other transport modes across TEN corridors

B2: Multimodal inland **Hub-Procter & Gamble**-Mechelen-Willebroek pilot site across TEN-T corridors

G: **Multiple test sites** across on Rhine-Alpine in Holland, Germany, Switzerland, Italy

A: **Customs corridor services** for T&L:- Fürnitz Pilot Site (South Austria) on the Baltic-Adriatic corridor

I1: Mediterranean and Baltic-Adriatic and the Motorway of the Sea of South-east corridors

Data visibility T&L services across the Spanish-Atlantic corridor between the main nodes and actors

I2:The Italian Rhine Alpine pilot site – **Dynamic Synchro-modal for sustainable multimodal logistic planning and operations**

GR: Greece Balkan-TEN-T network, Adriatic-Ionian Corridor-Cyprus **multimodal T&L services**

FENIX NETWORK

AT GLANCE

Test site Austria: Customs corridor -Fürnitz (South Austria) on the Baltic-Adriatic corridor
Test Site Belgium: PS BE 1- AirCcargo (Be)
PS BE2- Multimodal inland Hub-Procter & Gamble-Mechelen-Willebroek (Be)
Test site France: French Mediteranean – North Sea
Test Site Germany: Multiple test sites across on Rhine-Alpine in Holland, Germany, Switzerland, Italy
Test site Greece: Greece Balkan-TEN-T network, Adriatic-Ionian corridor-Cyprus multimodal
Test Site Holland (South Holland): Smart multimodal
Test Site Italy: PS IT1- Mediterranean and Baltic-Adriatic and the Motorway of the Sea of South-east - Trieste
PS IT2: The Italian Rhine Alpine – Dynamic Synchromodal Logistic
Test Site Slovakia: All TEN-T corridors and multimodal
Test site Spain: The Spanish-Atlantic Corridor

- ***Multi/syncromodal Transport***
- ***Intelligent bubs***
- ***Network Optimisation***

FENIX NETWORK

Strategic principles and features

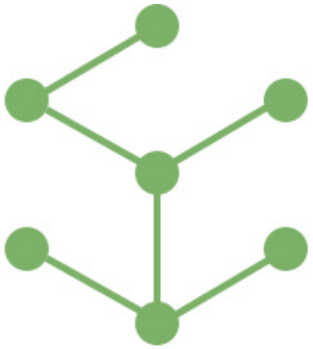
Federation

- According to businessdictionary.com, 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.
  - At **strategic level**, FENIX addresses the vision of a federated network of platforms concept, data sharing, trust and data access control.
  - At **tactical level**, FENIX' focus is on the governance model and the regulation (rules, guidelines, standards…).
  - At **delivery level**, FENIX provides the technological architecture specification for the federation of platforms and a technological demonstration together with project member's platforms.

FENIX NETWORK

Strategic principles and features

Decentralised approach



- FENIX architecture does not rely on a centralised platform or software approach.
- All trusted and certified platforms that are part of the federation are considered nodes of the network and always retain their internal control.
- Is not a single, central system that mandates one way of operating for everything. Instead, it is a framework. It is a networked collection of platforms that join together and understand each other, based on common rules.

FENIX NETWORK

Strategic principles and features

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.
- FENIX federation enables data sharing between individual platforms, which will be created by means of common protocols for supporting data sharing services (platforms interoperability).
- Stakeholders can communicate with their platform provider of choice, who are held to relevant trust, security, and performance standards by the authorities and FENIX specifications and coordinate with the rest of the network.

FENIX NETWORK

Strategic principles and features

Trustworthy and Data Sovereignty

- Trust is essential for digital services, logistics actors will not embrace digital services if they don't trust their data will be protected. FENIX provides guidelines to ensure the trustworthiness between the federated platforms and to support data sovereignty.

- Data sovereignty means maintaining authority and control of data within jurisdictional boundaries. Together with other security aspects, such as secure communication between nodes of the network, data sovereignty is essential for data security.

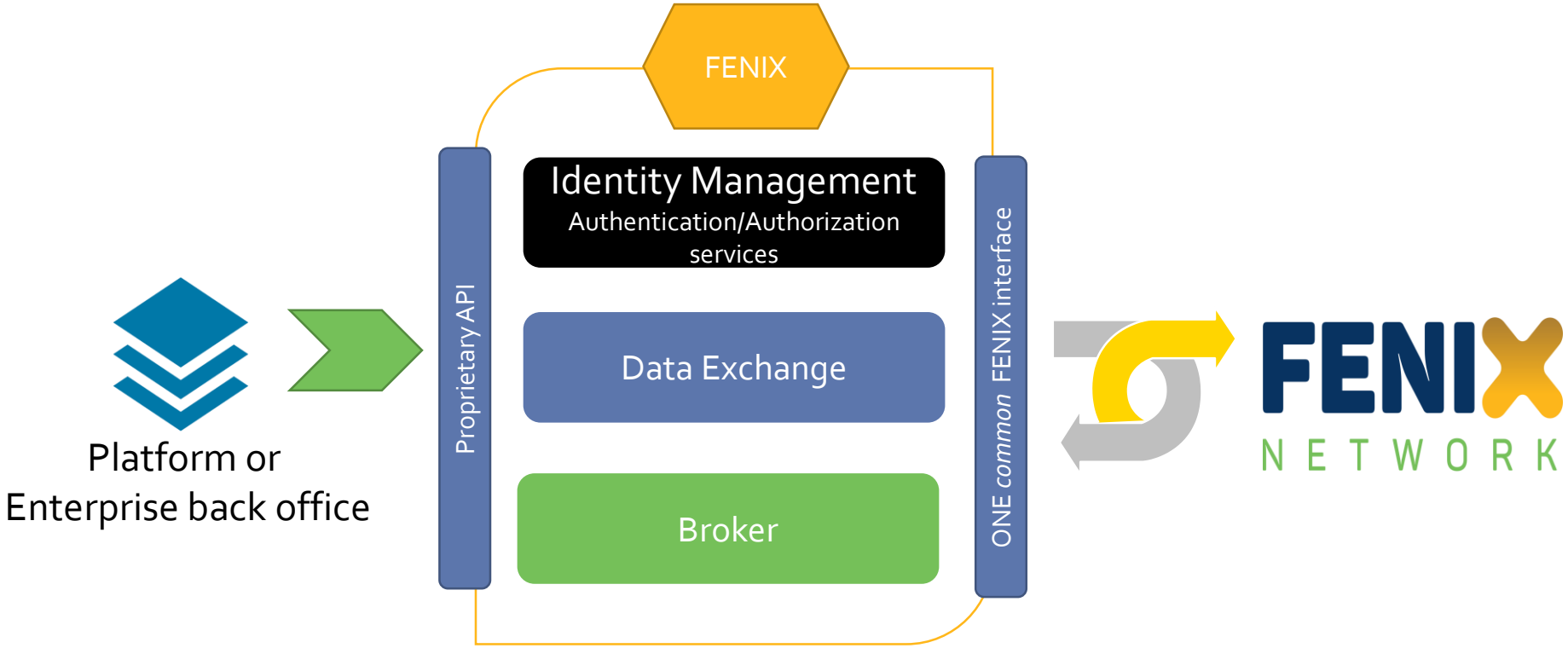
- FENIX is federating platforms, is not granting access to each of the fed-platforms.

FENIX NETWORK

FENIX Architecture & Connector Overview

- Federated resources will be implemented with 3 main pillars, which fit in the business processes based on:

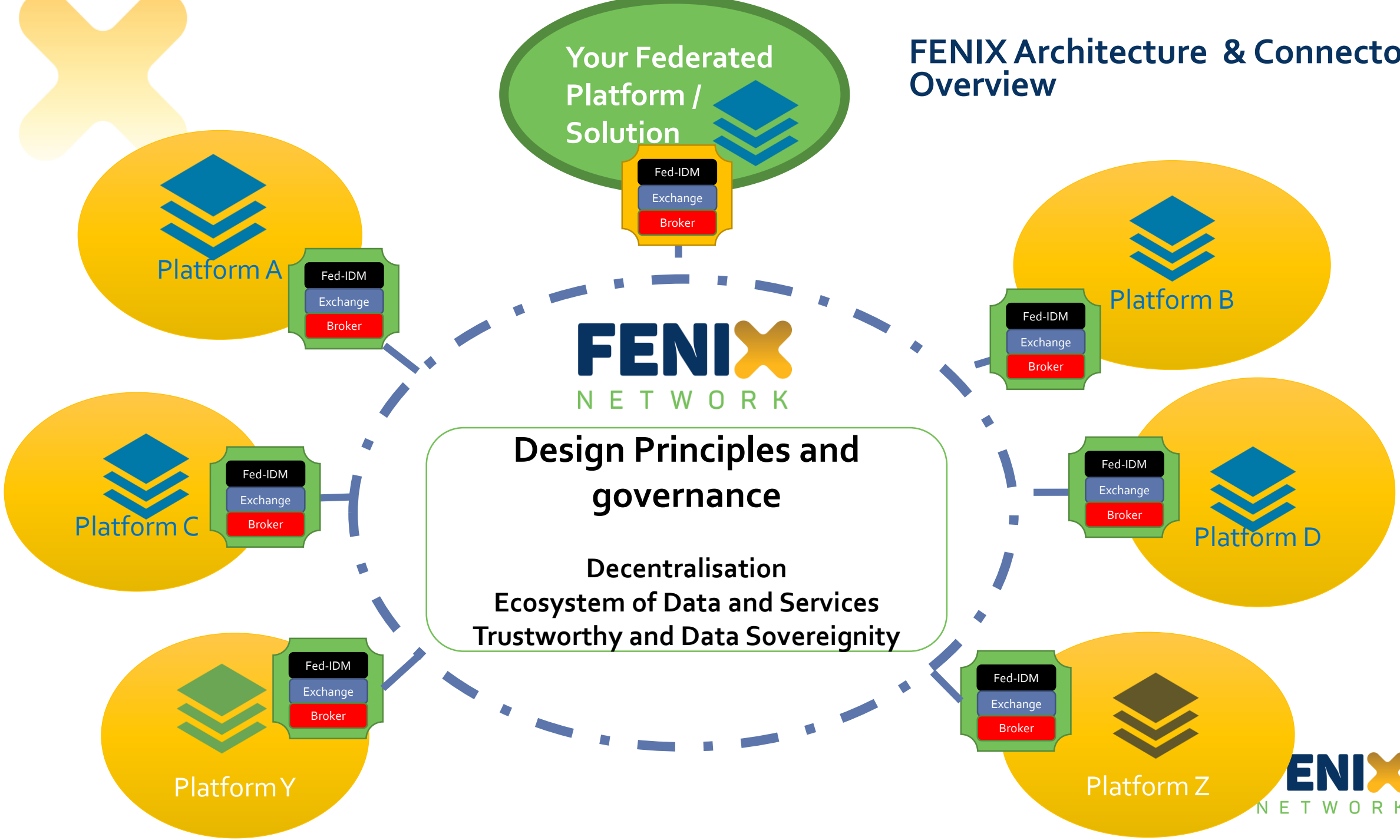
  - ***Identity Management*** *:* To ensure and authenticate the identities of the participants of the federation.
  - ***Data Exchange:*** Data exchange connector to enable the data sharing.
  - ***Broker :*** Search service of a distributed catalogue of services and data available in each node of the federation.



FENIX NETWORK

FENIX NETWORK

FENIX Architecture & Connector Overview



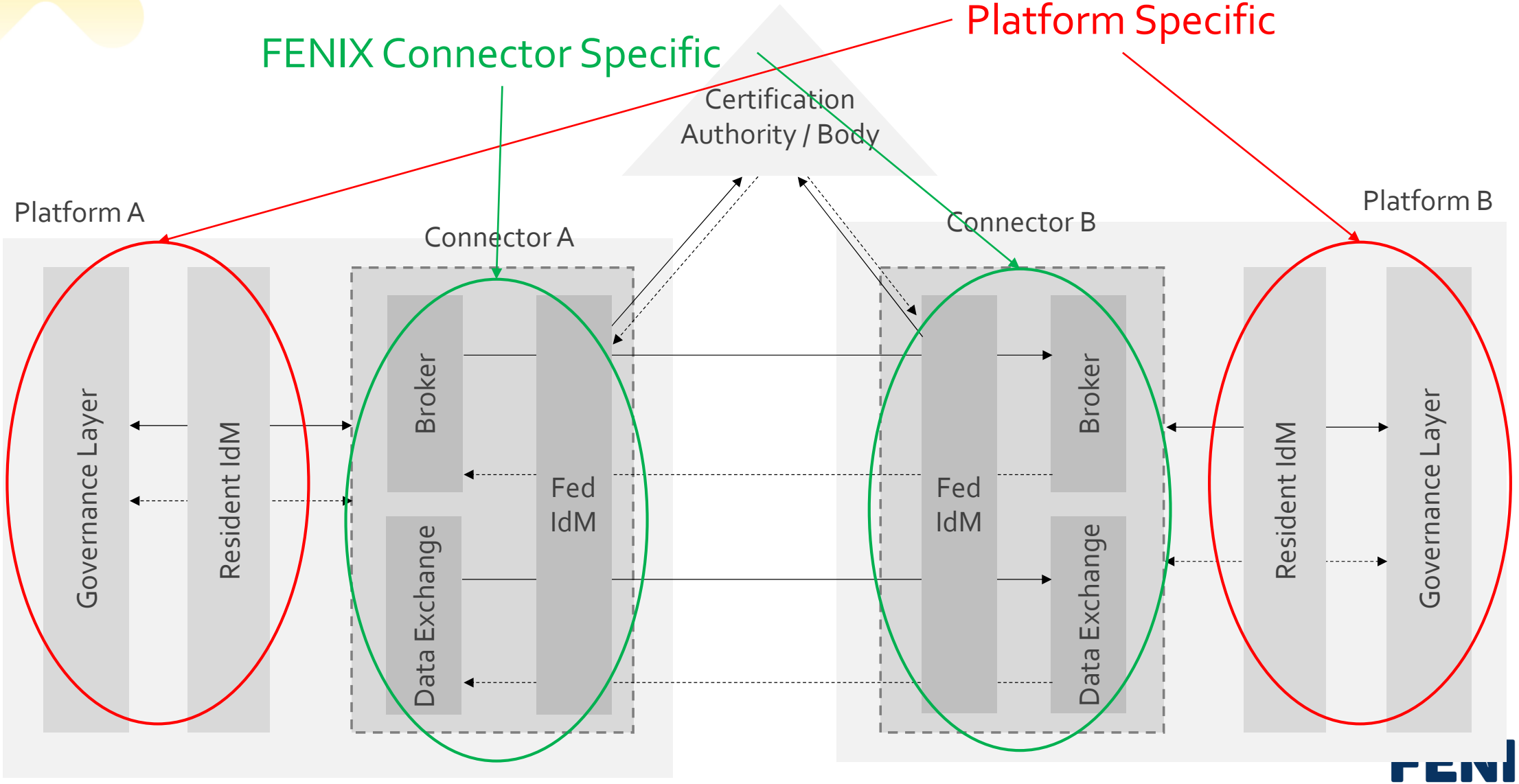
FENIX Connector Specifics

- Identified User Stories & Use Cases

User Story ID	User Story
F-US-001	**Become a member of the FENIX federation**
F-US-002	**Get available resources from other FENIX members**
F-US-003	**Request Access to make use of any available resource**
F-US-004	**Authorise to make use of a resource**
F-US-005	**Send/Receive Data through the FENIX connector**

FENIX NETWORK

FENIX Connector Specifics



The FENIX Connector Specification

- Security
  - Certificates –> Machine to Machine Communication
  - TLS v1.3 and mTLS
- Identification & Authorization – Access Token, Oauth 2.0
- Catalogue of Resources
- Data Exchange
  - Communication Patterns
- FENIX message Structure

FENIX NETWORK

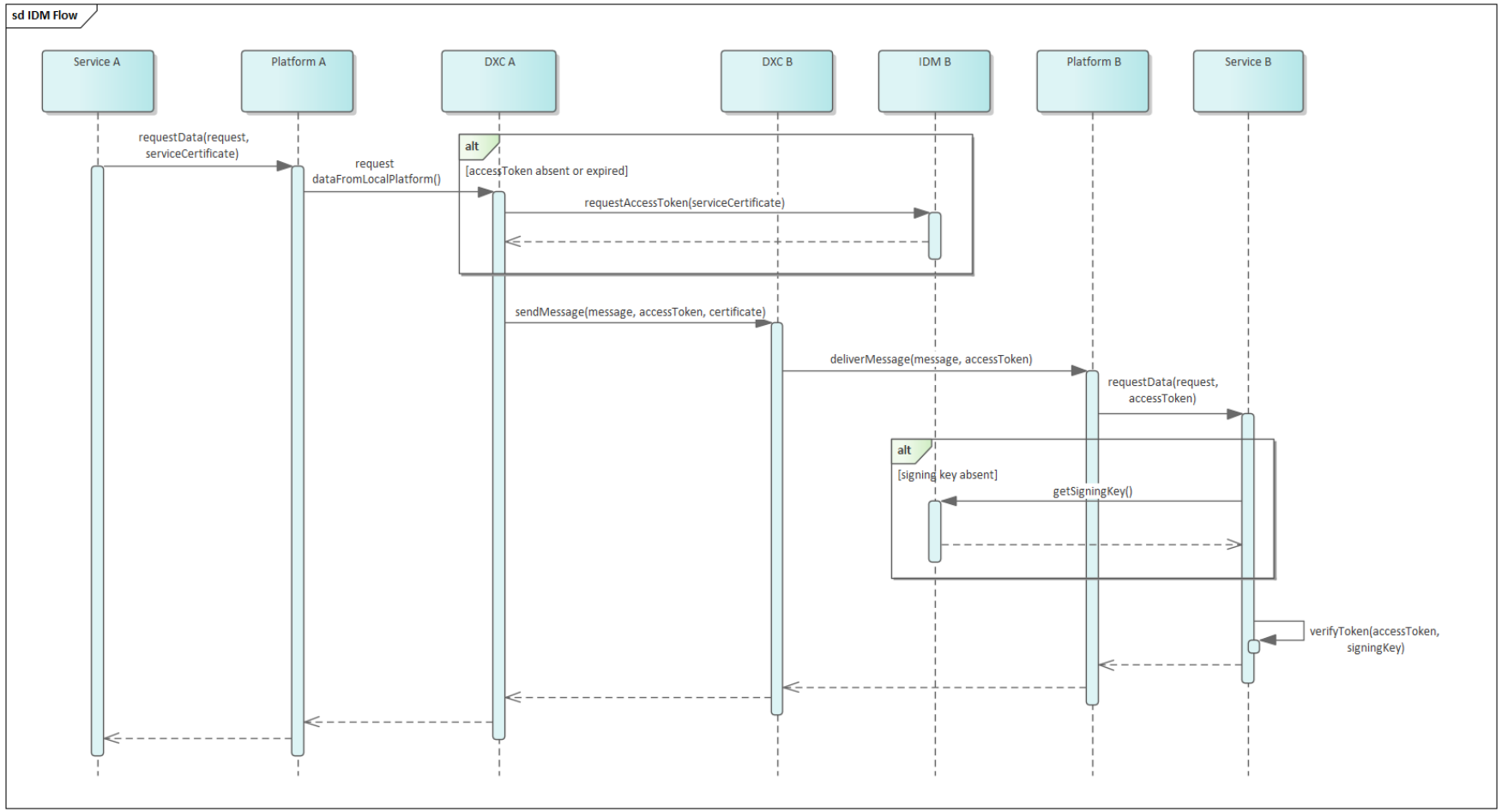
The FENIX Connector Specification - Security

- FENIX provides a Machine to Machine Communication through the FENIX connectors
  - The data platforms remain their operation in the same way
  - No need to identify users between connectors, only platform/services certificates
- Usage of Certificates
- TLS v1.3 and mTLS to provide a secure environment using HTTPS connections and data encryption using RSA ciphers

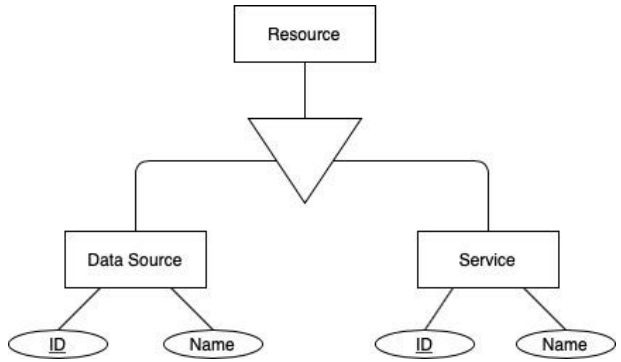
FENIX NETWORK

The FENIX Connector Specification – Identification & Authorisation

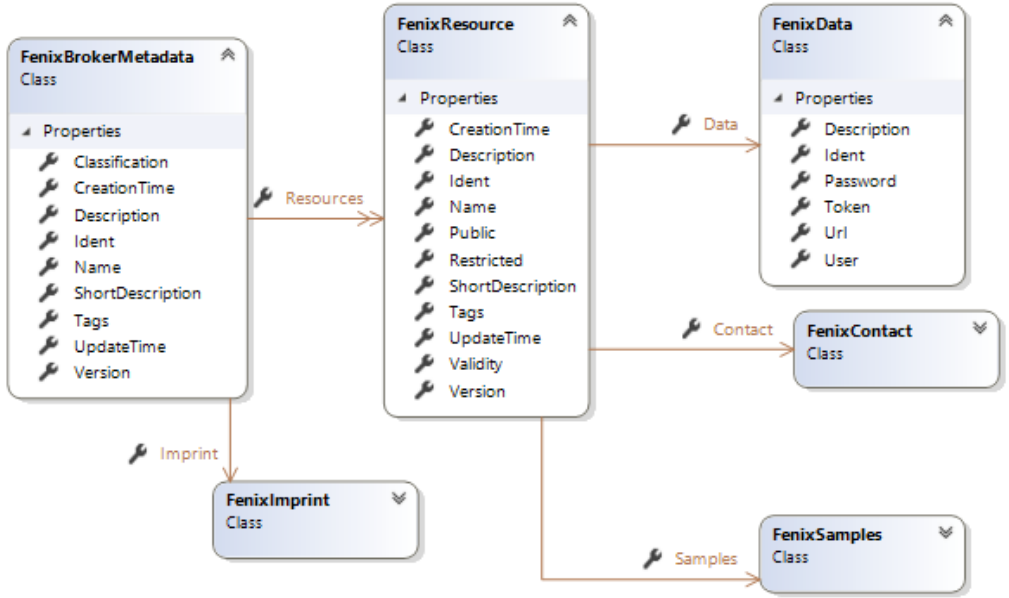
- FENIX Connectors must perform a negotiation to start exchanging information.
- Generation of access token between connectors to execute operations.
- Oauth 2.0 protocol based on JWT.



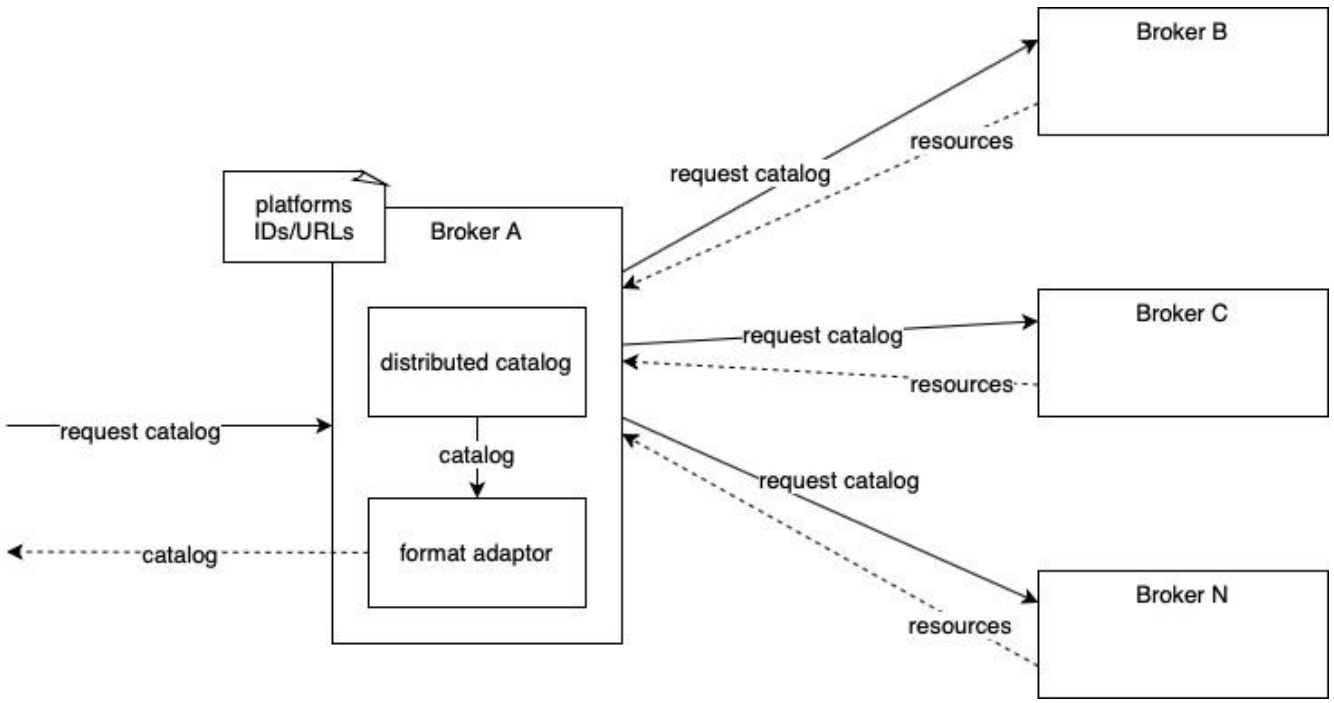
The FENIX Connector Specification – Catalogue of Resources



- Any member of the FENIX federation can share or consume **Resources.**
- Every platform must generate its catalogue of resources following a schema containing different kinds of information about the resource:
  - Identifier
  - Resource name
  - Fenix Classification
  - Description
  - Tags
  - Contact for the resource & Imprint
  - Data, Documentation & Samples
  - Scope: Public or Resticted



The FENIX Connector Specification – Catalogue of Resources & Access to Resource



- Any member can check the available resources in the FENIX federation.
- The FENIX connector must obtain every catalogue of resources from every member. This operation will be done using the Broker component.
- To access one resource, the data user must request access to the resource owner.
- The request is done via the FENIX connector, but it is up to the resource owner to grant access to it.

FENIX NETWORK

The FENIX Connector Specification – Data Exchange

- To exchange data between FENIX connectors, 3 different communication patterns have been specified:
  - Request/Response Pattern
  - Publish/Subscription Pattern
  - EDI Pattern
- Definition of the data exchange process for each of them (sequence diagrams)
- Definition of the API needed for the Request/Response Pattern (first version)
- Design of the Publish/Subscription pattern using a common Queueing System

FENIX NETWORK

The FENIX Connector Specification – Data Exchange

- Every message transferred between connectors must follow the same structure.
- It contains context information and can be provided in different formats: json, xml, …
- The FENIX Connector does NOT deal with the original content. It is encapsulated within the FENIX message structure.
- It is up to each platform to understand the original message format.

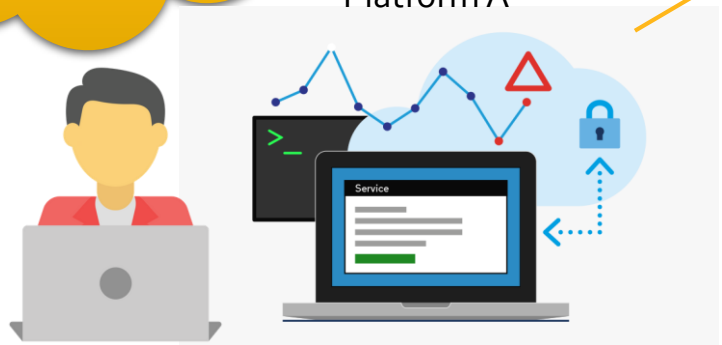
```
{
   "metadata": { //metadata related to the FENIX connector and resources sending info
     "message_id" : 'Unique FENIX message identifier',
     "conn_origin_id" : 'ID from the FENIX Connector at origin',
     "conn_origin_url" : 'URL from the FENIX Connector at origin',
     "conn_dest_id" : 'ID from the FENIX Connector at destination',
     "conn_dest_url" : 'URL from the FENIX Connector at destination',
     "usr_origin" : 'User that sends the message from platform A',
     "usr_dest" : 'User, from platoform B, that must receive the message',
     "sent_at" : 'Timestamp at the message is sent, expressed in UTC',

     "msg_type" : [ //Defines the type of message that is being sent
        "access_request": 'Access request',
        "data_record" : 'The message is a data record',
        "service_request" : 'The message is a service request',
        "service_response" : 'The message is a service response',
        "resource_catalogue" : 'The message is to retreive the catalogue of resource',
        "resource_grant_request" : 'The message is to request access to a resource',
        "resource_grant_response" : 'The message is a response to a resource_grant_request',
     ],

     "resource_type" : [ //Defines the type of resource sending information

         "dataSource" : { // The source of information is a Data Source,
            "ds_id" : 'If the Resource_type is a dataSource, the data source ID is needed',
            "ds_name" : 'If the Resource_type is a dataSource, the data source name is needed'
          }

         "service" : { //The source of information is a Service
           "srvc_id" : 'If the Resource_type is a service, the service ID is needed',
           "srvc_name" : 'If the Resource_type is a service, the service ID is needed'
         }
     ],

     "mic" : 'Message Integrity Code'
   },

   "original_msg" : { //Contains the message in its format at origin
      "msg_standard" : 'Specifies if the message follows an specific standard: EDIFACT, UBL...',
      "msg_body" : 'Original body of the message'
   }
}
```

FENIX NETWORK

FENIX message example

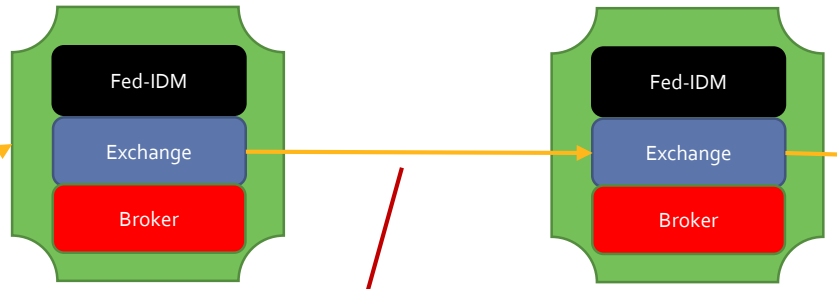
I want to send my position to user in platform X: Latitude, longitude

Platform A

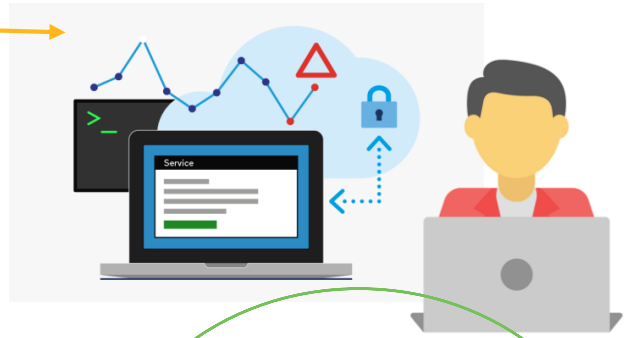


Connector A
ID: 001
URL: 172.167.21.43

Connector X
ID: 145
URL: 134.063.31.67



Platform X



```
entity {
  id: "vehicle_position_2403"
  vehicle {
     position {
          latitude: 28.06235
          longitude: -82.45927
          bearing: 360.0
          speed: 0.0
     }
  }
}
```

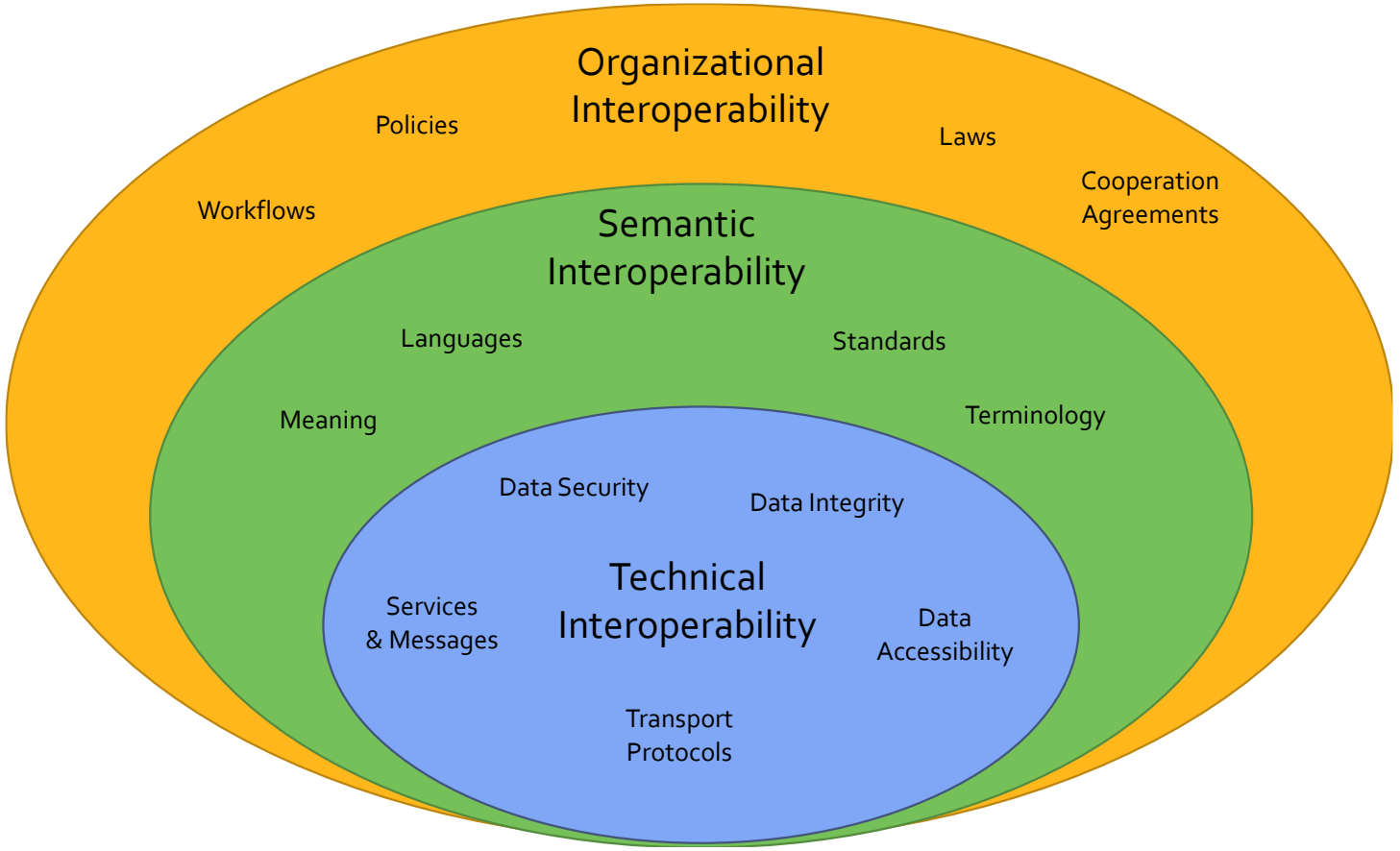

```
{
  "Metadata":{
    "Message_ID":"000123243423",
    "Conn_Origin_ID":"001",
    "Conn_Origin_URL":"172.167.21.43",
    "Conn_Dest_ID":"145",
    "Conn_Dest_URL":"134.063.31.67",
    "Usr_Origin":"somebody@platformA.com",
    "Usr_Dest":"somebody@platformX.com",
    "Sent_At":"Mon, 20 July 2020 11:51:57 +0012",
    "Msg_Type":"Data_Record",
    "Src_Origin":"Geocoding Service",
    "Src_Dest":"ETA calculator",
    "MIC":"tBrDrMNe2L8JSOgNSZpQQKDgfC5I9eIdDNUJmShnAyuhk3TjqGH6tB
KFs8nAEJkyCWI36oeQgOg1tOXO0OEQ"
  },
  "Original_Msg":{
    "Msg_Format":"GTFS",
    "Msg_Body":"entity {\n  id: \"vehicle_position_2403\"\n  vehicle {\n    position {\n
    latitude: 28.06235\n      longitude: -
82.45927\n      bearing: 360.0\n      speed: 0.0\n    }\n  }\n}"
  }
}
```


```
entity {
  id: "vehicle_position_2403"
  vehicle {
     position {
          latitude: 28.06235
          longitude: -82.45927
          bearing: 360.0
          speed: 0.0
     }
  }
}
```

FENIX NETWORK

Interoperability Levels

- The FENIX connector is the key technical interoperability enabler in the FENIX federation.
- It allows several data platforms to connect to each other in the same way and to consume and exchange data in a common way.
- The FENIX connectors use a common message structure to share information (FENIX message).
- The FENIX connector does not deal with content. Therefore, it sends data as the data owner sends it, in its original format. This message is encapsulated within the FENIX message.



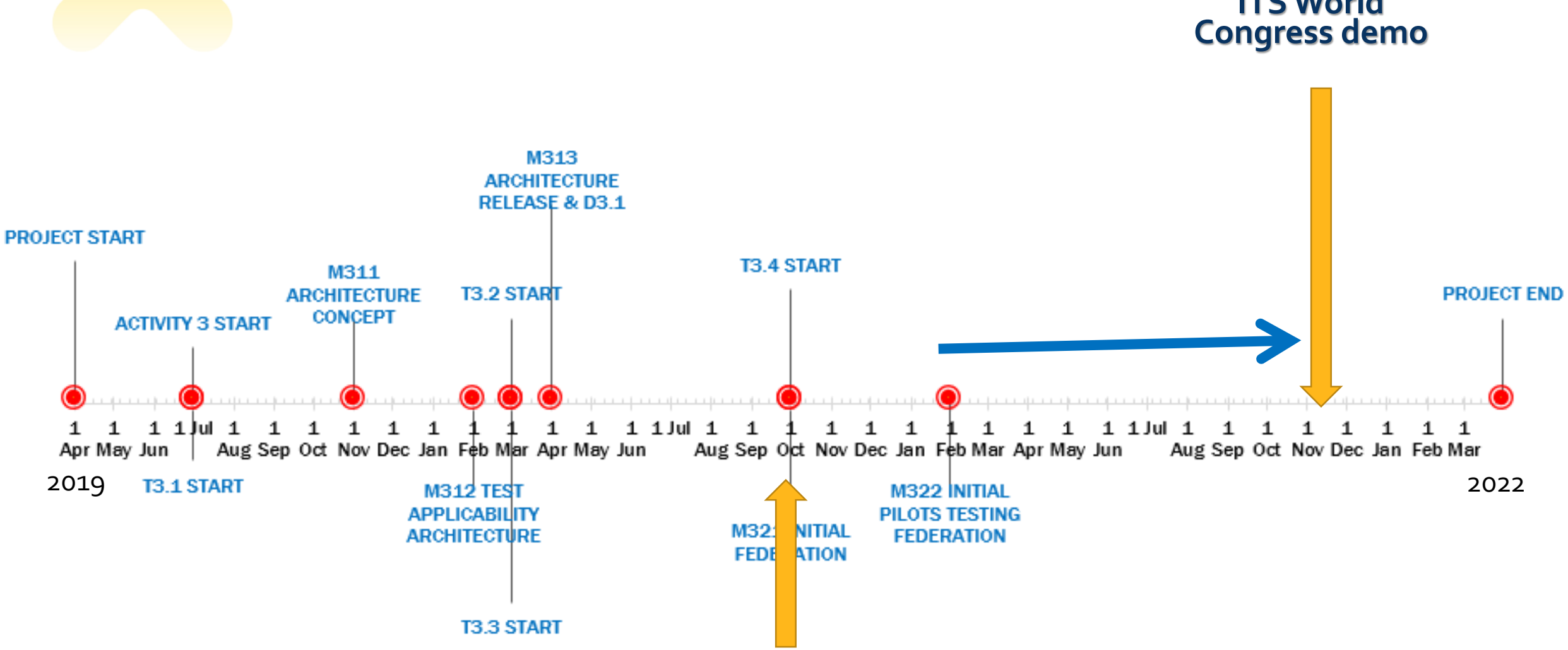
FENIX NETWORK

Some notes

- Specific task forces about FENIX connector: Identity, Broker and data Exchange (A3.2, A3.3).
- Discussions on governance model & certification process (A2.5).
- Discussions on interoperability approach for each level (A6.5, A2.4, A4.1).
- Cross-activity meetings between previous specifications.
- Alignment with business scenarios from FENIX Pilot use cases.
- FENIX-FEDeRATED.

FENIX NETWORK

Timeline


ITS World Congress demo
PROJECT START
ACTIVITY 3 START
M311 ARCHITECTURE CONCEPT
T3.2 START
M313 ARCHITECTURE RELEASE & D3.1
T3.4 START
PROJECT END
1 Apr 1 May 1 Jun 1 Jul 1 Aug 1 Sep 1 Oct 1 Nov 1 Dec 1 Jan 1 Feb 1 Mar 1 Apr 1 May 1 Jun 1 Jul 1 Aug 1 Sep 1 Oct 1 Nov 1 Dec 1 Jan 1 Feb 1 Mar 1 Apr 1 May 1 Jun 1 Jul 1 Aug 1 Sep 1 Oct 1 Nov 1 Dec 1 Jan 1 Feb 1 Mar
2019
T3.1 START
M312 TEST APPLICABILITY ARCHITECTURE
T3.3 START
M321 INITIAL FEDERATION
M322 INITIAL PILOTS TESTING FEDERATION
2022

FENIX contribution DTLF Subgroup II (i)

- **Plug&Play Building Block**:
  - Decentralised ecosystem > each platform runs its own connector and set of services.
  - Federation is 'hidden' to the users through its platform of choice.
  - FENIX specifies an onboarding process
    - Platform onboarding > focused on trust, security and technical onboarding
    - Technical onboarding > each platform develops its own connector following the FENIX connector specification
    - Member onboarding > focused on business and its description of service and data offering
  - Governance tasks aligning the mechanisms for the platform onboarding + alignment with technical onboarding.
  - Each entity can choose its own platform of choice and it is integrated according to the facilities offered by each platform.

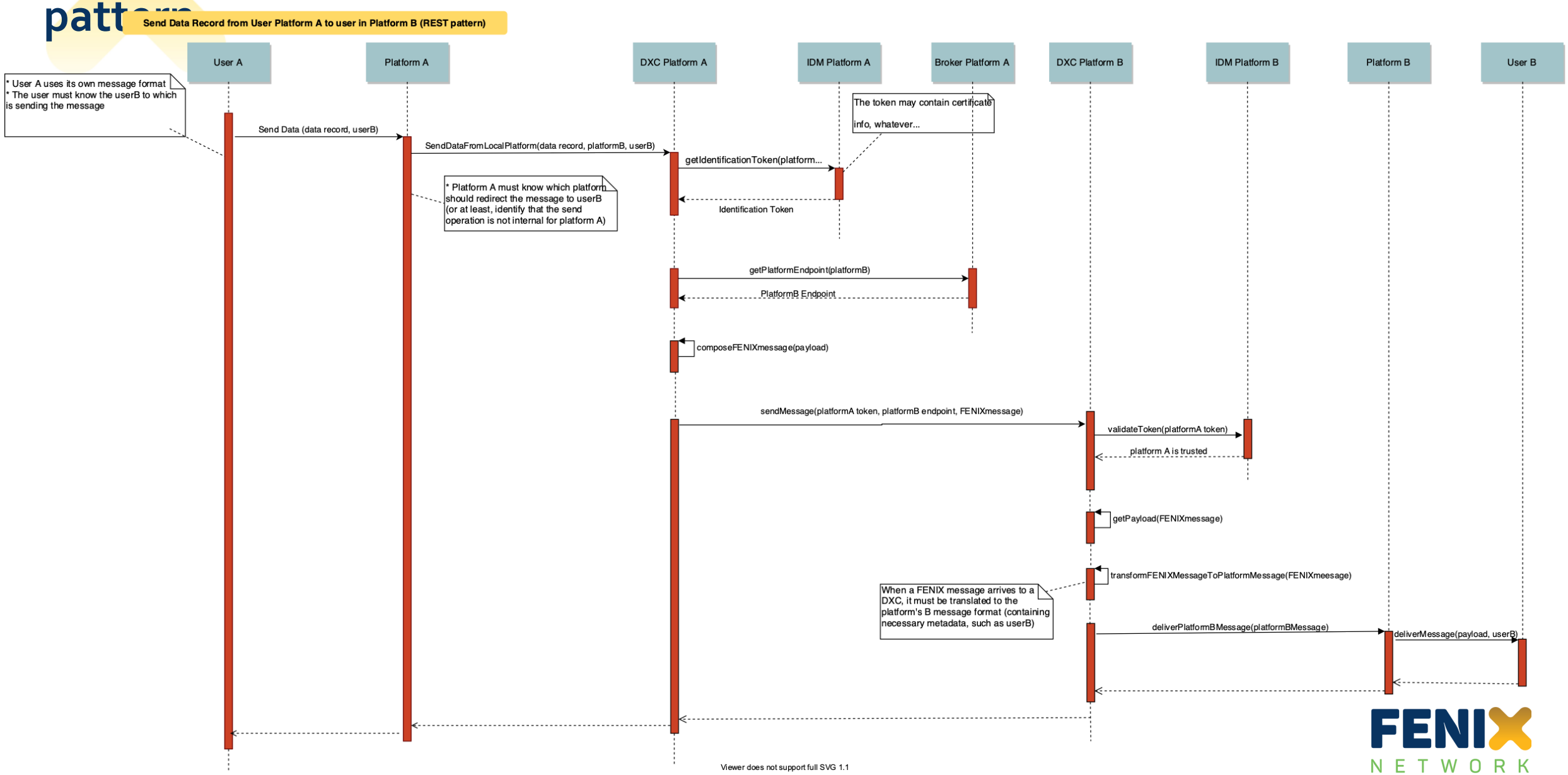
FENIX NETWORK

FENIX contribution DTLF Subgroup II (ii)

- **Technology Independent Services Building block**:
  - Connector specification must be implemented by each platform in its own technology and enables independence when it is validated
  - Interoperability between connectors is guaranteed
  - FENIX Connector Broker
    - Allows data/service owners to register, modify or remove metadata information of the resources. A common service description metadata model must be used.
    - The connector 'standardises' the metadata information given to enable discovery service to search and discover resources (data and services) available in brokers of the networked ecosystem.
    - FENIX distributed catalogue of services.
  - FENIX Connector Data Exchange
    - Different communitacion patterns to be supported to allow each platform to use their choice: request/response(REST), publish-suscribe, EDI.
    - At payload level, it is under discussion to use dictionaries in the Exchange operation.

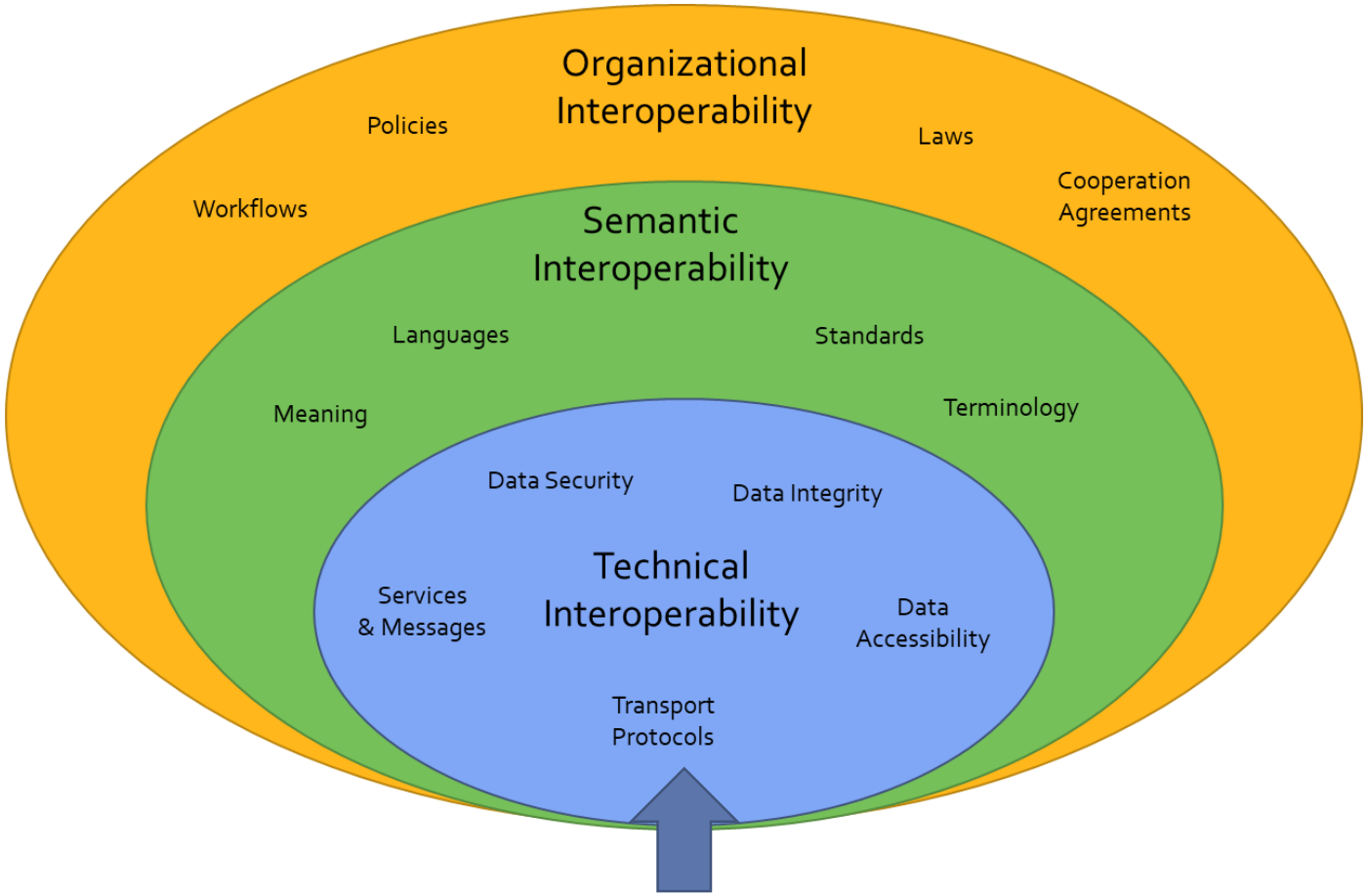
FENIX NETWORK

Sequence diagrams on the Data Sharing using Request/Response patt



FENIX contribution DTLF Subgroup II (iii)

- **Network of platforms and peer-to- peer solutions building block**:
  - Decentralisation, ecosystem of data and services, trustworthy and data sovereignty - not a centralised entity owning the ecosystem.
  - Connector as key element for the network of platforms.
  - Interoperability.
  - Certification process.



FENIX Connector ensures technical interoperability

FENIX NETWORK

FENIX contribution DTLF Subgroup II (iv)

- **Trusted, Safe & Secure Building Block**:
  - Governance model
    - Defines an on-boarding process for each platform to participate in the federation to ensure trust among participants
    - Under discussions in subactivity T2.5
  - Certification process
    - A Certification Body awards a certificate to the applicant with a limited validity period to guarantee trustworthy data exchange or service use within the FENIX network
    - An identity provider offers identity information for trustwothy access on network capabilities
  - Identity Management (at platform)
    - Identification, authentication and authorisation
    - Is responsible for validation of certificates and handling of the own FENIX certificate (in the future)
    - Access rights is up to each platform, information on requesting user service will be checked by requested IdM or related sub service
  - Decentralised approach, i.e. it is a distributed development and maintenance. The Federation must maintain and improve the specification (i.e. new communication patterns or security protocols to be supported, etc.)
  - Data privacy and user pseudonymisation must be respected

FENIX NETWORK

Thank you for your attention!

www.fenix-network.eu

Dr. Eusebiu Catana

Innovation & Deployment

ERTICO-ITS EUROPE

e.catana@mail.ertico.com

Co-financed by the European Union
Connecting Europe Facility