

Future Fédération des Plateformes caribéenne: Étude de cas Par: Le Projet Fenix

ASSOCIATION DES ÉTATS DE LA CARAÏBE (AEC)
XXXI^{ème} RÉUNION DU COMITÉ SPÉCIAL SUR LE TRANSPORT
Mardi 23 août 2022, République de Trinidad et Tobago



FENIX- A Federated Network of Information exchange in Future Logistics
-future Caribbean federation of platforms-
-ASSOCIATION OF CARIBBEAN STATES (ACS) –
31st MEETING OF THE SPECIAL COMMITTEE ON TRANSPORT

Dr. Eusebiu Catana
FENIX Project coordinator
Brussels, Belgium

Tuesday August 23rd, 2022 – via videoconference

OUTLINE



Activity - Objectives



Positioning



Timeline



Effort



Activity structure and tasks



Deliverables



Milestones and Risks



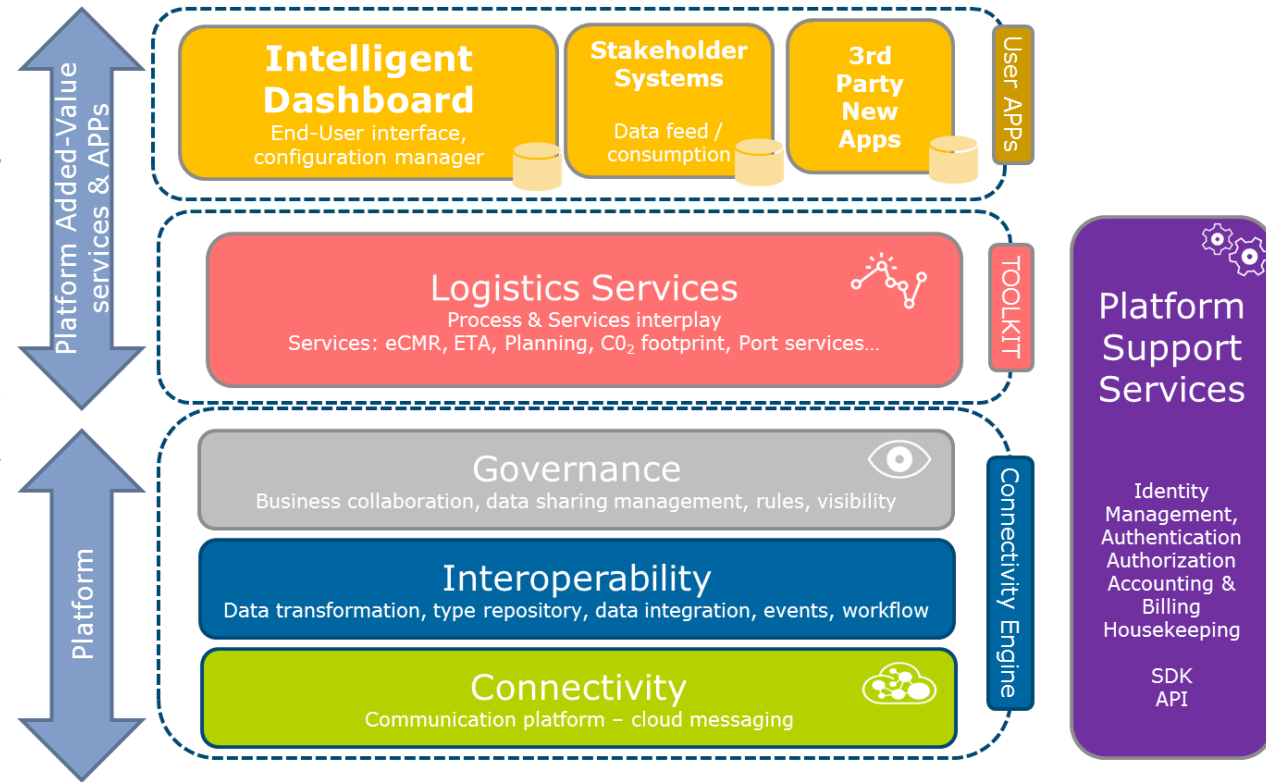
Methodology



Questions

Marketplace: AEOLIX ambition

- AEOLIX aims to overcome today's fragmentation and lack of connectivity around ICT-based systems for logistics decision making
- Develop a cloud-based, multi-enterprise "many-to-many" network which captures and streams data in real-time, and automatically translates "data format" from different IT systems giving companies the ability to rapidly respond to issues through a customised dashboard.
- 20% reduction in greenhouse emissions compared to the current situation.



118 MEMBERS

198 USERS

133 DATA SOURCES

25471049 MESSAGES SENT

11 SERVICES

33257 SERVICES REQUESTS
55644 SERVICES RESPONSES

AEOLIX Total counter

38,000,491

a few seconds ago

Last 24h Counter

232,817

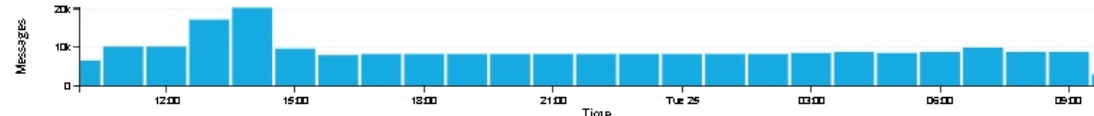
a few seconds ago

AEOLIX Dashboard counter

11,793,182

a few seconds ago

Last 24h Histogram



a few seconds ago

FENIX
NETWORK



Multi/syncromodal Transport

- Thessaloniki-Balkans & central Europe via rail/road
- Gothenburg-Hamburg, Bratislava load control centre, Trieste to three TEN-T corridors (Scandinavian-Mediterranean, Mediterranean, Baltic-Adriatic)
- Urban Bordeaux & Atlantic Corridor
- UK - Continental EU - China logistics
- Bucharest-Vienna: Inland waterway

Intelligent Hubs

- Sea ports: Hamburg, Gothenburg, Bordeaux, Trieste
- Railway hubs: Hamburg, Trieste Northamptonshire
- Inland waterway (barge) terminals: Bucharest Vienna
- Cities: Bordeaux, Gothenburg
- Virtual freight centres: Thessaloniki Industrial Area

Network Optimisation

- The whole logistics network, incl. ports, inland transport (road, train, barge) in The Netherlands, Germany and Spain
- All sites that will cover multi/ synchromodal transport



Logistics Living Labs

AEOLIX is testing, validating and demonstrating the collaborative logistics ecosystem in a number of living labs which cover all the nine TEN-T corridors.



INTELLIGENT
HUBS



MULTI-/
SYNCHROMODAL
TRANSPORT



NETWORK
OPTIMISATION

Living Lab 8:

UK - Europe - Far Eastern Logistics Control Enhancement - Northampton (UK) and mainland Europe

Living Lab 9:

Cross Chain Collaboration - Rotterdam, Venlo (Netherlands), Duisburg (Germany), Milano (Italy)

Living Lab 10:

Collaboration in automotive Industry - Galicia (Spain)

Living Lab 6:

Intelligent Port and City - Port of Bordeaux (France)

Living Lab 2:

Termi Lab - NTEX terminal network, hauliers, customs operatives (Sweden and around the North Sea)

Living Lab 7:

FMCG Logistics - Malmö intermodal terminal, COOP central DC in Bro (Sweden)

Living Lab 1:

Intermodal Logistics Management - Port of Hamburg, Frankfurt/Rhein-Main area (Germany)

Living Lab 11:

Mondelez Load Control Centre Connectivity - Bratislava (Slovakia)

Living Lab 5:

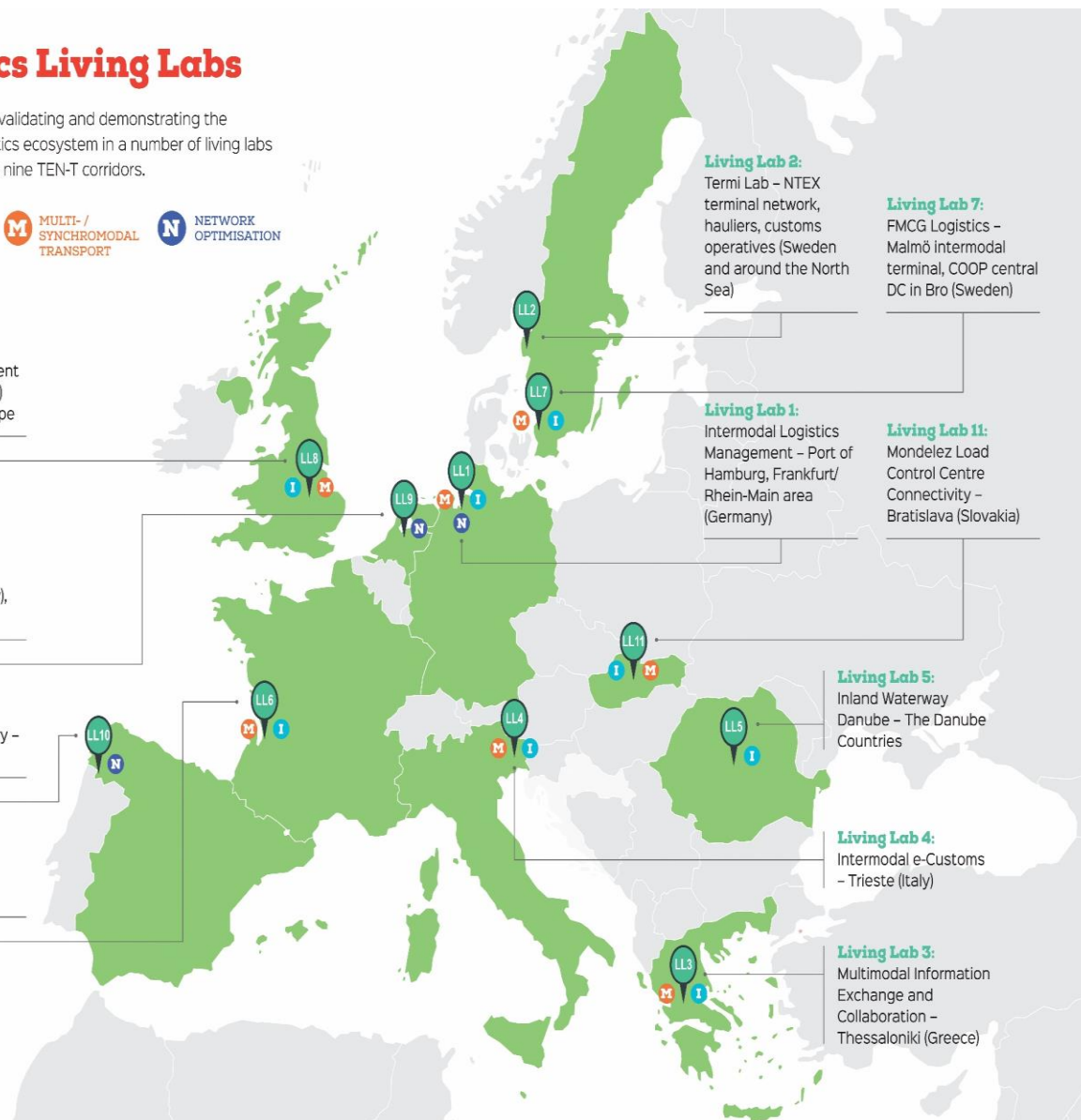
Inland Waterway Danube - The Danube Countries

Living Lab 4:

Intermodal e-Customs - Trieste (Italy)

Living Lab 3:

Multimodal Information Exchange and Collaboration - Thessaloniki (Greece)



Why FENIX?

FENIX - A European Federated Network of Information exchange in Future Logistics-federation of platform

based on the work and recommendation of the Digital Transport and Logistic Forum (DTLF) sub-group 2 (corridor information systems) to create a viable and valid federative network of platforms as enabler for Business to Administration (B2A) and Business to Business (B2B) data exchange and sharing by transport and logistics operators.

GA negotiations:

FENIX does not strive to develop a new centralised solution with its own specific functionalities and does not create another platform.

FENIX is planned as non-commercial "open solution", not "privately owned" and technologically independent.

- All the new pilot sites guarantee that they will not replicate or duplicate work conducted in AEOLIX and SELIS projects.
- The two mentioned research projects permitted the development of a PoC(TRL5/6).
- FENIX will pre-deploy and deploy of the future pan-European innovative architectures for the management of logistics services(TRL8) across the TEN-T corridors.

OBJECTIVES

Main project objectives:

- 1 establish a federated network of transport and logistics actors across Europe, enabling sharing of information and services needed to optimise TEN-T (A2&A3)
- 2 demonstrate the operational feasibility and benefits through the organised national pilots –focus on testing the achieved interoperability capabilities (A4)
- 3 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 Test sites

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



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

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



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



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



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



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

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

AT GLANCE+many NON-EU contries

Test site Austria: Customs corridor -Fürnitz (South Austria) on the Baltic-Adriatic corridor

Test Site Belgium: PS BE 1- AirCargo (Be)

PS BE2- Multimodal inland Hub-Procter & Gamble-Mechelen-Willebroek (Be)

Test site France: French Mediterranean – 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

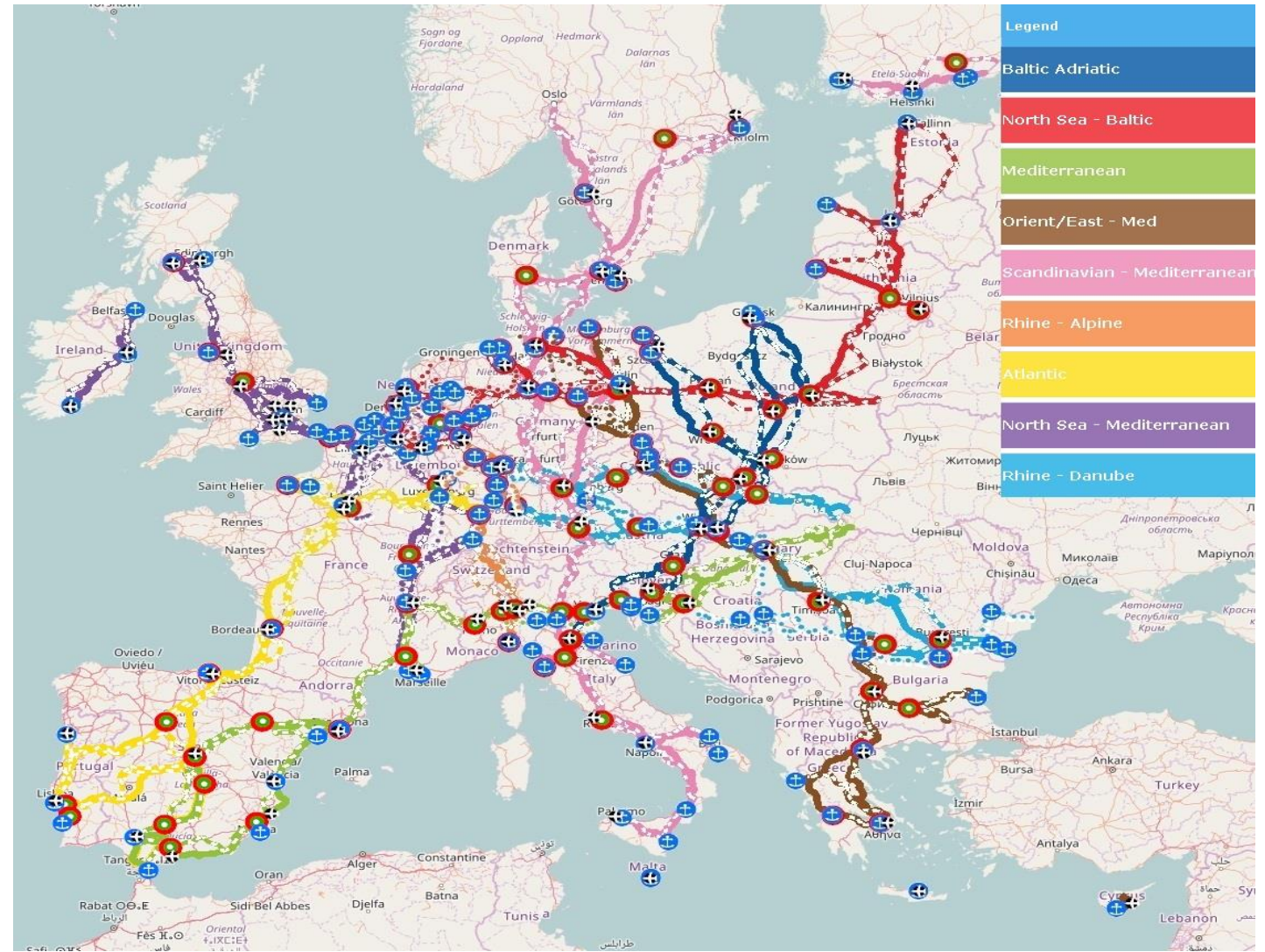
Test Site Italy: PS IT1- Mediterranean and Baltic-Adriatic and the Motorway of the Sea of South-east - Trieste

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 hubs**
- **Network Optimisation**



Technology Integration



Activity 3 objectives



Platform Federation



Security (Encryption + Auth)



T&L corridor services



Software integration



Test cases



Quality



Activity 3 Positioning

Activity 1 – Project Management

Activity 3 – Technological Integration

T3.1 – Fenix Architecture

T3.2 – Fenix Fed Infrastructure

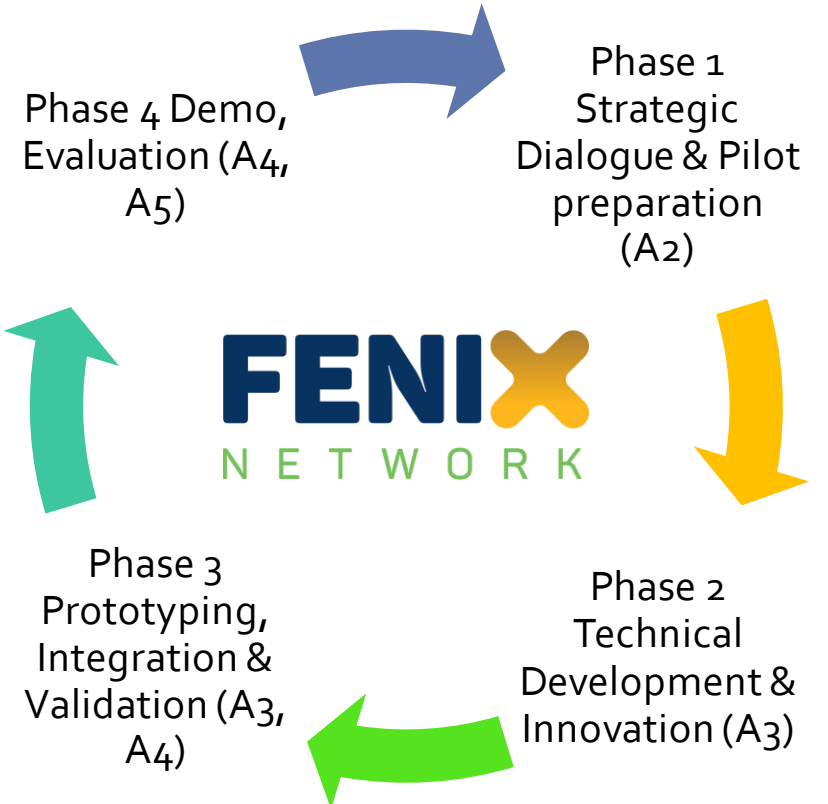
T3.3 – Services & Applications

T3.4 – Integration & Verification

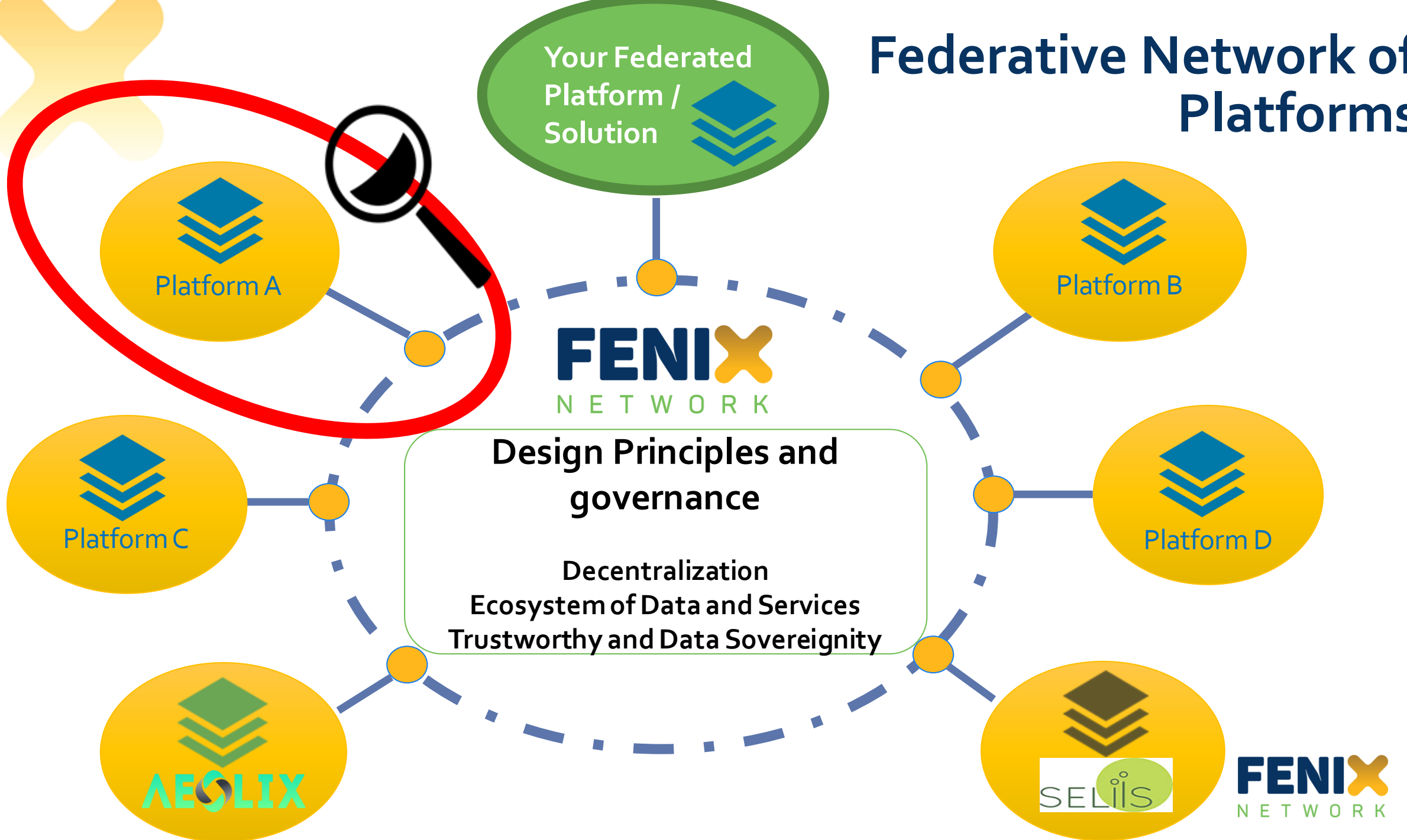
Activity 5 – Evaluation

Activity 4 – Pilots roll out

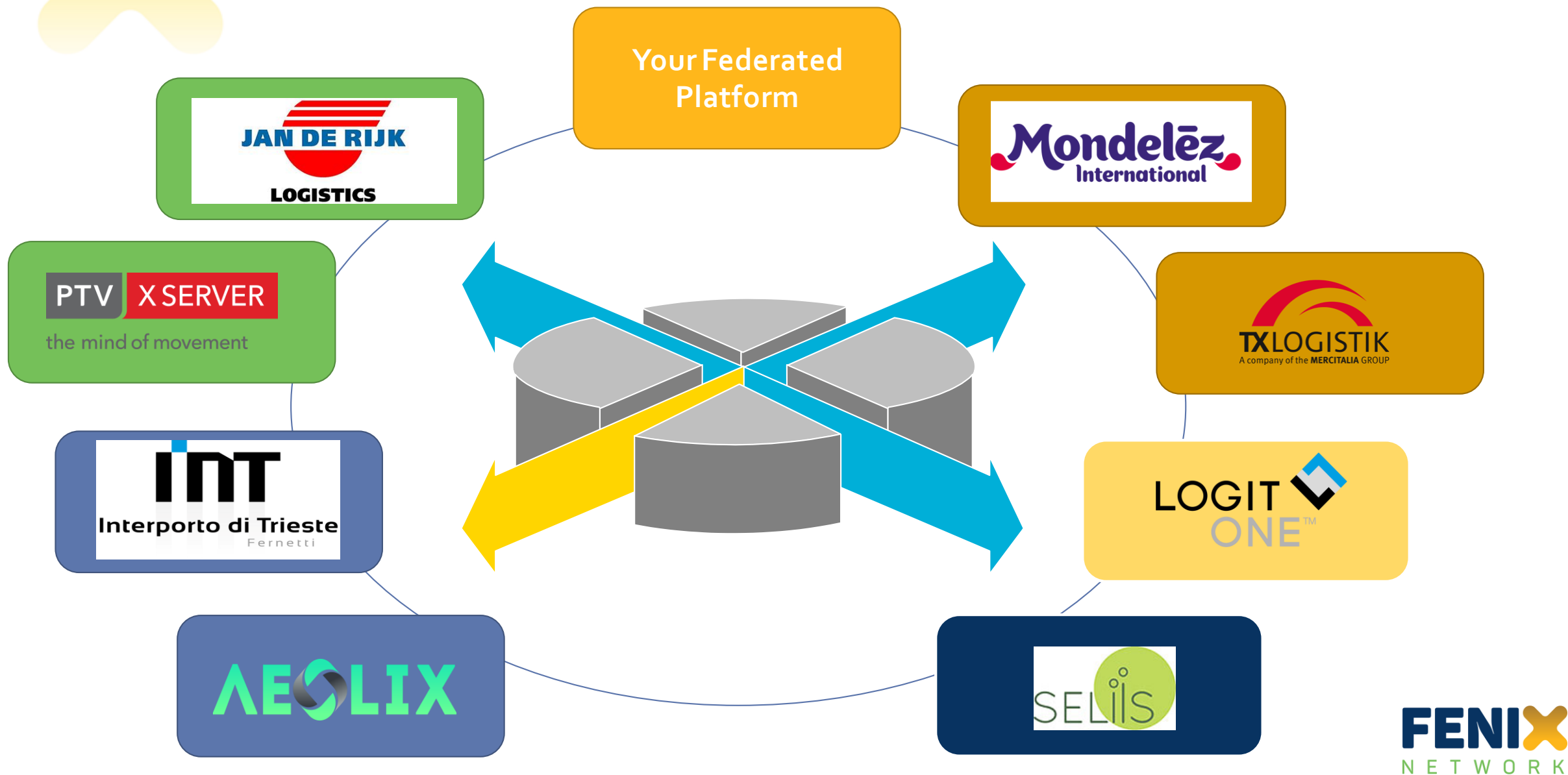
Activity 6 – WG, Recommendations & Best Practices



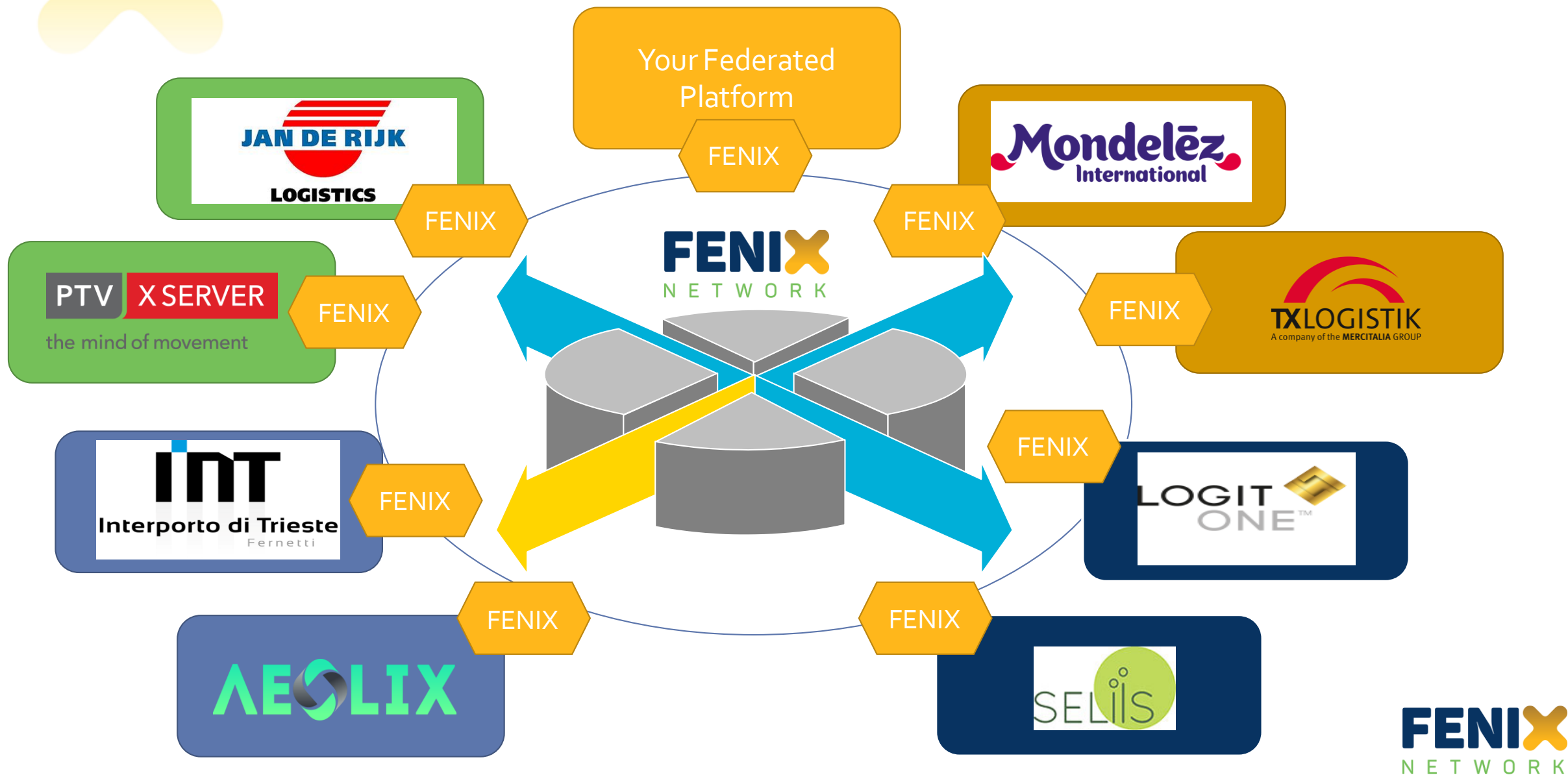
Federative Network of Platforms



FEDERATIVE NETWORK OF PLATFORMS



FEDERATIVE NETWORK OF PLATFORMS





FENIX IT Framework - Design Principles and governance

- **Decentralization:** FENIX does not strive to develop a new centralized solution with its own specific functionalities and does not create another platform. *In federation the different nodes of the network retain their internal control.* **Decentralized access control to data or services** should be put in place.
- **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.
- **Trustworthy and Data Sovereignty:** *Trust is the basis of the FENIX IT Framework,* which should provide guidelines to ensure the trustworthy between the federated platforms and support data sovereignty. As well, the communication between the nodes of the federation must be secure.

Strategic principles and features

Federation

- According to [businessdictionary.com](https://www.businessdictionary.com/definition/federation.html), a federation is an organization that consists of a group of smaller organizations or companies that works to bring attention to issues that are of importance to all of its members. Each organization that comprises the federation maintains control over its own operations.



- At **strategic level**, FENIX addressing 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

Strategic principles and features

Decentralized approach



- FENIX architecture does not rely on a centralized 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

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

Strategic principles and features

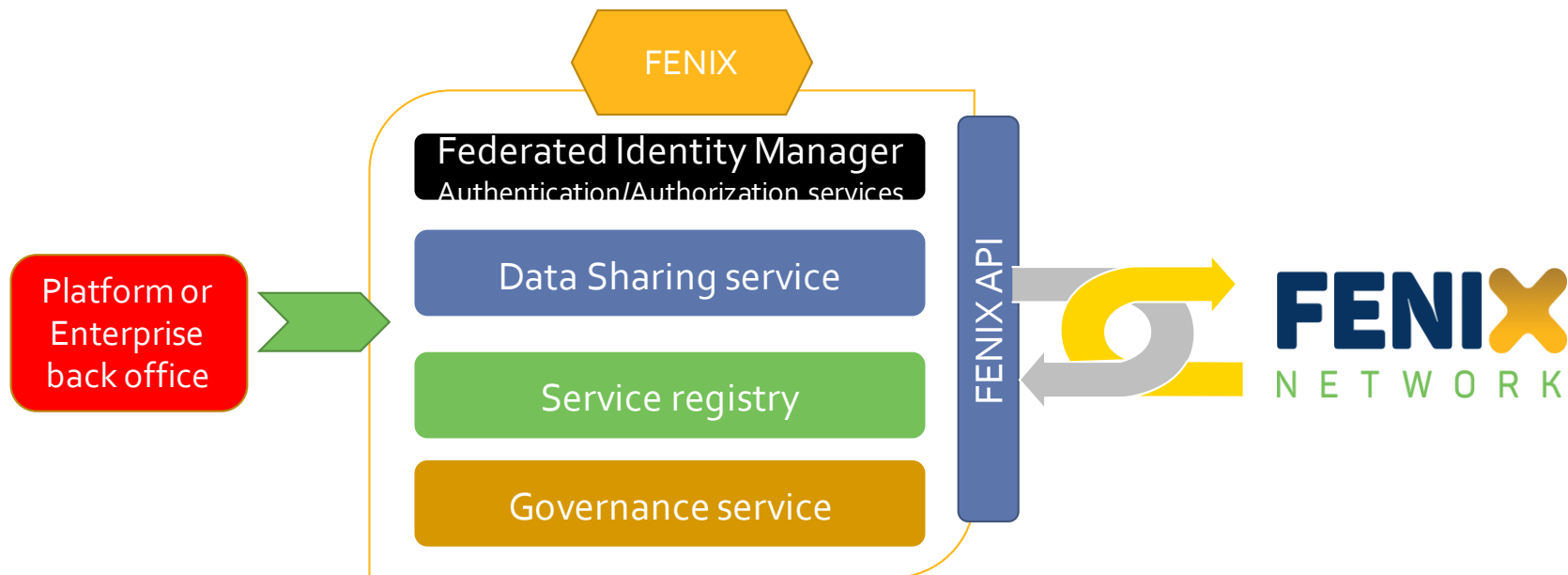
Trustworthy and Data Sovereignty



- 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 trustworthy between the federated platforms and 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 – A federated ecosystem

- Federated services will be implemented with 3 main pillars:
 - Federated Identity Registry***
 - Governance and Data Sharing Federated Services***
 - Corridor Service Registry***
- A new “Gateway/AP/protocol” specification which fits in the business processes based on:
 - Federated identity systems and management: common recognition of credentials, single authentication, common privacy and security policy
 - Building block specification for sharing of logistics-related data governance, services and data sharing (API): Data sharing service, Service (registry) offering, Data / Service discovery





More technical detail > ongoing work

User Stories + scenarios + use cases

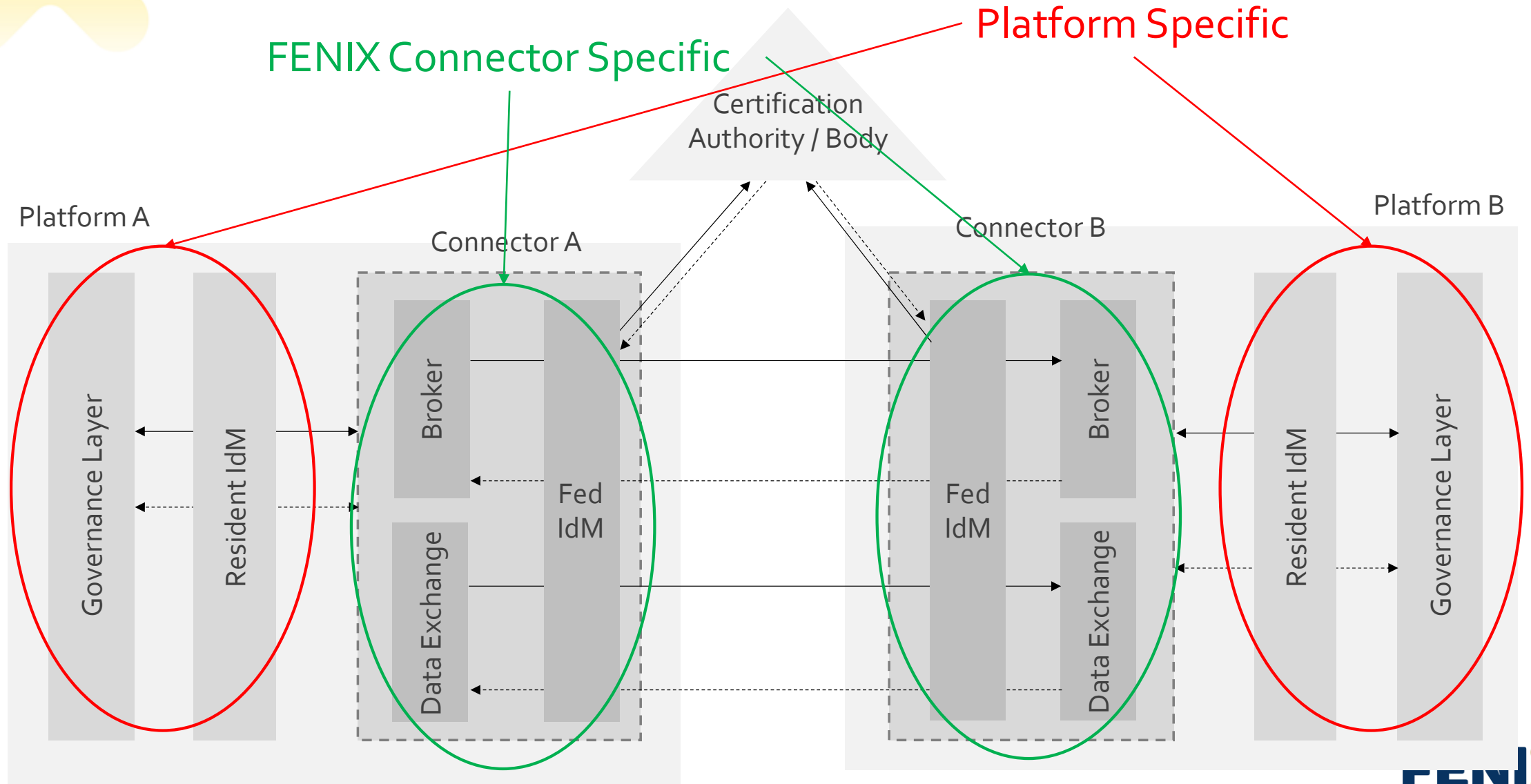
- Federation members agrees on governance model and rules of the ecosystem.
- Each node of the federated network maintains their own internal control, but share the fed-functionalities with the rest of the federated platforms
 - The federation will have a special node in the network, acting as 'Certification Node' which its main technical functionality at operational level is to keep an updated registry of the certified and trusted federation nodes that are participants of the network
- Each node of the network must enable data exchange functionalities and communication among the different nodes to allow members of the federation the ability of collaboration between them and share data assets or access to services. Access policies for data and services
- Each node of the federation provides a broker functionality composed by a service catalog and discovery service, > lookup of the available members, data assets or services available in each of the fed-nodes + a distributed catalog of services and data
 - harmonized data and service description
- Data privacy and user pseudonymization must be respected.
- To use the data, the data consumer must fully accept the data owner's usage policy

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	Authorize to make use of a resource
F-US-005	Send/Receive Data through the FENIX connector

FENIX Connector Specifics





The FENIX Connector Specification

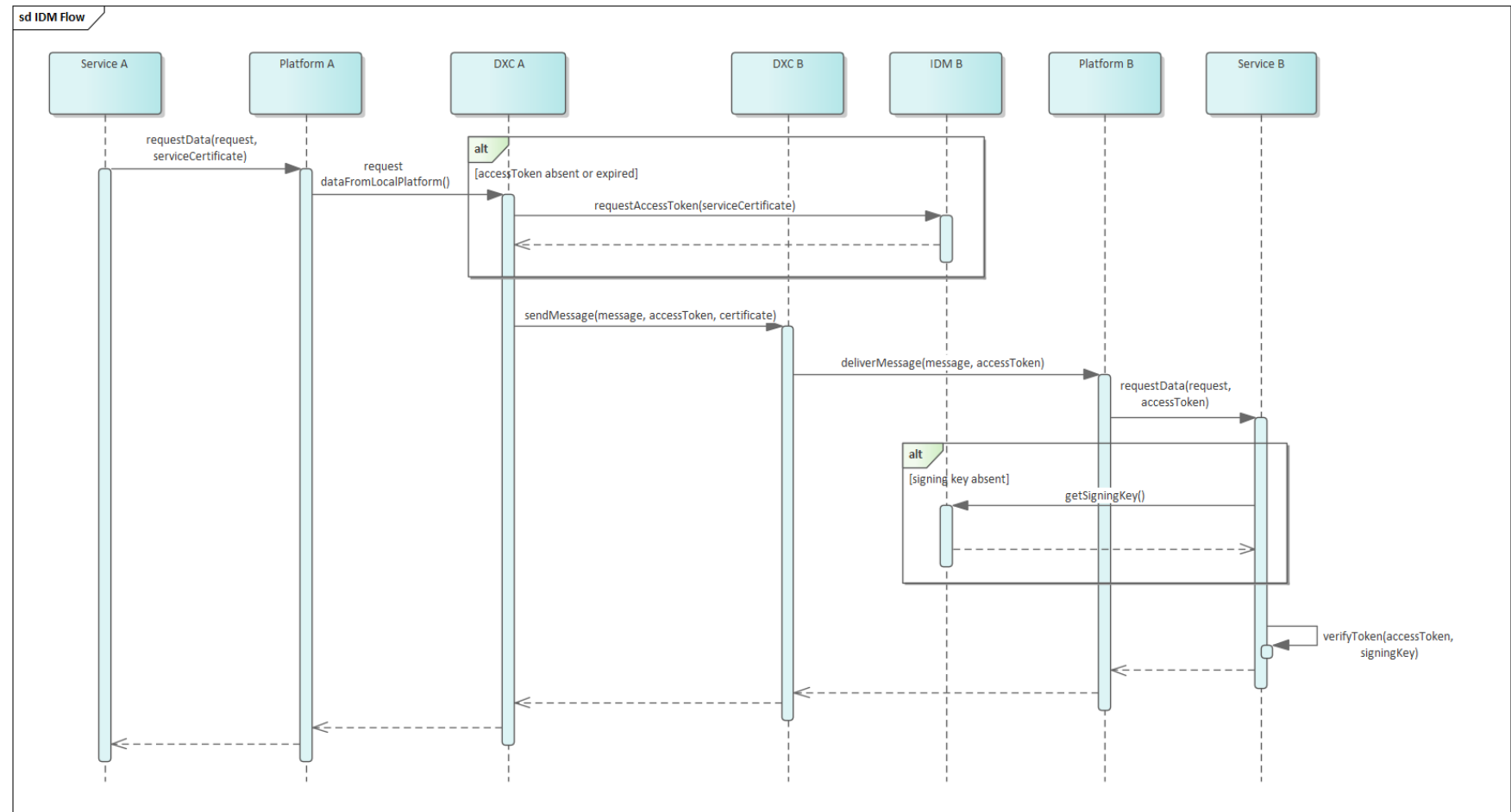
- Security
 - Certificates → Machine to Machine Communication
 - TLS v1.3 and mTLS
- Identification & Authorization – Access Token, Oauth 2.0
- Catalogue of Resources
- Data Exchange
 - Communication Patterns
- FENIX message Structure

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

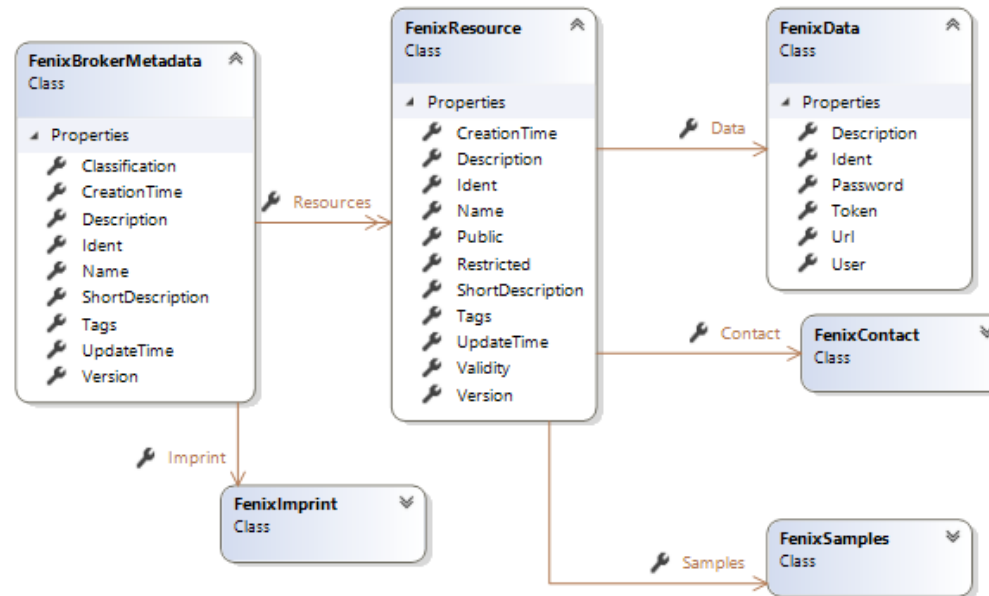
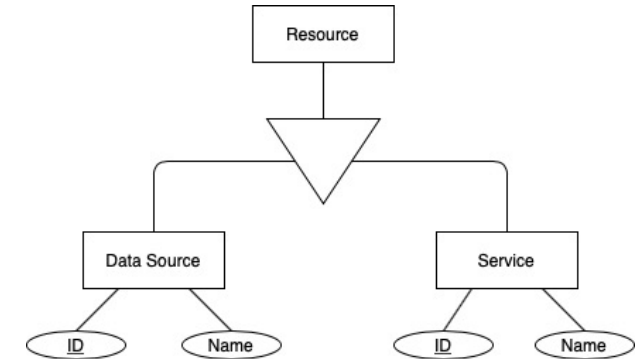
The FENIX Connector Specification – Identification & Authorization

- 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

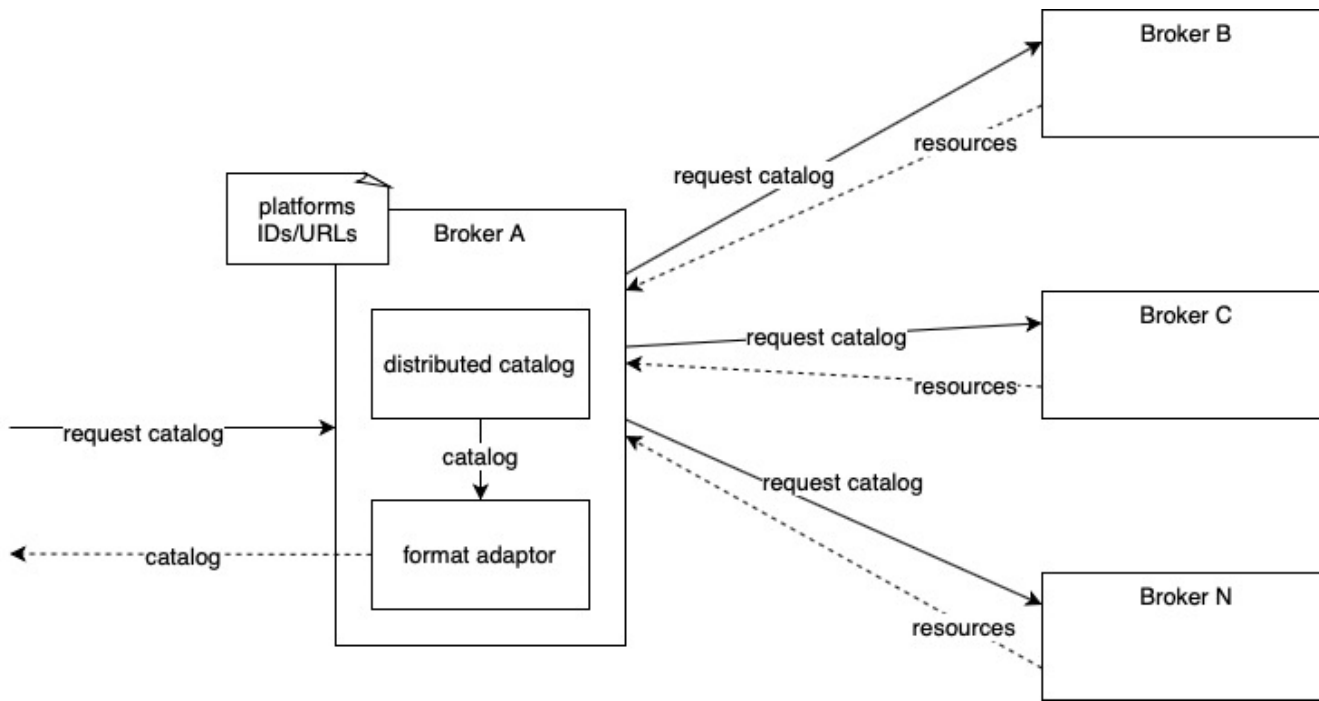


The FENIX Connector Specification – Catalogue of Resources

- Any member of the FENIX federation can share or consume **Resources**
- Every platform must generate its catalogue of resources following an 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 Restricted



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

The FENIX Connector Specification – Data Exchange

- To exchange data between FENIX connectors, it has been specified 3 different communication patterns:
 - 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

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 platform 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 retrieve 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'
      }
    ],

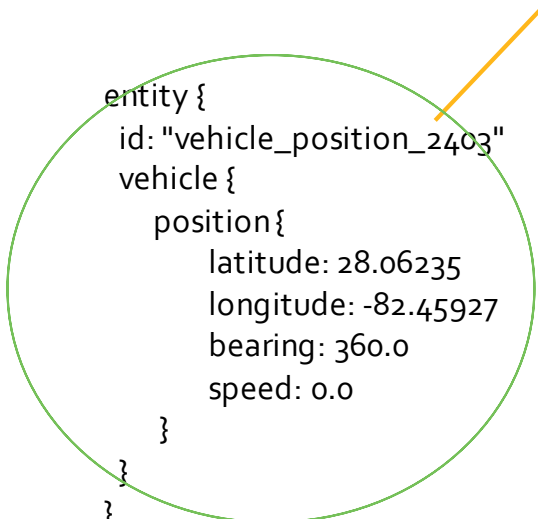
    "mic" : 'Message Integrity Code'
  },

  "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 me



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



The diagram illustrates the Fed-IDM architecture stack. It consists of three main components stacked vertically within a green container:

- Fed-IDM** (black box, top layer)
- Exchange** (blue box, middle layer)
- Broker** (red box, bottom layer)

An orange arrow points to the **Exchange** component, indicating its role in the system.

The diagram illustrates the Fed-IDM architecture. It consists of three main components stacked vertically within a green container: a black box labeled 'Fed-IDM' at the top, a blue box labeled 'Exchange' in the middle, and a red box labeled 'Broker' at the bottom. An orange arrow points into the 'Exchange' box from the left, and another orange arrow points out of the 'Exchange' box to the right, indicating its role as a central hub for data exchange.

```
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":"tBrDrMNe2L&JSOgNSZpQQKDgfC5I9eldDNUJmShnAyuHk3TjqGH6tB
KFs8nAEJkyCWI36oeQgOg1tOXO0OEQ"
  },
  "Original_Msg":{
    "Msg_Format":"GIFS",
    "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 → Future of Logistics

- **TRUST:** Trust is the basis of the FENIX. To use the data, the data consumer must fully accept the data owner's usage policy.
- **ECOSYSTEM OF DATA:** pursues the idea of decentralization of data storage, which means that data physically remains with the respective data owner until it is transferred to a trusted party.
- **STANDARDIZED INTEROPERABILITY:** is implemented in different variants and can be acquired from different vendors.
- **VALUE ADDING APPS:** includes also services for data processing, data format alignment, and data exchange protocols.
- **DATA MARKETS:** FENIX enables the creation of novel, data-driven services that make use of data apps.
- **PI:** FENIX enables the creation of new ICT infrastructure to support operations in future PI logistics networks



Q&A





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