

IATA – ONE Record LL - Internet of Logistics

Henk Mulder – March 2023

Architectural Overview
For the
FEDeRATED Architecture Board



ONE Record

Ontology:

- 74 classes
- 205 object properties
- 289 data properties

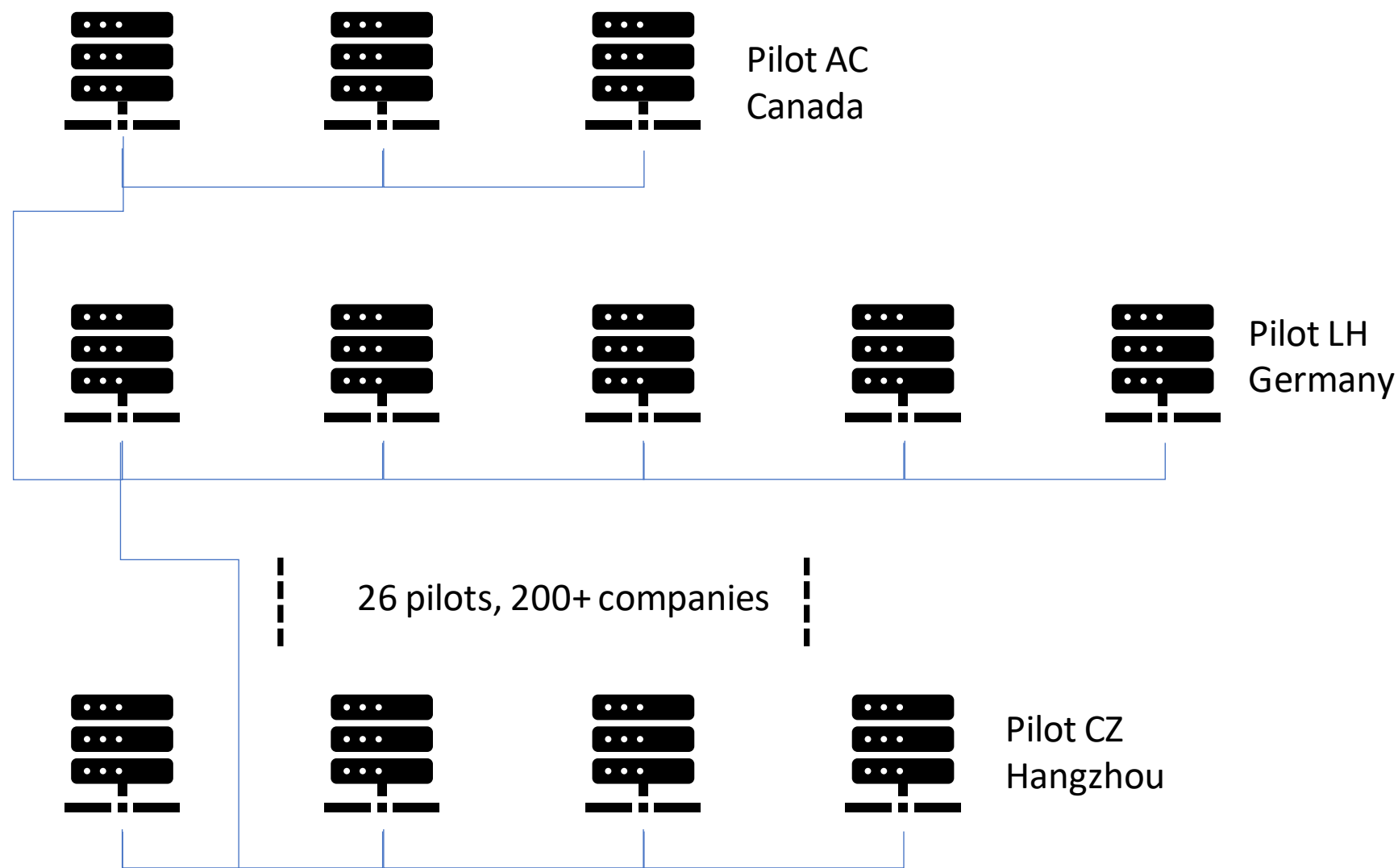
API:

endpoints for:

- Logistics Objects
- Pubsub
- Events
- ACL & delegation

IAA:

- X.509 certificates
- Mutual TLS
- OAUTH2.0





ONE Record / FEDeRATED Network bridge

Ontology mapping

- Common events (ETA etc)
- Digital Twins (transport twins)

Index:

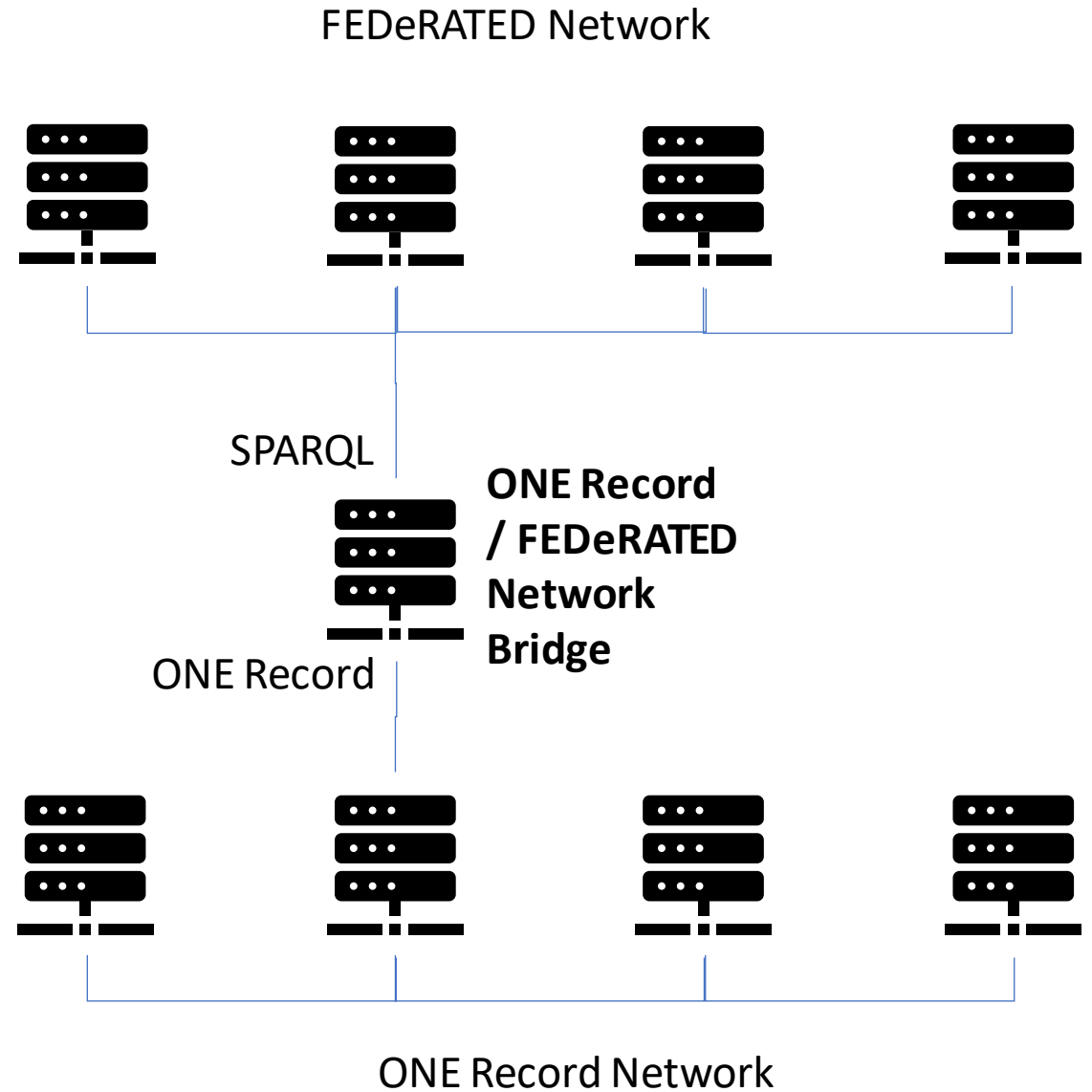
- Index specs mapping onto 1R / FeD bridge API

IAA:

- TBD

Registry

- Mapping possible but not until registry specs are understood

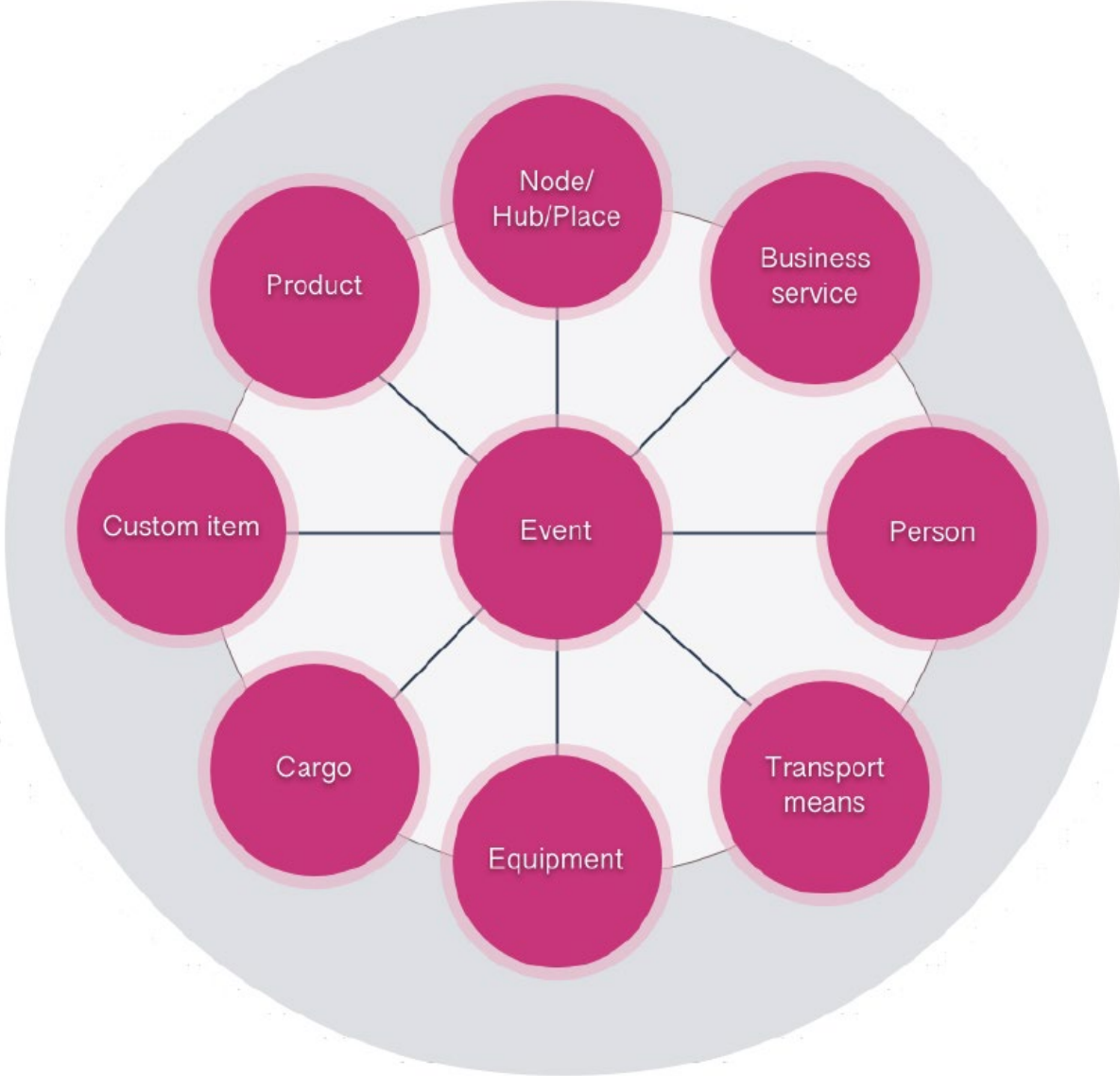


FEDeRATED ↔ ONE Record Network interoperability

IATA ONE Record – semantic model



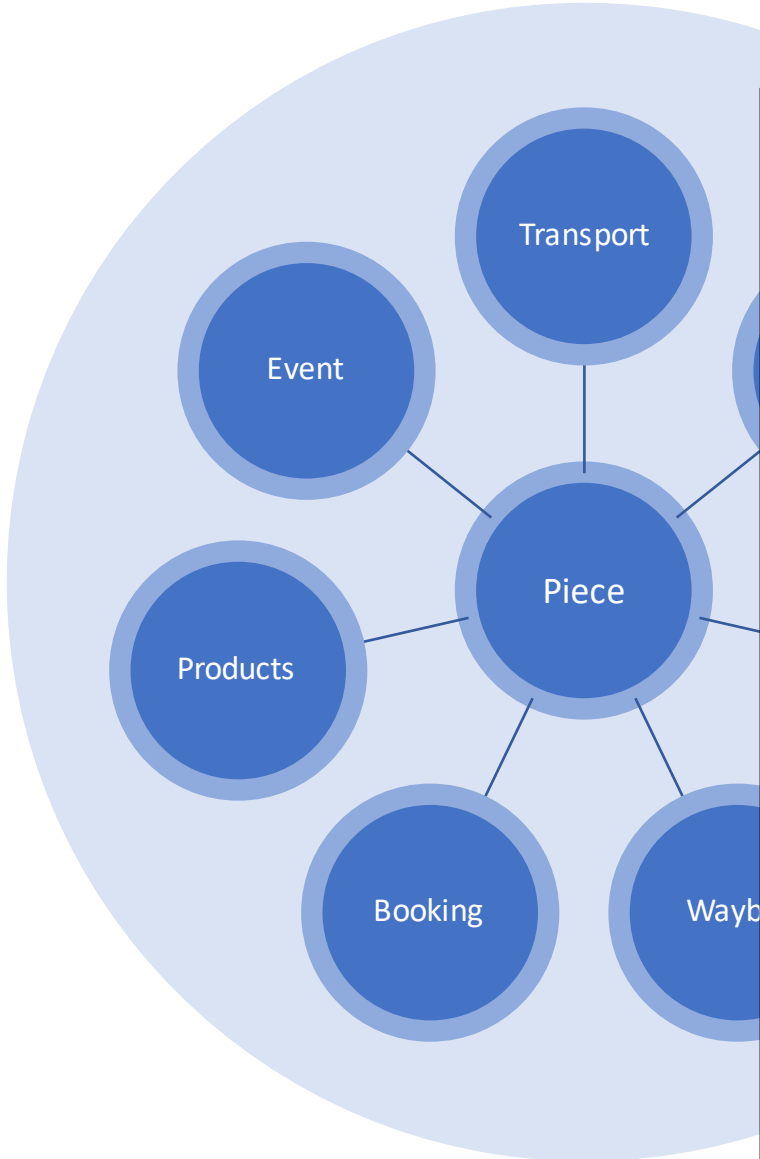
FEDeRATED semantic model



FEDeRATED ↔ ONE Record semantic models

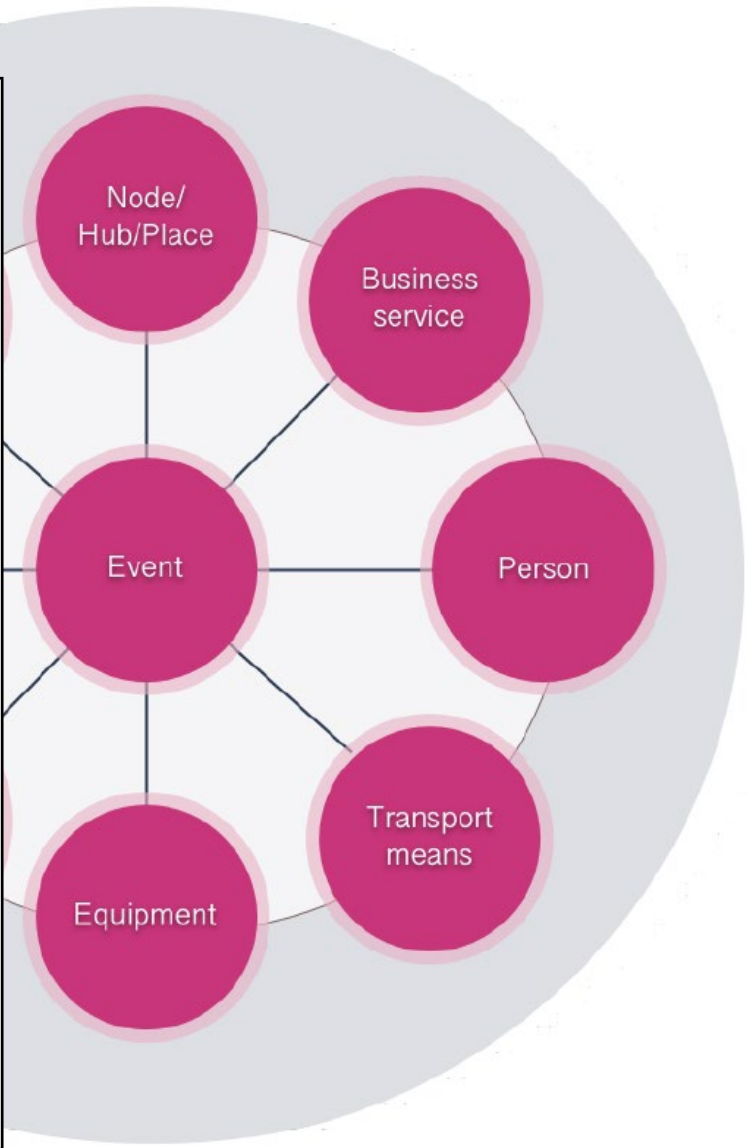
IATA ONE Record – semantic model

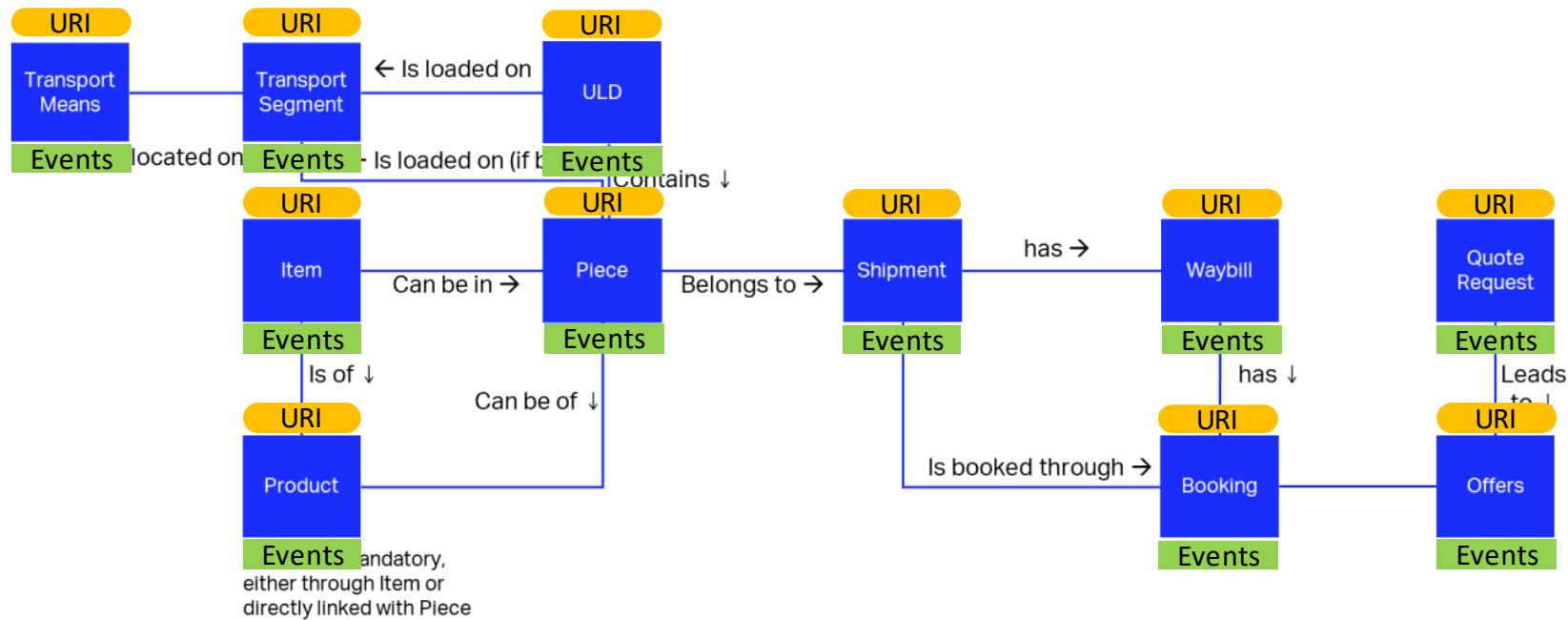
FEDeRATED semantic model



ONE Record the same semantic technologies, tools and concepts as FEDeRATED. There a few differences:

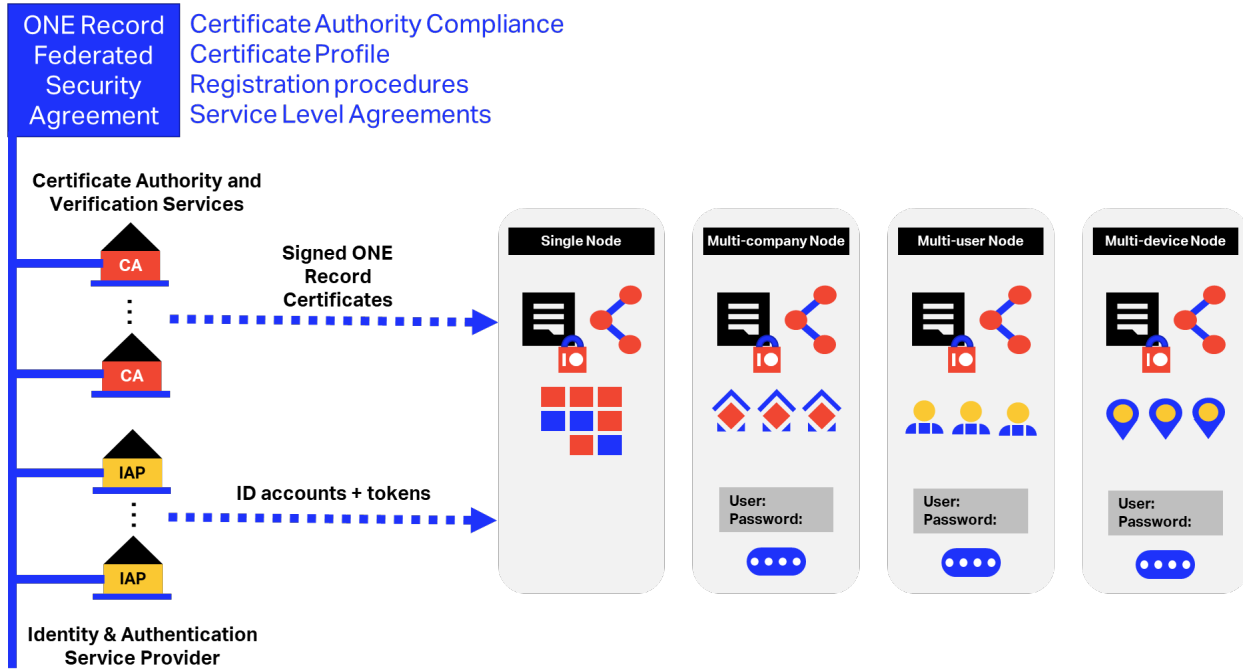
- ONE Record is **piece-centric**, i.e. it puts freight at the center of its model. FEDeRATED is **event-centric** which is at the basis of logistics chains. One of partners is a global logistics provider and they put their **service-centric** at the center of their model.
- This reflects a fundamental difference between transport vs logistics. Using semantic queries, ALL necessary data is accessible, but logistics and transport provides cannot use eachother models as a basis for development.





- ONE Record makes all its Logistics Objects available via their URIs. This allows 3rd parties to access relevant data, whether that concerns transport planning, operations, tracking, financial process or logistics.
- In ONE Record, an event is an attribute in the superclass of any logistics object, i.e. *every* object can have events.
- FEDeRATED focuses on publishing logistics events only.
- From this perspective, ONE provides a multi-dimensional holistic view of freight. To produce a FEDeRATED index, we would define a subset of events related to tracking publish these on a dedicated FEDeRATED endpoint.

- ONE Record has an identity & authorization scheme based on X-509 certificates, mutual TLS authentication and OAUTH2 tokens.
- Initial, we implemented a dedicated Certificate Authority (CA) to issue identities and certificates to ALL ONE Record servers.
- This dedicated IATA CA was not the right solution since it required trust from ALL stakeholders which wasn't realistic.
- ONE Record now accepts and X.509 certificate issues by a trusted CA

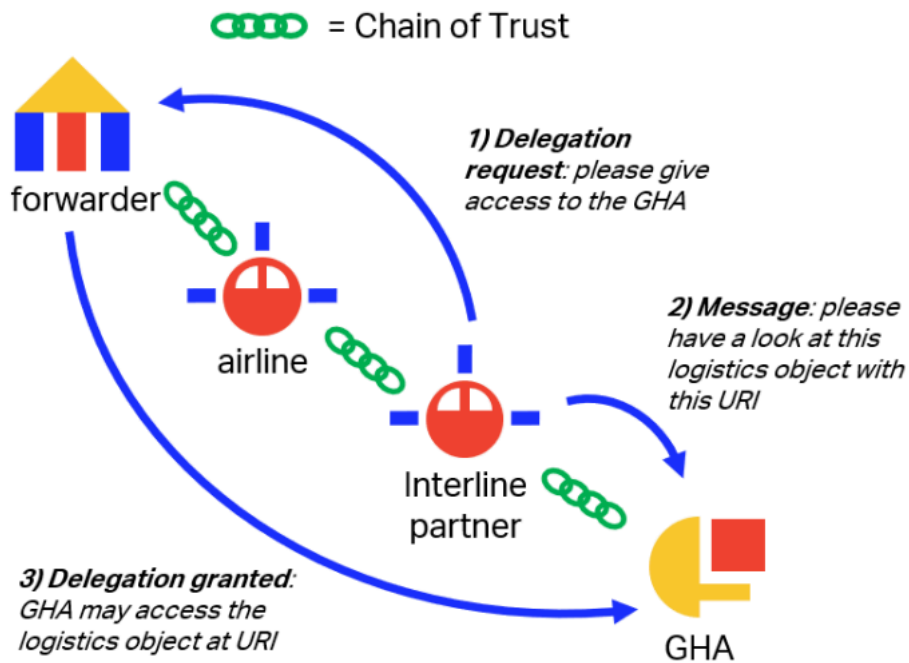


- 1R-ID**
URI that refers to a 1R identity of the node, with the form <https://<FQDN>/<COMPANYID>>
- 1R-SERVER**
Application that accepts ONE Record API requests from a 1R-CLIENT
- 1R-CLIENT**
Application that sends ONE Record API requests to a 1R-SERVER
- TRUSTED CA**
Certificate issuer that is approved by IATA
- ENDPOINT**
Either a 1R-CLIENT or a 1R-SERVER application
- END USER**
Entity that uses a 1R-CLIENT application
- TOKEN**
Authorization token, refers to the OAuth2 standard
- IAP**
Identity & Authentication Provider. Authentication service that implements OAuth2

ONE Record implements the W3C Access Control List recommendation without modification:
→ [Web Access Control standard from W3C](http://www.w3.org/2001/05-28/xmlsec/acl/)

```
# Contents of https://party1.server.com/company/logisticsObject/acl
@prefix acl: <http://www.w3.org/ns/auth/acl#>.

<#authorization1>
  a          acl:Authorization;
  acl:agent  <https://party1.server.com/company>; # Company Identifier in the IoL
  acl:accessTo <https://party1.server.com/company/logisticsObject>;
  acl:mode   acl:Read,
             acl:Write,
             acl:Control.
```

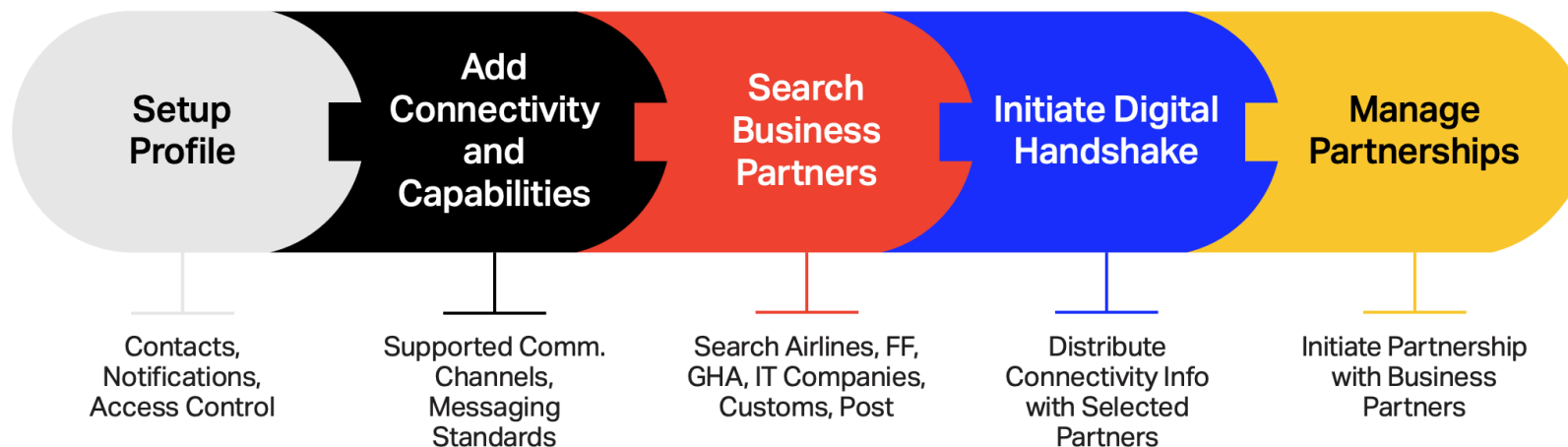



ONE Record implements the concept of **access delegation**.

- By default, all access to any resource is forbidden to all 3rd parties.
- The data owner / publisher is «data sovereign» and may choose to give access to resources to nominated 3rd parties.
- These nominated 3rd parties may request that the data owner / publisher gives access to other parties known to the 3rd parties authorized by the data owner / publisher.
- The data owner / publisher may
 - Refuse such a request,
 - Grant the request
 - Grant the request and subsequently revoke it
- The process and policies for granting access to resource to known or unknown parties is up to the data sovereign data owner.
- In practice, they will include access delegation request decision into their ACL policies.

Enhanced Partner Identification and Connectivity

- IATA uses a centralized digital service registry for all air cargo digital connectivity protocols, including Telex, Telephone, FAX, EDI, Cargo IMP, Cargo XML, **ONE Record and FEDeRATED**
- This connectivity data is managed by the data platform owner which ensures that it is updated.
- Users of the registry use it to ensure their partners have all the connectivity data to minimal manual support.
- User can set up rules to limit access to certain connectivity protocols, to certain markets and to certain partners.



- IATA uses a centralized digital service registry for all air cargo digital connectivity protocols, including Telex, Telephone, FAX, EDI, Cargo IMP, Cargo XML, **ONE Record and**

The screenshot shows the IATA ONE Record API Hub interface. At the top left is the IATA logo. A search bar contains the text "Search for APIs". On the right side of the header, there are links for "Create Team", "Add Your API", "Provider Manual", "Log In", and a "Sign Up" button. Below the header, the main section is titled "Cargo APIs" with a subtitle "APIs related to the distribution, transport and tracking of Cargo." and a search input field. On the left side, there are two sections: "COLLECTIONS" with links for "Recently Added", "Distribution", and "View All Collections"; and "CATEGORIES" with links for "Customer Experience", "Retailing", "Cargo" (highlighted in yellow), "Flight and Ground Operations", and "Financial Processes". The main content area displays three API cards, each with an airplane icon, a bookmark icon, a title, a description, and "REST" and "Airline" tags. The cards are: "Station Information" (description: "With this API you can easily retrieve information about our global Lufthansa Cargo stations."), "Shipment Tracking" (description: "With this tracking API you can easily retrieve the status of your air freight shipment. The API provides you maximum shipment transparency and"), and "Routing Offer" (description: "Benefit from the broad LH Cargo network: Check your product's flight options and timing.").