MASTERPLAN - TECHNICAL SPECIFICATION
IDENTIFICATION, AUTHENTICATION AND AUTHORISATION (IAA)

Identification and authentication is the ability to undisputable establish one's identity. Authorization is the permission or power to perform one or more actions granted by an authority. With respect to data, authorization is the permission to Create, Retrieve (access), Update, or Delete data (so-called CRUD actions).

In a federated network of platforms, each node in the network manages its own data access (CRUD), can have access to data of another organization, and can provide access to data by another organization (R-read).

1. Security framework

IAA is an element of a **security framework** addressing passive – and active attacks to data, processes, and IT systems, where **cyber security** – and other measures (like GDPR and the implementation of other Acts)[1] are another element. With respect to data sharing, the security goals are formulated as:

- **Identification and authentication** (this note). This is part of an active attack, where a malicious organization acts as if it is another organization.
- **Data confidentiality** – when sharing, data is not readable by unintended data users. Passive attacks by intercepting data are not possible. This also relates to (authorized) data access.
- **Data integrity** – during data sharing, data cannot be altered by third parties.
- **Non-repudiation** – an immutable proof provided by the logs and audit trails of data holder and – user that data has been shared (including timestamps of sharing).

Data confidentiality and – integrity can be achieved by signing and encrypting data with an asymmetric encryption algorithm. This is offered by for instance link encryption with https or TLS for data in transit between two nodes. Non-repudiation can be provided by blockchain technology or what has been identified as a clearing house[2] in the IDSA (International Data Space Association) architecture.

2. Inter-organizational trust

IAA is built upon two pillars[3]:

- **Organizational trust** – each organization that wants to become a node[4] must implement measures that assure trust as addressed by the security framework, for instance cyber security measures and an Identity and Access Management (IAM) registry. Authorization is thereby internal to each organization and each organization is responsible for authorizing their own employees only and not those of other organizations. Authorization must

[1] The set of measures that needs to be implemented must be formulated by a regulator.
[2] A clearing house function can also be implemented by blockchain technology.
[3] There is also trust at business level, i.e. the trust in properly executing business activities for customers according to agreements made with them. This trust is outside scope of IAA.
[4] 'Node' is introduced in the high-level architecture document.

consider access to links in an Index of an organization. Rules for creating this type of trust may be formulated by a legal framework.

- **Inter-organizational trust** – each organization must share an identity with another organization that can be verified by that other organization when sharing events, queries, and/or query results.

With respect to creation of (inter-)organizational trust, a separation of concerns is required based on the following roles:

- **Regulator** – a role defining the legal framework and its implementation for data sharing according to an agreed security framework. This is preferably a public (EC) role since many private roles will create competition which does not lead to a federated network of platforms. A regulator must assign registration authorities and certification bodies and monitor their behavior.
- **Registration Authority** – a role that issues a verifiable identity to a node in the network that is used for sharing data. A node receives a verifiable identity if it has been certified according to the implementation rules of a legal framework and its technical specifications established by a Regulator. Existing organizations that already register enterprises and provide an identification may act as issuer.
- **Certification Body** – a role that certifies a participant according to the legal framework and its implementation established by a regulator.

The certification level will be defined by a Regulator. Validation of the implementation of legal framework and its technical specification is **minimal**. A legal framework must be applicable to all organizations.

The implementation of a legal framework may include a continuous monitoring and awareness of each node, especially for cyber security measures. Thus, an identity of a node can be withdrawn if an organization does not meet the required implementation rules.

3. Data

A legal framework and its implementation relate to the types of data in a federated network of platforms. The data can be twofold:

- **Service Registry data** (see Service Registry). This is about a (1) design (SHACL constraints to the multimodal ontology) and (2) organizational profile discoverable via business services.
- **Event (Index) data**. This is about sharing access to data by events with links to that data. Whenever an organization changes data (CUD) in the context of a business transaction, an indication of changes is shared according to a choreography (see semantic model).

Sharing design data is prone to **governance procedures**, where industry associations, communities, etc. operate as nodes. Since design is extendible and flexible, these nodes may include new organizations that need to register themselves. Besides potential cyber-security -and other measures, the **minimal** elements of a security framework for sharing design data are identity and authentication and data integrity. Data confidentiality and non-repudiation are not required. Certification of a design role is based on the agreed governance procedures.

The security framework is applicable to discoverability of business services, supporting organizational profile, and sharing of event data with links.

4. Proposal for Identity and Authentication

Since Authorization is internal to each organization, Identity and Authentication for data sharing must be solved. A distinction between a long-term and a short-term solution is made.

The (long-term) solution is to implement the proposed framework of roles where verifiable credentials (VCs) are issued by trusted (mutual recognized) Regulation Authorities according to a legal framework and its implementation established by a Regulator for both sharing design – and operational (event/queries/query results) data. Any node in a federated network of platforms must be able to verify the credentials based on trust in the issuer.

This solution must be developed as part of the EU (Mobility) Data Space. Since development and implementation will take time, a **(short-term) solution** is preferably a fully distributed solution with limited or no central functionality and OAUTH2.1 tokens. Limited central functionality requires at least a Regulator with a list of trusted Registration Authorities. Such a solution can currently only be based on private bodies (there is not yet a public regulating body) like FENIX and iSHARE, which implies a limited span of control and acceptance of the solution by the market. In the case of iSHARE, so-called iSHARE Satellites must operate as Registration Authorities. These Satellites are like the approach taken by FENIX. No central functionality requires agreement between each pair of communicating stakeholders or platforms, which might be time consuming and hinder rapid on-boarding.

After development of the long-term solution, the migration of the short-term solution for private regulators, registration authorities, and nodes must be formulated.