Are Trust Frameworks ready? Towards achieving Digital Sovereignty in Decentralized Ecosystems and its role in Credentials Exchange

Dr. Bithin Alangot

bithin.alangot@huawei.com

25.04.2023 ASSURE Scientific Workshop 2023 Darmstadt

Disclaimer: Opinions in this presentation are those of the presenter and do not necessarily represent his employers or of working groups, agencies or other associations he is involved in.

HUAWEI

Contents

Motivation

President of the **EU Commission Ursula von der Leyen** on Digital Sovereignty

"Digital sovereignty is the capacity of Europe *to make its* ***own choices****, based on its* ***values****, respecting its* ***own rules.***"

(https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260)

When we talk about digital sovereignty, it is also about our ***ability to guarantee these rights for all Europeans***.

'Digital sovereignty' is not just an economic concept. We are a Union of values. One of the great questions is: How can we preserve and promote our values in a digitized world?

(https://ec.europa.eu/commission/presscorner/detail/fr/statement_20_1999)

EC view on (European) Digital Sovereignty:

European Commission

Europe's ability to act independently in the digital world in accordance to European core values and rules

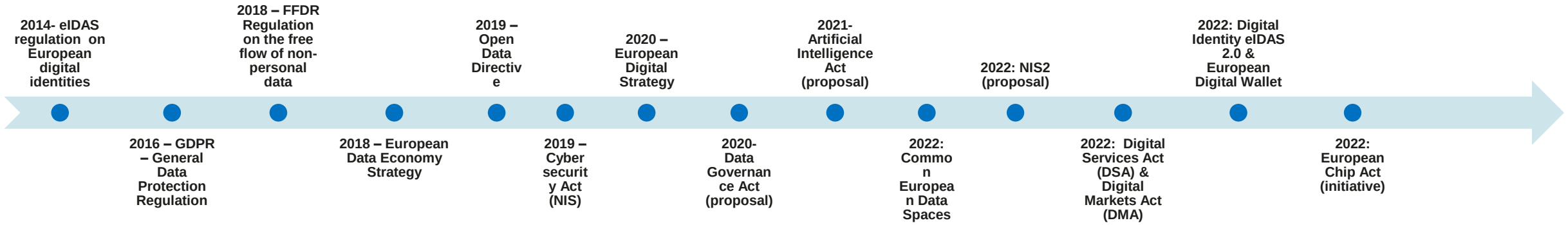
Cultural: core (European moral) values are extended to the digital public sphere

Political: regulation to translate societal rights and obligations in legal requirements

Socio-technical aspects: EU **data economy** and **innovation**, **privacy and data protection, Cybersecurity, data control** and online **platforms' behavior**

Technical building blocks: (i) building a **data framework**; (ii) promoting a **trustworthy environment**, and (iii) adapting competition and regulatory **rules**.

- To build digital ecosystems that comply with European Core Values such as *data belongs to an individual, self-determination of own assets, and privacy being a fundamental right.*
- The challenge is to enable **Trust;** however Trust Framework/Trust Governance helps to address it.
- **Are the Trust Frameworks Ready?**



Laws to ensure compliance to Core Values

Digital sovereignty is about the ability of a state, coalition and individual to **govern the use** of their **digital assets** in a **trustworthy environment, operating** in accordance to agreements and regulations that underpin **rule-based** digital ecosystems

- **Govern the use** includes confidentiality, privacy, provenance, transparency, visibility, consent, intervenability, value sharing
- **Digital assets** include data, information, computation workloads, operational processes and knowledge/intelligence
- **Digital ecosystems** include data-spaces, virtual organizations, virtual communities, supply chains, coalitions/unions of sovereign states

Trust Governance & ID Sovereignty

- **Trust framework** agreements underpin trust establishment in rules-based ecosystems
- **Sovereign IDs** put the identity owner in control of their personal information and privacy

Data and information Sovereignty

- **Data Sharing Agreements** govern the exchange and use of data within rules-based ecosystems
- **Transparency and control** over the protection, residence and use of your data
- **Compliance services** help attest the correctness

Competition and regulatory rules

Trustworthy environment

Digital Sovereignty in a digitally transforming world

Data framework

infrastructure

Operational sovereignty

- **Visibility and governance** over digital infrastructure / ecosystem **operations (incl. cyber)**
- Operational agreements offer a reference for the **terms operational engagement** including the **sharing of cyber threat intelligence (CTI)**
- **Collaborative CTI**: How to share and analyze threat intelligence and coordinate response to protect ecosystems **without losing sovereignty**

Computational processing & workload Sovereignty

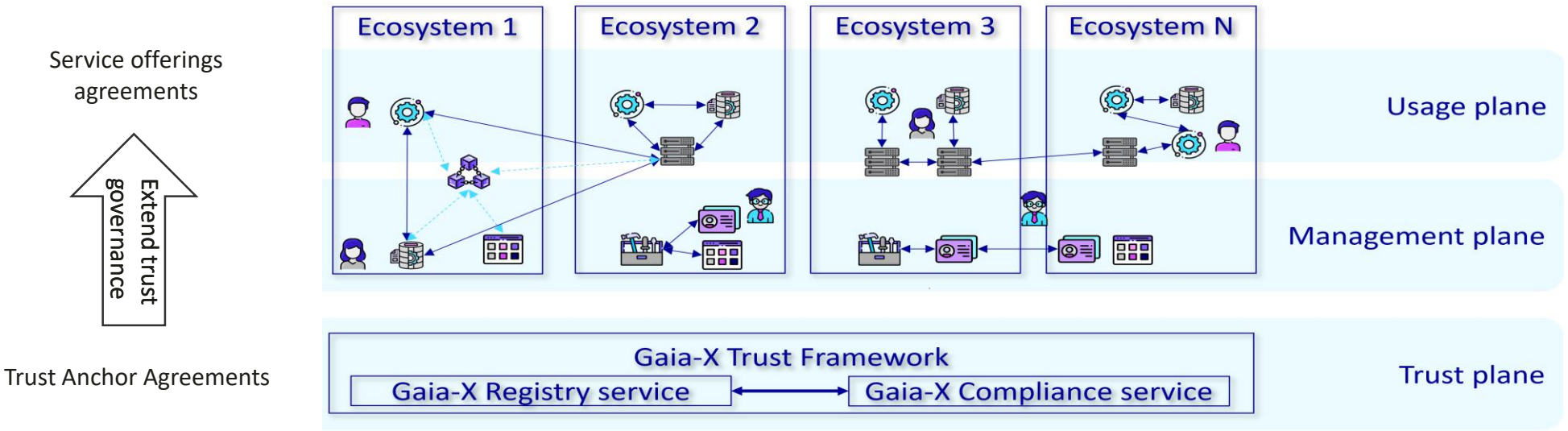
- Securely run computation and workloads cross-platform in **compliance with regulation** and **without lock-in dependence** on any provider
- **Service offerings** govern the workload distribution and sharing of responsibility

Gaia-X Trust Framework

Trust Framework automates trust establishment in Gaia-X ecosystems

Gaia-X is an initiative that develops, based on European values, a digital governance that can be applied to any existing cloud/edge technology stack to obtain transparency, controllability, portability and interoperability across data and services.

https://gaia-x.eu/



Trust Frameworks:

- The set of rules that define the minimum baseline to operate in Gaia-X Ecosystem. Those rules ensure a common governance and interoperability across ecosystems while letting the users in full control of their choices.
- Ecosystem would consist of the set of participants and service offerings complying with Trust Framework requirements.
- To be compliant with the Trust Framework, all keypairs used to sign claims must have at least one of the TAs in their certificate chain.
- List of valid Trust Anchors is stored in the Gaia-X Registry as defined by Gaia-X AISBL.

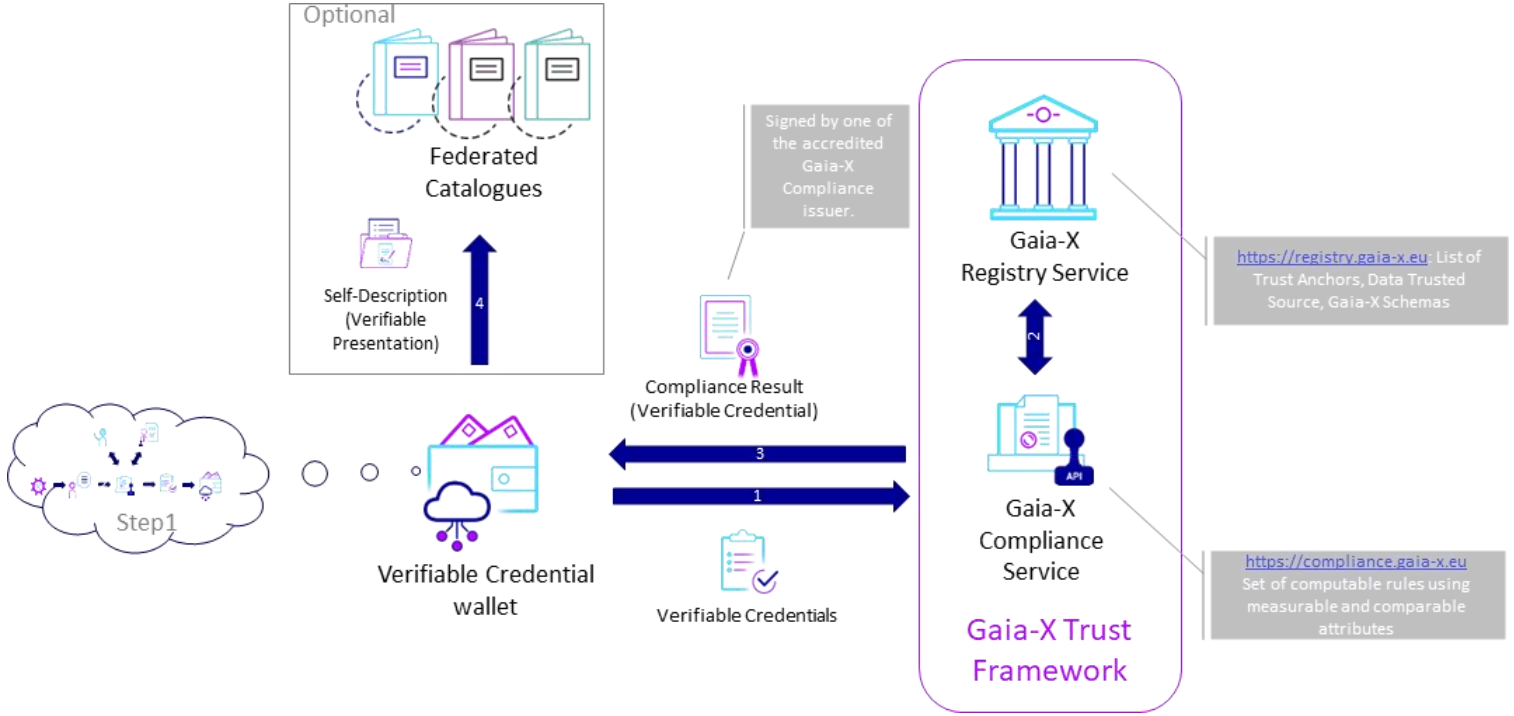
Reference: https://gitlab.com/gaia-x/technical-committee/architecture-document/-/blob/22.10/architecture_document/ecosystem.md

Gaia-X Trust Framework

Trust Framework automates trust establishment in Gaia-X ecosystems

Gaia-X Self-Description describes entities such as participants, service offerings and resources in an ecosystem and can be used for:

- Tool-assisted evaluation, selection, composition and orchestration of Services and Resources
- Enforcement, continuous validation and trust monitoring together with usage policies
- Negotiation of contractual terms



The steps involved in generating a **Gaia-X compliant Self-Description**

Challenges:

- How can trust go beyond authenticating participants keypair to check e.g., statements about their scope, utility and usage?
- Rigorous specification, consensus and standardization
- Authority and control over the Gaia-X registry
- Extension and interoperability among federations

Reference: https://gaia-x.gitlab.io/technical-committee/architecture-document/self-description/

Governance Framework in European Sovereign Digital Identity

As we move to decentralized identity systems, there is need for a governance framework that all parties agree on.

Governance Framework

- Decentralized systems must coordinate across multiple parties, all exercising their own sovereignty while respecting their obligations upon which others may rely.
- Rules of engagement and interaction must be explicit and agreed by all relevant stakeholders ahead of transacting.

What a Governance Framework offers

- **TRUST Over IP** proposes (2022) a layered governance stack where TAs (aka "Governing Authorities") cover: (1) Utility, (2) Agent/Wallet, (3) Credentials/Trust and (4) Ecosystem.
- Discovery/Utility of authoritative issuers and verified members, e.g. **TRAIN** tries to answer the question "How do I know I can trust the issuer of the credential?".
- Trust Assurances, Levels of Assurance, e.g. **eIDAS 2.0**

Challenges

- Developing **open standards specifications** that maximizes interoperability and transitive trust.

Reference: https://trustoverip.org/

Contract-based Trust Framework

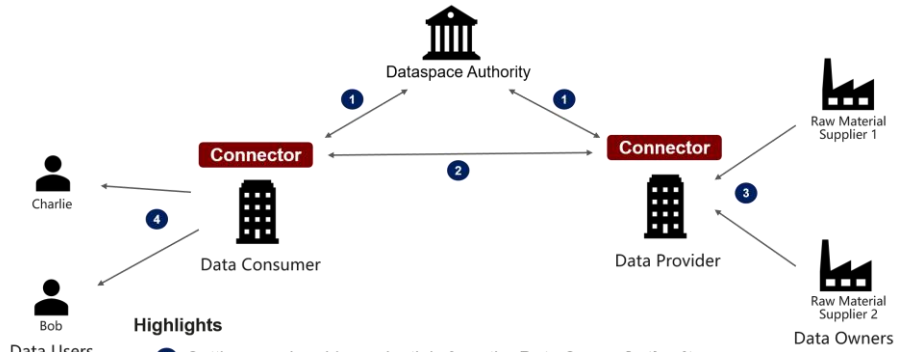
- ***Rules and Polices about Trust Anchors (language/model)*:** These policies would regulate acceptable trust anchors, the scope of their authority, and rights and obligations related to their use by the stake-holders. These are extensible baseline of the policies, procedures and mechanisms for the operation of digital trust that are accepted across a decentralized ecosystem.

- a **reference architecture** to evaluate/enforce these rules and policies

Credentials Exchange with Trust Framework

Dataspace Use-Case: Automotive Supply Chain

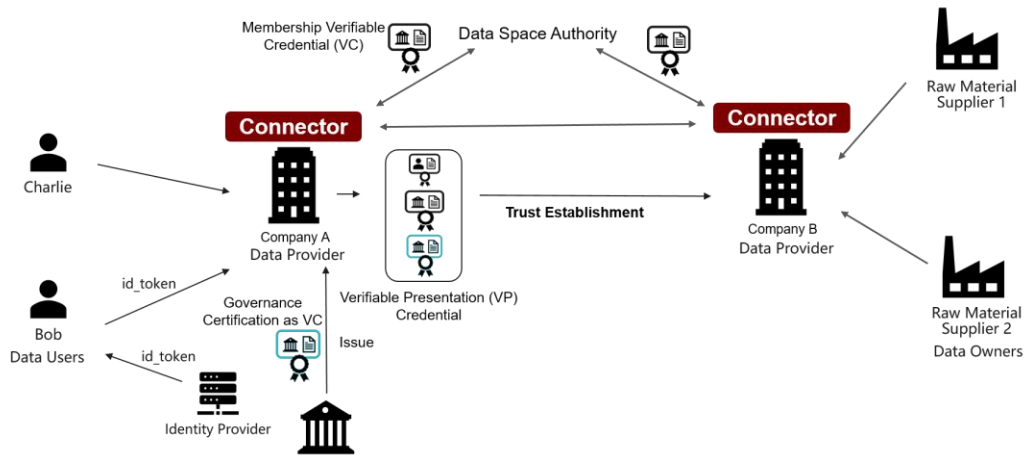
What is a Data space?
A data space is defined as a decentralized infrastructure for trustworthy data sharing and exchange in a data ecosystem based on commonly agreed principles.



Highlights

1. Getting membership credentials from the **Data Space Authority**.
2. Trust Establishment between **Data Consumer** and **Data Provider.**
3. **Data Owner** announce the availability of data to the **Data Provider.**
4. **Data User** use the data in the dataspace through the **Data Consumer.**

Role	Description
Data Provider	Is the organization in the dataspace that provide data and in our case it is the tire company that provide the detail about the raw materials from the supplier and manufactures.
Data Consumer	An organization who is a participant in a dataspace that consume data provided by the data provider. In our case it is the car manufacture who helps its consumer to trace the components or detail of the tires from the raw material supplier.
Data Owner	The raw material supplier who provide the data related to the raw materials to tire company that are used to make the tires sold to car company or used by the company in its cars.
Data User	The end-user of the data who (trace the details about the raw materials) is associate with the car manufacturer (the user owns the car).



- The use-case scenario starts with Bob requesting Company A the details about the tires in his car.
- Bob authenticate using the credentials at the Keyclock server managed by Company A.
- Company A`s connector need to establish trust with Company B supplier connector before it start with further data access processes.
- Company B might have additional requirements on the acceptance of a credential for trust establishment hence Company A creates a verifiable presentation and stored in an identity hub that is accessible by Company B.

Challenges

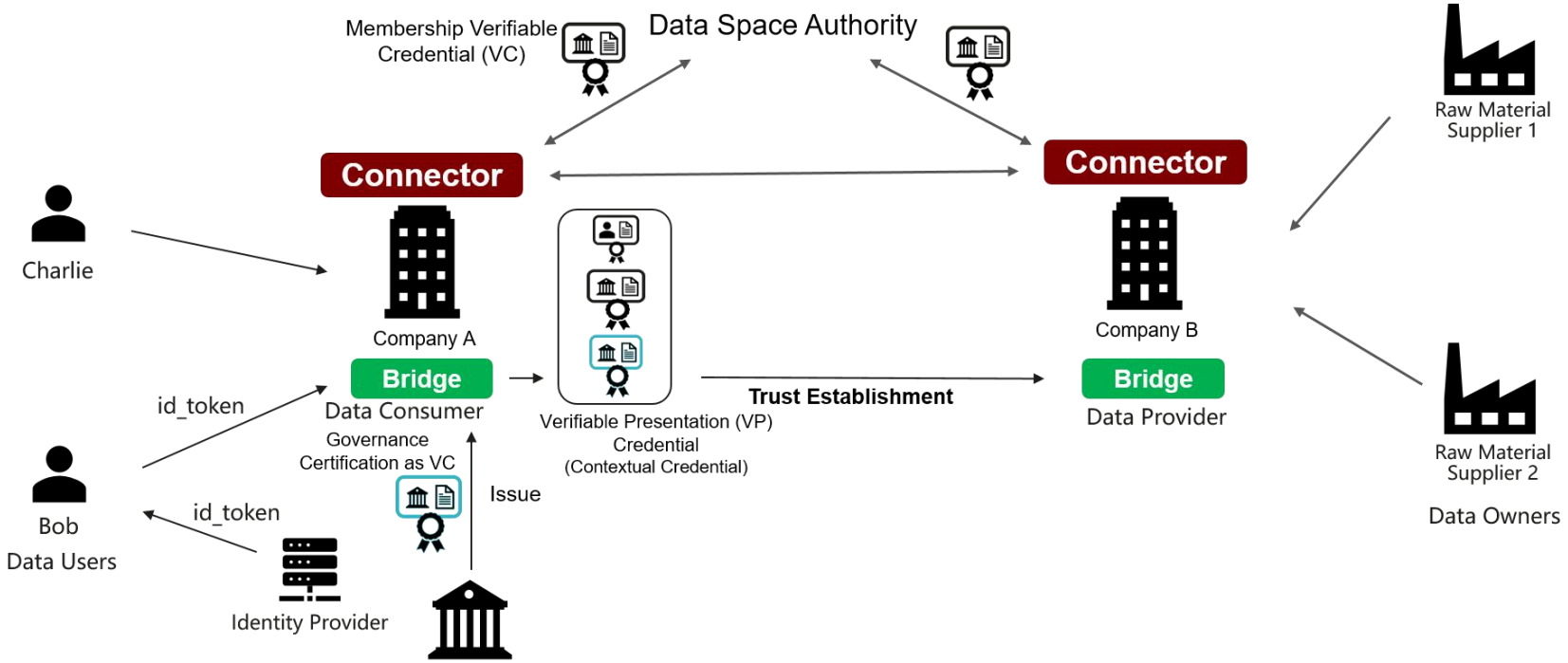
- The entities in a Data Space ecosystem might be across **different trust domains** or use different credential/protocols.
- It is hard to adapt when **use-case requirements** change every time that an ecosystem creates a Data Space or when **local regulations/international agreements change**.

Examples:

- Bob who is a Data User manages his credentials in a legacy identity system (e.g. OIDC) managed by company A, how can he use it for data space transactions?
- How to establish Trust between consumer and provider while being compliant to data spaces rules and meeting the provider specific requirements?
- How to build a shared responsibility model to manage credentials between data users and data consumer while being compliant with data space requirements?

Credentials Exchange with Trust Framework

We need to **Bridge** credentials/protocols in data spaces since different **roles** may belong to different Trust Domain or use different identity systems/protocols to establish trust

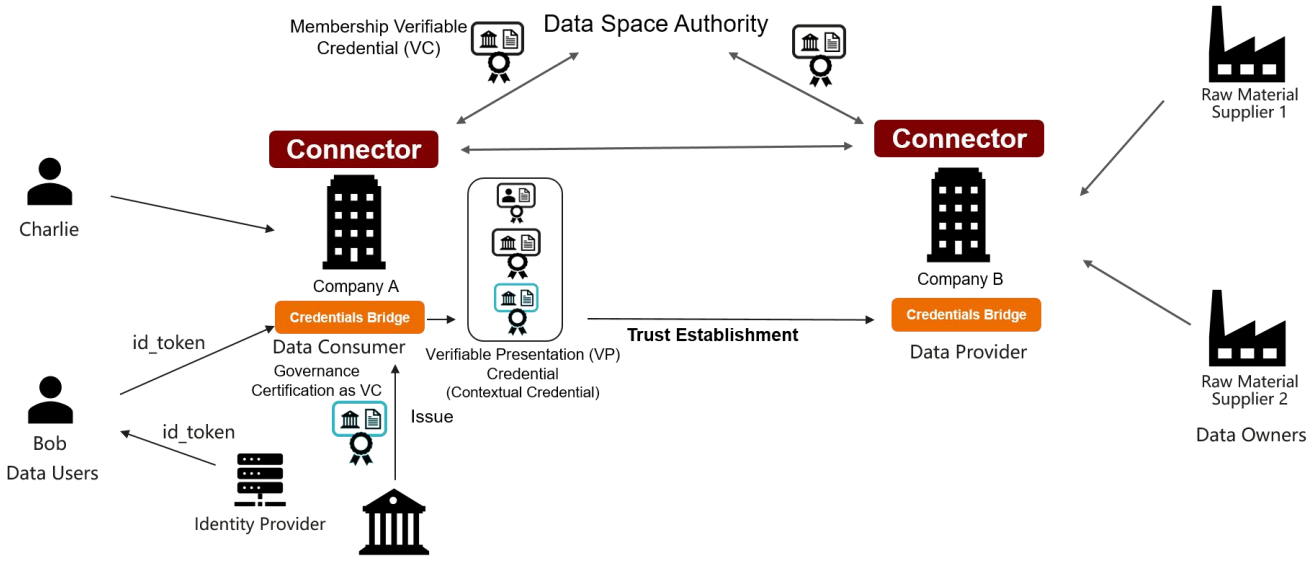


Our solutions is to build a Credentials Bridge technology that can overcome the challenges with,

- Support for **identity systems federation** in data spaces.
- **Contextualize and enrichment** of credentials based on use-case requirements.
- **Configurable** credential exchange using dynamic policy framework.
- Support for **integration to Trust Frameworks** that provides the trust governance rules.

Credentials Exchange with Trust Framework

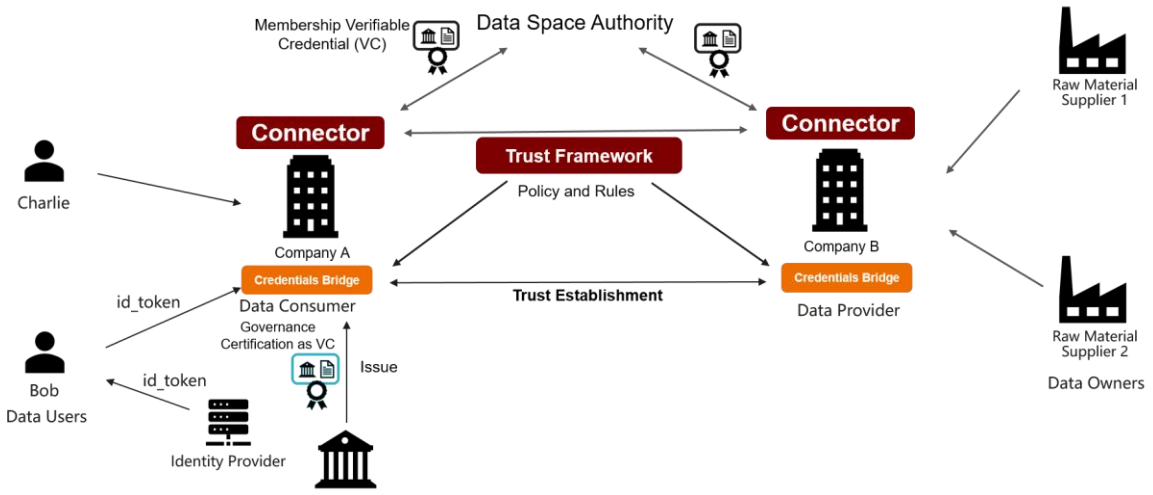
Technology Background



Credentials Bridge **leverage on usage control policies to enact actions and obligations such that credential transformation can be expressed with obligations and actions are about obtaining additional information.**

- We leverage on our Usage Control (UCON) framework as an implementation mechanism for the credentials bridge since it provides an uniform policy framework. One can create a Credentials Bridge using any dynamic policy framework due to its configurability feature.
- The framework evaluate credential transformation and recognition of authority policies that contains rules and obligations that helps with credential mapping/transformation. Using of rules help to make the process of credential transformation more dynamic.
- Obligations also state actions that might requires to fetch additional credentials/information from trust authorities defined by the federation.

Trust Framework



Credentials Bridge integrated with Trust Frameworks to obtain rules for credentials/protocol interoperability and acceptance of Trust Anchors.

- *Trust Frameworks* define a common set of rules that govern interactions between the participants in an ecosystem or across different ecosystems.
- Unlike DPKI which only incudes rules about which trust anchors to accept, the Trust Framework in addition set rules on how to use credentials generated by them. These rules apply both to issuance and to validation and may necessitate enrichment or exchange of credentials both for interactions between organizations in a data spaces/ ecosystem but also (and in particular) for data exchanges across ecosystems

Conclusion

Is Trust Frameworks ready? **Yes,** but lot more need to be done to realize its full potential however with,

- Develop specifications.
- Policies and Rules that can define acceptance, usage and scope of authority of Trust Anchors.
- A reference architecture for the evaluation of these policies and rules.

We can build a sovereign digital ecosystem.

A shared responsibility model to support cross border and cross organizational federation on top of decentralized and self-sovereign identity: Architecture and first PoC

Michael Kubach[1], Isaac Henderson[12], Bithin Alangot[3], Theo Dimitrakos[3], Juan Vargas[12], Matthias Winterstetter[12], and Ioannis Krontiris[3]

Our paper in cooperation with Fraunhofer IAO got accepted at **Open Identity Summit 2023**

Thank you.

Bring digital to every person, home and organization for a fully connected, intelligent world.

HUAWEI