

Landscape and technological research considerations on digital sovereignty & future digital/data spaces security

Prof. Theo Dimitrakos

Huawei Technologies Duesseldorf GmbH

& University of Kent

NECS – PhD Winter School 2024
8th January – 12th January 2024
Cortina d’Ampezzo (BL)

About the lecturer: Prof Theo Dimitrakos



Business Strategy & Technology Innovation Development

- **Huawei TTE-DE:** Senior Expert at Huawei based in Munich - Technical program director for (European) **Digital Sovereignty** and Digital/Data Spaces security – Lab director of the recently formed **Digital Spaces Trust** lab.
- **Visiting Fellowships:**
 - NICT Visiting Research Fellow at **KDDI Research**, Japan;
 - Chief Research Fellow (visiting) at **EBTIC**, the Research Centre of Etisalat, BT, Khalifa at UAE (Abu Dhabi).
- **British Telecom :** Chief Researcher at BT HQ globally responsible for Cloud Security Innovation & Technology Research Strategy.
- **UK STFC:** Principle researcher, supported W3C UK & Ireland office; Scientific Coordinator of major European research initiatives

Collaborative Innovation

- **ENISA:** Expert member of WGs (2021-) Foresight in Emerging and Future Cybersecurity Challenges; (2009-16) of WGs on [Cloud Security and Resilience](#) and on [Virtualization Security](#). [Coauthored ENISA advisory reports](#) to European Commission, **EU Cloud Stakeholder DSM** (2017)
- **CSA:** Contributor to [Cloud/Virtualization security guidance and standards](#) and invited speaker in CSA congress since 2010
- **EU Innovation Project collaborations:** Technical lead the largest and EU research collaborations involving over 400 research

Education / Research

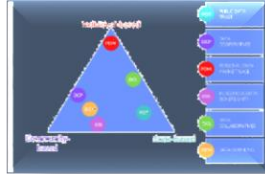
- **Cybersecurity Research Centre – University of Kent:** Professor of Computer Science and member of the Interdisciplinary Research Centre in Cyber Security at the University of Kent. Chair of advisory board.
- **IFIP:** Member of the Security Technical Committee and previous Chair of WG on Trust Management ; *silver core medal award recipient*
- **PhD Imperial College London (1998):** KBSE, Semi-automated program synthesis of verifiable code using formal methods
- **BSc/MSc:** Mathematics, Formal Logic, AI

Publications

- 7 books, 3 journal editions, 100+ international publications in ACM, IEEE, IFIP conferences. 40+ EU/World patents

Contents

Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)	<ul style="list-style-type: none">• Business Continuity: Compliance is mandatory for business continuity in EU• Business Growth: Data space service offering enables verticals with national and international supply chains• Business Scale: Opening Cloud and Data Markets to Software vendors
A holistic execution approach is required across the entire ecosystem players:	<ul style="list-style-type: none">• Regulation: For impact analysis and to ensure neutrality for non-EU players• Standardization: For co-authoring in essential specs Architecture, Sovereignty & Labelling standards• Implementation: For rapid prototyping Developed first Gaia-X compliant data space prototype (Huawei Boot-X)• Adoption: Participation in global lighthouse projects
There are several industry associations on play...	<ul style="list-style-type: none">• DSBA, Gaia-X, IDSA and Eclipse and Open Source• DSSC (Dataspace support center) funded by EC to support vertical Dataspace formation• 10+ lighthouse projects in different verticals Catena-X and upcoming Manufactura-X are the biggest.
Towards a converging Data Space (Security) Architecture	<ul style="list-style-type: none">• DSBA defines convergence and MVF that builds on Gaia-X, IDSA architectures and TM Forum and OpenDEI principles in order to• What is a data space? Ecosystem, basic services, connectors, common capabilities• TTE-DE specifies a data space security reference architecture
Reference implementation: OSS on Eclipse foundation	<ul style="list-style-type: none">• Eclipse becomes the common platform for data space development:• Eclipse Dataspace Connector (next gen IDS),• Eclipse XFSC (gaia-x Federation Services)• Eclipse Tractus-X (Catena-X OSS baseline)
Standardization is going global	<ul style="list-style-type: none">• ISO S38: Cloud computing and distributed platforms – Dataspaces (Microsoft driven)• CEN CWA Trusted Data Transaction (TNO-NL, FhG ISST-DE, Dawex-FR driven)• Standards baseline
Competition is investing heavily	<ul style="list-style-type: none">• Pro-active public communication• Moving fast(er) with more manpower• Microsoft driving Global Dataspaces standard in ISO
An overview of data space initiatives in Europe	<ul style="list-style-type: none">• IDSA data space radar• Exemplar verticals
Emerging architectural variants	<ul style="list-style-type: none">• Industrial / International Data Spaces• Personal Data Spaces• IoT Data Spaces – eg. ITS/CCAM data spaces
Huawei contributions in Hua-X and Digital Sovereignty projects: technical	<ul style="list-style-type: none">• Pro-active public communication• Moving fast(er) with cooperation with ICTL (Cloud BU R&D and Fraunhofer ISST), PACD and SID• Microsoft driving Global Dataspaces standard in ISO – we need to join up
Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap	<ul style="list-style-type: none">• Pro-active public communication• Moving fast(er) with cooperation with ICTL (Cloud BU R&D and Fraunhofer ISST), PACD and SID• Microsoft driving Global Dataspaces standard in ISO – we need to join up
Recommendations	<ul style="list-style-type: none">• Architectural priority• Technology priority• Standards priority• Community involvement
Appendix I: Core technologies	<ul style="list-style-type: none">• Trust services• Identity and Credentials• Contracts• Access / Usage Control / Policy• Auditing and Logging



Concise analysis of digital sovereignty models & definitions



Political voices



Business definitions



Academic definitions

EC view on (European) Digital Sovereignty:



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.

Digital Sovereignty: Normative Claims

State Autonomy & national infrastructure protection

- Nation or region should be able to take autonomous actions and decisions regarding its digital assets including infrastructures and technology deployment
- Policy (rule) driven approach for governance with emphasis on regulatory compliance
- Data Localization challenge examples: (1) "Schengen Routing" – i.e. avoid routing data flows within Europe via exchange points and routes outside of Europe; (2) e-evidence package that rules how authorities can collect digital evidence in EU and Non-EU states
- Negative economic and political impact is feared if global internet is re-territorialized and eventually fragmented into national internet segments

Economic Autonomy & Competition

- EU's economic and industrial policy strategy is threatened by the perceived market dominance of USA and China
- Economic goal to achieve more independence from foreign technologies and to promote the innovative power of the domestic industry

User Autonomy & Individual Self- Determination

- Strong concern primarily in Germany and then the rest of the EU
- Focus on the autonomy of citizens in their identities and roles as employees, consumers, and users of digital technologies and services
- Empower individuals to govern personal digital assets (including but not restricted to data) and how these are perceived, used and monetized by others
- Empower users to choose between technological options, understand the assurance of these options and avoid vendor bias and lock-in

Digital sovereignty as recapture of state sovereignty

History / Etymology:

- The term sovereignty is derived from the latin word *superanos* which means *over* or *superior* and first considered as the ruler's authority to make final decisions (by Bodin) and later coined as popular sovereignty (by Rousseau) with a clear implication on governing, the rule of law and territoriality (attachment to a specific territory).

Disappearance of state in digital:

- Digital transformation and global tech infrastructure challenge traditional state sovereignty, concepts like state and territoriality clash with global digital networks, digital applications and communication practices perceived to defy legal governance and stately control

State reclaiming sovereignty in digital:

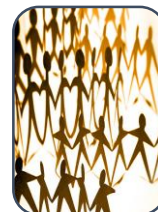
- State actors claim the cyber space by the enforcement of laws and governmental interventions in the digital sphere, public is convinced that sovereignty and state authority act for the common good
- Governance of digital infrastructures and development of digital technologies now invokes nation, national economy and directly impacts nation's citizens

Alternative (contrasting) concepts to digital sovereignty



Cyber Exceptionalism (outdated)

- separation between "physical" and "digital" spheres leading to cyberspace viewed as a new and autonomous virtual realm with its own "cyber sovereignty"
- **Examples:** Early days of cryptocurrency & cyber-activism



Multi-Stakeholder Internet Governance (fading)

- States are limited to non-sovereign roles in a regulatory ideal where governance of the internet belongs to those (industries and communities) directly affected by it. Development and application of shared norms, rules and procedures to maintain and develop the internet.
- **Examples:** Partly accepted in the form of industry self-regulation and industry standards but inefficient and under increasing political pressure.

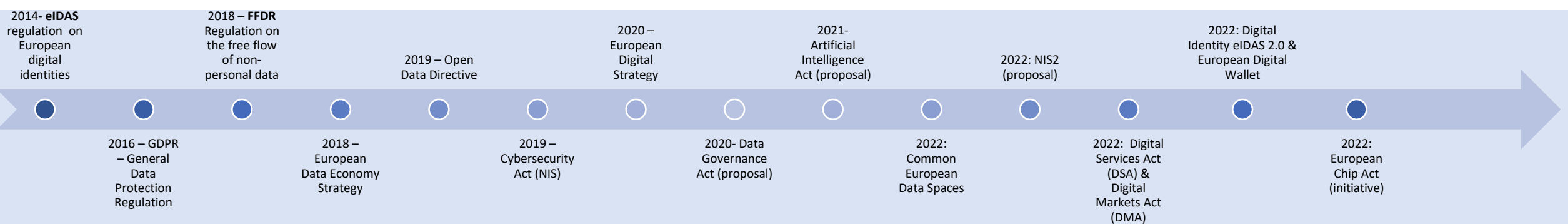
European legislation and policy making initiatives intensify in 2021 & 2022 for data & identity

Possible EU initiatives and actors proposed in 2020 by EU Parliament Research Service (EPRS)

Project	Actor responsible	What should be done?
1 European digital infrastructure	Commission, Parliament, Council	Foster the creation of an EU-wide digital infrastructure (networks and storage)
2 EU data regulatory framework	Commission, Parliament, Council	Adopt a new set of measures to foster EU innovator's access to and use of personal and non-personal data (e.g. open access to government data). Assess the opportunity to include data sovereignty clauses in public procurement contracts. Adopt a new regulatory framework, including a new Directive on the Digital Europe programme to support investments in frontier technologies (e.g. AI, IoT, blockchain, high performance computing and quantum technologies), and/or advanced digital skills.
3 Multi-national financial framework for digital Europe	Commission, Parliament, Council	Set up public-private partnerships (PPP) in AI, data and robot code development in innovation hubs.
4 Public-private partnerships in AI, data and robotics	Commission, Parliament, Council	Support the creation of a large-scale EU research cooperation framework in frontier technologies.
5 Large-scale EU research cooperation framework	Commission, Parliament, Council	Amend the GDPR to introduce guidance for data protection in specific sectors, such as health or financial services. Assess the opportunity to amend the GDPR to create an innovation-friendly environment for AI.
6 GDPR review	Commission, Parliament, Council	Complete the revision of the ePrivacy Directive, accompanied by ensuring that all communications over public networks maintain respect for a high level of data protection and confidentiality.
7 ePrivacy Directive	Commission, Parliament, Council	Amend the EU framework for cybersecurity certification to make certification compulsory in order to ensure robustness.
8 Set compulsory EU-wide cybersecurity certification	Commission, Parliament, Council	Set up a joint Cybersecurity Unit to reinforce cooperation between the Member States and organise mutual assistance. Finalise the adoption of new protocols to assist in European Cybersecurity Cooperation. Consider to support the development and deployment of cybersecurity technologies.
9 Foster coordination in cybersecurity at EU level	Commission, Parliament, Council	Revise the NIS Directive to strengthen the protection of the EU's critical digital sector.
10 Revise the NIS Directive	Commission	Foster definition of common EU standards for 5G networks and/or smart connectivity systems.
11 Standardisation for 5G and beyond	Commission	Define common EU standards for IoT devices.
12 Standardisation of IoT transparency of decision-making systems	Commission, Parliament, Council	Adopt specific legislation to set ethical rules and put safeguards and accountability measures in place on the development and use of facial recognition technology.
13 EU framework on the use of facial recognition technology	Commission, Parliament, Council	Amend the EU product safety and liability regime to address safety and liability issues brought about by emerging technology, such as IoT and AI. Amend the Product Liability Directive.
14 EU product safety and liability regime	Commission, Parliament, Council	Amend the current liability rules applicable to online platforms and strengthen the EU legal regime for the accountability of platforms.
15 e-Commerce Directive (Digital services act)	Commission, Parliament, Council	Ensure coordinated implementation of the EU's public procurement rules to take better account of the critical aspects of digital technologies in sensitive sectors (in particular 5G). Finalise the adoption of an international procurement instrument, to ensure reciprocal market access in public procurement.
16 Coordinated implementation of the EU's public procurement rules	Commission, Parliament, Council	Adopt new EU instruments to assist takeover of EU high tech companies, especially 'killer acquisitions'.
17 New instrument to assist takeover of high-tech companies	Commission, Parliament, Council	Assess the opportunity of creating an EU Task Force on Strategic Industries and Technologies tasked with identifying strategically important industries for which limits on foreign investment and exceptions to state aid policies and competition policy may apply.
18 Create an EU Task Force on Strategic Industries and Technologies	Commission, Parliament, Council	Explore the possibility to finalise the adoption of a harmonised digital tax.
19 EU digital taxation framework	Commission, Parliament, Council	Explore the possibility to adopt specific start-up related taxation legislation to foster the development and growth of high-tech start-ups in the EU.
20 EU digital taxation framework	Commission, Parliament, Council	Explore the opportunity to impose ex-ante rules (e.g. on algorithm transparency and neutrality and data sharing) to better control digital platform behaviour, including increasingly acting as digital gatekeepers.
21 Control digital gatekeepers	Commission, Parliament, Council	Assess whether the EU framework should promote digital tools and solutions (e.g. operating systems) that avoid technology lock-ins and foster open digital ecosystems in the EU.
22 Foster open digital ecosystems	Commission, Parliament, Council	Rethink the governance mechanisms and interaction between regulators to promote collaboration and joint decision-making for digital topics.
23 Governance mechanisms and coordination between digital regulators	Commission, Parliament, Council	

- **Digital Identity in Europe:** Trusted and Secure European Electronic ID Regulation, 2021.6 Proposal for a European Digital Identity Framework. Digital wallet initiatives for eIDAS2.0 from September 2022.
- **Cybersecurity:** NIS 2 Directive in December 2020, and unanimously adopted in May 2022.
- **European data strategy:**
 - European Data Governance Act:** Introduced in November 2020, took effect on June 23, 2022, and will apply from September 2023.
 - Data Act: 2022.2** The Data Act: Proposals for Regulations on Harmonization Rules on Fair Access to and Use of Data, which aims to maximize the value of data in the economy.
 - Common European Data Spaces:** Currently, 12 vertical data spaces are under development, with the ultimate goal of forming a single data market within the EU.
 - Reuse of high-value dataset with social and economic benefits.**
- **Digital Services Package:** Digital Services Act (DSA) and Digital Markets Act (DMA). Proposals in December 2020, agreed on the DMA on March 25, 2022, and on April 23, 2022.
- **Artificial Intelligence:** Ban unacceptable risk AI apps (e.g. social scoring), regulate high-risk.
- **The European Chip Act: 2022.2** Address semiconductor shortages and strengthen Europe's technological sovereignty. Increase to 20% of global production by 2030 from 10% in 2020.

Legislation and policymaking initiatives for sovereignty and in Digital Europe



Contents

Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)

- **Business Continuity:** Compliance is mandatory for business continuity in EU
- **Business Growth:** Data space service offering enables verticals with national and international supply chains
- **Business Scale:** Opening Cloud and Data Markets to Software vendors

A holistic execution approach is required across the entire ecosystem players:

There are several industry associations on play...

Towards a converging Data Space (Security) Architecture

Reference implementation: OSS on Eclipse foundation

Standardization is going global

Competition is investing heavily

An overview of data space projects in Europe

Emerging architectural variants

Huawei contributions in Hua-X and Digital Sovereignty projects: technical

Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap

Recommendations

Appendix I: Core technologies

Gaia-X/IDSA/DSBA Compliance will ensure Continuity, Growth & Scale

Gaia-X and IDSA with massive government and industry support is now a synonym for European data economy, **developing technical specs, reference implementations and issuing certifications for compliance** and being the core forces behind **DSBA**, which is the leading body for convergence between data space initiatives and support of standardization and operationalization

Implications and Opportunities for Huawei

- 1 Business Continuity**

Compliance with the DSBA (Gaia-X, IDSA, DSSC) specifications will become **mandatory for business continuity** of Huawei's partner clouds, early adoption will become a unique asset for business growth.
- 2 Business Growth**

As potential candidate for **global standard**, unleashing the **ecosystem growth** by accelerating cloud and federated data usage. **Leveling the playing field** by respecting the data ownership and limiting the dominance of big three cloud providers as data aggregators.

Huawei can grow its **market share** by bringing the existing customers from different industry and geographical domains together in **open, federated data spaces** and providing **new data federation services**.
- 3 Business Scale**

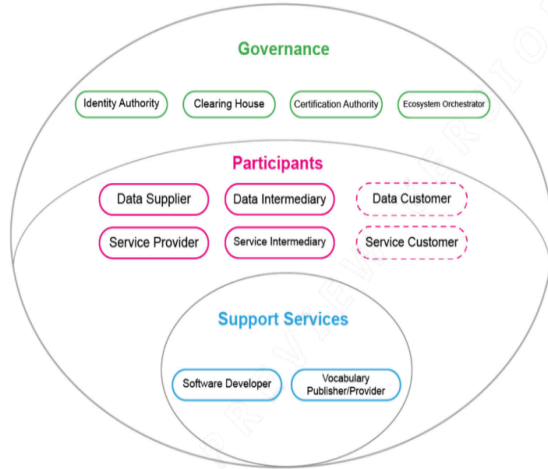
Catalyzing ecosystem growth and builds on top of Huawei's vision of **Open Services Cloud** as a framework to open the cloud data and services ecosystem. **Eclipse** hosts **open source software** reference implementations by **Gaia-X (GXFS/XFSC)**, **IDSA (EDC)** and **Catena-X (Tractus)** under Eclipse. The open source strategy **remediates the potential reservations** against Huawei products and services.

Huawei has been involved in Gaia-X, IDSA and Eclipse since 2021

Business models relating to data spaces and smart “super-apps”

Roles examined in IDSA position paper: New Business Models for Data Spaces Grounded in Data Sovereignty

Source <https://internationaldataspaces.org/wp-content/uploads/IDSA-Position-Paper-New-Business-Models-sneak-preview-version.pdf>



In Hua-X project Cloud BU R&D (ICTL) and TTE are building together with Fraunhofer ISST (lead in Gaia-X and IDSA) a blue-print of a “Data Space as a Service) that includes:

- data space access (connector) service that allows one to join an existing data space (in Europe or China)
- data space (operations) service that allows to create new data spaces

Gaia-X Digital Clearing House (GXDCH) [LINK] was launched at Market-X conference & Expo in 2023. [LINK]

One-stop solution for verifying compliance with the Gaia-X rules in an automated way. First GXDCH nodes: **Aruba** and **T-Systems**

Emerging business models for data space enabling software and operations based on 2023 analysis

Data space intelligent service providers / intermediaries

- Offer algorithms, AI ops, and smart applications (“super-apps”) for specific vertical markets that leverage the power of data spaces in these markets. Examples: SAP, BOSCH, CDQ, Amadeus, T-Systems [LINK] (super-apps), NLAIC [LINK] (large AI on data spaces)

Data intermediaries

- Acts as a trusted data broker, manages data exchange. May not have access to or visibility of the data exchanged but offers assurance of the conformance of the exchange to relevant data usage agreements, data contracts. Examples: Meta Data Broker Data Intelligence Hub, Deutsche Telekom [LINK]; Smart Connected Supplier Network (SCSN), TNO [LINK]; Helsinki City MyData Operator [LINK]; Digital Flanders services [LINK]; Prometheus-X for DASES [LINK]

Data Clearing House

- Verifies data-based transactions both in terms of data exchange and associated value/monetary transactions. Example: SCSN Data Clearing House, TNO [LINK]

Data space operations & domain specific stack of building blocks

- Offer domain specific data space components and support data space operations. Examples: Confinity-X (joint venture of Mercedes-Benz, BASF, BMW Group, Henkel, SAP, Schaeffler, Siemens, T-Systems, Volkswagen and ZF) [LINK]

Data space as a service

- Offer the ability to create and operate data spaces through a cloud service. Examples: Huawei (Hua-X2)

Data space access as a service

- Offer the ability to deploy a connector and join existing data spaces. Examples: Confinity-X [LINK] , Huawei (Hua-X2)

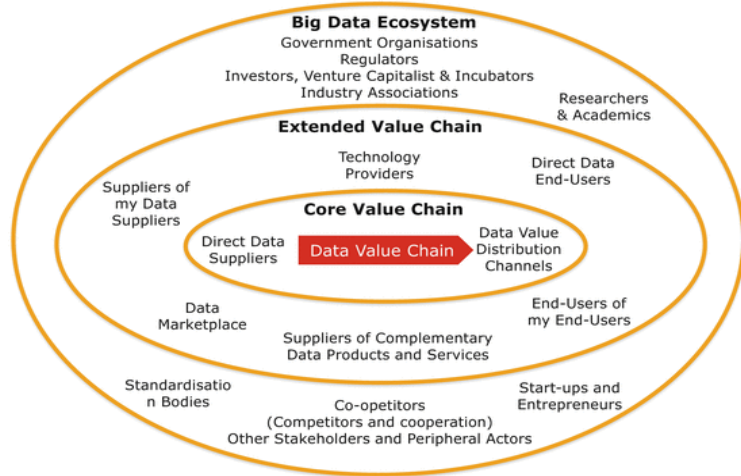
Digital/Data space federation enabler

- Offer a software stack that enables the creation of digital ecosystem federation and/or data spaces based on community standards. Examples: Tractus-X (Catena-X KIT & domain specific standards) [LINK] , XFSC (GXFSv2 spec) [LINK]

Digital/Data space trust enabler (CXGDH digital trust clearing house)

- Offer trust and compliance services, such as clearing house and basic federation services. Examples: Aruba and T-Systems operating first CXGDH (Gaia-x trust and compliance services) nodes [LINK]

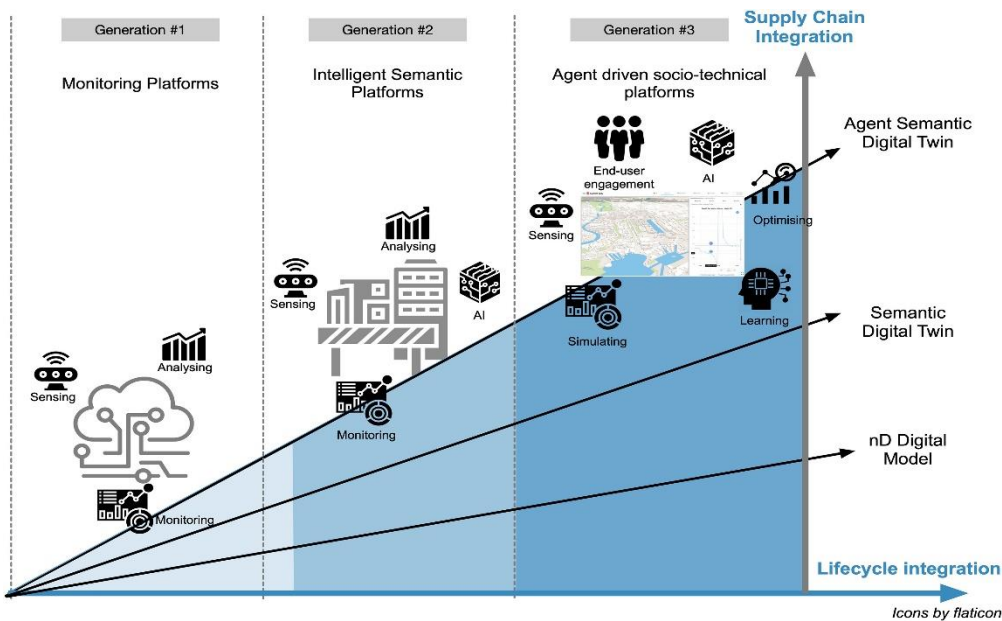
Data value chain overview



- Data Value Chain (DVC) can be defined as a multi-stakeholder data-driven business model where data is securely exchanged between parties (individuals or organizations) to create value for all relevant stakeholders
- Through legislation and innovation projects (DIH and Horizon), the EU has deeply deployed industry data, digital smart cities, and personal data spaces.
- Non-profit organizations are actively defining DataSpace reference architectures, standards, and governance rules, and developing and providing corresponding reference technology prototypes.

<https://www.reach-incubator.eu/what-are-data-value-chains/>

Emerging business models for data space enabling software and operations



Data space app providers

- Offer smart applications for specific vertical markets that leverage the power of data spaces in these markets. **Examples: SAP, BOSCH, CDQ, Amadeus**

Data space operations & software stack

- Offer domain specific data space components and support data space operations. **Examples: Confinity-X (joint venture of Mercedes-Benz, BASF, BMW Group, Henkel, SAP, Schaeffler, Siemens, T-Systems, Volkswagen and ZF)**

Data space as a service

- Offer the ability to create and operate data spaces through a cloud service. **Examples: Huawei (Hua-X2)**

Data space access as a service

- Offer the ability to deploy a connector and join existing data spaces. **Examples: Confinity-X, Huawei (Hua-X2)**

Data space & digital ecosystem federation enabler

- Offer trust and compliance services, such as clearing house and basic federation services. **Examples: T-Systems operating CXGDH (Gaia-x trust and compliance services)**

In Hua-X project Cloud BU R&D (ICTL) and TTE are building together with Fraunhofer ISST (lead in Gaia-X and IDSA) a blue-print of a "Data Space as a Service" that includes:

- data space access (connector) service that allows one to join an existing data space (in Europe or China)
- data space (operations) service that allows to create new data spaces

<https://linkinghub.elsevier.com/retrieve/pii/S0926580519314785>

Connecting Europe Facility (CEF) <https://joinup.ec.europa.eu/collection/connecting-europe-facility-cef>

Contents

Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)

A holistic execution approach is required across the entire ecosystem players:

- **Regulation:** For impact analysis and to ensure neutrality for non-EU players
- **Standardization:** For co-authoring in essential specs Architecture, Sovereignty & Labelling standards
- **Implementation:** For rapid prototyping Developed first Gaia-X compliant data space prototype (Huawei Boot-X)
- **Adoption:** Participation in global lighthouse projects

There are several industry associations on play...

Towards a converging Data Space (Security) Architecture

Reference implementation: OSS on Eclipse foundation

Standardization is going global

Competition is investing heavily

An overview of data space projects in Europe

Emerging architectural variants

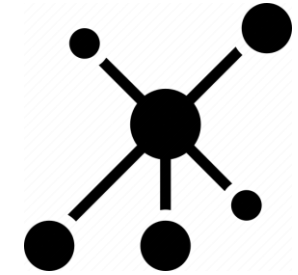
Huawei contributions in Hua-X and Digital Sovereignty projects: technical

Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap

Recommendations

Appendix I: Core technologies

Huawei's Industry Research Strategy for Data Spaces Requires 4 Pillars



Regulation

Engagement with relevant industry associations and standardization bodies of the European Commission including ENISA, DGs and DSSC

Analyzing Gaia-X Certification Req. w/ TUEV Süd (likely CAB)

Standardization

Participate in GAIA-X and IDSA working groups to shape standards and architecture

Get involved in forthcoming ISO and CEN standardization initiatives

Participate in other relevant standardization initiatives in DIF, W3C, IETF, OASIS Open, TMF

Implementation

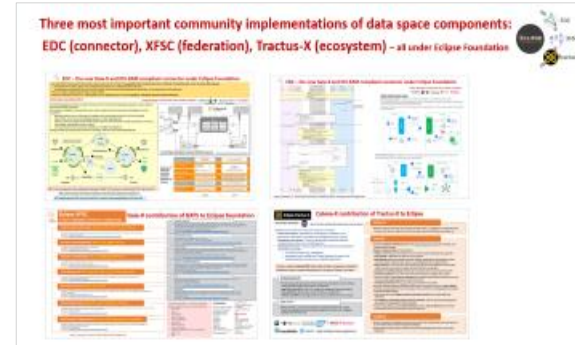
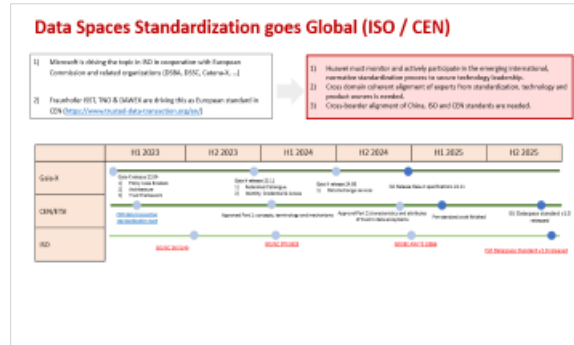
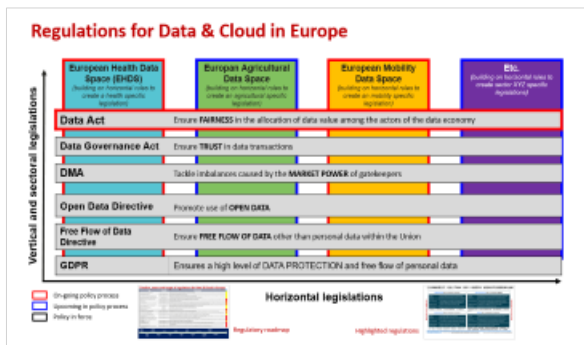
Eclipse Foundation is becoming official open source partner of Gaia-X, Catena-X and IDSA (EDC)

Support Eclipse Open Source project contributions to XFSC and EDC (e.g. via Hua-X2 and DUCA & EU projects)

Bring Open Services Cloud framework and TTE key technologies into XFSC and EDC

Adoption

Collaboration with key academic institutions and industry players to drive proof of concepts and industry adoption



Contents

Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)

A holistic execution approach is required across the entire ecosystem players

There are several industry associations on play...

DSBA, Gaia-X, IDSA and Eclipse and Open Source

DSSC (Dataspace support center) funded by EC to support vertical Dataspace formation

10+ lighthouse projects in different verticals Catena-X and upcoming Manufactura-X are the biggest.

Towards a converging Data Space (Security) Architecture

Reference implementation: OSS on Eclipse foundation

Standardization is going global

Competition is investing heavily

An overview of data space projects in Europe

Emerging architectural variants

Huawei contributions in Hua-X and Digital Sovereignty projects: technical

Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap

Recommendations

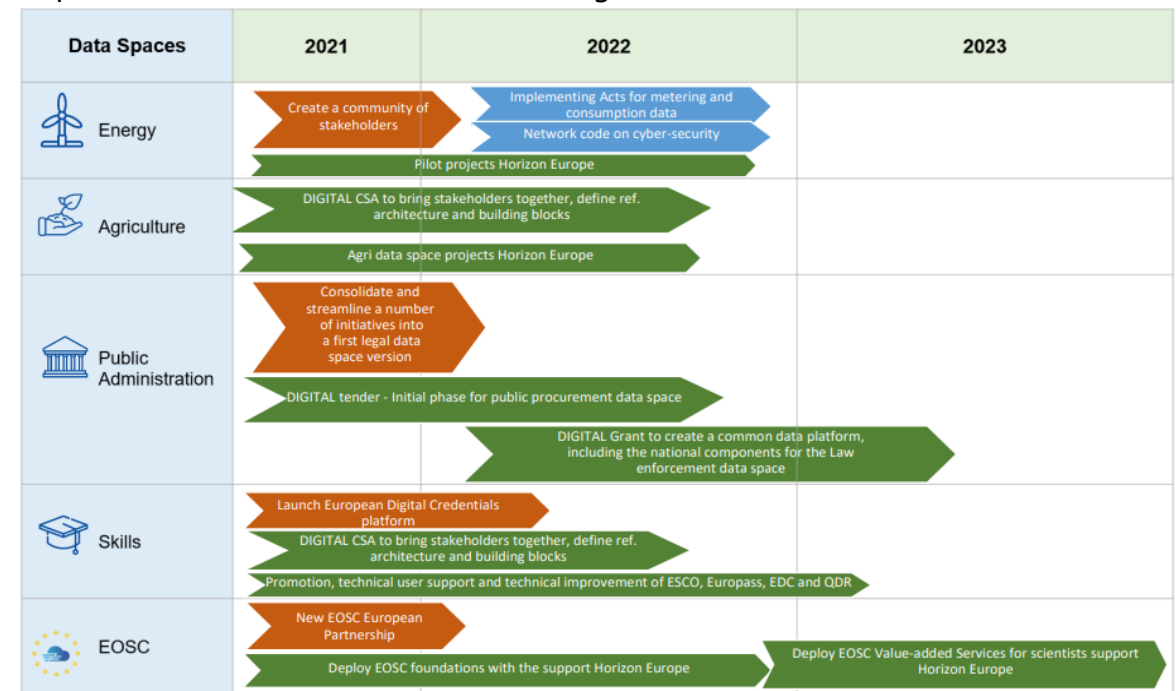
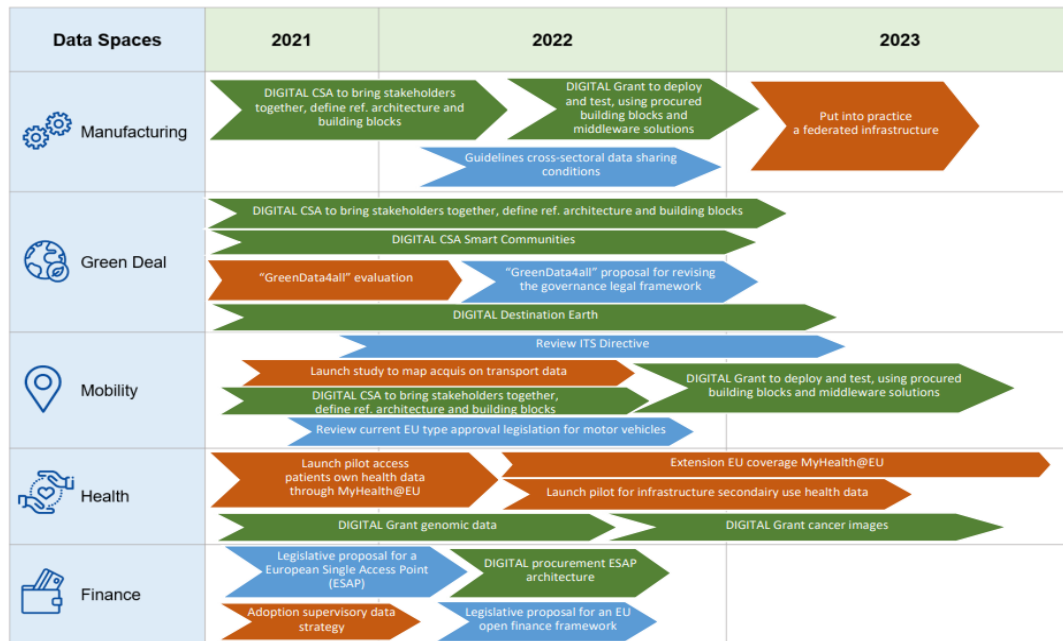
Appendix I: Core technologies

Appendix II: Data spaces examples

The EU is intensively developing DataSpaces in various industries.

- ❑ The amount of data is growing, from 33 Zbits generated in 2018 to 175 Zbits expected by 2025, and 80% of industrial data is never used. The Data Act: Commission proposes measures for a fair and innovative data economy, submitted on 23 February 2022, addresses the legal, economic and technical issues that lead to underutilization of data. The new rules will make more data available for reuse and are expected to generate an additional €270 billion of GDP by 2028.
- ❑ The European Data Strategy in February 2020 announced the creation of data spaces in 10 strategic areas: health, agriculture, manufacturing, energy, mobility, finance, public administration, skills, the European Open Science Cloud and meeting the cross-cutting key priority targets of the Green Deal. Data spaces for other important areas, such as media and cultural heritage, have been added. The ultimate goal is that together these data spaces will form a single European data space: a truly single data market.
- ❑ In February 2022, Staff working documents on data spaces were submitted to support data spaces in various industries in terms of legislation and funds.

The blue colour represents legislative and political initiatives. The green colour represents funding initiatives of the Commission. The brown colour describes other actions.

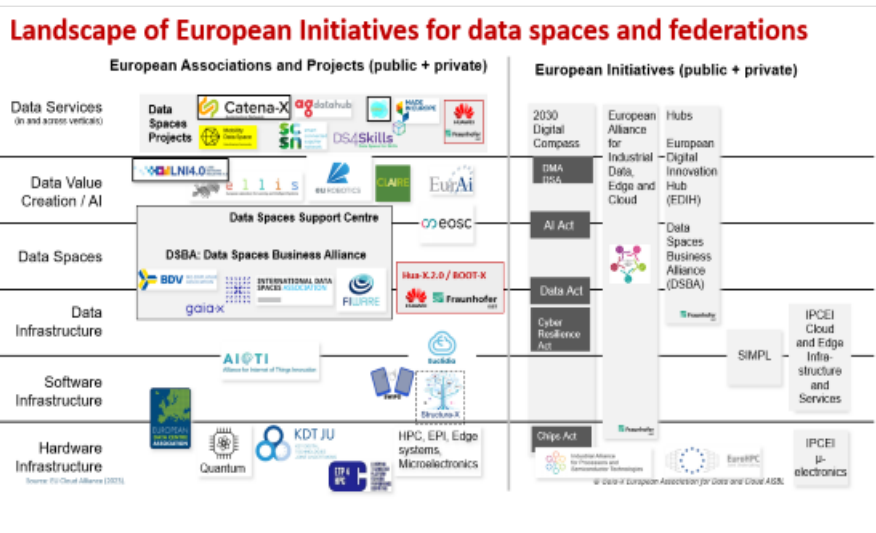


https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

<https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces>

Main industry associations defining the future and leading adoption of data spaces in Europe (DSBA, Gaia-X, IDSA, DSSC)

- DSBA**
 - Leadership
 - Convergence
- DSSC**
 - Governance
 - Facilitator of adoption
- IDSA**
 - industrial / international data spaces RAM
- Gaia-X**
 - Framework for Trust Compliance & Interoperability



Leadership in data space convergence, support, coordination: DSBA & DSSC

In September 2021, the Big Data Value Association (BDVA), FIWARE Foundation, Gaia-X and the International Data Spaces Association (IDSA) joined forces and formed the **Data Spaces Business Alliance (DSBA)** aimed at defining a common direction and driving convergence of data spaces.

- DSBA defines a Minimum Viable Framework (MVF) to enable the creation of data spaces.
- In September 2022 and April 2023 DSBA published a convergence discussion paper explaining a converging direction for data spaces

The Data Spaces Support Centre (launched in **October 2022** with EU funding by DSBA, My Data Global and Fraunhofer ISST) in order to **explore the needs of data space initiatives, define common requirements and establish best practices to accelerate the formation of sovereign data spaces as a crucial element of digital transformation in all areas.**

- Aimed at public sector and companies that want to create sovereign data spaces
- Funded by the European Commission as part of the Digital Europe Program

DSBA leads convergence of major data space infrastructure initiatives

Source: DSBA Technical Convergence paper V2 - 23rd of April 2023

3. Data Spaces Support Center

<https://dssc.eu/>

- The Data Spaces Support Centre will explore the needs of data space initiatives, define common requirements and establish best practices to accelerate the formation of sovereign data spaces as a crucial element of digital transformation in all areas.
- Aimed at public sector and companies that want to create sovereign data spaces
- Funded by the European Commission as part of the Digital Europe Program

DSBA Alliance Established, GAIA-X Complemented with IDSA and DSSC Accelerating the Transformation of Various Industries in the Data Economy

Data Spaces Business Alliance

Unleashing the Data Economy

implement a universal framework for data space and enhance collaboration between hubs

September 23, 2021

Big Data Value Association (BDVA) (from 2021 GAIA-X), Data, Artificial Intelligence and Robotics (AIDR), is an industry-driven international non-profit organization with more than 200 members in Europe, consisting of large, small and medium-sized industries, as well as research and user organizations. BDVA/BDVO focuses on digital transformation of the economy and society through data and artificial intelligence through the advancement of big data and artificial intelligence technologies and services, data platforms and data spaces, industrial artificial intelligence, data-driven value creation, and standardization, and skills. BDVA/BDVO has been the driving party of the H2020 Horizon Big Data Value PPP, a private member of EuroHPC, AI and one of the founding members of Horizon Europe's AI, Data and Robotics Partnership.

The FIWARE Foundation is a non-profit organization that drives the definition and management of open standards based on open source technologies, software architectures, and more than 800 intelligent data models to make it faster and easier to develop portable and interoperable smart solutions and affordable ways to avoid vendor lock-in scenarios. Founded in 2016, the foundation includes Altn, Engineering, INEC, Red Hat, Telefónica and many other leading technology companies in 483 plus members.

Gaia-X is a digital ecosystem created by its members. The initiative aims to create an environment where data can be stored, organized and shared in a trusted environment. Users always retain sovereignty over their data. As a result, a federated system has emerged that connects many cloud service providers and users.

IDSA mission is to shape the future of the global digital economy. More than 130 of its member companies and institutions have created the International Data Spaces Architecture (IDSA) a secure system for sovereignty and trusted data exchange in which all participants can realize the full value of their data. IDSA enables new intelligent services and innovation business processes. It works across companies and industries, while ensuring that control of data remains in the hands of data providers, it calls it data sovereignty.

BDVA, FIWARE, Gaia-X and IDSA
<https://dsba.eu/news/latest-news/dsba-fiware-gaia-x-and-idsa-launch-an-alliance-to-accelerate-business-transformation-in-the-data-economy/>

Gaia-X overview

Created as an international not-for-profit organization (ASBL) under the auspices of **van der Leede Commission of European strategic advisors** HQ in Brussels and 15 original members in Germany and France in 2020 has grown to 37 members internationally by beginning of 2023

Value proposition for Hubs!

European strategic alignment: Compliance with the Gaia-X becomes mandatory for business contracts of several & partner deals.

Global impact potential: Federated approach levels the playing field for all players regarding the data sovereignty and being the dominant of big data use cases in data application.

Member benefits: By offering European access to services, Hubs can give its members access to:

- Helping the existing customers (non-affiliated industry and governmental) services in Spain, Italy and the UK.
- Attracting Chinese companies to access EU integration being the technological transition for new data related services.

Openness:

- Hubs can align with Hubs' role of DSBA (Open Services) as a framework to open the cloud and services ecosystem making use with trust.
- Hubs can offer a secure extension of Hubs' Cloud offered services.
- Hubs can offer a secure extension of Hubs' Cloud offered services under DSBA (DSBA) wrap-up mechanism for potential member-joined Hubs' products and services.

Gaia-X structure and participation from Hubs' cross lab team

The 3 Pillar Gaia-X Framework

Gaia-X aims to connect the Data and Infrastructure Ecosystems and relies on three conceptual pillars to achieve that:

- Data Compliance:** Decentralized services to enable compliant and responsible trust.
- Data Spaces / Federated / Interoperable & portable (Cross-) Sector Data sets and services**
- Data Exchange:** Anchored contract rules for access & data usage.

For each pillar there are three types of deliverables: **Functional specifications, Technical Specifications and Software**

Industrial Data Spaces: IDS Trusted Data Spaces Provide Trusted Technical Contracts for Data Element Market Participants

Strategic industry requirements determine the design of the international data spaces architecture

Trust

Data market

Privacy and data sovereignty

Interoperability

Standardized interoperability

Members

Reference: <https://internationaldataspaces.org/wp-content/uploads/2023/04/ids-data-spaces-overview-2022.pdf>

Landscape of European Initiatives for data spaces and federations

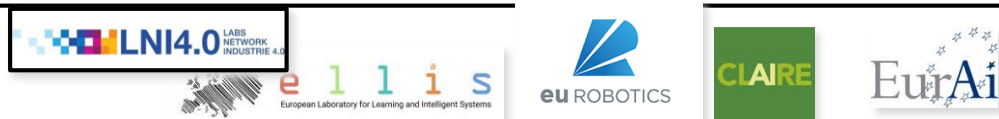
European Associations and Projects (public + private)

European Initiatives (public + private)

Data Services
(in and across verticals)



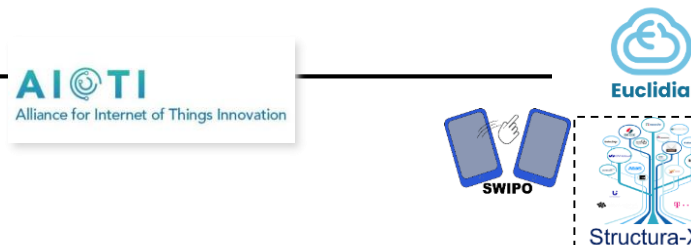
Data Value
Creation / AI



Data Spaces



Data
Infrastructure



Software
Infrastructure



Hardware
Infrastructure



2030
Digital
Compass

European
Alliance
for
Industrial
Data,
Edge and
Cloud

Hubs
European
Digital
Innovation
Hub
(EDIH)

DMA
DSA

AI Act

Data Act

Cyber
Resilience
Act

Chips Act



Data
Spaces
Business
Alliance
(DSBA)



SIMPL

IPCEI
Cloud
and Edge
Infra-
structure
and
Services

Industrial Alliance
for Processors and
Semiconductor Technologies



EuroHPC
Joint Undertaking

IPCEI
μ-
electronics

Source: EU Cloud Alliance (2023).

Leadership in data space convergence, support, coordination: DSBA & DSSC

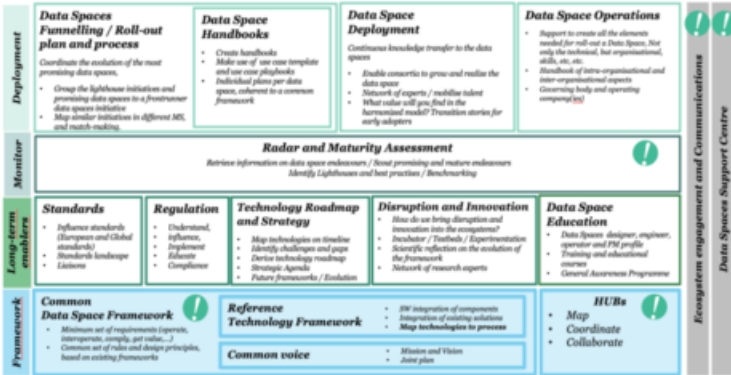
In September 2021, the **Big Data Value Association (BDVA)**, **FIWARE Foundation**, **Gaia-X** and the **International Data Spaces Association (IDSA)** joined forces and formed the **Data Spaces Business Alliance (DSBA)** aimed at defining a common direction and driving convergence of data spaces

- DSBA defines a Minimum Viable Framework (MVF) to enable the creation of data spaces.
- In September 2022 and April 2023 DSBA published a convergence discussion paper explaining a converging direction for data spaces
- The Data Spaces Support Centre (launched in **October 2022** with EU funding by DSBA, My Data Global and Fraunhofer ISST) in order to **explore the needs of data space initiatives**, define **common requirements** and establish **best practices** to **accelerate the formation** of sovereign data spaces as a crucial element of **digital transformation in all areas**.
- Aimed at public sector and companies that want to create sovereign data spaces
- Funded by the European Commission as part of the Digital Europe Program <https://www.egi.eu/project/dssc/>

DSBA leads convergence of major data space infrastructure initiatives

Data spaces are viewed as a key step to the Data Economy of the future.

In September 2021, the Big Data Value Association (BDVA), FIWARE Foundation, Gaia-X and the International Data Spaces Association (IDSA) decided to join forces and formed the Data Spaces Business Alliance (DSBA) aimed at driving convergence and the adoption of data spaces.



- Workstream 1 deliverables for Minimum Viable Framework**
- **Data interoperability:** NGSI-LD API and smart data models for actual data exchange, extending the interoperability mechanisms of the IDS-RAM with a special focus on Data Sovereignty and Trust;
 - **Data Sovereignty and Trust:** Trust Anchors and decentralized IAM including
 - Compatibility with eIDAS and EBSI
 - Verifiable Credential and presentation protocols ([OIDC4VC](#), [OIDC4VP](#), [SIOpV2](#), [DIDComm](#), [VP Exchange](#))
 - An ABAC (Attribute Based Access Control) framework enabling authorization based on VC
 - **Data value creation:** Centralized Service Catalogue and Marketplace functions based on TM Forum standards
- **Workstream 2:** Incorporation of IDS Connector functions and support to ODRL for the definition of access/usage control policies
- **Workstream 3:** Shared Catalogue and Federated Marketplace services based on TM Forum standards and aligned with Gaia-X & IDS-RAM specs
- **Workstream 4:** Additional IDS architectural elements for usage control

Source: DSBA Technical Convergence paper V2 – 21st of April 2023

https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf

To simplify slide

3. Data Spaces Support Center

<https://dssc.eu/>



- The Data Spaces Support Centre will explore the needs of data space initiatives, define **common requirements** and establish **best practices** to **accelerate the formation** of sovereign data spaces as a crucial element of **digital transformation in all areas**.
- Aimed at public sector and companies that want to create sovereign data spaces
- Funded by the European Commission as part of the Digital Europe Program <https://www.egi.eu/project/dssc/>

Benefits for Public Administrations and Businesses:

- Enabling the availability of technologies, processes, legal frameworks, standards, and tools (e.g. Community of Practice, Blueprint) for the deployment of data spaces;
- Fostering the adoption of above technologies and standards to enable the reuse of data across sectors by different stakeholders with a multidisciplinary approach based on co-creation and interaction;
- Shared data in business model development or in efficient, effective and repeatable policy decision-making.
- More data becomes available for use in the economy and society, while keeping those who generate the data in control;
- Giving confidence to businesses and public administrations to share data in data spaces.
- Improving contributions to the objectives of the Green Deal and the SDG'20.

Consortium members



Associated and collaboration partners



DSBA Alliance Established, GAIA-X Complemented with IDSA and DSSC Accelerating the Transformation of Various Industries in the Data Economy

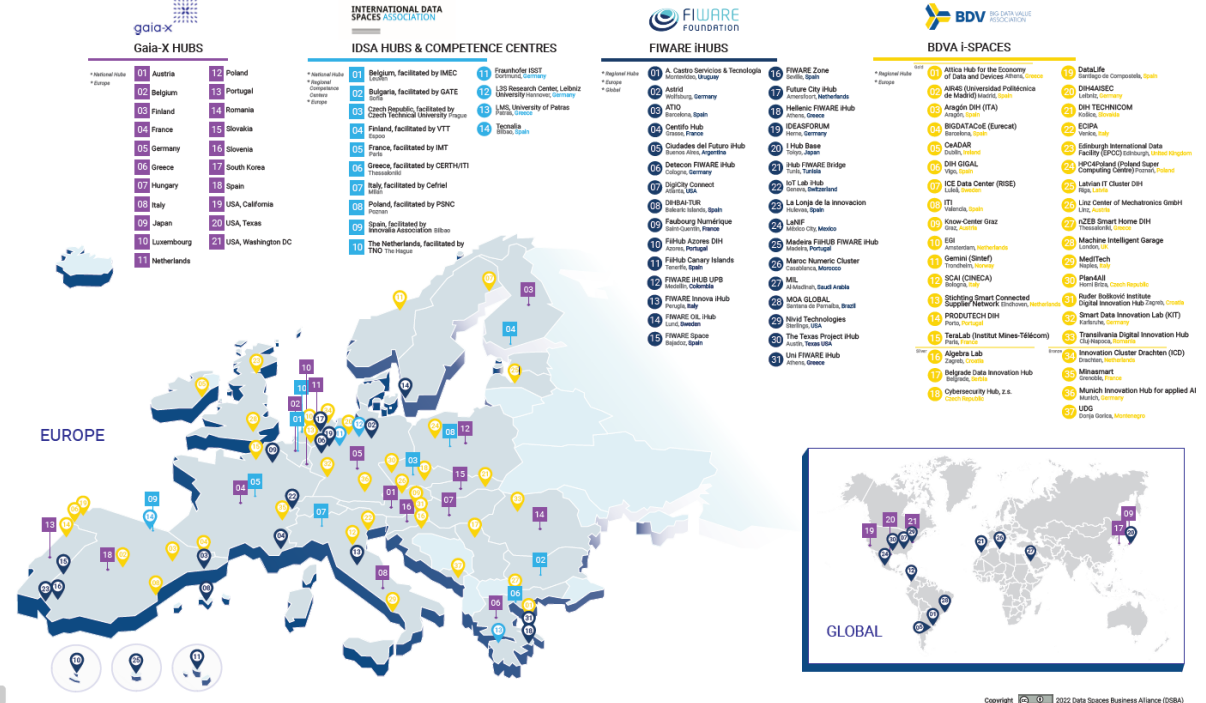
Data Spaces Business Alliance Unleashing the Data Economy

Implement a universal framework for data space and enhance collaboration between hubs



September 23, 2021

- Big Data Value Association - BDVA** (From 2021 DAIRO - Data, Artificial Intelligence and Robotics AISBL) It is an industry-driven international non-profit organization with more than 230 members in Europe, consisting of large, small, and medium-sized industries, as well as research and user organizations. BDVA/DAIRO focuses on digital transformation of the economy and society through data and artificial intelligence through the advancement of big data and artificial intelligence technologies and services, data platforms and data spaces, industrial artificial intelligence, data-driven value creation, and standardization. and skills. BDVA/DAIRO has been the private party of the H2020 Partner Big Data Value PPP, a private member of EuroHPC JU and one of the founding members of Horizon Europe's AI, Data and Robotics Partnership.
- The Fireware Foundation** is a non-profit organization that drives the definition and encouragement of open standards based on open source technologies, reference architectures, and more than 800 intelligent data models to make it faster and easier to develop portable and interoperable smart solutions and affordable ways to avoid vendor lock-in scenarios. Founded in 2016, the foundation includes Atos, Engineering, NEC, Red Hat, Telefónica and Trigyn Technologies among its 430-plus members.
- Gaia-X** is a digital ecosystem overseen by its members. The initiative aims to create an environment where data can be served, organized and shared in a trusted environment. Users always retain sovereignty over their data. As a result, a federated system has emerged that connects many cloud service providers and users.
- IDSA** mission is to create the future of the global digital economy. More than 130 of its member companies and institutions have created the International Data Space Architecture (IDS): a secure system for sovereign and trusted data exchange in which all participants can realize the full value of their data. IDS enables new intelligent services and innovative business processes to work across companies and industries, while ensuring that control of data remains in the hands of data providers. We call it data sovereignty.



Gaia-X Hub 21↑
FIWARE iHubs 31↑
IDSA HUB 14↑
BDVA i-Spaces 37↑

BDVA, FIWARE, Gaia-X and IDSA
<https://gaia-x.eu/news/latest-news/bdva-fiware-gaia-x-and-idsa-launch-an-alliance-to-accelerate-business-transformation-in-the-data-economy/>
<https://data-spaces-business-alliance.eu/dsba-hubs/>
<https://www.fiware.org/wp-content/uploads/DSBAHubsLandscape.pdf>

Gaia-X overview

Created as an international not-for-profit organization (AISBL) under the auspices of [von der Leyen Commission](#) of European [strategic autonomy](#)
 HQ in Brussels and 15 original members in Germany and France in 2020 has grown to 377 members internationally by beginning of 2023

Value proposition for Huawei

European strategy alignment

- **Ecosystem:** Gaia-X as is tightly coupled to EC regulatory framework initiatives for EU open Cloud & Data ecosystem.
- **De-risk:** Compliance with the Gaia-X becomes mandatory for business continuity of Huawei & partner clouds.
- **Growth:** Early adoption to Gaia-X standards is an asset for business growth.

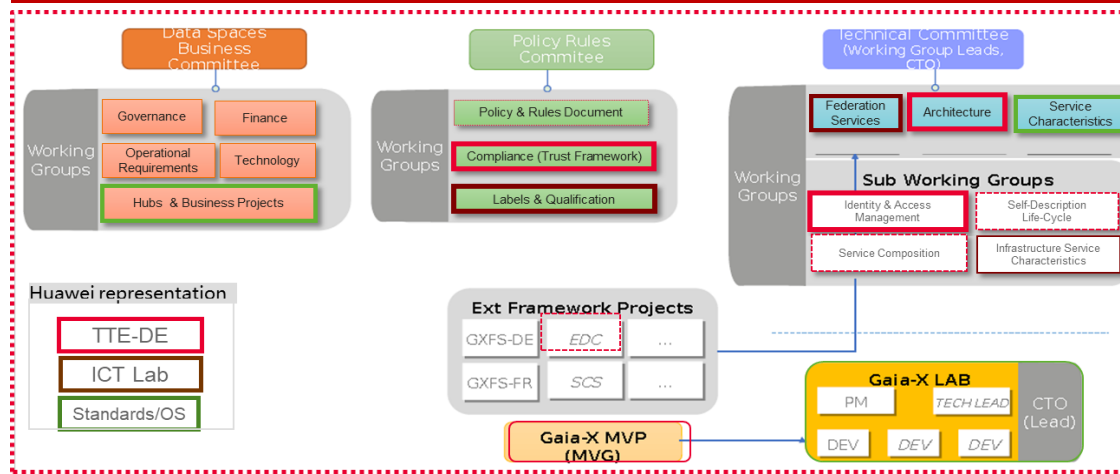
Global impact potential

- **Incubating Global standard:** Gaia-X and IDSA aim to selectively standardize architecture and specifications into ISO via CEN
- **Game changing:** Federated approach levels the playing field for all players respecting the data ownership and limiting the dominance of big three cloud providers as data aggregators.
- **Accelerator:** By offering dataspace access as a service, Huawei can grow its market share by
 - Bringing the existing customers from different industry and geographical domains together in open, federated data spaces
 - Enabling Chinese companies to access EU dataspace
 - Being the technological foundation for new data federation services

Openness

- **OSC vision alignment:** Huawei's vision of OSC (Open Services Cloud) as a framework to open the cloud data and services ecosystem matches well with Gaia-X requirements
- **Cloud Futures:** Dataspace access services offer are well positioned as a future extension of Huawei Cloud aPaaS product family
- **Open source strategy:** Gaia-X, IDSA and Catena-X board all open source under Eclipse. OSS strategy remedies the potential reservation against Huawei products and services.

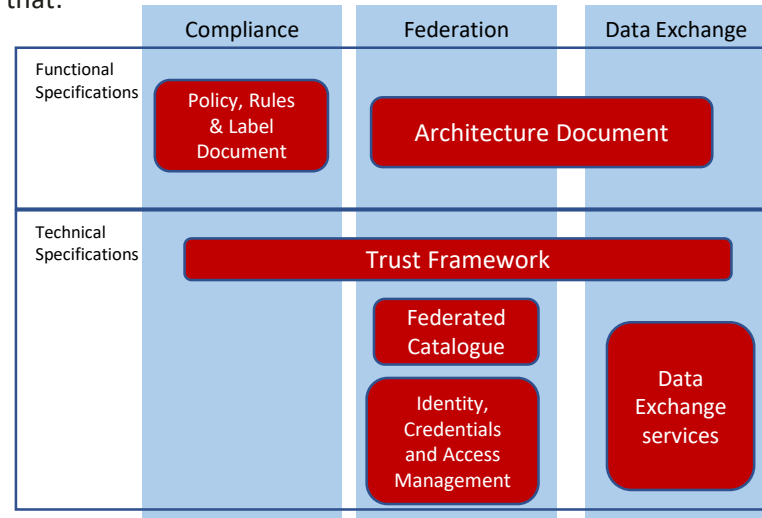
Gaia-x structure and participation from Huawei cross-lab team



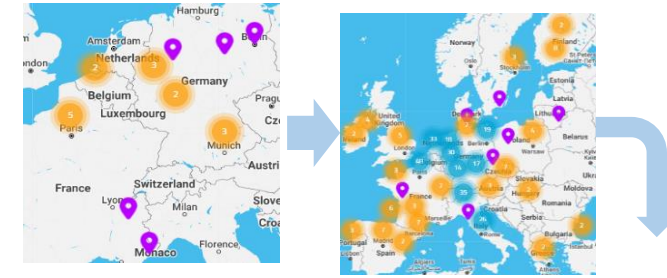
The 3 Pillar Gaia-X Framework

Gaia-X aims to connect the Data and Infrastructure Ecosystems and relies on three conceptual pillars to achieve that:

1. **Gaia-X Compliance:** Decentralized services to enable objective and measurable trust
2. **Data Spaces / Federations:** Interoperable & portable (Cross-) Sector data-sets and services
3. **Data Exchange:** Anchored contract rules for access & data usage



For each pillar there are three types of deliverables: **Functional specifications, Technical Specifications and Software**



- **377 total number of members in 2023.H1**
- **40% Membership increase since 2021**
 - 24% increase in Germany
 - 33% increase in France
 - 40% increase in Italy
 - 67% increase in UK
 - 100% increase in USA
 - 100% increase in South Korea
 - 300% increase in Japan
 - 300% increase in China

Industrial Data Spaces: IDS Trusted Data Spaces Provide Trusted Technical Contracts for Data Element Market Participants

Strategic industry requirements determine the design of the international data spaces architecture

INTERNATIONAL DATA SPACES ASSOCIATION

Trust 1

Trust is the basis of the International Data Spaces. It is supported by a comprehensive identity management focusing on the identification of participants and providing information about the participant based on the organizational evaluation and certification of all participants.

Data markets 6

The International Data Spaces enables the creation of novel, data driven services that make use of data apps. It also fosters new business models for those services by providing clearing, billing and the creation of domain specific brokers and marketplaces. In addition, usage restrictions and legal aspects are provided as templates and with methodological support.

Value adding apps 5

The International Data Spaces enables app injection to connectors to add services on top of the pure data exchange. This includes services for data processing as well as the alignment of data formats and data exchange protocols, but also enables analytics on data by the remote execution of algorithms.

2 Security and data sovereignty

Components of the International Data Spaces rely on current security measures. Next to architectural specifications, this is realized by the evaluation and certification of the components. In line with the central aspect of ensuring data sovereignty, a data owner in the international data spaces attaches usage restriction information to its data before it is transferred to a data consumer. The data consumer may use this data only if it fully accepts the data owner's usage policy.

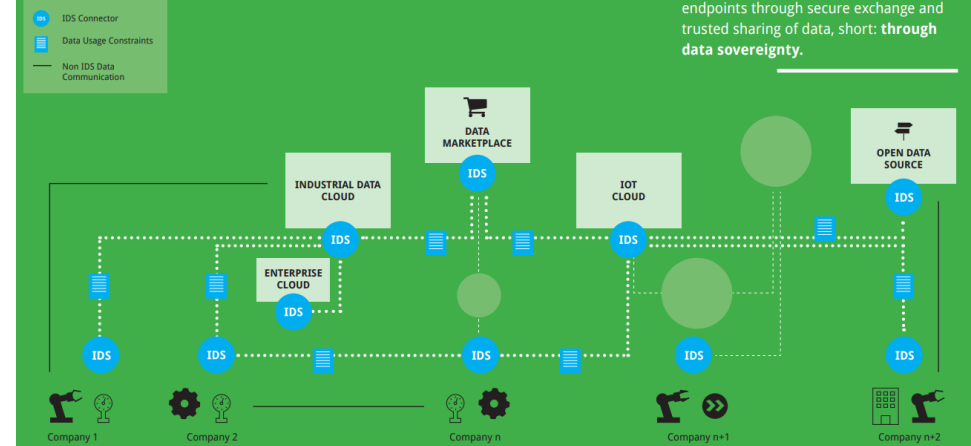
3 Ecosystem of data

The architecture of the International Data Spaces does not require central data storage capabilities. Instead, it 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. This approach requires a holistic description of the data source and data as an asset combined with the ability to integrate domain specific vocabularies for data. Brokers in the ecosystem enable comprehensive realtime search for data.

4 Standardized interoperability

The International Data Spaces Connector, being a central component of the architecture, is implemented in different variants and from different vendors. Nevertheless, each connector is able to communicate with every other connector or component in the ecosystem of the International Data Spaces.

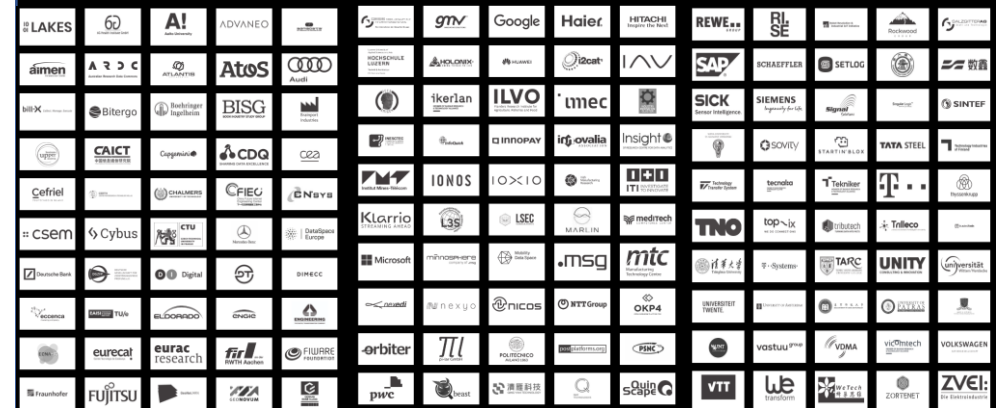
The International Data Spaces approach connects all kinds of data endpoints



When broadening the perspective from an individual use case scenario to a data space view, the IDS architecture becomes the link between different cloud solutions, platforms, marketplaces, and other data endpoints through secure exchange and trusted sharing of data, short: through data sovereignty.

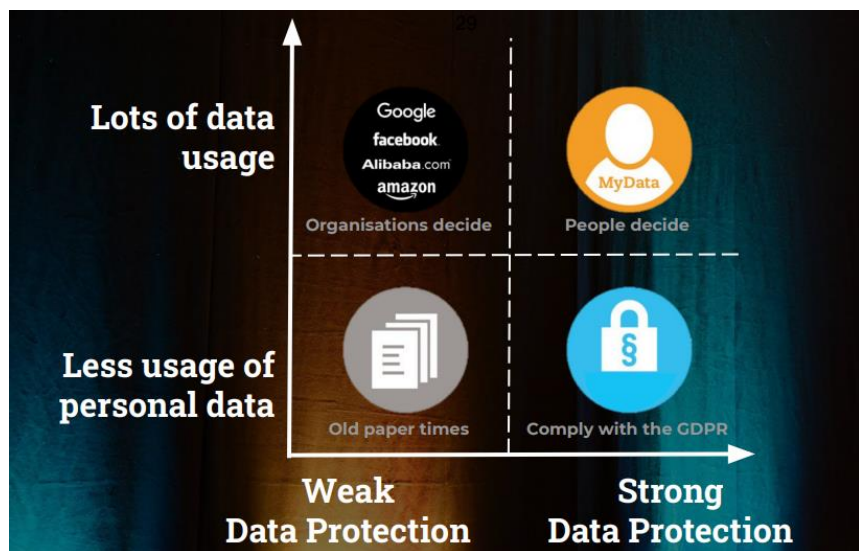
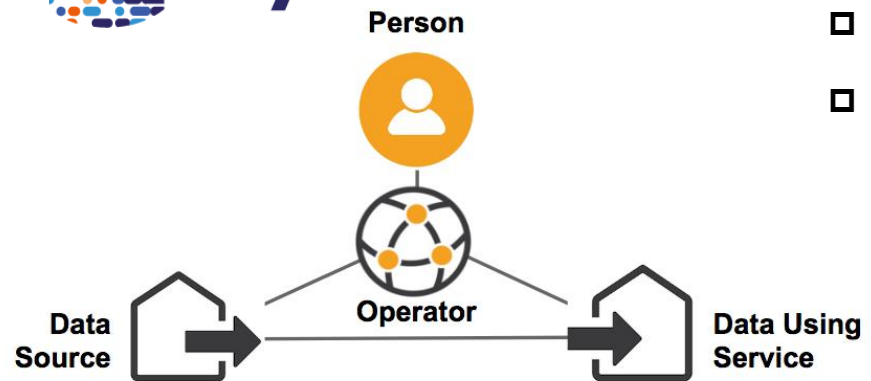
One software component connects all kinds of data clouds, platforms, and marketplaces - the IDS Connector.

Members:



Reference: <https://internationaldataspaces.org/wp-content/uploads/IDSA-data-spaces-overview-2022.pdf>

Personal Data Spaces: Personal data carriers help individuals build self-controllable data space.



- ❑ Personal data operators enable individuals to securely access, manage and use their personal data, and control the flow of personal data to data sources and data usage services
- ❑ MyData Global is an award-winning international non-profit organization. MyData Global aims to empower individuals by enhancing their right to self-determination over their personal data.
- ❑ MyData Global has nearly 100 organizational members and nearly 400 individual members from more than 40 countries on six continents. Promotes the more than 2,000 strong MyData Global community dedicated to the ethical use of personal data.

MYDATA OPERATORS 2022



来源: <https://www.mydata.org/>

Contents

Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)

A holistic execution approach is required across the entire ecosystem players:

There are several industry associations on play....

Towards a converging Data Space (Security) Architecture

What is a data space? Ecosystem, basic services, connectors, common capabilities

DSBA defines convergence and MVF that builds on Gaia-X, IDSA architectures and TM Forum and OpenDEI principles

TTE-DE specifies a data space security reference architecture

Reference implementation: OSS on Eclipse foundation

Standardization is going global

Competition is investing heavily

An overview of data space projects in Europe

Emerging architectural variants

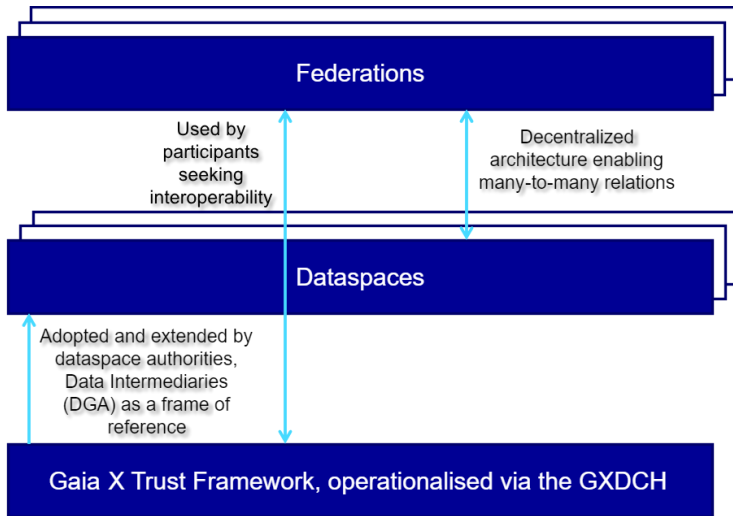
Huawei contributions in Hua-X and Digital Sovereignty projects: technical

Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap

Recommendations

Appendix I: Core technologies

What is a dataspace? Digital ecosystem federation & data spaces



The **Gaia-X Trust Framework** is the set of rules that define the minimum baseline to be part of the **Gaia-X Ecosystem**.

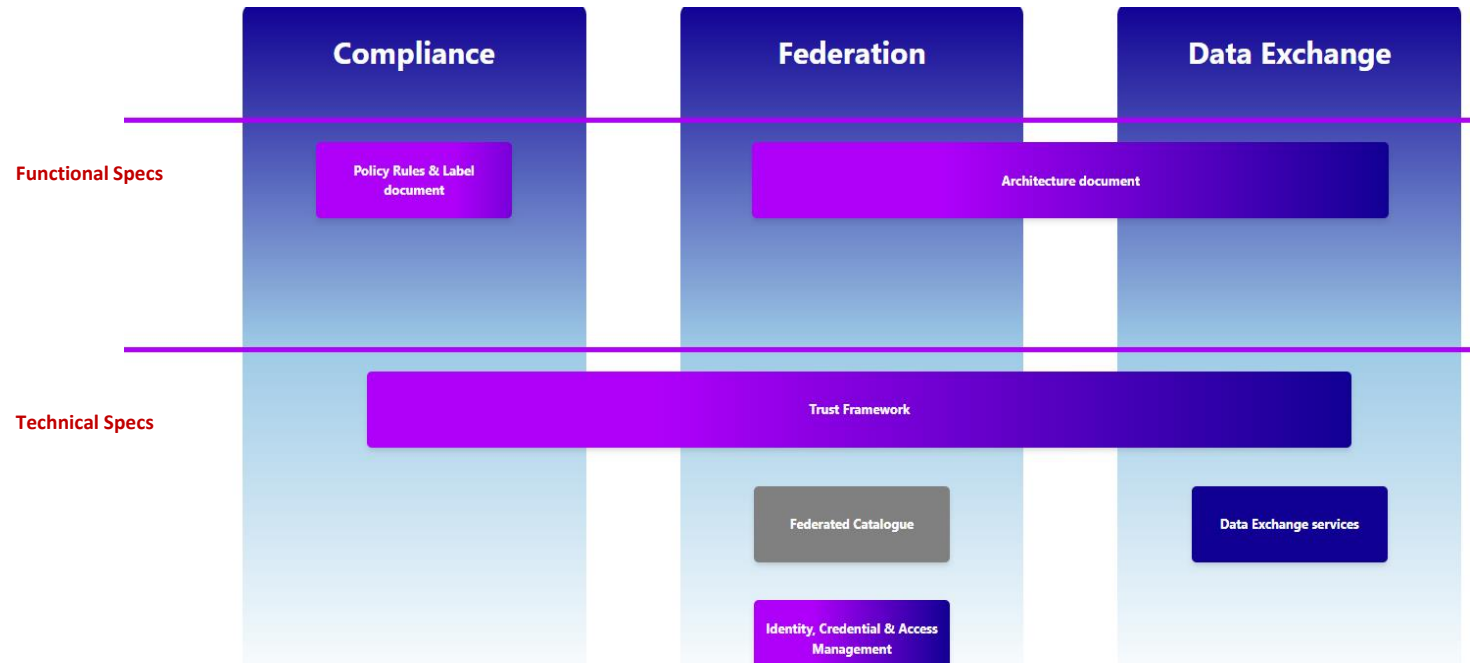
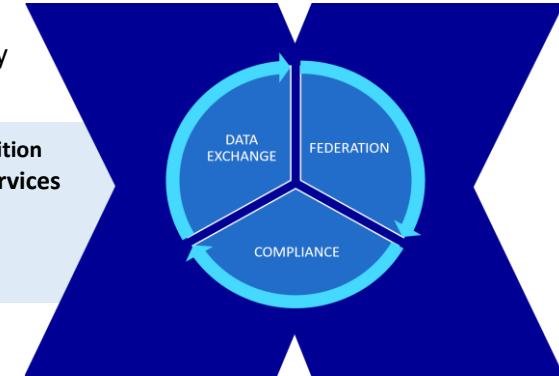
Those rules provide a common governance and the basic level of interoperability across individual ecosystems while letting the users in full control of their choices.

GXDCH is a reference architecture of a Digital Clearing House to operationalize conformity assessment and verification of Gaia-X compliant trust framework agreements and credentials

The Gaia-X Association developed its **Gaia-X Framework**, which enables the transition from disjoint data & infrastructure ecosystems, to composable, interoperable & portable cross-sector data sets and services.

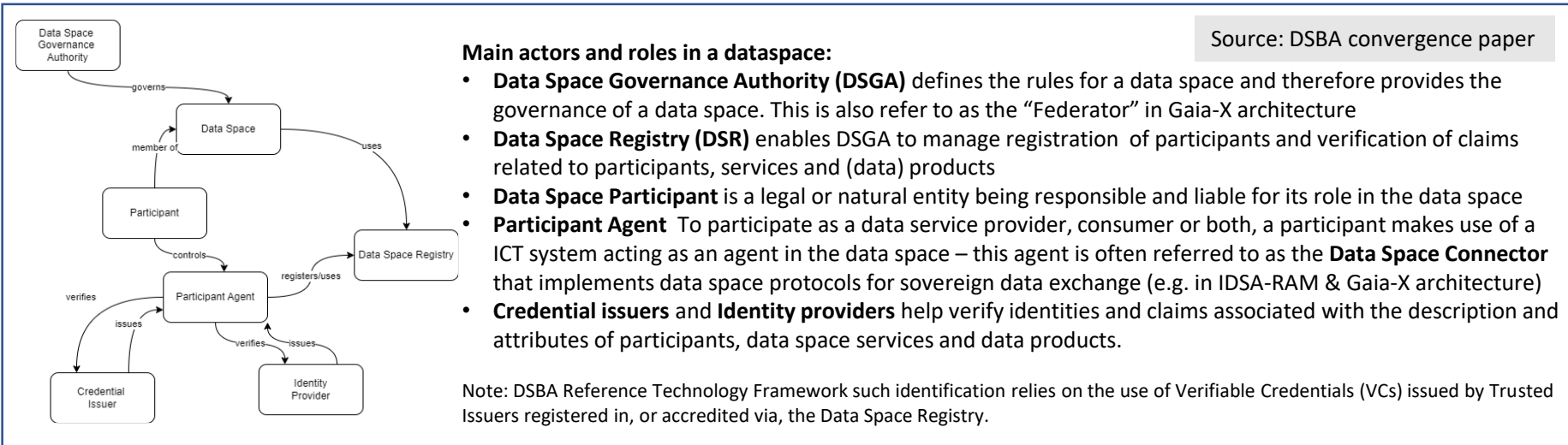
Gaia-X Framework builds on top of the X-Model in order to enable trust and interoperability within and across data spaces and federations <https://gaia-x.eu/gaia-x-framework/>

- **Advanced services:** New (cross-) sector innovations and applications build from **service composition**
- **Data Spaces / Federations:** Enable **interoperable** and **portable** (cross-) sector **data-sets and services**
- **Data Exchange:** Anchored contract rules for access and data usage
- **Gaia-X Compliance:** Decentralized services to enable measurable trust
- **Label framework:** Gaia-X ecosystem specific Labels to ease market adoption



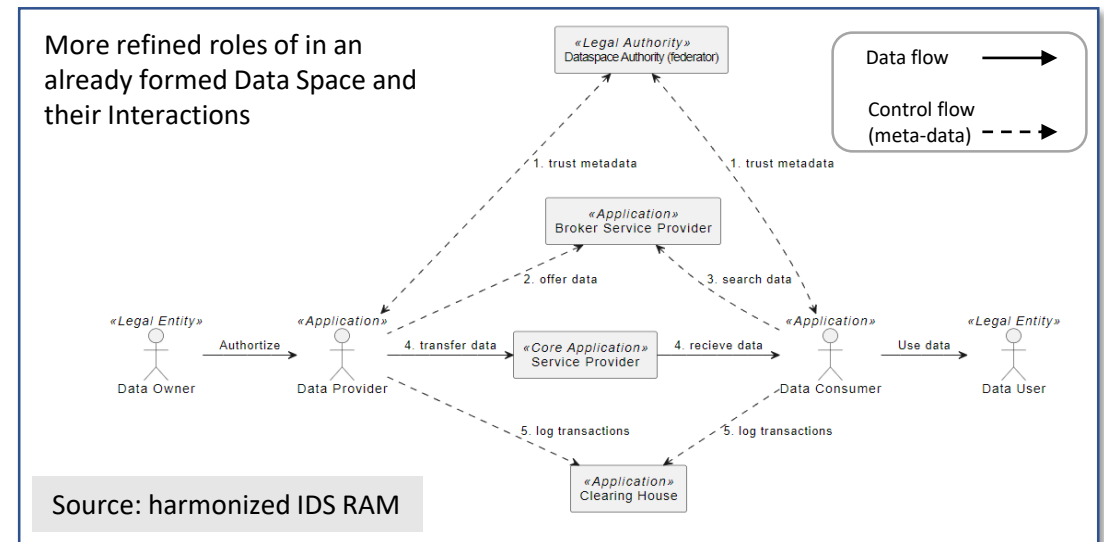
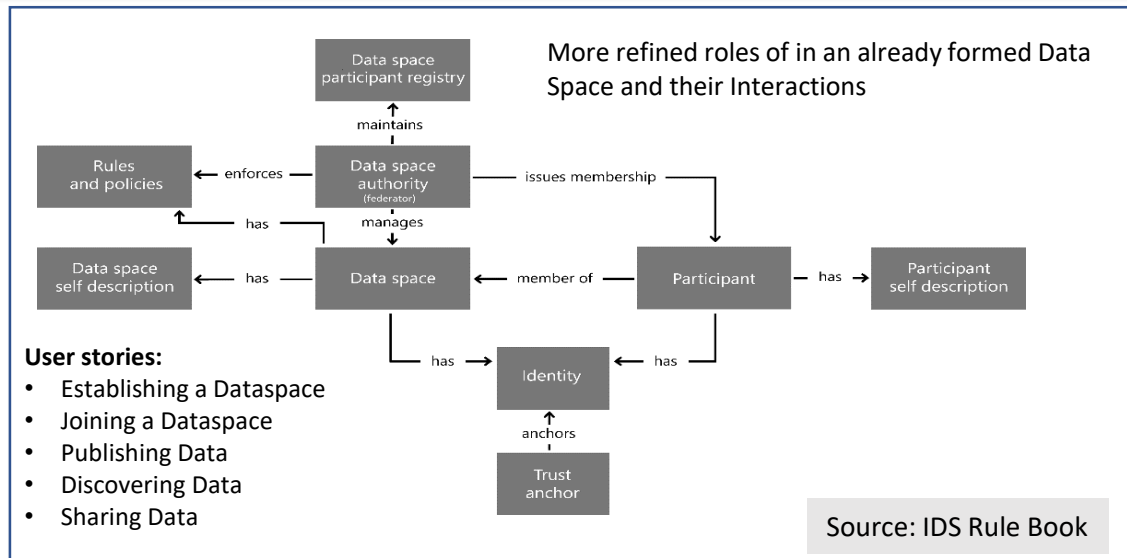
What is a dataspace? Definition, common capabilities and use-cases

- A *dataspace* is a (distributed) data ecosystem built around commonly agreed building blocks that enable a common governance framework to be established for secure and **sovereign data storage, management, sharing / exchange and utilization** among participants for the creation of value.
 - > *Data Sovereignty* is the ability of a natural or legal person to exclusively and sovereignly decide concerning the usage of data as an economic asset. This translates to the ability of the data owner and stakeholders to set the policies for the use and access of the data to be exchanged while conforming to local regulation and international agreements.



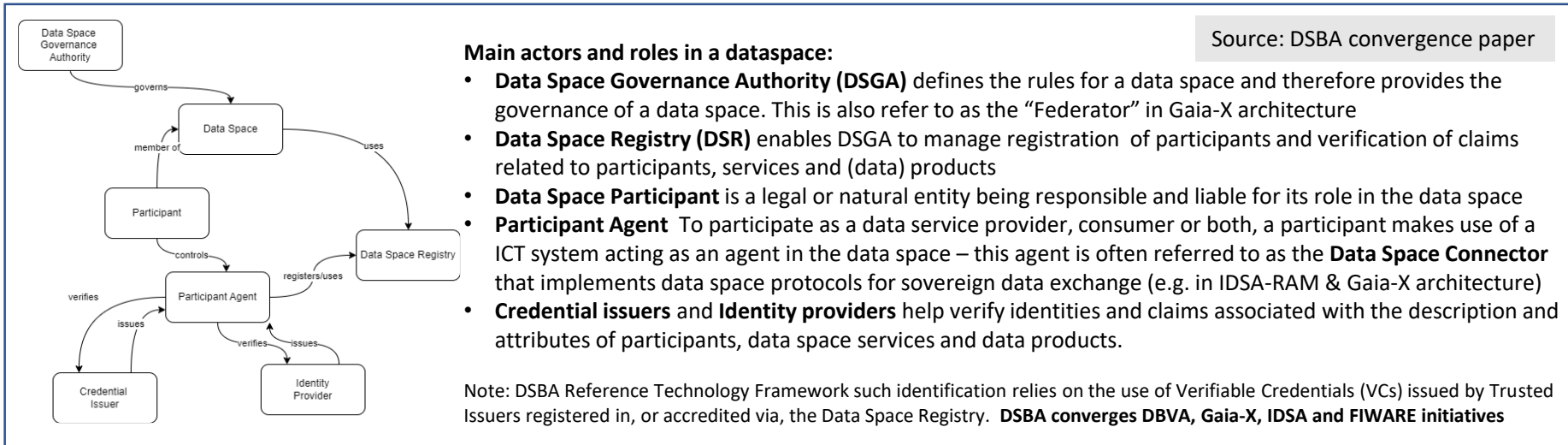
DSBA converges and synchronizes the work at DBVA, Gaia-X, IDSA and FIWARE initiatives

DSBA is leading the convergence between the architectures, technology and standard baselines, interoperability and compliance requirements of the major data space associations



What is a dataspace? Definition, common capabilities and use-cases

- A *dataspace* is a (distributed) data ecosystem built around commonly agreed building blocks that enable a common governance framework to be established for secure and **sovereign data storage, management, sharing / exchange and utilization** among participants for the creation of value.
 - > *Data Sovereignty* is the ability of a natural or legal person to exclusively and sovereignly decide concerning the usage of data as an economic asset. This translates to the ability of the data owner and stakeholders to set the policies for the use and access of the data to be exchanged while conforming to local regulation and international agreements.



Dataspaces are being defined in several communities with common concerns of data sovereignty: A dataspace may include different patterns and protocols of data exchange and a set of interoperable data-exchange applications by other actors in a specific sector, either by their own development or through a certified software vendor, data broker, or marketplace.


However, **common capabilities and building blocks can be identified to present a minimal dataspace architecture.**

Data space building blocks (source: DSBA Convergence paper & OpenDEI design principles)			
Technical building blocks			Governance building blocks
Interoperability	Data Sovereignty & Trust	Data Value Creation	Governance
Data models & formats	Access & usage Control / Policies & agreements	Descriptions of Data, Services and Offerings	Business Agreements
Data exchange protocols & APIs	Identity & credentials management	Metadata schemes. Publication & Discovery	Operational Agreements
Provenance & Traceability	Trust Services	Marketplace & usage accounting	Organizational Agreements
<p>Functions extending data space connectors</p> <p>To enable data space interoperability as in ISO/IEC 21823-1:2019 a common set of rules should be adopted by all data space governance authorities with the use of a common meta-registry such as Gaia-X Registry</p>			
<p>Realize the Data Space (Verifiable Data) Registry provided by the Data Space Authority</p>		<p>Federated services enabling the lifecycle, sovereignty, compliance and interoperability of data spaces</p>	



What is a dataspace? Comprehensive conceptual model

<https://design-principles-for-data-spaces.org/>



- Lead architects and representatives from the different associations of DSBA have produced a conceptual model for data spaces as a reference and baseline for convergence between the different associations: DBVA, Gaia-X, IDSA and FIWARE as well as alignment with TM Forum recommendations.
 - > Huawei input was captured through our participation and review of the convergence baseline in Gaia-X Architecture WG (represented by Pierre Gronlier Gaia-X CTO and Klaus Ottradovetz, ATOS) and IDSA Architecture working groups (represented by Sebastian Steinbuss IDSA and Anna Maria Schleimer, Fraunhofer ISST)

Trust Framework 


Trust: Trust Frameworks specify recognized authorities and a set of rules and policies that define the minimum baseline to be part of a data space, enable interoperability of claims within and across data spaces and provide features to automate compliance

Identity (ICAM)  


Identity: ICAM (identity, credential and access management) services enable trust in the digital identity and verifying claims of participants and resources across different trust domains

Data Sovereignty  

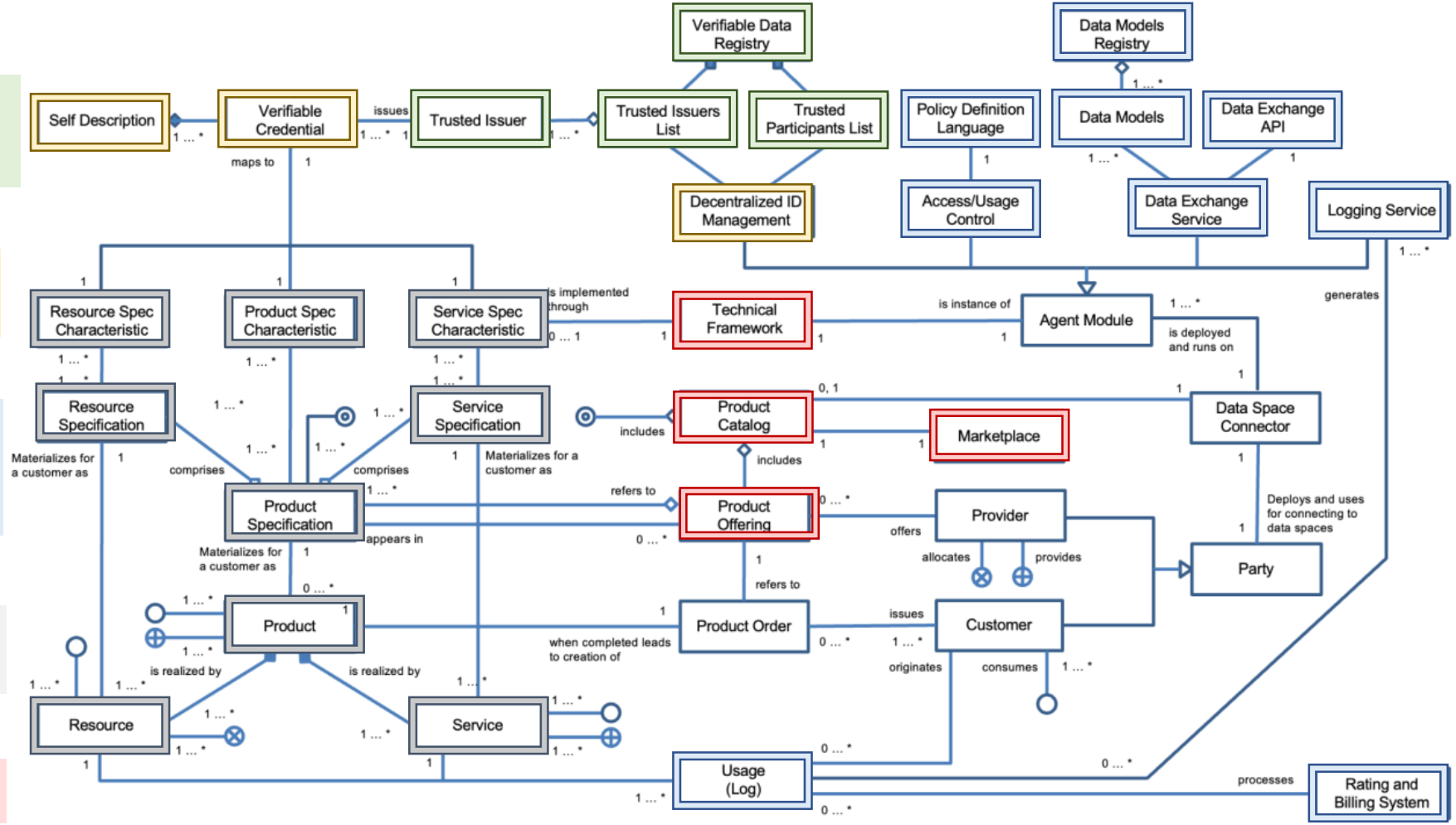
Sovereignty: this functional unit that contain the essential services required to achieve data sovereignty. The crucial part is to utilize contracts /agreements and usage policy as an artifact to reflect how a data provider wishes their assets to be used while ensuring compliance with regulation and agreements

Data Product 

Product: Description of Data (Product) offers the means to describe data based on extensible vocabularies to enable services utilizing and extending (data) ecosystem services

Ecosystem Data 

Ecosystem Data services enable to find or advertise data and data-value creation applications within and across data spaces



Additional insights gained: Common data exchange patterns

The Exchange Services in Gaia-X & IDS-RAM generalize the concept of data exchange and define different functions for different phases of exchanges: **before** | **during** | **after** transaction

Extensive analysis of different dataspace examples has identified the following data exchange patterns

Dataspace connector

- Used mainly in **International & Industrial Data Space**
- Focus of Boot-X and Hua-X2
- **Covered in v1 of DS architecture (DS2)**

Compute-to-data

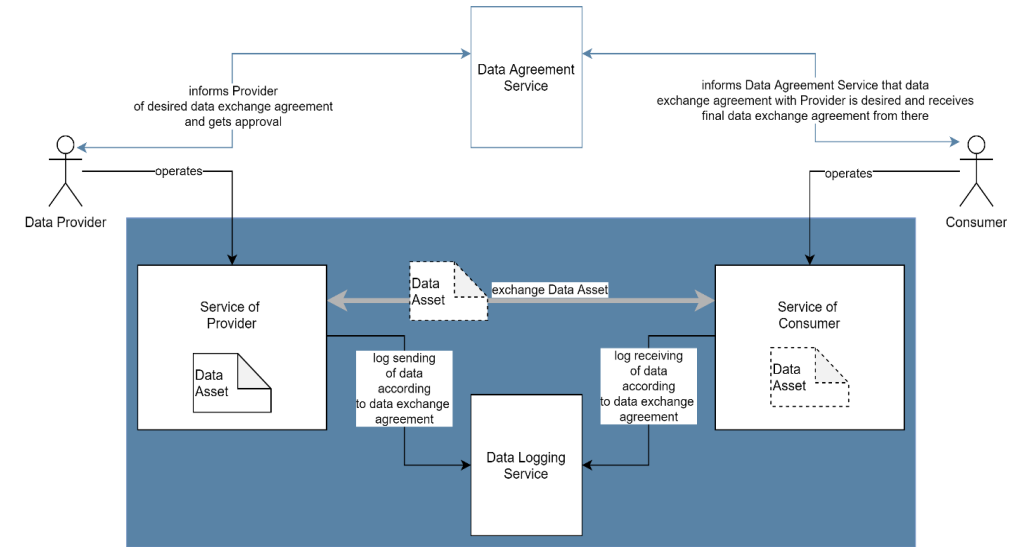
- Used in some C-CTI pilot platforms
- Used in some AI pilot services on industrial data spaces
- Examples include OPAL, NTT Virtual Data Lake, Copernicus AP
- To be covered in **V3 of DS architecture (DS3)**

Data Pod network of linked data

- Used mainly in **personal data spaces**
- Examples include
 - W3C Solid Data Pods
 - DIF Web Data Nodes
- To be covered in **V2 of DS architecture (DS3)**

Protected Data Bundle

- Used in some C-CTI pilot platforms
- Focus of some DUCA use-cases
- Covered in **V3 of DS architecture (DS3)**



Source: https://gaia-x.gitlab.io/technical-committee/architecture-document/data_exchange_services/

Examples of components and data exchange patterns in known data sharing architectures

Data Space Connector

W3C SOLID Data Pod

DIF Web Data Node

OPAL data node

Protected Data Bundle

What is a dataspace? Data space connector (IDS-RAM perspective)

What is a dataspace? Data pods (example: inrupt.com / W3C solid)

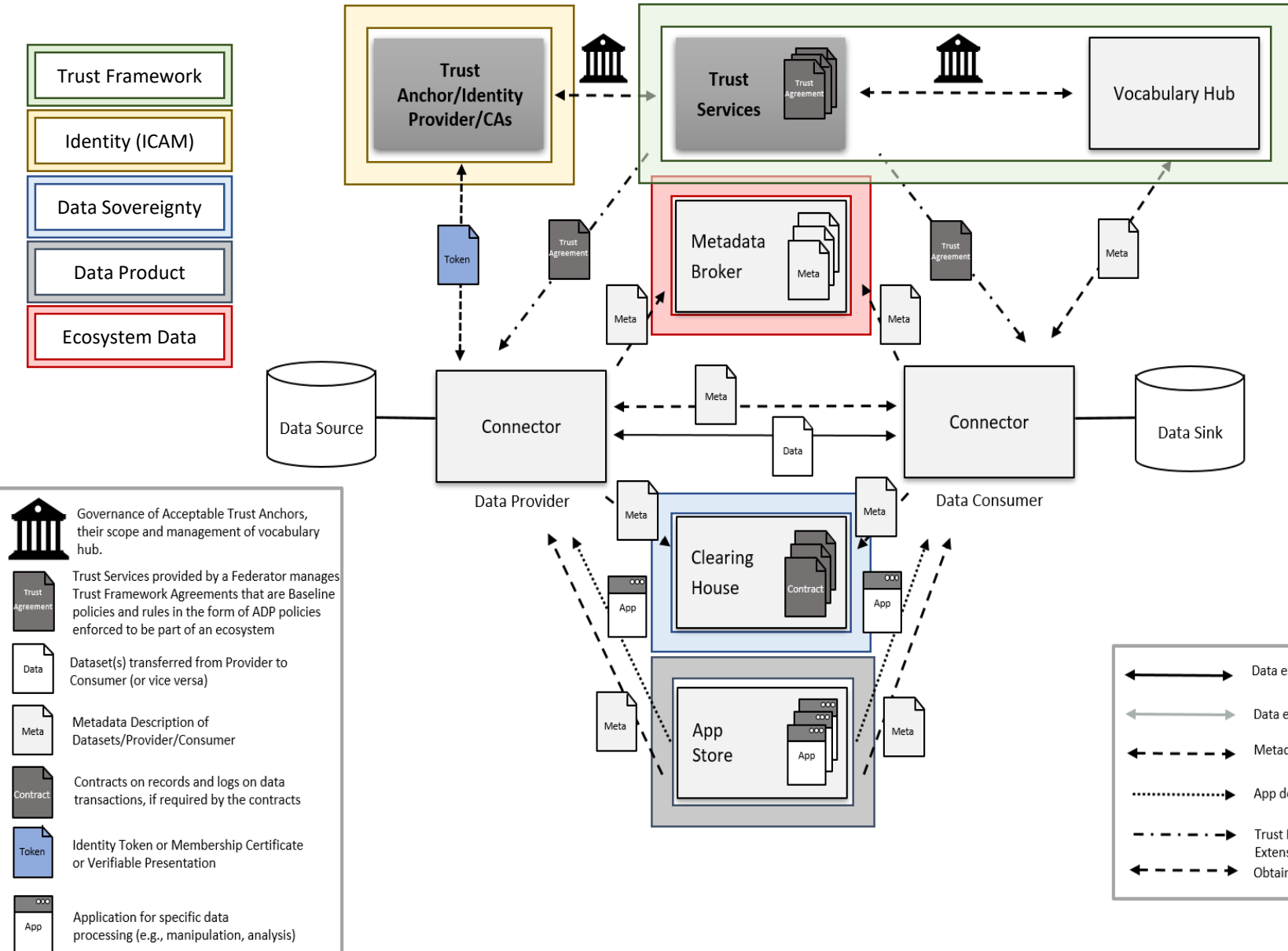
What is a dataspace? Distributed data store mesh (example: DIF WBDN)

What is a dataspace? Compute-to-data (example: MIT OPAL: Open Algorithms)

What is a dataspace? Protected data bundles with data contracts (example: C3ISP: E-CORRIDOR)



What is a dataspace? IDS connector used on Gaia-X federation



- **Dataspace Connectors:** A technical core component required for a participant to join the industrial dataspaces.
- **Metadata Broker:** The Metadata Broker contains an endpoint for the registration, publication, maintenance, and query of Self-Descriptions.
- **Trust Framework:** Provides Trust Framework Agreements that are **enactable digital contracts** about trust anchors that state permissions, prohibitions and obligations in using trust anchors and the credentials they produce.
- **Trust Anchor/Identity Provider:** An entity that provides digital identities to the participants/principles in an industrial dataspace so that aspect of identification, authentication, and authorization can be defined
- **Vocabulary Hub:** The interoperability requirements in the industrial dataspace directly lead to the usage of commonly known, standardized terms to describe data, services, contracts, and so on
- **Clearing House:** logging service that records information relevant for clearing and billing as well as usage control.
- **App Store:** An App is an independent, functional, and re-usable software asset that is deployable, executable, and manageable on a dataspace Connector and app store host these app for the participants to use it for various aspects of data management in a dataspace.

Governance of Acceptable Trust Anchors, their scope and management of vocabulary hub.

Trust Services provided by a Federator manages Trust Framework Agreements that are Baseline policies and rules in the form of ADP policies enforced to be part of an ecosystem

Dataset(s) transferred from Provider to Consumer (or vice versa)

Metadata Description of Datasets/Provider/Consumer

Contracts on records and logs on data transactions, if required by the contracts

Identity Token or Membership Certificate or Verifiable Presentation

Application for specific data processing (e.g., manipulation, analysis)

Data exchange (active)

Data exchange (inactive)

Metadata exchange

App download

Trust Framework Agreement Extension

Obtaining Credentials

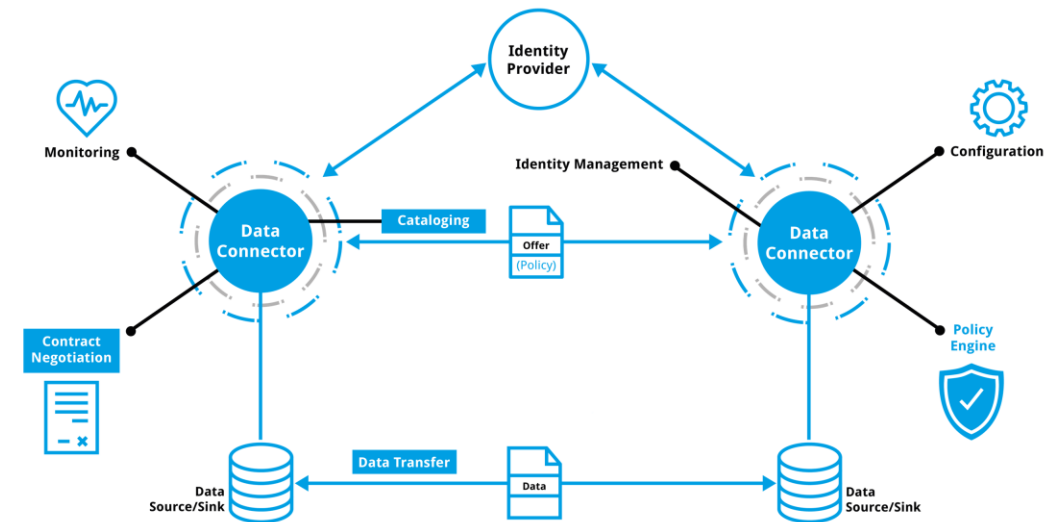
What is a dataspace? Main building blocks, challenges and design reference

Data space building blocks (source: DSBA Convergence paper& OpenDEI design principles)

Technical building blocks			Governance building blocks
Interoperability	Data Sovereignty & Trust	Data Value Creation	Governance
Data models & formats	Access & usage Control / Policies & agreements	Descriptions of Data, Services and Offerings	Business Agreements
Data exchange protocols & APIs	Identity & credentials management	Metadata schemes. Publication & Discovery	Operational Agreements
Provenance & Traceability	Trust Services	Marketplace & usage accounting	Organizational Agreements

Interoperability building blocks ensures that providers of data products within data spaces must be able to offer data services at well defined endpoints knowing that customers, unknown by them a priori, will know how to consume their data services through those endpoints.

- This means that all participants in data spaces should address interoperability at several levels (see [ISO/IEC 21823-1](#)):
 - **transport** and **syntactic** level, e.g. by common APIs
 - **semantic** level, e.g. by common data models/vocabularies
- DSBA proposes [NGSI-LD](#) for transfer of digital twin data and **Dataspace Connector Protocols** (e.g. [IDSA Dataspace Protocol](#)) for the **Control of data transfer**. Other Relevant standards:
 - [ISO 19941 Cloud Computing Interoperability and Portability](#), which is referenced in the EU Data Act
 - [European Interoperability Framework \(EIF\)](#), which aims to create a digital single market in Europe.
- Adoption of **common data models** is encouraged and there are multiple references that may consider for different domains (e.g. ISO/IEC CIM for Energy, etc)
 - The [Smart Data Models initiative](#) brings a hub to help map different data models into **JSON**, **JSON-LD** and other data serialization formats
- **Provenance and traceability** have not been aligned as yet but lighthouse project [Catena-X \(Tractus-X Traceability KIT\)](#) leads the way
 - Current approach investigates mechanisms to store evidence in big-chain, examine against data usage policies and interact with linked data notifications
 - See also XFSC logging service specification (mature service yet to be designed)



Overview on IDSA data space protocol and context
<https://docs.internationaldataspaces.org/ids-knowledgebase/v/dataspace-protocol/>

What is a dataspace? Main building blocks, challenges and design reference

Data space building blocks (source: DSBA Convergence paper& OpenDEI design principles)			
Technical building blocks			Governance building blocks
Interoperability	Data Sovereignty & Trust	Data Value Creation	Governance
Data models & formats	Access & usage Control / Policies & agreements	Descriptions of Data, Services and Offerings	Business Agreements
Data exchange protocols & APIs	Identity & credentials management	Metadata schemes. Publication & Discovery	Operational Agreements
Provenance & Traceability	Trust Services	Marketplace & usage accounting	Organizational Agreements

Data Sovereignty and trust building blocks should provide the technical means for guaranteeing that participants in a data space can trust each other and exercise sovereignty over the data they share. Requires common standards and services for:

- managing the identity of participants,
- verification of their truthfulness of claims,
- Specification and enforcement of policies agreed upon data access and usage control

Trust services constitute the **Trust Anchor Framework** that defines and enforces a set of rules for the data space that extend the ones specified by the Gaia-X Trust Framework. It addresses the following concerns:

- **ID Binding:** Verify a digital identifier against a valid legal identity
- **Proof of participation:** Verify an entitled ecosystem participant
- **Proof of Issuing Authority:** Verify that the credentials presented by a participant have been issued by a Trusted Issuer of that type of credentials in the correct ecosystem and for the right purpose and calculate trust level.

XFSC implementation by Gaia-X:

- W3C verifiable credentials
 - Verifiable Data Registry to store/query relevant information
- Gaia-X Registry deployed at Digital Clearing House (GXDCH) nodes
<https://gaia-x.eu/gxdch/>

Identity & credentials management ensures all actors (including organizations, individuals, services, etc.) are provided with acknowledged identities, and that those identities can be authenticated and verified, including additional information provisioning needed to enable access and usage control.

- **Catena-X** is building an implementation of this using a **Managed Identity Wallet** that complies with the following standards: VC, DID, DID Auth, DKMS
<https://catena-x.net/en/catena-x-introduce-implement/standardisierung>

- **EDC Identity Hub extension** follows a similar approach using in addition the DIF WDN pattern and protocol

https://github.com/eclipse-edc/Publications/blob/main/Identity%20Management/DID_EDC.md

Policies & agreements building block guarantees enforcement of data **access and usage policies** defined as part of the terms and conditions established when data resources or services are published, negotiated and used.

- Data access control used by provider to prevent misuse of resources
- Data usage control used to prevent misuse of data by consume.
- Both are combined by prosumers in data value chains.

Catena-X has issued guidance (Catena-X community standard) for authentication where the following are recommended:

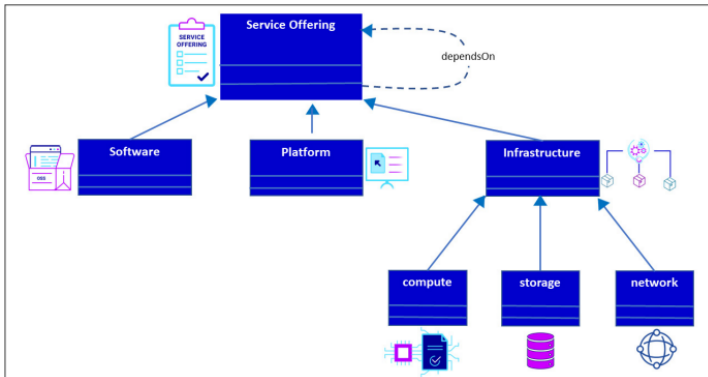
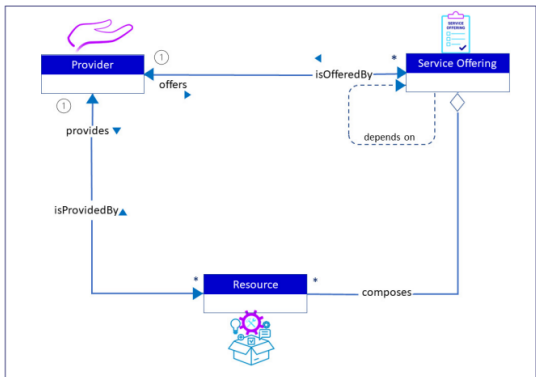
- Authentication: OIDC and KeyCloak (OAuth, OIDC, SAML)
 - Authorization: ABAC via XACMLv3
 - Data usage agreements: ODRL extension profile by IDSA
- Catena-X standard on IAM explicitly mentions all providers **should NOT** have static access management such as ACL or RBAC

<https://catena-x.net/en/catena-x-introduce-implement/standardisierung>

What is a dataspace? Main building blocks, challenges and design reference

Data space building blocks (source: DSBA Convergence paper & OpenDEI design principles)

Technical building blocks			Governance building blocks
Interoperability	Data Sovereignty & Trust	Data Value Creation	Governance
Data models & formats	Access & usage Control / Policies & agreements	Descriptions of Data, Services and Offerings	Business Agreements
Data exchange protocols & APIs	Identity & credentials management	Metadata schemes. Publication & Discovery	Operational Agreements
Provenance & Traceability	Trust Services	Marketplace & usage accounting	Organizational Agreements



Data Value Creation enables the following aspects of data life-cycle in a data space:

- Describe data, services and data products in an interoperable manner
- Data and service publication methods to discover offerings and connect providers and consumers
- Add value-adding services such as marketplaces for commercialization

Those steps are covered by the **DSBA technical convergence framework** and designed consistently in Gaia-X and IDS RAM (v4.0 onwards)

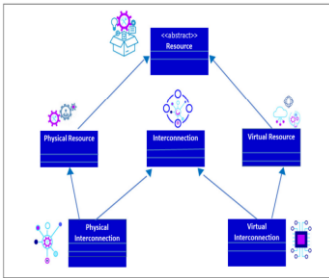
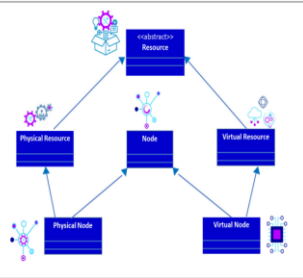
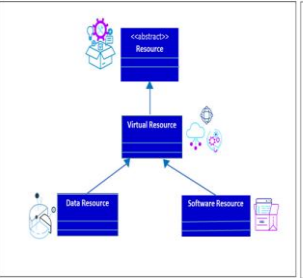
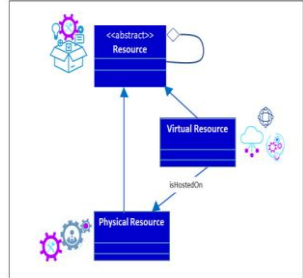
Market place & usage accounting services provide the basis for accounting access to and/or usage of data by users in order to support functions for clearing, payment, billing, etc.

The **Data Space Information Model** provides the schema for (Self-)Descriptions of data, services and offerings and their basic building blocks, like Usage Contracts, endpoint descriptions, or the internal structure of data assets.

Catalogs should be accessible via endpoints in the **Connector** exporting [TM Forum Open APIs](#) and using the (IDSA) [Dataspace Protocol Catalog](#) functionality implements [DCAT V3](#).

- **DCAT** is an RDF vocabulary designed to facilitate interoperability between data catalogs published on the Web. This document defines the schema and provides examples for its use.
- **Gaia-X (Self-)Descriptions** may be extended to also include elements of domain specific ontologies or generic key/values depending on the domain of the ecosystem

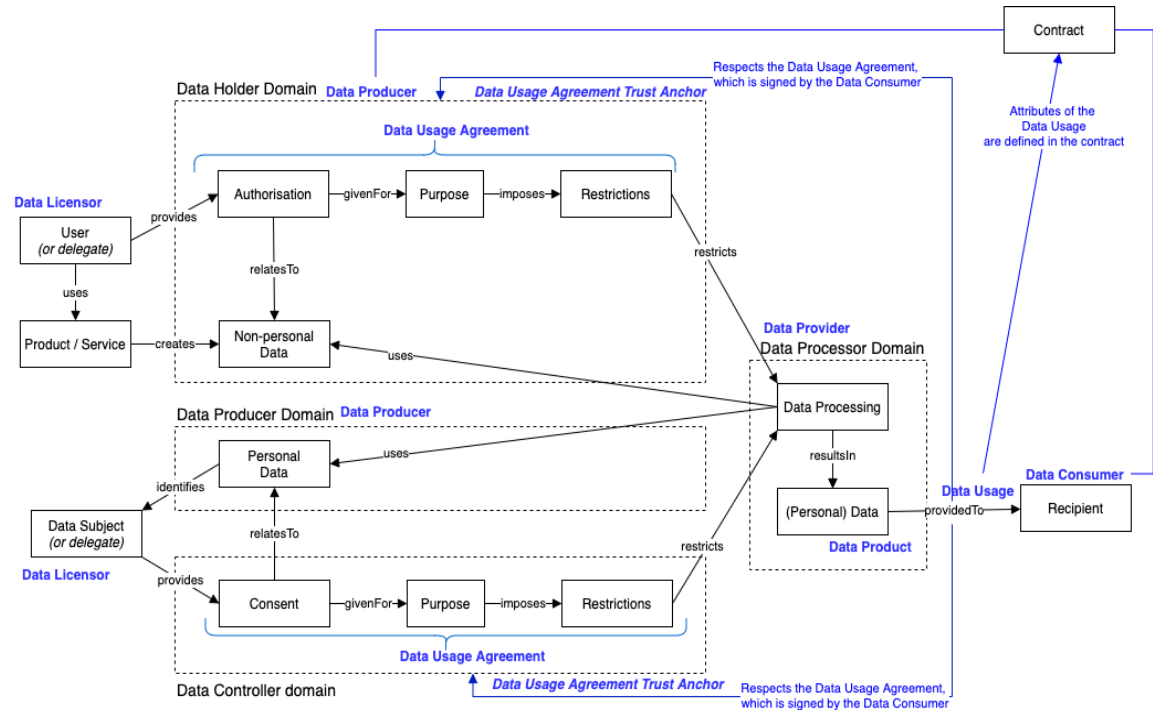
Catena-X has defined such elements for Catena-X compliant data spaces as Catena-X standard under [Catena-X standards library](#) as part of [Eclipse Automotive](#)



<https://www.w3.org/TR/vocab-dcat-3/>
<https://www.tmforum.org/oda/open-apis/>
<https://www.tmforum.org/oda/open-apis/table>
<https://docs.internationaldataspaces.org/ids-knowledgebase/v/dataspace-protocol/overview/readme>

What is a dataspace? Mapping EU regulation to data exchange architecture

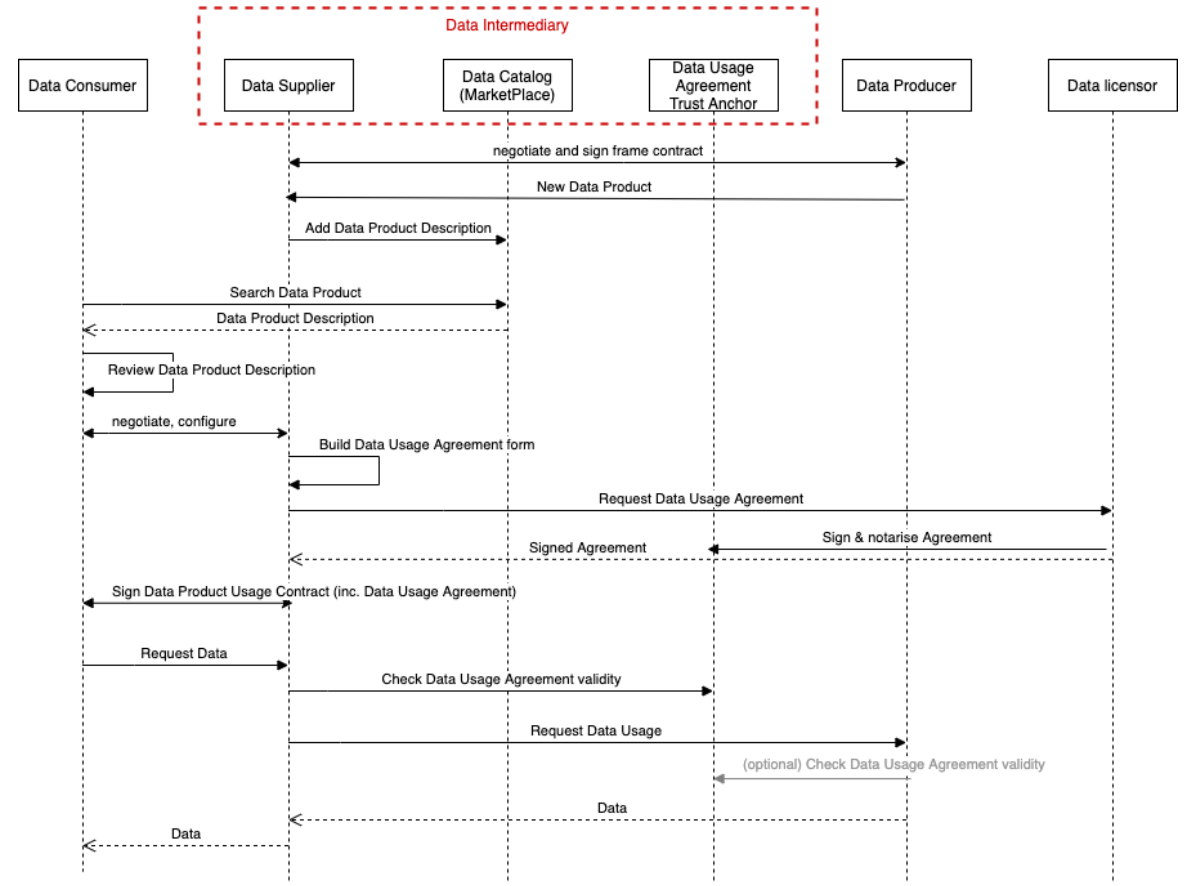
Mapping between the Gaia-X/DSBA concepts (in blue) and the concepts used in the EU regulation



Data intermediary services an important concept in EU acts around data:

"Data intermediation services may support users or third parties in establishing a commercial relation for any lawful purpose on the basis of data of products in scope of this Regulation e.g. by acting on behalf of a user" (cf. Regulation (EU) 2022/868).

Several Gaia-X lighthouse projects implement Data Intermediary with the following design pattern



WIP: Towards a Security Reference Architecture of Data Spaces

- Comprehensive architecture following the “4+1” model and initial focus on industrial / international data spaces
- Consistent with DSBA convergence paper (especially the unifying conceptual model)
- Builds on top of IDS-RAM4.0 by IDSA
- Consistent with Gaia-X architecture
- Consistent with NIST cloud federation
- Includes additional innovations from Huawei based on Hua-X.2.0 contributions

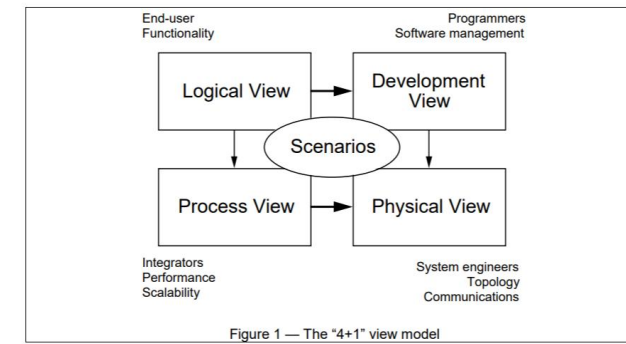
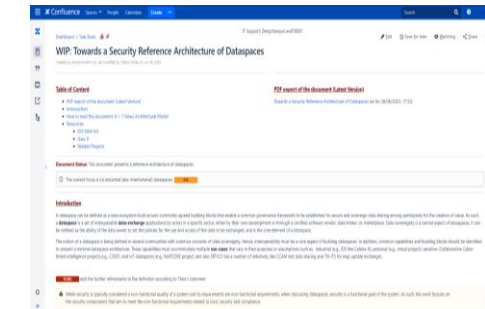
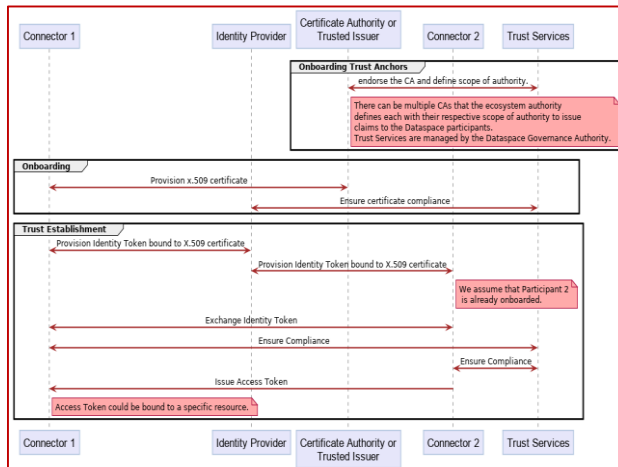
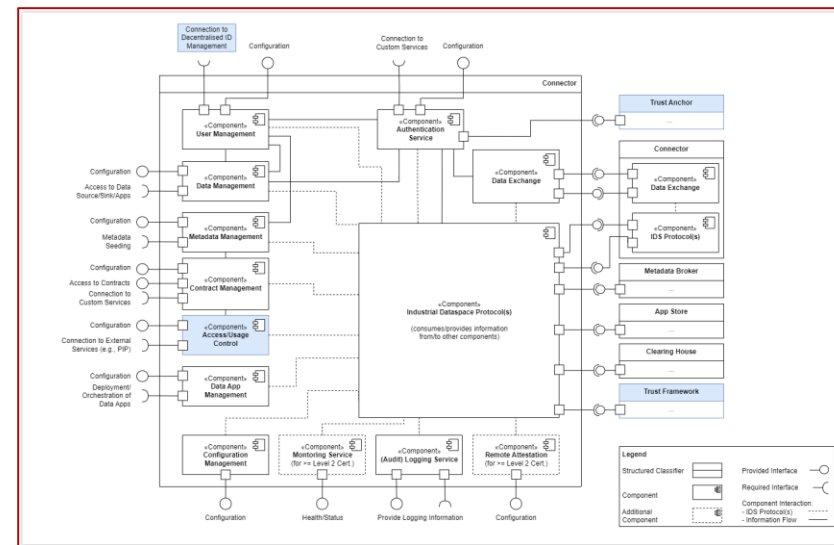
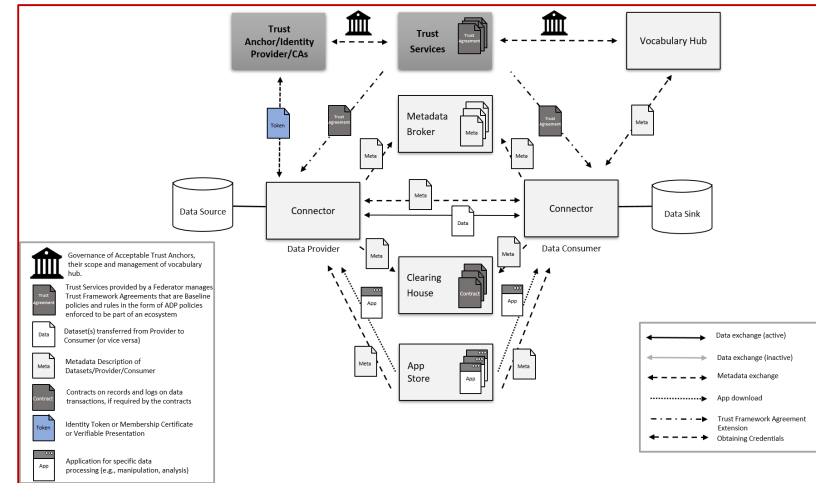
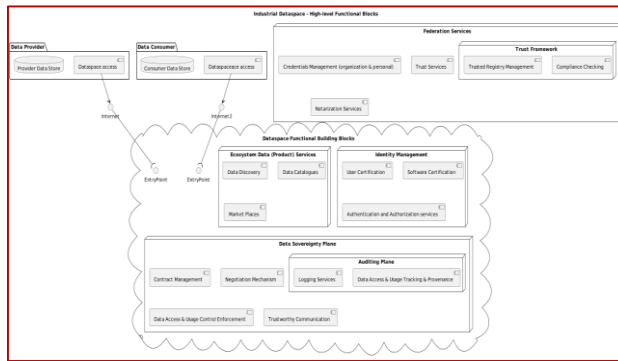
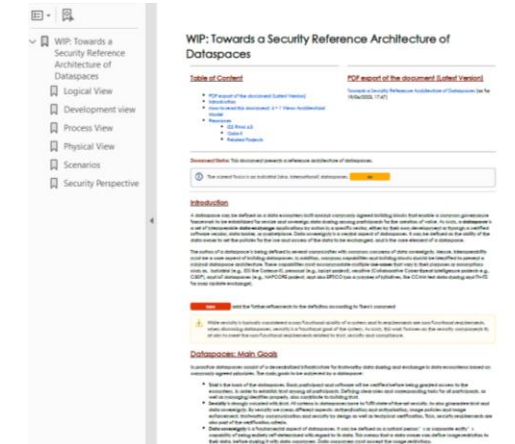


Figure 1 — The “4+1” view model



Continuously updated at a dedicated Confluence page



PDF copy regularly updated at One Box

Contents

Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)

A holistic execution approach is required across the entire ecosystem players:

There are several industry associations on play....

Towards a converging Data Space (Security) Architecture

Reference implementation: OSS on Eclipse foundation

- Eclipse becomes the common platform for data space development:
- Eclipse Dataspace Connector (next gen IDS),
- Eclipse XFSC (gaia-x Federation Services)
- Eclipse Tractus-X (Catena-X OSS baseline)

Standardization is going global

Competition is investing heavily

An overview of data space projects in Europe

Emerging architectural variants

Huawei contributions in Hua-X and Digital Sovereignty projects: technical

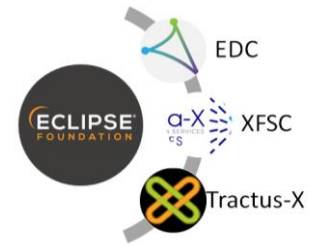
Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap

Recommendations

Appendix I: Core technologies

Appendix II: Data spaces examples

Three most important community implementations of data space components: EDC (connector), XFSC (federation), Tractus-X (ecosystem) – all under Eclipse Foundation



EDC – the new Gaia-X and IDS-RAM compliant connector under Eclipse Foundation

One main difference between the EDC and the previous connectors of the IDS is the separation of the communication into a channel for the metadata and one for the actual data exchange.

- The channel for the data supports various transmission protocols via so-called data plane extensions.
- The metadata is transmitted directly via the EDC interface, while the actual data exchange then takes place via the appropriate channel extension. In this way, a highly scalable data exchange is made possible.

Another key difference is that EDC is re-architected to have a small core and to facilitate modularity, extensibility and policy-based automation.

<https://eclipse-edc.github.io/eds/>

Eclipse DataSpace Components active member companies:

The Eclipse DataSpace Connector provides a framework for the International Data Spaces standard as well as relevant protocols associated with Gaia-X.

The connector is designed in an extensible way in order to support alternative protocols and integrate in various ecosystems:

- Extensible framework and architected to integrate other technological solutions in the following areas:
 - Data transfer wire protocols including data streams, IoT data sets
 - Identify providers including OAuth2 based implementations and DID based DID standards (DIDComm, DWN, etc)
 - Data storage, cataloging, telemetry systems
 - Host environments from on-premise installations to multiple cloud platforms

Guiding principles in developing the connector is simplicity, small core, few external dependencies.

EDC is a core component in the collaboration between TTT-OC, ICT, (Cloud BU) and Fraunhofer ISST under H2020.

EDC is the connector of choice for Catena-X who drive the roadmap for extensions.

EDC deployments for MS Azure and AWS are currently under development by MS and AWS.

EDC – the new Gaia-X and IDS-RAM compliant connector under Eclipse Foundation

Eclipse DataSpace Components active member companies:

Other reference use cases:

Manufacturing example: a manufacturer needs repair parts for one of its production robots. The manufacturer and the robot repair agency can use the DataSpace Connector technology to exchange the required information without disclosing sensitive data. In addition, the documents that are shared between the organizations can have usage conditions and policies attached to them.

ITS/Net-Safety Example: the DataSpace Connector technology enables trusted communications between the vehicle operator and the original equipment manufacturer.

Catena-X standard: CX-0028 ECLIPSE DATASPACE CONNECTOR (EDC): Architecture of EDC deployment

Eclipse XFSC Cross Federation Services Components

Gaia-X contribution of GXFS to Eclipse foundation

- Authentication/Authorization: OAuth2.0, ODBC, W3C VC, DID, DIDComm**
 - Description of Code: based on Java Spring Boot framework, Spring Authorization Server, OAuth implementation, ODBC to DID bridge
 - Community: T-Systems International, Verigo
 - Repository: <https://github.com/eclipse-edc/xfsc-authentication-authorization>
- Personal Credential Manager: W3C VC, DID, DIDComm, DID Auth**
 - Description of Code: Java, JAX-WS, REST, OAuth2.0, DID, DIDComm, DID Auth
 - Community: T-Systems International, Verigo
 - Repository: <https://github.com/eclipse-edc/xfsc-credential-manager>
- Organization Credential Manager: X.509, DID, DIDComm, DID Auth, W3C VC**
 - Description of Code: Java/JSP: federative approach, client framework, REST, AWS IAM Federation, Amazon
 - Community: T-Systems International, Verigo, Splunk
 - Repository: <https://github.com/eclipse-edc/xfsc-organization-credential-manager>
- Trust Services API: DNS, Hardware, DPK, LD Proof Chain/Sets, BBS+**
 - Description of Code: information, going, hardware, vdr, signing, verification, proof creation, Open policy engine, policy resolution
 - Community: T-Systems International, Verigo
 - Repository: <https://github.com/eclipse-edc/xfsc-trust-services-api>
- Authorization Service: W3C VC, DID, DIDComm**
 - Description of Code: Java, JAX-WS, REST, OAuth2.0, DID, DIDComm, DID Auth, W3C VC, DIDComm, DID Auth, W3C VC
 - Community: T-Systems International, Verigo, SAP
 - Repository: <https://github.com/eclipse-edc/xfsc-authorization-service>
- Data Contract Service: W3C ODR and UCON profile extensions**
 - Description of Code: The component is composed of a Java application. The application uses REST API endpoints to other components. The user interface is for Generation response to external applications. <https://github.com/eclipse-edc/xfsc-data-contract-service>
 - Community: GSA, BSH/Bosch
 - Repository: <https://github.com/eclipse-edc/xfsc-data-contract-service>
- Data Exchange Logging Service: W3C ODR, Data Usage Policies, W3C VC, W3C VC extensions**
 - Description of Code: The component is composed of a Java application. The application uses REST API endpoints to other components. The user interface is for Generation response to external applications. <https://github.com/eclipse-edc/xfsc-data-exchange-logging-service>
 - Community: GSA, BSH/Bosch
 - Repository: <https://github.com/eclipse-edc/xfsc-data-exchange-logging-service>

<https://projects.eclipse.org/projects/technology/xfsc>

Eclipse Tractus-X Catena-X contribution of Tractus-X to Eclipse

Part of Eclipse automotive <https://projects.eclipse.org/projects/automotive/tractus-x>

Tractus-X connects the three major parts of Catena-X ecosystem:

- Catena-X association:** responsible for standardization, certifications, and governance of the Catena-X ecosystem and managing the Tractus-X project
- Development environment:** Tractus-X repositories provide initial reference implementations of the core and enabling services
- Operating environment:** Tractus-X supports the use of reference implementation components by providers:
 - enabler service provider (e.g., marketplace),
 - enabler service provider (e.g., Eclipse DataSpace Connector), and
 - business application provider (e.g., traceability applications).

Tractus-X supports **Catena-X KITS** that provide software components, standards, installation scripts to support development in the area of Catena-X use cases.

The Business Partner Kit

- Provides high-quality data records of business partners called golden record including a unique identifier and the business partner number (BPN)
- Legal Entity Level (EPN L):** Search for a legal entity and get the high-quality data set.
- Site Level (EPN S):** Get the site (or sites) information of a legal entity.
- Address Level (EPN A):** Each legal entity and site has an address to find the company.

Digital Twin Kit

- Enables building a comprehensive landscape of distributed Digital Twins of assets (implies parts) along the entire lifecycle of the supply chain on top of the Traceability, DataChain and Connector KITS.

DataChain Kit

- enables to apply business logic along a distributed data chain, e.g. aggregation of certificates along the value chain, ad-hoc provisioning of continuous data chains across company boundaries, etc.

Connector Kit

- provides a connector framework, based on the **Eclipse DataSpace Connector** for sovereign, cross-organizational data exchange.
- Catena-X design principles for EDC utilization:
 - simple, maintaining a small and efficient core with as few external dependencies as possible
 - interoperable, independent of platforms and ecosystems
 - decentralized, software components with the necessary capabilities for participating in a data room are located on partners' side, data is only exchanged between the agreed points
 - data protection is more important than data sharing, data to be transmitted are fundamentally linked to policies via contracts, a transfer without a contract is not possible
 - separation of metadata and data enables high-throughput rates for the actual data transfer
 - consistent semantics for the data to be the basis for the consistency of digital twin creation
 - As far as possible, all processes are automated (from determining the identity through to ensuring the contractually agreed regulations to data transmission)
 - metadata and protocols from **ISO/IEC** and **ISO** are used as far as possible
 - where major differences between the EDC and the previous connectors of the **IDS** is high **scalability** achieved via the separation of the communication into a channel for the metadata and one channel for the actual data exchange.
 - The channel for the data supports various transmission protocols via so-called data plane extensions.
 - The metadata is transmitted directly via the EDC interface, while the actual data exchange then takes place via the appropriate channel extension.
 - Another major difference is the modular architecture with a small and efficient core combined with advanced functionality offered by connector extensions

Traceability Kit

- Aims to trace parts and materials across the entire value chain to enable data driven use cases over all tier levels without compromising data sovereignty
- Enables data and app providers to deliver solutions for building data chains and to send quality notifications.

<https://eclipse-tractusx.github.io/>



EDC – the new Gaia-X and IDS-RAM compliant connector under Eclipse Foundation

One main difference between the EDC and the previous connectors of the IDSA is the **separation of the communication into a channel for the metadata and one for the actual data exchange.**

- The channel for the data supports various transmission protocols via so-called data plane extensions.
- The metadata is transmitted directly via the EDC interface, while the actual data exchange then takes place via the appropriate channel extension.

In this way, a highly scalable data exchange is made possible.

Another key difference is that, EDC is re-architected to have a **small core** and to facilitate **modularity, extensibility and policy-based automation**

<https://eclipse-edc.github.io/docs/>

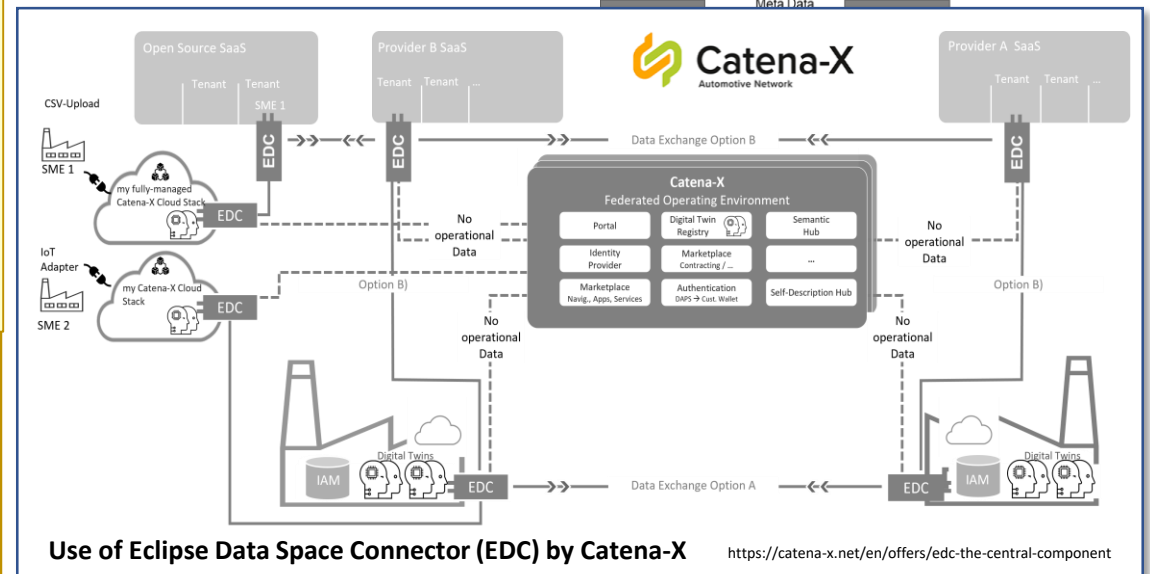
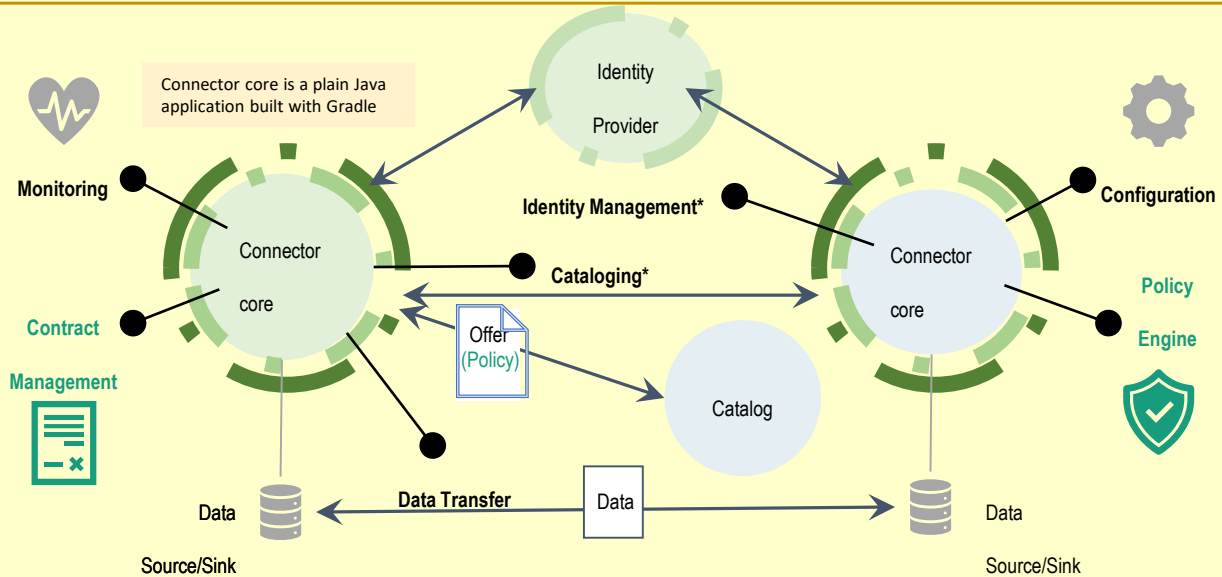
Eclipse Dataspace Components active member companies:

The Eclipse Dataspace Connector provides a framework for the International Data Spaces standard as well as relevant protocols associated with Gaia-X.

The connector is designed in an extensible way in order to support alternative protocols and integrate in various ecosystems

- Extensible framework and architected to integrate other technological solutions in the following areas
- Data transfer wire protocols including data streams, IoT data, large data sets
- Identity providers including OAuth2-based implementations and DID based DIF standards (DIDComm, DWN, etc)
- Data storage, cataloguing, taxonomy systems
- Host environments from on-premise installations to multiple cloud platforms

Guiding principles in developing the connector is simplicity, small core, few external dependences



Use of Eclipse Data Space Connector (EDC) by Catena-X <https://catena-x.net/en/offers/edc-the-central-component>

Roadmap of Dataspace Connector extended functions for Catena-X

Authentication (DAPS)	DAPS Connection DAT Validation	SSI – Gaia-X Self Description
Contract Offering	Via Web-Portal EDC-Dashboard	Interface to Contract Offer Module
Contract Negotiation	UI for EDC Contract Negotiation	(Automated Policy/Contract Handling)
Data Transfer	https, S3 File Transfer Push, REST	Extended Support of Data Transfer Techniques, like streaming, polling, events, Kafka, MQTT, ...
Agnostic Extensions	Basic Brokering/Registry Support	Extended Brokering/Registry Support
Use Case specific Extensions	Phasade APIs, Data Lake solutions	ERP, MES and PPS systems, Aspect Cache
	available	planned

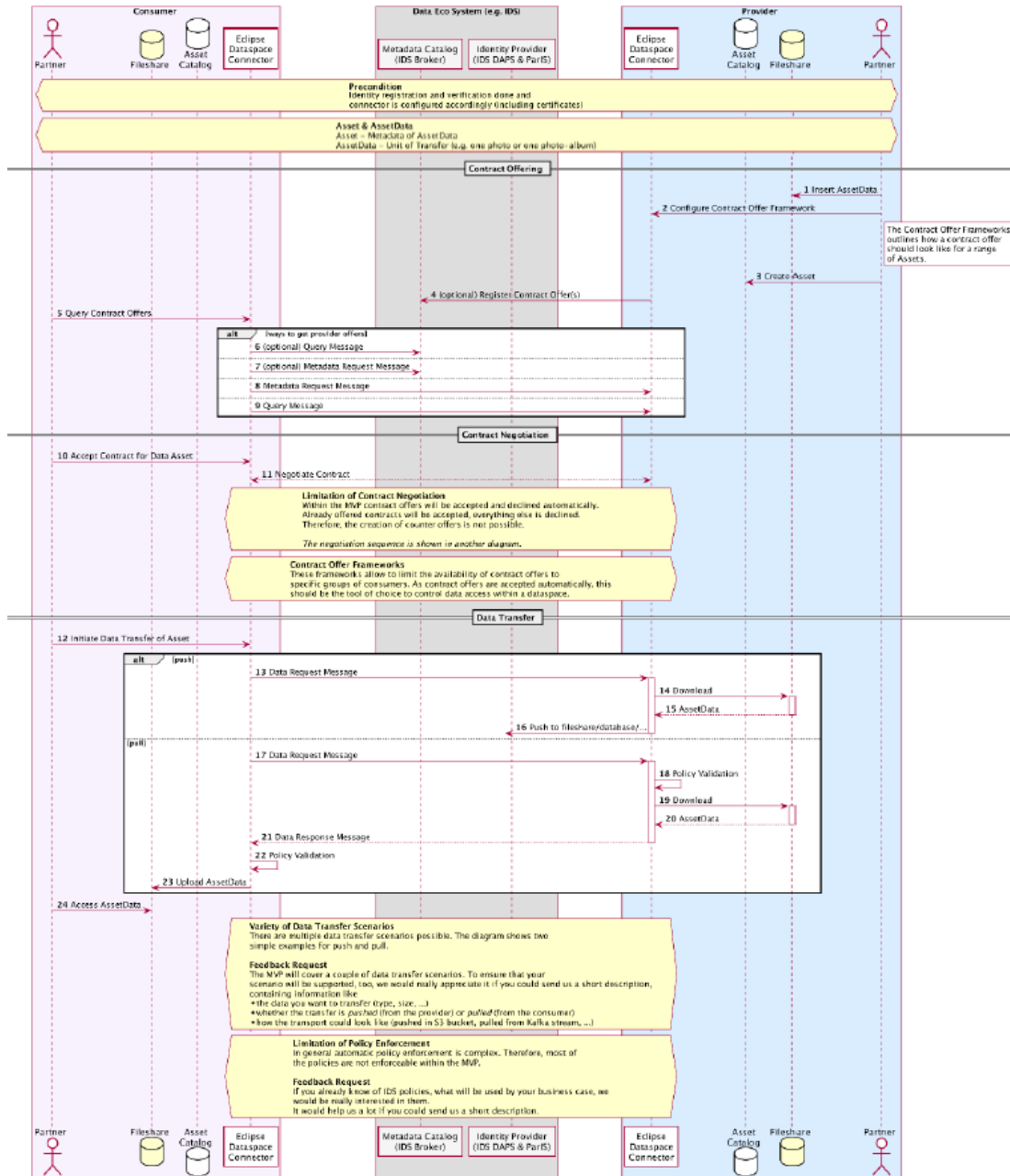
EDC is a core component in the collaboration between TTE-DE, ICTL (Cloud BU) and Fraunhofer ISST under Hua-X2.0

EDC is the connector of choice for Catena-X who drive the roadmap for extensions

EDC deployments for MS Azure and AWS are currently under development by MS and AWS



EDC – the new Gaia-X and IDS-RAM compliant connector under Eclipse Foundation

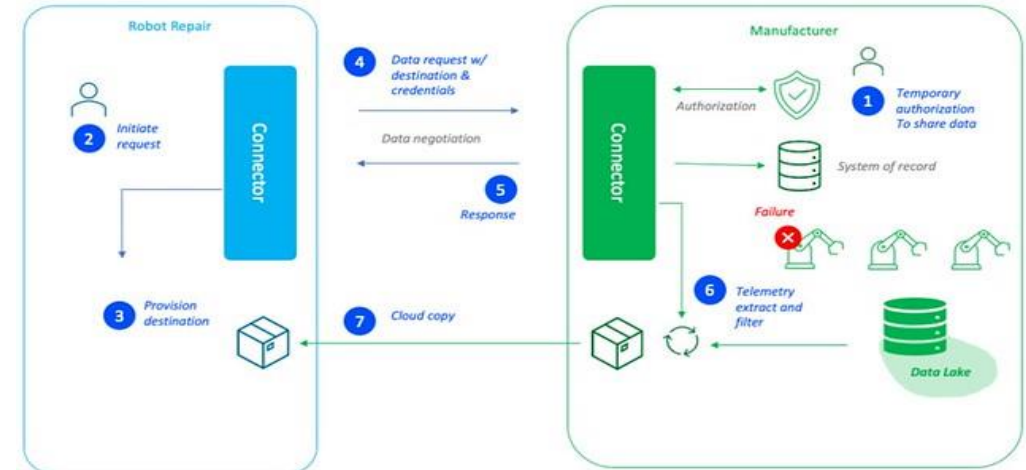


Eclipse Dataspace Components active member companies:

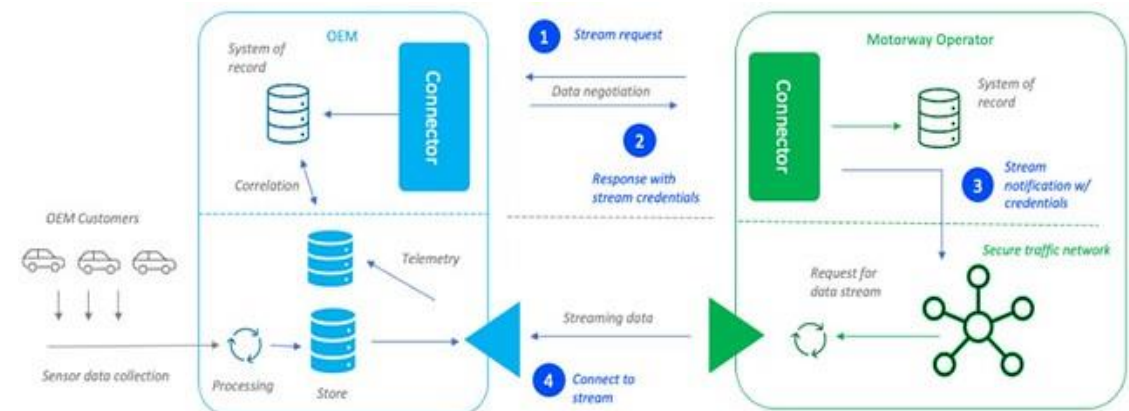


Other reference use cases:

Manufacturing example: a manufacturer needs repairs made to one of its production robots. The manufacturer and the robot repair agency can use the Dataspace Connector technology to exchange the relevant information without disclosing sensitive data. In addition, the documents that are shared between the organizations can have usage conditions and policies attached to them.



ITS/Rad-Safety Example: the Dataspace Connector technology enables trusted communications between the motorway operator and the original equipment manufacturer.





Eclipse XFSC

Cross Federation Services Components

Authentication/ Authorization: OAuth2.0, OIDC, W3C VC, DID, DIDComm

- Description of Code: based on Java Spring Boot framework, Spring Authorization Server, IDP Broker implementation, OIDC to SSI bridge
- Community: T-Systems International
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/authenticationauthorization>

Personal Credential Manager: W3C VC, DID, DKMS, DID Auth

- Description of Code: Base SSI wallet based on Javascript, react
- Community: T-Systems International, Vereign
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/pcm>

Organization Credential Manager: Aries, Indy, DKMS, DIF DWN, W3C VC

- Description of Code: Javascript, microservice approach, prisma framework, nats, Aries REST framework, Aries Indy framework, Anoncreds
- Community: T-Systems International, Vereign, Spherity
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/ocm>

Trust Services API: DSS, Hashicorp, OPA, LD Proof Chains/Sets, BBS+

- Description of Code: microservices, golang, hashicorp vault, singing, verification, proof creation, Open policy agent, policy execution
- Community: T-Systems International, Vereign
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/tsa>

Notarization Service: W3C VC, DSS, eIDAS

- Description of Code: Acapy, Java, JavaScript, Node.js, Quarkus, Indy Network, Compliance, W3C credential, Anoncreds, RabbitMQ, DSS (Digital Signing Service), eIDAS bridge
- Community: T-Systems International, Spherity, ecsec
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/not>

Data Contract Service: W3C ODRL and UCON profile extensions

- Description of Code: The component is composed of a Node.js application. The application uses REST API endpoints to other components. The User Interface for Self-Description registration is developed in JavaScript, using React.js.
- Community: IDSA, BigchainDB
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/dct>

Data Exchange Logging Service: W3C ODRL (Data Usage Policies) W3C LD notifications

- Description of Code: The component is composed of a LDN inbox server implemented on top of a Node.js server and a PostgreSQL database. The Administrative GUI uses the React framework.
- Community: IDSA, BigchainDB
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/del>

<https://projects.eclipse.org/projects/technology.xfsc>

Gaia-X contribution of GXFS to Eclipse foundation

Federated Catalogue

- Description of Code: developed with Java, Spring Boot framework, Spring Security, Tomcat, Keycloak, PostgreSQL, Neo4J, Apache Jena, RDF/JSONLD processing tools. Mainly accessible through REST API; simple partial HTML frontend for demonstration and testing.
- Community: Fraunhofer FIT, T-Systems International
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/cat>

Self-Description Tooling

- Description of Code: Angular JS, Java, Python
- Community: Fraunhofer (FIT, IOSB, IAIS), Cloud&Heat
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/self-description-tooling>

Workflow Engine

- Description of Code: developed using JavaScript and built on the Node.js runtime, low-code workflow engine. Fork of the popular node-red project with added features, microservice architecture, enhanced user interface, GUI generator with JSON data
- Community: original node-red contributors, LEANEA GmbH (former Sys4it)
- Repository: https://gitlab.com/gaia-x/data-infrastructure-federation-services/GXFS_OAW

Continuous Automated Monitoring

- Description of Code: The CAM consists out of Go-based microservices with a gRPC-based communication suite between them. Its core functionality is based on the OpenSource compliance checking tool Cloudfitor (<https://github.com/clouditor/clouditor>) and is released as Apache 2.0.
- Community: Fraunhofer AISEC
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/cam>

Portal

- Description of Code: React.js is used on Frontend, Java and Spring Boot framework are in the Microservices composing Backend
- Community: T-Systems International
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/por>

Orchestration

- Description of Code: Python, Go, OASIS TOSCA, Terraform, Flask, Kubernetes, Docker, Traefik, Postgresql, SQLAlchemy, OpenAPI, Swagger UI, Connexion, Tornado, xOpera, FastAPI, Gevent
- Community: XLAB
- Repository: <https://gitlab.com/gaia-x/data-infrastructure-federation-services/orc>

Further functionalities in a second specification phase focusing on the area of "Identity & Trust":

- W3C OCM
- AIP 2.0
- OpenID4VC
- Schema Registry
- W3C compatibility
- Cloud PCM
- TRAIN-Extension
- Consent Manager
- Self-Description Extension for Attestation
- References
- EBSI

Community:

Bundesdruckerei/ Health-X
TrueOcean/ Marispace-X
RIP Software SE/ iEco
Software AG/ AMS
carTRUST
Fraunhofer
Stackable
WOBCOM
Embeteco
Datarella/ MoveID
Airbus Defence and Space /
Cooperants project

EuroDaT project
IONOS/ Health-X project
Fraunhofer
Cappemini/ MERLOT
VTT
BMW/ Catena-X
IDSA
Gaia-X Hub Austria
K-BusinessCom AG
Delta DAO
OSB Alliance / SCS Project
Gaia-X Hub Germany
Wobcom
EDC project

Part of Eclipse automotive  <https://projects.eclipse.org/projects/automotive.tractusx>

Tractus-X connects the three major parts of Catena-X ecosystem:

- **Catena-X association:** responsible for standardization, certifications, and governance of the Catena-X ecosystem and managing the Tractus-X project
- **Development environment:** Tractus-X repositories provide initial reference implementations of the core and enabling services
- **Operating environment:** Tractus-X supports the use of reference implementation components by providers:
 - core service provider (e.g., marketplace),
 - enablement service provider (e.g., Eclipse Dataspace Connector), and
 - business application provider (e.g., traceability applications).

Tractus-X supports **Catena-X KITS** that provide software components, standards, installation scripts to support development in the area of Catena-X use cases

The BusinessPartner Kit

- Provides high-quality data records of business partners called golden record including a unique identifier and the business partner number (BPN)
- **Legal Entity Level (BPN L):** Search for a legal entity and get the high-quality data set.
- **Site Level (BPN S):** Get the site (or sites) information of a legal entity.
- **Address Level (BPN A):** Each legal entity and site has an address to find the company

Digital Twin KIT:

- Enables building a comprehensive landscape of distributed Digital Twins of assets (mostly parts) along the entire lifecycle of the supply chain on top of the Traceability, DataChain and Connector KITS.

DataChain Kit

- enables to apply business logic along a distributed data chains, e.g. aggregation of certificates along the value chain, ad-hoc provisioning of continuous data chains across company boundaries, etc.

Connector Kit

- provides a **connector framework**, based on the [Eclipse Dataspace Connector](#) for sovereign, cross-enterprise data exchange.
- **Catena-X design principles** for EDC utilization:
 - **Simple**, maintaining a small and efficient core with as few external dependencies as possible
 - **Interoperable**, independent of platforms and ecosystems
 - **Decentralized**, software components with the necessary capabilities for participating in a data room are located on partners' side, data is only exchanged between the agreed points.
 - **Data protection** is more important than data sharing, data to be transmitted are fundamentally linked to policies via contracts; a transfer without a contract is not possible.
 - **Separation of metadata and data** enables high throughput rates for the actual data transfer.
 - **Consistent semantics** for the data is the basis for the consistency of digital value creation.
 - As far as possible, all **processes are automated** (from determining the identity through to ensuring the contractually agreed regulations to data transmission)
 - **Standards and protocols** from [GAIA-X](#) and [IDSA](#) are used as far as possible.
- One major difference between the EDC and the previous connectors of the [IDSA](#) is **high scalability** achieved via the separation of the communication into a channel for the metadata and one channel for the actual data exchange.
 - The channel for the data **supports various transmission protocols** via so-called data plane extensions.
 - The **metadata is transmitted directly via the EDC interface**, while the actual data exchange then takes place via the appropriate channel extension.
- Another major difference is the **modular architecture** with a **small and efficient core** combined with advanced functionality offered by connector extensions

Traceability KIT

- Aims to trace parts and materials across the entire value chain to enable data driven use cases over all n-tier levels without compromising data sovereignty.
- Enables data and app providers to deliver solutions for building data chains and to send quality notifications.

Contents

Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)

A holistic execution approach is required across the entire ecosystem players:

There are several industry associations on play....

Towards a converging Data Space (Security) Architecture

Reference implementation: OSS on Eclipse foundation

Standardization is going global

- ISO S38: Cloud computing and distributed platforms – Dataspaces (Microsoft driven)
- CEN CWA Trusted Data Transaction (TNO-NL, FhG ISST-DE, Dawex-FR driven)
- Standards baseline

Competition is investing heavily

An overview of data space projects in Europe

Emerging architectural variants

Huawei contributions in Hua-X and Digital Sovereignty projects: technical

Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap

Recommendations

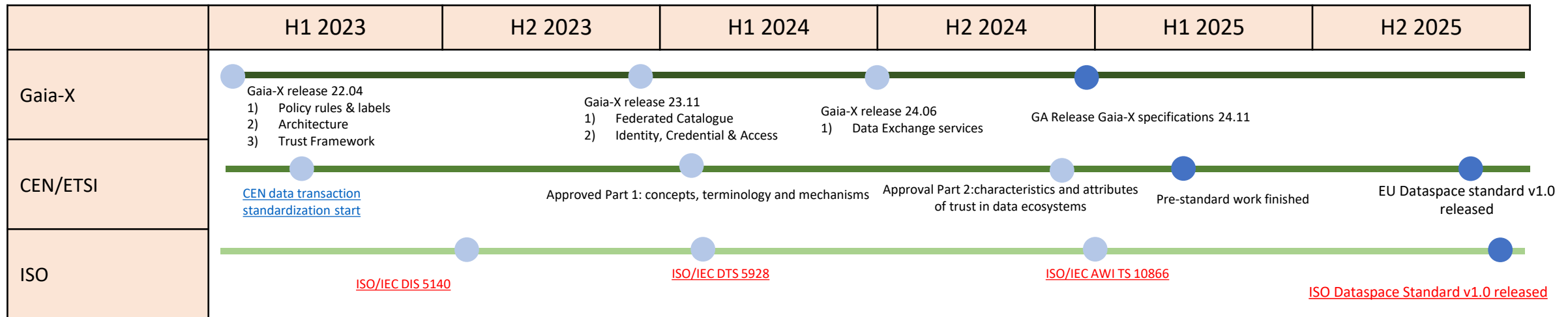
Appendix I: Core technologies

Data Spaces Standardization goes Global (ISO / CEN)

- 1) Microsoft is driving the topic in ISO in cooperation with European Commission and related organizations (DSBA, DSSC, Catena-X, ...)
- 2) Fraunhofer ISST, TNO & DAWEX are driving this as European standard in CEN (<https://www.trusted-data-transaction.org/en/>)



- 1) Huawei must monitor and actively participate in the emerging international, normative standardization process to secure technology leadership.
- 2) Cross domain coherent alignment of experts from standardization, technology and product owners is needed.
- 3) Cross-boarder alignment of China, ISO and CEN standards are needed.



Build a standardized data infrastructure modeled in Europe to facilitate data flow and value creation (main standards and community initiatives of the emerging data infrastructure stack)

INTERNATIONAL DATA SPACES ASSOCIATION

Referenced in IDS-RAM and Dataspace Protocol



- Protocol baseline [ISO OSI model \(ISO/IEC 7498-1:1994\)](#)
- W3C. [JSON-LD 1.1](#): Linked Data
- W3C [DCAT](#) v3 for Data Catalog
- XACML v3 for access control <https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html>
- ODRL Open Digital Rights Language <https://www.w3.org/TR/odrl-model/>, relevant profiles:
 - [Big Data Profile](#): Data Usage Control (DUC)
 - [ODRL Profile for Expressing Consent](#) (Granular Access Control Policies in Solid)
 - Data Privacy Vocabulary (DPV) <https://w3c.github.io/dpv/dpv/>
- [DIN SPEC 27070](#) reference architecture of a trustworthy gateway for the exchange of industry data and services.
- W3C. (2015). [Semantic Web](#): RDF, SHACL, OWL, SKOS

In [Rules and labels document](#):

Art. 40 GDPR (currently CISPE, EU Cloud CoC), certifications acc. Art. 42 GDPR, C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA, SWIPO IaaS, SaaS and merged code CoC

In architecture

- W3C. [JSON-LD 1.1](#): Linked Data
- W3C. [ODRL](#) Information Model 2.2
- W3C [Verifiable Credentials Data Model](#) 1.0.
- W3C. [Semantic Web](#).
- W3C. Decentralized Identifiers ([DIDs](#)) v1.0.
- W3C [DCAT](#) v3 for Data Catalog

In EDC and XFSC: [OIDC](#), [DKMS](#) / [KERI](#), [DIF DID Auth.](#), [DIF DWN](#), [LD Proof Chains/Sets](#), [BBS+](#)

Catena-X
Vision & Ziele | Mehrwerte | Angebote & Standards | Catena-X einführen & umsetzen | Aktuelles & Termine | Über uns

<https://catena-x.net/de/standard-library>

The Catena-X Standard Library

Our Standard Library lists all our published standards. They are categorized in the official roles of the Catena-X Operating Environment (determining where you come from) and use cases (determining the field you focus on). Use the filter to display the standards that are relevant for your certification in Catena-X. Below you will find details on the categories.

Roles

The Catena-X operating environment is based on the idea that there are multiple but distinct roles that aim at providing an attractive and fully functional ecosystem. Each provider can take on one or more of the following roles in any combination:

(1) Core Service Provider, (2) Enablement Service Provider, (3) Business Application Provider, (4) On-Boarding Service Provider, (5) Consulting Provider, (6) Data Provider and Consumer, and (7) Conformity Assessment Body.

Catena-X Standards defined so far for the following five roles

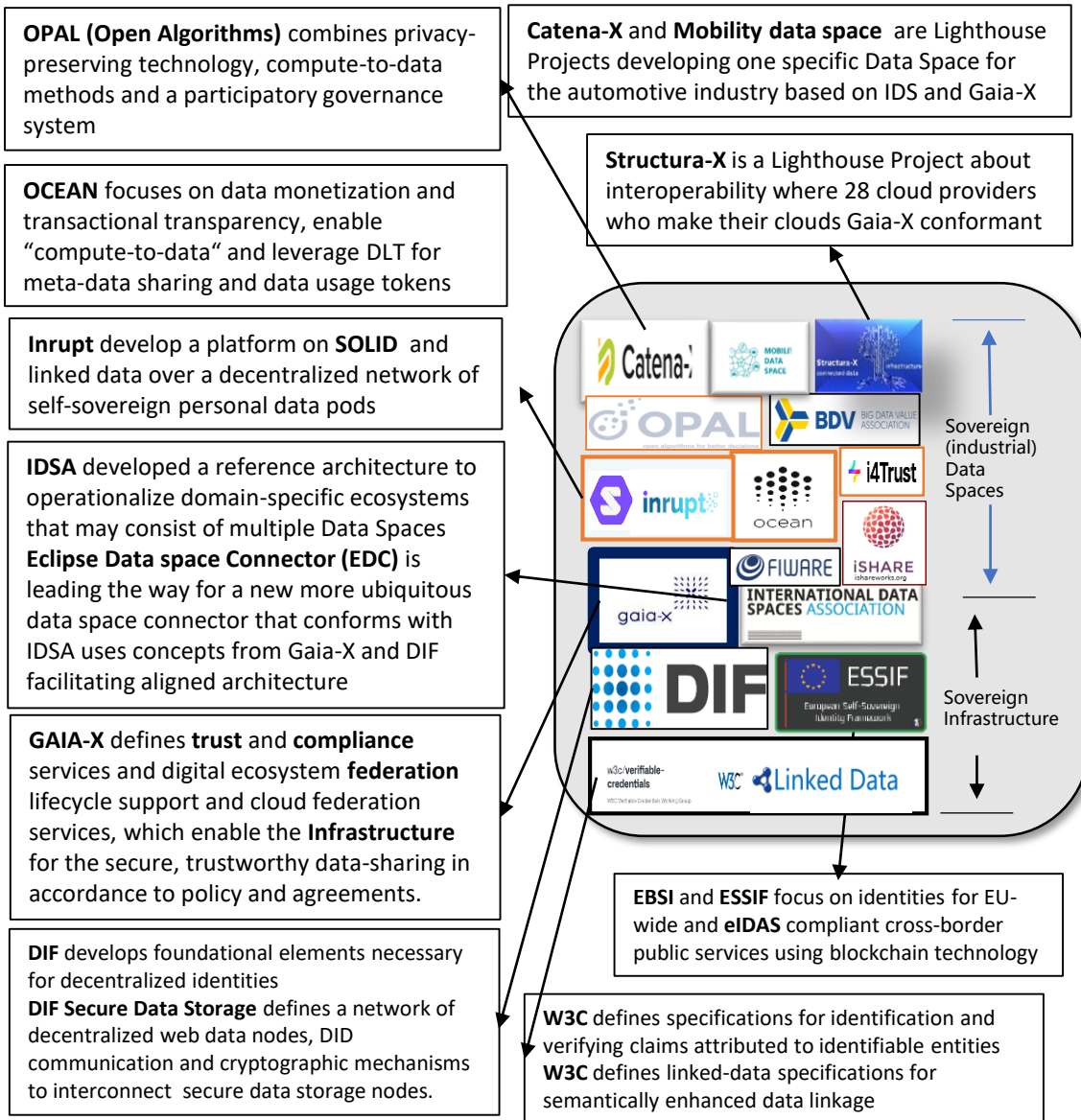
- Data provider & consumer
- Core service provider
- Enablement service provider
- Business App provider
- On-boarding service provider

Standards not defined by Catena-X so far for the following two roles

- Consulting provider
 - Conformity Assessment Board
- But..

Catena-X confirmed intend to conform with Gaia-X (Trust) Framework and Gaia-X Digital Clearing House (GXDCH)

Community Initiatives



Contents

Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)

A holistic execution approach is required across the entire ecosystem players:

There are several industry associations on play....

Towards a converging Data Space (Security) Architecture

Reference implementation: OSS on Eclipse foundation

Standardization is going global

Competition is investing heavily

An overview of data space projects in Europe

Emerging architectural variants

Huawei contributions in Hua-X and Digital Sovereignty projects: technical

Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap

Recommendations

Appendix I: Core technologies

Appendix II: Data spaces examples

EU Dataspaces Market Overview

Manufacturing-X announced at Hannover fair.
5 times bigger than Catena-X [[Link 1](#), [Link 2](#)]

KEY MESSAGES

Catena-X member & Confinity operations

- The rules of the data economy are being rewritten in Europe with general and sector specific data legislation, trust infrastructure and standards
- Hyperscaler “gatekeepers” are not favored
- **Common data spaces are central to EU data strategy for a single market, through which organizations and industries shall co-operate in Europe.**
- **Huawei must develop an Dataspace offering to participate in this future regulated EU digital Economy**

Examples of government supported Dataspaces

- EU & National bodies are funding formation of vertical dataspaces in different verticals. There are over 30 dataspaces announced

Mobility Data Space

Sponsored by the German Government with over **200 stakeholders** including BMW, VW, Mercedes, Caruso, DB, HERE

Sharing sensitive data such as **floating car data and mobile network movement** without the fear of data exploitation.

Being redesigned according to an **IDSA GAIA-X Architecture**

Catena-x

is data space community formed by the **Germany automotive industry**

Most advanced data space project in Europe at present with **€220 million** in funding

Founding partners of the consortium include **BMW, VM, Mercedes, DT, Bosch, MSFT, SAP, Siemens.**

Membership will increase to 1000 members as the network scales up

CN Taskforce active

Structura-X

European cloud providers have launched Structura-X, fully meeting Gaia-X requirements. 28 companies and organizations have agreed to make their cloud services Gaia-X compliant.

Atos, Aruba.it, DE-CIX, DT, IONOS, KPN and Vivacom are main founding partners

Examples of enterprises investing in Dataspaces

TMFORUM Telco Dataspace

New TMF initiative to build a trusted ecosystem for data in the telecoms sector for collaborative use cases.

Aims to enable Telcos and their partners to execute **collaborative use cases while reducing integration costs**

Allows members to **retain sovereign control** of their data and stay in **compliance with industry and government regulation**

Airbus SKYWISE

A company-led private data ecosystem running for a number of years that encourages data sharing **between Airbus and its supplier and customers**

By **combining in-flight, engineering and operational data from 10,000 aircraft and airlines** in an analytic rich environment

Skywise provides a **purpose-built industry data platform** to address Aircraft Operations

Confinity -X


T-Systems, BASF, BMW Group, Henkel, Mercedes-Benz, SAP, Schaeffler, Siemens, Volkswagen and ZF formed **the joint venture Cofinity-X, for the operations of Catena-X applications in the automotive value chain.**

Sovereign Cloud developed in cooperation with Google and DT will be used as platform


Dataspace Operator

Data Market € Billions	2025	2030 Baseline
EU27	90	105
EEA	8.4	10
Total	98.4	125

Data Governance Strategy of Competitors (in EU)



Partnering with the heavy-weight champions and expanding to their supply chains to build data-ecosystems, e.g. DPP with VW. Member of EDC



AWS became day-2 member and stays **silent in Gaia-X** in public events and working groups but contributes to **EDC** (Eclipse Data Space components) focusing on EDC extensions for integration of with the **AWS stack**.

Leveraging no 1 market position




Hosting Catena-X through Confinity-X

Developing **co-offering with EU market sector champions**, e.g. Thales for “Defense cloud” in FR and Telekom for “Sovereign cloud” in DE.



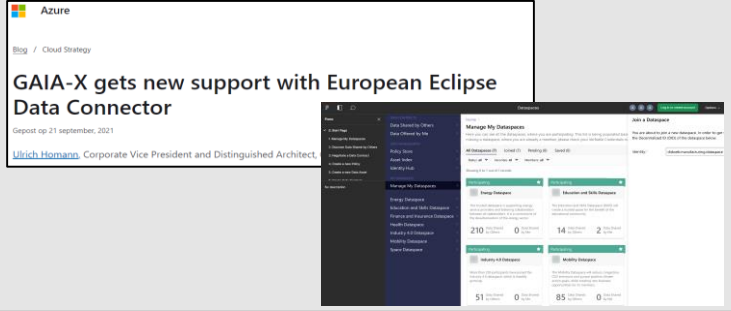

Google joint as **day-2 member of Gaia-X**. Since then, GCP supports Gaia-X in different public events and participates in many working groups in “listener” mode. GCP focus on strategic alliances and contributions to **Catena-X, EDC**, etc., through partnership with EU companies such as **T-Systems** and **Thales**

Similar to Huawei’s OTC model





Driving Dataspace standardization in ISO

Azure has a **Gaia-X / OSS contribution** strategy, to build a compliant service offering with **first-mover ambition**



Microsoft as day-1 member of Gaia-X and **contributes significantly** (mainly Architecture, Federation & ICAM). Big contributor in **EDC** (Eclipse Dataspace Components) focusing on **EDC Identity Hub** and conformance to **DIF, IETF, W3C** for identity & linked data


Similar to Huawei strategy


EU cloud providers are day-1 members of Gaia-X and Dataspace initiatives with substantial financial support from EU programs.




New European join ventures and startups are initiated to provide Dataspace operation services in different vertical domains.



Intel has a limited contribution focused around bringing SGX technology into the deployment options of **EDC**



Alibaba is on of the 20+ companies in China who have shown interest in IDSA China Hub and were informed about the MVD demo of EDC

Contents

Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)

A holistic execution approach is required across the entire ecosystem players:

There are several industry associations on play...

Towards a converging Data Space (Security) Architecture

Reference implementation: OSS on Eclipse foundation

Standardization is going global

Competition is investing heavily

An overview of data space projects in Europe

- IDSA data space radar - focus on industrial data spaces
- My Data Global – focus on personal data spaces
- Emerging data space models in smart city and IoT (ITS/CCAM)

Emerging architectural variants

Huawei contributions in Hua-X and Digital Sovereignty projects: technical

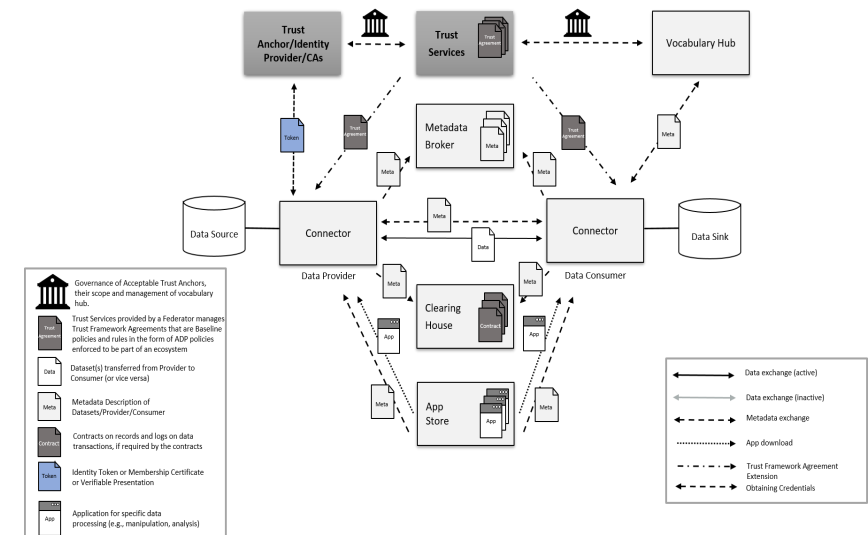
Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap

Recommendations

Appendix I: Core technologies

Established data space trend 1: Industry & International Data Spaces

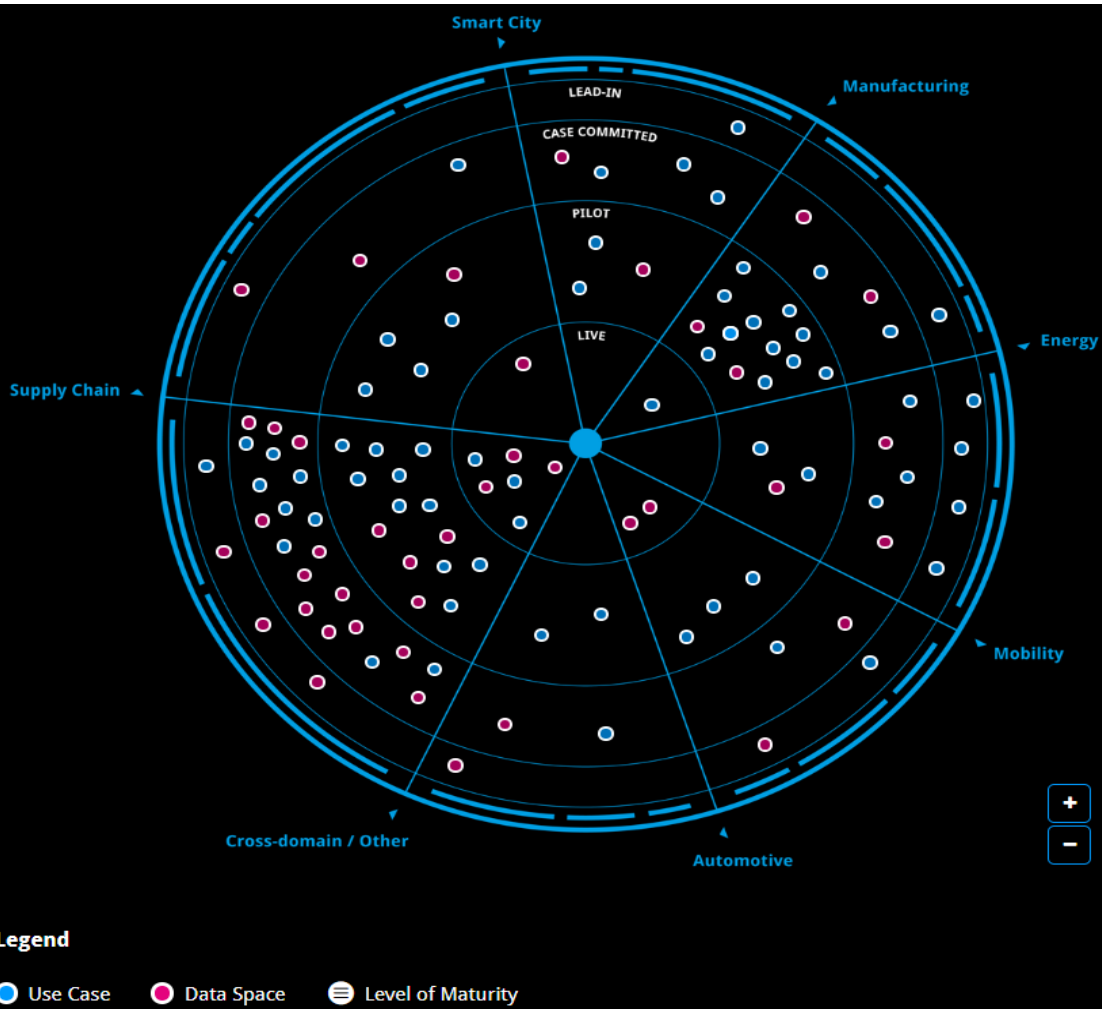
- **Industrial / international data spaces are designed for scalable enterprise data exchange and collaboration among businesses and organizations.**
- They must handle a wide variety of structured and unstructured data, often at high volume and velocity.
- They provide robust data ingestion, processing, management and usage control mechanism of the data based on commonly agreed policy.
- **Industrial Data Spaces** are build to facilitate data exchange and collaboration at an industrial or organizational level. In these environments, data from various sources, including IoT devices, operational data, business data, etc., is pooled and made accessible to participating entities under specific conditions.
- The governance model in industrial dataspaces ensures a secure, controlled and equitable sharing of data, respecting data privacy laws, facilitating collaboration and value creation.
- Gaia-X Framework offers a reference architecture for the **trust model** underpinning the digital ecosystem federations upon which industrial data spaces are established and operate.
- The **typical data exchange pattern** for industrial / international data space is that of an IDS connector architecture and the **IDSA Data Space Protocol**
- The emerging reference architecture of **data exchange in** such data spaces is based on a convergence of the **IDS-RAM** and the **Gaia-X Architecture** on a **baseline defined by the DBSA convergence** activity
- Most of the current **European lighthouse projects** follow this model with **Catena-X**, and the German **Mobility Data Space (MDS)** and (more recently) **Manufacturing-X** being the most widely recognized initiatives in this domain
- The **EDC data space connector** is become the de-facto industry standard reference implementation of a connector for an industrial data space replacing previous implementations of IDS connectors that were monolithic, synchronous and hard to scale.
- **EDC** and **XFSC** (OSS GXFS) constitute the key elements of an OSS for this type of dataspaces with **Tractus-X** being a first domain specific ecosystem OSS of this model focusing on automotive data spaces.
- All elements of the OSS reference implementation stack for this model are under the auspices of **Eclipse Foundation**
- TTE-DE has been producing a reference architecture detailing this convergence and how certain technologies for decentralized identity federation and data usage control fit on such architecture.
- Hua-X.2.0 project between TTE-DE, ICTL (Cloud BU) in cooperation with Fraunhofer ISST is building a reference implementation for offering (access to) such a data space as a service







Roadmap of Dataspace Connector extended functions for Catena-X

Authentication (DAPS)	DAPS Connection DAT Validation	SSI – Gaia-X Self Description
Contract Offering	Via Web-Portal EDC-Dashboard	Interface to Contract Offer Module
Contract Negotiation	UI for EDC Contract Negotiation	(Automated Policy/Contract Handling)
Data Transfer	https, S3 File Transfer Push, REST	Extended Support of Data Transfer Techniques, like streaming, polling, events, Kafka, MQTT, ...
Agnostic Extensions	Basic Brokering/Registry Support	Extended Brokering/Registry Support
Use Case specific Extensions	Phasade APIs, Data Lake solutions	ERP, MES and PPS systems, AspectCache
	available	planned

Landscape of Data Space initiatives: “data space radar” - focus on industrial data spaces



Class	Name	Purpose	Key partners	Maturity	Baseline
Manufacturing	Manufacturing-X [Link 1] [Link 2]	Manufacturing-X will create a decentralized and collaborative data space (ecosystem) for Industry 4.0 (I.4.0) in order to realize an intelligently networked industry . <ul style="list-style-type: none"> • Turnkey use of value-added services in diverse production environments. • Combine production infrastructure & cloud • Enable fast composition of I.4.0 services to reduce integration time & cost-to-market 	BMWK (German Gov.) invests €152 million for R&D pilots to implement cross-industry use cases of Industry.4.0 data space. <ul style="list-style-type: none"> • To be designed and developed in close collaboration with GAIA-X & GAIA-X hubs. • Announced April 2023 	Lead-In Data space ecosystem (recent and in yet in IDSA data space radar)	Gaia-X Framework Eclipse XFSC
	Boost 4.0  https://boost40.eu/	Foundations of a sovereign manufacturing oriented European Industrial Data Space (EIDS) including. Set up 11 lighthouse factory trials. OSS implementation of data connectors, certification process, and aligns data space data models with EIDS-RAMI 4.0 the European reference architecture model for Industry 4.0	Boost 4.0 was the Biggest EU initiative in Big Data for Industry 4.0, with a 20M€ and 53 partners including IDSA , VW, Volvo, Siemens , Telefonica, i2CAT, FIWARE , ERCIM , IBM Israel among others	Data space ecosystem Pilot (likely to be superseded by Manufacturing-X)	IDS Identity Provider (CA, DAPS) IDS App Store IDS Connectors
	ManuSpace [LINK]	Optimize process, reduce cost and time it takes to get these life-saving medicines to people that need them.	Irish Manufacturing Research ServBlock NEXA EAM Ingeniero Solutions Unison Process Solutions ISHARE FIWARE	Data Space Case Committed	i4Trust components iShare delegation (OAuth/XACML)
Green Data Hub	Green Data Hub – DIO: Data Space Energy Transition  https://www.greendatahub.at/7lang/en	Manage supply chain in the energy sector, form energy communities and optimized energy supply and demand / power grid stabilization. Offer new data services and products for renewable energies such as: <ul style="list-style-type: none"> • Better plan energy production with multi-factor data from many sources & locations • Intelligent energy distribution & storage and on demand utilization in energy communities • AI forecasting and optimization models – e.g. for dynamic charging management of e-cars 	Data Intelligence Initiative (DIO) , KELAG, Siemens, E&Y, AWS , Microsoft , HPE among others	Data Space Case Committed	EDC (Eclipse Dataspace Components) Nexyo as the hub for testing
Mobility	Mobility Data Space (MDS)  https://mobility-dataspace.eu/	MDS . enables the sovereign handling of data for digital mobility solutions. <ul style="list-style-type: none"> • common rules for trustworthy transactions • reduces the economic and technical dependence on large private providers • creates a basis for a cross-modal and intermodal mobility system 	ADAC, BMW, DB, DENSO, FhG ISST , Software AG, T-Sytems , Tom Tom, Sovity among others	Data Space Pilot / Live	IDSA compliant stack on top of EDC Switched to EDC in 2023 [LINK]
Automotive	Catena-X 	To create the first uniform standard for data exchange along the entire automotive value chain An extensive ecosystem for all stakeholders of the automotive value chain (manufactures, suppliers, dealers, app/platform/infrastructure providers)	BMW DT Bosch SAP Siemens ZF Mercedes-Benz BASF Henkel Schaeffler German Edge Cloud ISTOS SupplyOn DLR Fraunhofer ARENA2036	Data Space Case Committed	IDSA compliant stack on top of EDC Switched to EDC in 2023 [LINK]

- Levels of Maturity**
- **Lead In:** A need has been identified and organization or consortium is in the phase of shaping use cases
 - **Case Committed:** The use cases, value, roles and an initial implementation plan are defined & committed
 - **Pilot:** First prototypes have been tested in a use case pilot
 - **Live:** Use case is running live and data flows in a sovereign way between data sharing parties.

Source: <https://internationaldataspaces.org/adopt/data-space-radar/>

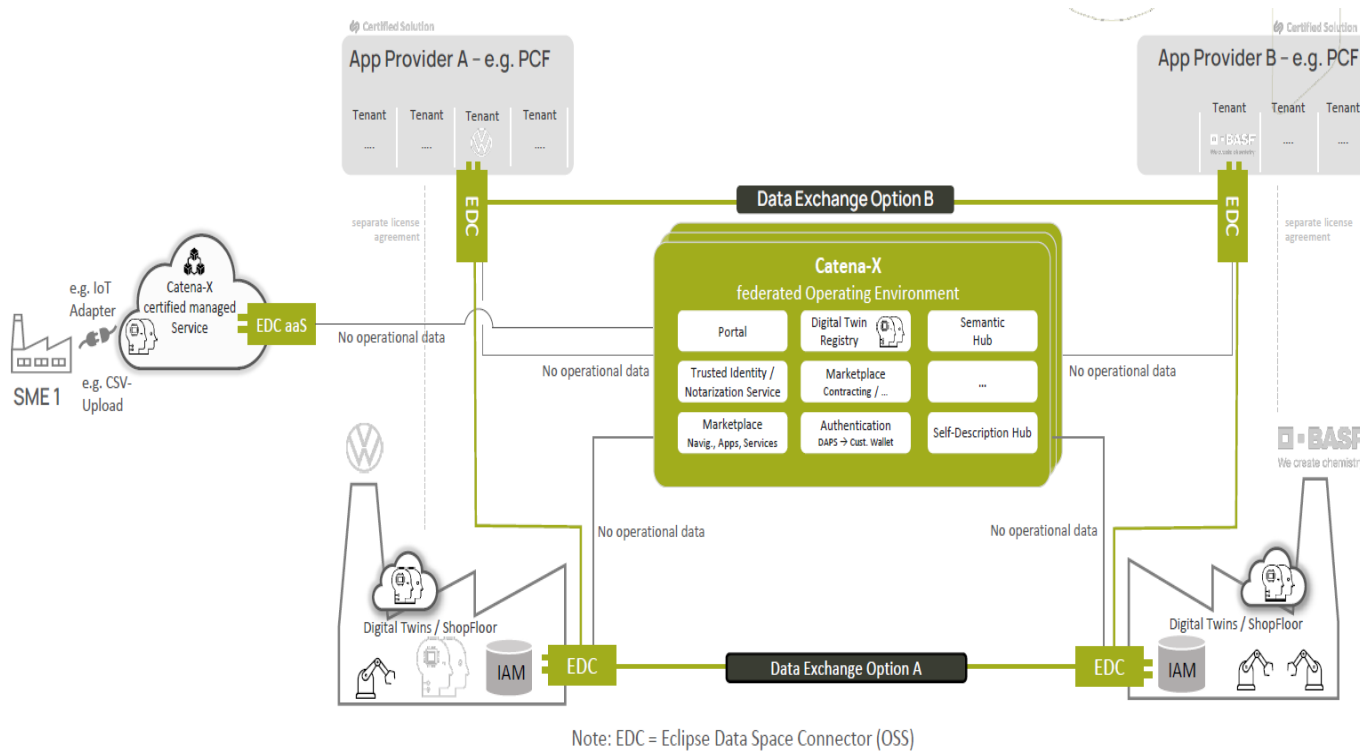
示例: Catena-X (Automotive industry)

<https://catena-x.net/>



Value Proposition: "Network of Networks": A global data space ecosystem for the automotive industry

- **Comprehensive:** A sovereign, multi-tier data exchange and use case collaboration across the entire value chain
- **Sovereign, federated and interoperable:** Incorporating GAIA-X principals and frameworks
- **Industry baseline:** One operating model and federated operating system for the data space
- **Global impact:** Key lighthouse project offering use-cases for both Gaia-X and IDSA
- **Future proof:** Drives the improvement and adoption of Eclipse data space components (EDC) and IDS-RAM(v4.0+)
- **Neutral governance,** including (Gaia-X compliant) conformity assessment body (CAB)
- **Foundational services and standards** built upon OSS (KITs) with dedicated developer journeys
- **OSS under Eclipse Foundation** via a new Eclipse data space project Tractus-X under Eclipse Automotive



First Data Space Verticals go Global – Example: Catena-X

International Catena-X Hubs shall empower regional adoption to ensure cross-region data flow



Catena-X involvement and Hua-X 2.0

- 1) Huawei Cloud should offer Dataspaces as a service (PaaS) in CH enabling vertical dataspaces
- 2) Huawei with partner can operate dataspaces globally for cross & upscaling in Automotive supply chain
- 3) Huawei can ensure compliance service in cross-region data flow

4. Huawei as CSP for Catena-X in China (Hua-X2.0 Scenario)



- Catena-X**
 - Biggest & most mature Dataspaces Ecosystem initiative
 - German Gov. supporting with 220M started in 2021
- Confinity-X**
 - Joint venture for operating CX Dataspaces in Europe
 - Sovereign Cloud JGCP – DT Partnership as CSP
- China Taskforce**
 - Initiated in Feb 23 to accelerate globalization.
 - We are planning our participation

: Confinity-X (Automotive industry data space app store)



Confinity-X is essentially the first data space "app store" providing common capabilities for data space development that build on EDC and are Catena-X compliant

<https://www.cofinity-x.com>

In January 2023 the Cofinity-X GmbH was founded as a joint venture of: **BASF, BMW Group, Henkel, Mercedes-Benz, SAP, Schaeffler, Siemens, T-Systems, Volkswagen and ZF.**

Vision:

- Cofinity-X aims to implement parts of the Catena-X network, which allows for the easy and fast deployment of compliant products and services across the automotive industry.
- EDC is one of the key technologies for the sovereign data exchange within a dataspaces for every company.
- Companies can deploy Cofinity-X's EDC as-a-service or as-a-license depending on their specific needs and requirements.
- Cofinity-X will follow all Catena-X standards without any central data storage.
- Cofinity-X enables cross-company data exchange with full data sovereignty and peer-to-peer data exchange, but will not have any access to the exchanged data.

Current Goal:

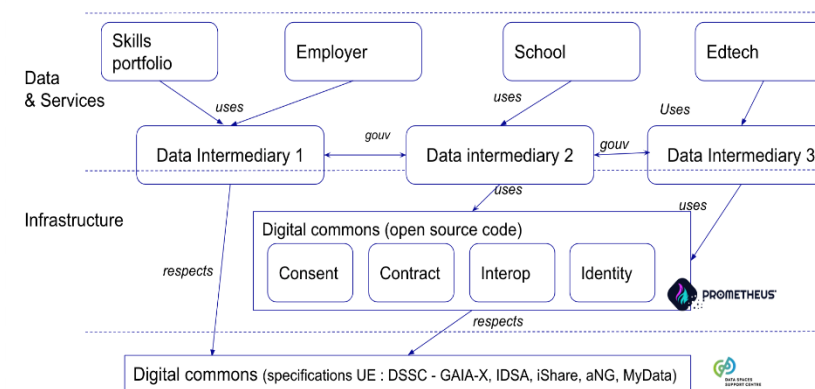
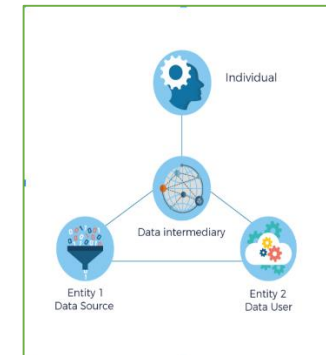
- The current goal of Cofinity-X is that the Eclipse Dataspaces Connector (EDC) is used by each company to have one set standard for data exchange across the entire automotive industry.
- These standards will allow a uniform and sovereign data transfer, the creation of data chains, cross-company interoperability, and an open and safe network. The Cofinity-X vision is technologically agnostic and allows the adaptation of all different standards.

EDC is the connector of choice for Catena-X and the baseline technology for Confinity-X

Industry (SAP)	SAP Connector (SAP Partner)	EDC-Open (SAP Partner)
Central China	Auto/Truck EDC Connector	Vehicle Data/Service Hub
Central Europe	EDC Connector	Automotive/Industrial
Data Transfer	Auto/Truck/Truck/Truck/Truck	General Support of Data Transfer Network (Automotive/Industrial/Truck/Truck/Truck)
Special Connectors	Bank/Banking/Finance/Support	General/Banking/Finance/Support
Use Cases (SAP)	Product/Service/Innovation	ERP/HR/IT/Systems/Support/Case
Timeline	available	planned

New data space trend 2: Personal Data Spaces

- Personal Data Spaces are designed around individual users, enabling them to maintain control and portability over their own data, deciding who has access and for what purpose.
- This includes diverse types of personal data like photos, texts, health records and more. In personal dataspace, users can decide where their data is stored, who can access it and for what purposes.
- The architecture of personal dataspaces usually prioritizes ease of use, transparency and privacy.
- The typical data exchange pattern used in personal data spaces is that of a data pod with either SOLID data pods, DIF Web Data Nodes being and digital wallets / vaults being the most characteristic examples
- MyData Global is the main forum where new projects focusing on personal data spaces are concentrated
- The Gaia-X Framework aims to support ecosystem federations also for personal data spaces although Gaia-X use-cases and lighthouse projects in this domain are not as well developed as for industrial data spaces.
- Inrupt (a start-up by Sir Tim Berners-Lee and Dr Bruce Schneier) is a noticeable new industry player in this domain that is at present a disruptive outlier that remains outside the influence of the MyData Global and Gaia-X communities.
- The focus is on empowering the individual, ensuring they have complete autonomy over their personal data, enabling them to leverage their data for personal benefit while protecting it from unauthorized access or misuse.



MyData Global Principles and emerging model: focus on consent management

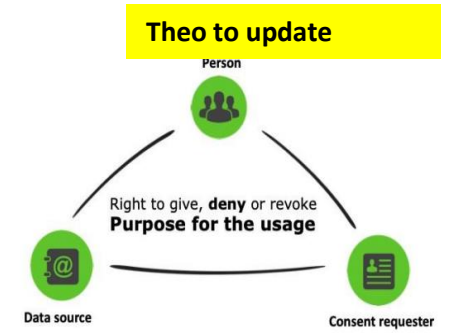
- Consent as a cornerstone of MyData principles

Use-case 1: Driving license check (UK DVLA R&D requirement)

<p>Background:</p> <ul style="list-style-type: none"> • An insurer wants to calculate the correct fee for a driver in the UK • The insurer requires information about the identity, age, health conditions and convictions of the driver in order to produce a competitive quotation 	<p>Current state (As-is):</p> <ul style="list-style-type: none"> • The driver needs to complete input forms and provide the necessary information over the web/email and authorize the insurance company to access or verify DVLA information at a later stage with the risk of invalidating the offer or agreement <p style="text-align: center;">Personal data space consent enablement →</p>	<p>Future vision (To-be):</p> <ul style="list-style-type: none"> • I can authorize the DVLA to verify that I have a valid driving license, I am in a given age range, have no convictions and/or no penalty points in my driving license and no known medical conditions requiring additional check-up. • The insurer never gets exact age, health record, conviction or penalty history • The insurer provides and accurate offer for driver insurance that can be binding. . • I can authorize the insurer to provide privacy preserving input to financial and driver risk assessment services in order to benefit from further low risk discounts.
---	---	---

Use-case 2: Reduced daycare fee for families project (2020-2021)

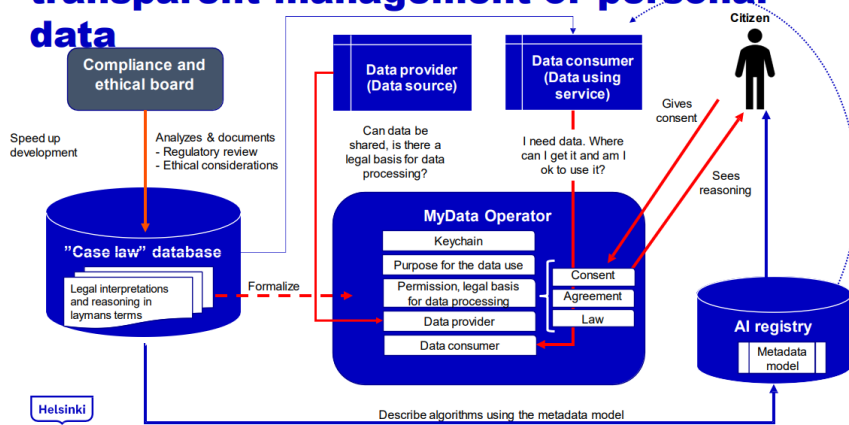
<p>Background:</p> <ul style="list-style-type: none"> • By law in Finland: • Cities have to organize daycare services • Parents' financial situation defines the rights to reduced day-care fees • Helsinki daycare is organized for ~27 000 children p.a. • To be eligible for a reduced daycare fee, both parents must provide city with requested documents to justify their financial status 	<p>Current state (As-is):</p> <ul style="list-style-type: none"> • Family income data has to be submitted by filling manual forms in pdf format either by mail or secure email to the City of Helsinki's customer fee unit. <p style="text-align: center;">Personal data space consent enablement →</p>	<p>Future vision (To-be):</p> <ul style="list-style-type: none"> • Citizen can authorize the city to verify his/her annual income. • With my consent, the city can automatically check my income from the National Income Registry and determine the correct applicable daycare fee with potential reductions for my child.
--	---	--



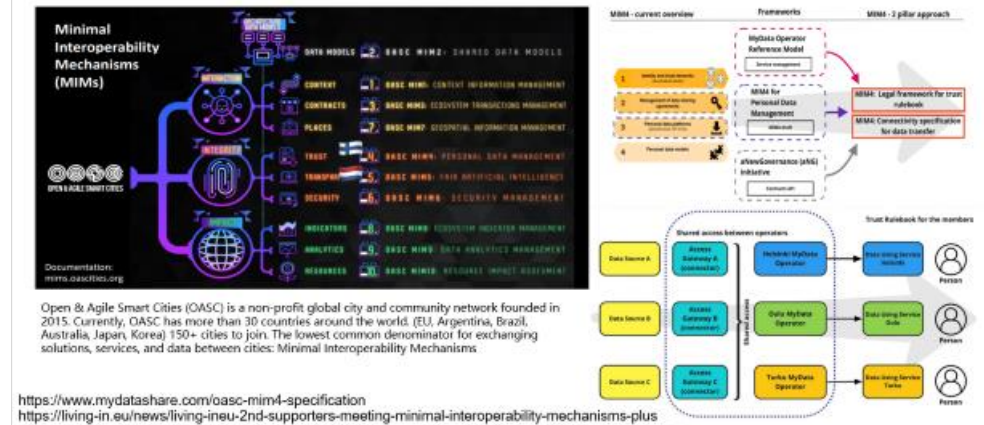
Example: Minimum Viable Product for City of Helsinki's MyData Operator implementation

- Citizens can authenticate themselves to access a city service
- Citizens can grant, deny or revoke consents on personal data use for a specified service (as in compliance with regulation)
- Human-centric approach in Human Computer Interaction
- Users understand the purpose consent for data use is requested

Helsinki's approach to ethical and transparent management of personal data



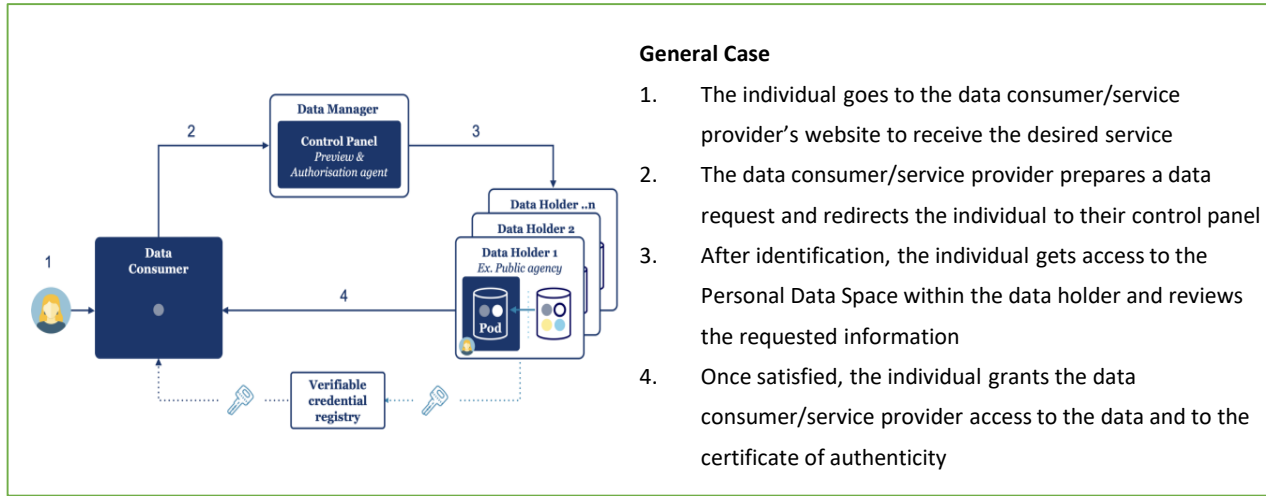
OASC: MIMs Promote Digital Smart City and Combine Personal Data Space to Build Digital Life



Open & Agile Smart Cities (OASC) is a non-profit global city and community network founded in 2015. Currently, OASC has more than 30 countries around the world. (EU, Argentina, Brazil, Australia, Japan, Korea) 150+ cities to join. The lowest common denominator for exchanging solutions, services, and data between cities: Minimal Interoperability Mechanisms.

<https://www.mydatashare.com/oasc-mim4-specification>
<https://living-in.eu/news/living-in-eu-2nd-supporters-meeting-minimal-interoperability-mechanisms-plus>
 Report of TWG Smart Cities: Landscape of Smart Cities Standards <https://zenodo.org/record/5785688/files/YyAGlnZBYUn>

MyData Global Principles and emerging model: local & international transactions



Real-life Pilot by the Swedish Public Employment Service:

- Data infrastructure for competence provision and lifelong learning
- gives individuals control over their data,
- allows them to access personal information in public agencies and to share it with 3rd parties

Use-cases:

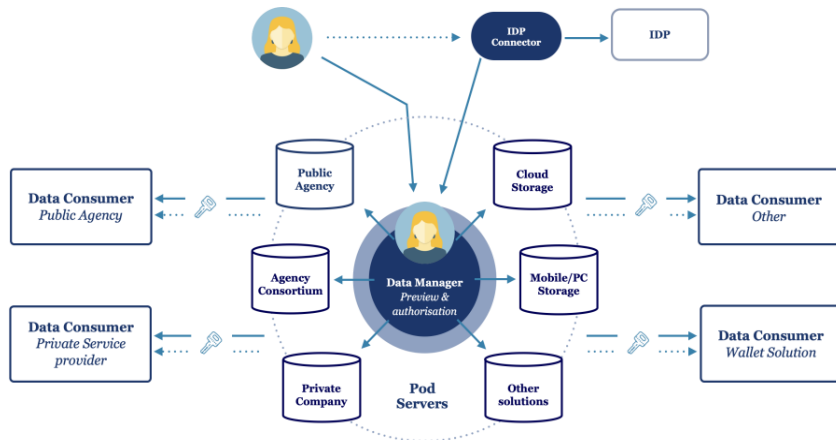
- **Certificate exchange:** Individual requests public agency certificate to share with private company
- **Aggregation of data points & exchange – Internship program:** An individual collects information from many sources and shares it with another agency in exchange of an authorization certificate.

Some current issues:

- Personal data has a loose definition and traverse many data domains
- Law treats personal data differently effecting technology/usability
- Data is distributed and duplicated across agencies
- Individuals do not own the data
- Data is (largely) inaccessible to the individual
- Data won't be deleted at source
- Some Data have an expiration date
- Data will most likely be copied at destination

Focus:

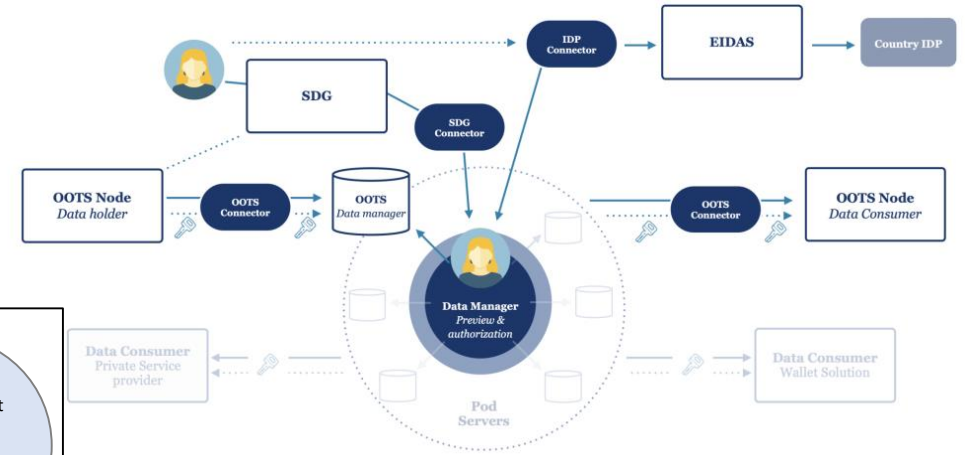
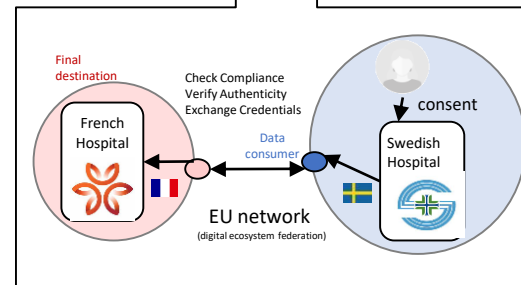
- Put the individual at the center to maximize control
- Ensure portability of data
- Minimize duplication of data unless necessary by use case
- Create data spaces from data source only accessible by the individual
- Controlling data at source and allowing access to it, is more efficient than storing information in intermediary apps and poses less security / legal risk



Technology choice:
W3C Solid protocol

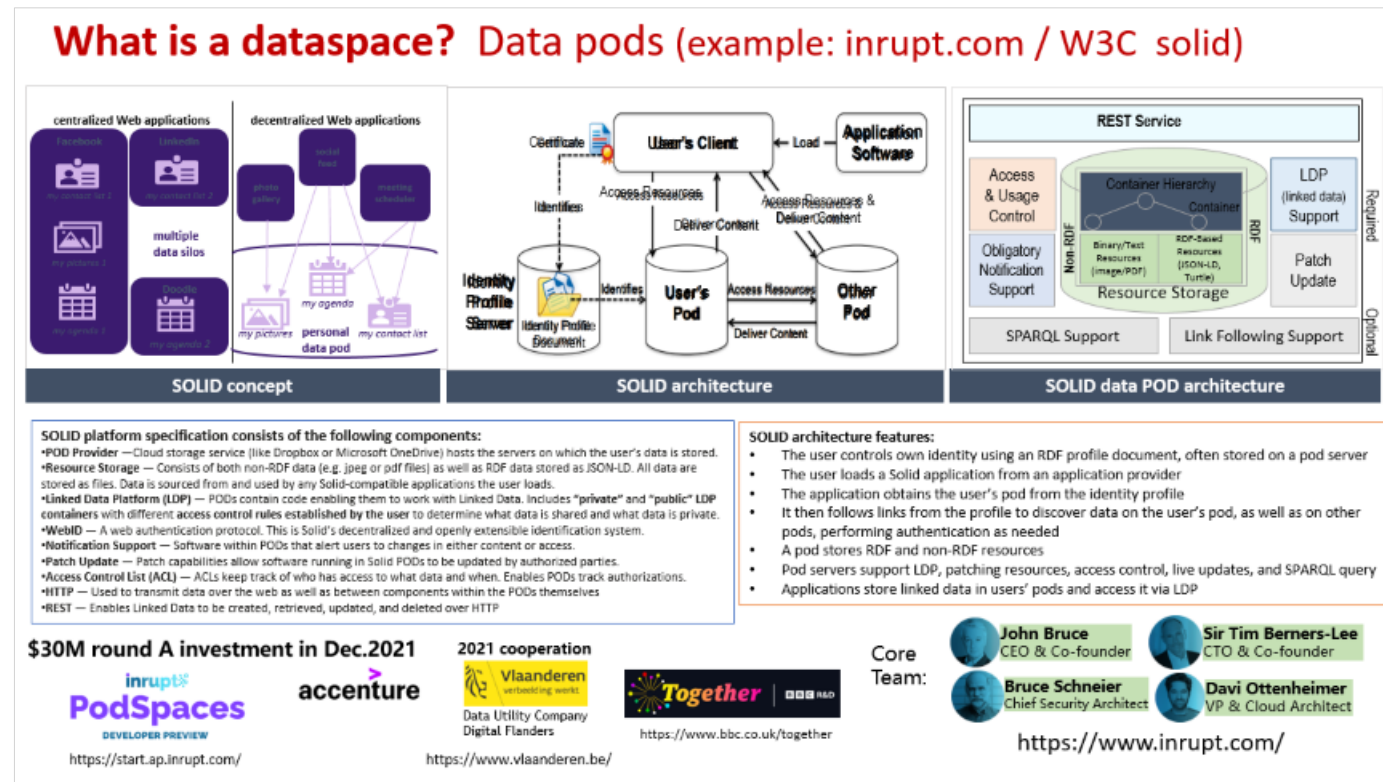
- Solid is a W3C standard / protocol focusing on data sovereignty & portability:
 - Define semantically how applications, resources etc. relate to each other
 - OSS reference implementation
 - Growing community for support
 - Data oriented (rather than service oriented)
 - Enables interoperable distribution of application
 - Allows for loose coupling and does not impose configuration of elements

International configuration Exchange in EU network



Digital Flanders project becomes main Solid Data Pod pilot (Flemish Government in Belgium)

- Digital Flanders is currently conducting a number of projects using Inrupt Enterprise Solid Server to securely share data, including:
 - MyDigitalMove:** With a citizen's consent, it takes data from the national register and places it in a personal data store. The citizen can then choose with which organizations they want to share their new address, fulfilling data compliance requirements and simplifying the moving process.
 - MyProfessionalData:** allows work-related data—such as an employee's place of residence, diplomas, salary slips and holiday certificates—to be shared with a new employer in a way that relieves the employee of the burden of transferring this data manually. The project also allows service providers to organize their processes more efficiently.
- Digital Flanders has also established the **Data Utility Company**, which will explore the possibilities of providing services using personal data stores to organizations and governments outside of Flanders.
- All 6.5 million citizens of Flanders will have the opportunity to activate their own data Pods. Citizens can choose which data they share, which organizations should have access to the data and for how long the data is shared.
- The data is stored in a standardized format that all participants in the Solid data ecosystem can use.
- Once users have activated their Pods, they can interact with Digital Flanders' pilot projects to better utilize their data.



<https://www.vlaanderen.be/digitaal-vlaanderen/athumi-het-vlaams-datanutsbedrijf/the-flemish-data-utility-company>

DIGITAAL VLAANDEREN

SEMIC Expert group proposes EU strategy on personal data spaces

Personal Data Spaces: session 1
Workshop
Thursday, 12 January 2023
09:30 - 16:30 Brussels time
interoperable

Personal Data Spaces: session 2
Workshop
Wednesday, 1 March 2023
09:00 - 17:00 Brussels time
interoperable

Personal Data Spaces: session 3
Workshop
Friday, 31 March 2023
09:00 - 17:00 Brussels time
interoperable

Together with the Interoperable Europe unit & the EU JRC (Joint Research Center), the **first workshop on Personal Data Spaces was held on Thursday 12th of January 2023**. Both the MyData Global and SOLID communities were brought together to discuss and frame the interoperability challenges between various personal data space implementations.

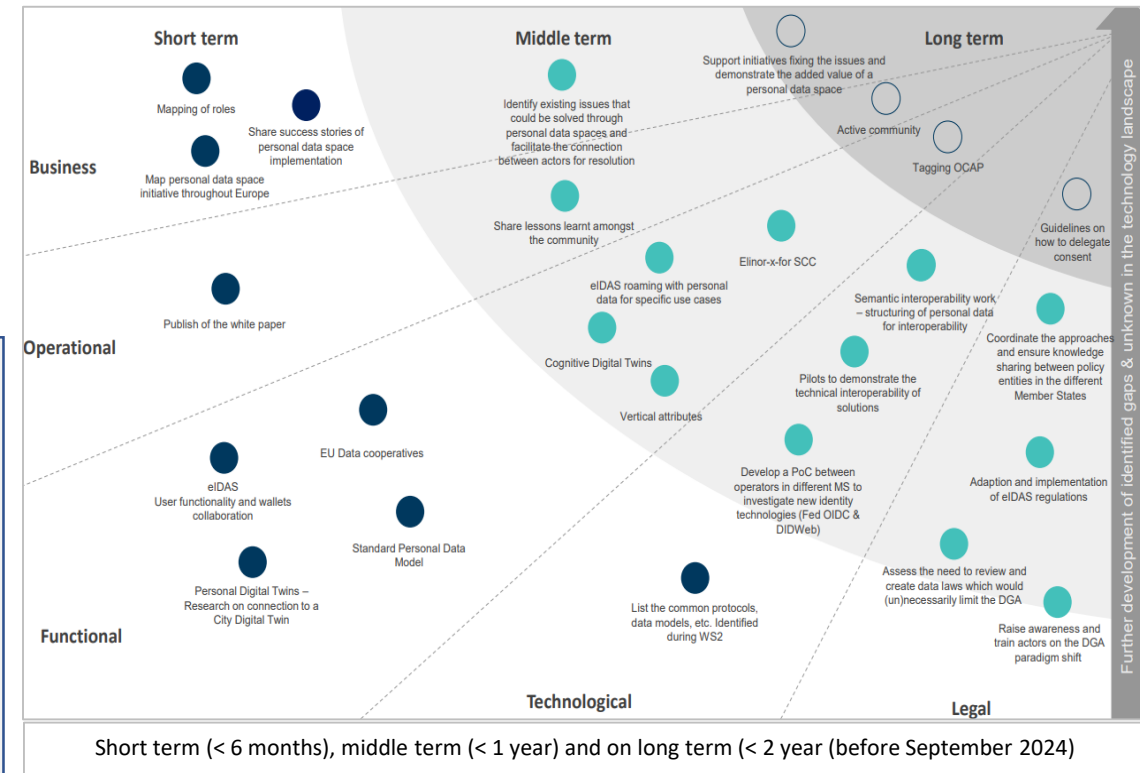
The objective of the second workshop was to identify how existing and potential personal data space technologies can ensure **semantic and technical interoperability**. Use case driven analysis was used to identify the **key building blocks** of personal data space technologies in an **architecture** that is conformant to **MyData Global principles**. These building blocks will include **Identity, Data Modelling, Service Management, Access Control, Governance and Logging**.

The third workshop focused on the co-creation of a **common vision** on what **personal data space providers** will bring to EU Member States for the next two years (2023 and 2024). The goal was to draft a roadmap up until 2025 on some of the questions raised above for the advancement of EU-wide interoperable personal data spaces in the coming years in preparation of the EU launching future initiatives to accelerate R&D in the area of personal data spaces and facilitate convergence.

Technical	
Short term:	<ul style="list-style-type: none"> •Common requirements and capabilities; which ontologies, data models,... •Continuing implementation of business use cases. •Prometheus-X as a reference example in Gaia-X •Data spaces involved in the Olympics, Paris 2024.
Middle term:	<ul style="list-style-type: none"> •Improve the cross-over between AI, large language models and data spaces. •Build bridges between data spaces and interoperability. •Finding sponsorship.
Long term:	<ul style="list-style-type: none"> •Implementation in browsers.

Business & Operational	
Short term:	<ul style="list-style-type: none"> •Visibility; promotion of our activities; Improve Clarity ; Creation of focus groups; Highlight success stories & lessons learned; Create list of concrete issues + owners of the issues to validate & stimulate MVP (minimum viable product) creation
Middle term:	<ul style="list-style-type: none"> •Proposal to have a road tour across Europe to identify solutions •Promote the road tour to create awareness •Create 360 degrees guide: technical, practical, and legal aspects •Reduce cost of adoption by creating a common layer (technical, semantical,...) that everyone can relate to. •DPP: Digital Product Passport
Long term:	<ul style="list-style-type: none"> •The current market response for accessing data is often a data dump. In personal data spaces, accessing data is key and thus is data access control. •To establish an interoperable data access control mechanism, legislative support will be needed.

Roadmap for personal data space development is based on building on MyData Global principles and W3C Solid Protocol alignment with DSSC support for personal dataspace and and Gaia-X architecture & DSBA convergence



Short term (< 6 months), middle term (< 1 year) and on long term (< 2 year (before September 2024))

Prometheus-X personal data space project becomes the basis of Gaia-X DASES

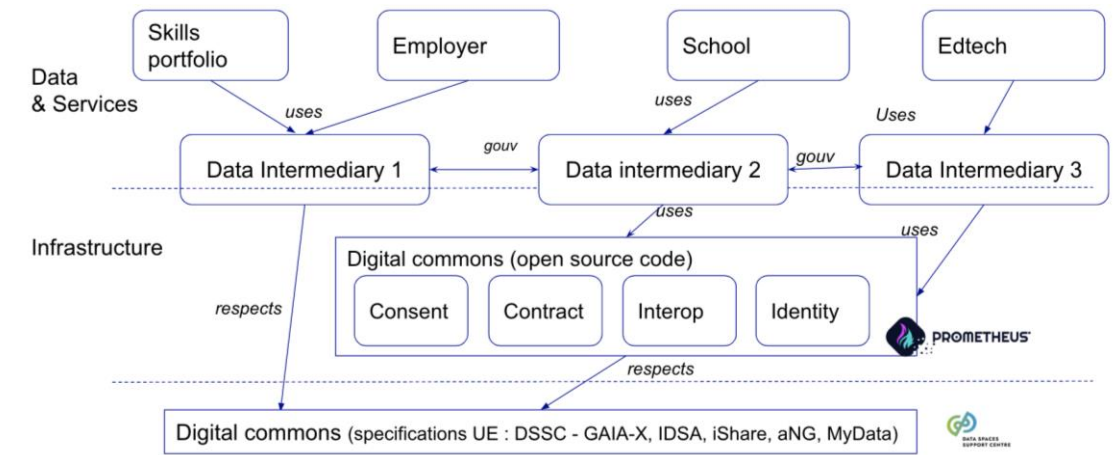
- Data Space Education and Skills (DASES) has created a WG in Gaia-X French hub for bringing together various actors in the educational sphere in order to facilitate European personal data spaces for education and skills data.
- Prometheus-X portal is put forward as a MVP (minimal viable product) for sovereign ecosystems of education and skills data in Europe.
- Gaia-X and DASES aim to provide the network, the governance and the infrastructure necessary for the interoperability of education data.



<p>Use-cases for skills:</p> <ul style="list-style-type: none"> - Pooling data to offer better services to people (employment, training, education, etc.) - Creating ethical networks of personal data - Enabling the individual to receive personalized lifelong learning - Providing interoperability of skills data 	
<p>Use-cases on data sets: pool aggregated data in order to train artificial intelligence algorithms.</p> <ul style="list-style-type: none"> - Allow actors to cross data sets that are currently fragmented - Limit cold start problems - Exploit unused data in a trusted environment - Larger datasets open up training possibilities for ML models - Interoperability of educational data 	
<p>Use-cases on data sets: Impact study.</p> <ul style="list-style-type: none"> - Allows stakeholders to easily access data that measures the impact of their solutions - Ensures interoperability of datasets in order to compare over longer periods of time or with more data - Interoperability of educational data 	

Data intermediary principles:

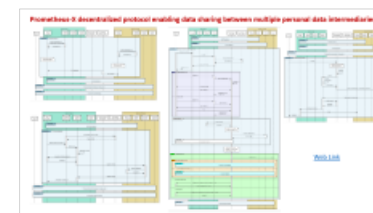
- People manage their consents from a central place
- Data intermediary do not store the personal data nor provide services on it: Separation of Powers Principle
- Data intermediaries are interoperable
- Data intermediaries rely on open governance and standards
- Data intermediaries allow open and decentralized ecosystem



Prometheus-X building blocks

- aim to help build data intermediaries and guarantee their interoperability.
- together with the governance layer guarantee that organizations that are connected to one data intermediary can share data with organizations connected to another intermediary
- respect GAIA-X, IDSA and Data Space Support Centre specifications

Prometheus-X full decentralized protocol enabling data sharing between multiple personal data intermediaries



New data space trend 3: intelligent transport and cooperative mobility

Intelligent Transportation System (ITS) Data Spaces and mobility data spaces are designed to offer an open ecosystem that enables the trustworthy exchange of data between different traffic participants, providers and operators in order to optimize traffic flows, increase safety and protect the environment.

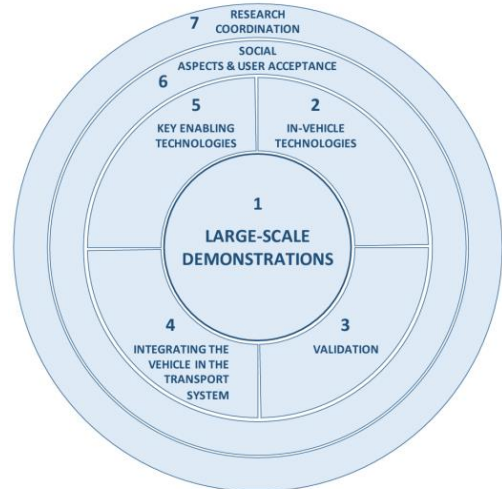
- Sensitive data, such as travel documents or passenger flows, which are generated by vehicles or privately owned mobile devices, may be collected and processed by public transport providers, navigation service providers, fleet operators (OEMs) and mobile communication providers (MNOs).
- In such a multi-OEM, multi-MNO and multi-vendor environment, generated data need to move between different trust domains and even different legal jurisdictions.

Trust challenges in ITS and Mobility Data Spaces:

- ITS data spaces aim to create data sovereignty and a trusting environment for data providers in order to give data users the assurance about data origin and quality.
- Due to the dynamic environment of mobility, these assurances cannot always be created on evidence coming from fully trusted sources.
- ITS data spaces should be able to provide such assurances under measurable assurance and confidence in the presence of uncertainty, so that data that had previously not been usable, can not be exploited.



Budget 1.2 B€



The CCAM Partnership aims to promote and facilitate pre-competitive research on Connected, Cooperative and Automated Mobility (CCAM) within the European Research Area, by bringing together the different actors of the CCAM value chain.

- **Avoid fragmentation**
 - consolidate all EU CCAM activities in one single industry platform.
- **‘Kick-start’ deployment of CCAM in Europe**
 - large scale pre-commercial deployments
- **Influence policy and standardization**
 - regulatory needs, standardization (ISO, ETSI, et al)
- **CCAM association under establishment**
 - open for all, low membership fee to attract SMEs.

CCAM stakeholders supporting the Partnership development

Research providers	AVL, AIT, CEA, Cerema, DLR, Eurecat, Everis, FEV, fka, Fraunhofer, ICCS, ICOOR, IDIADA, IFPEN, Lero, Ricardo, RISE, SAFER, SINTEF, TNO, VTI, VTT
Universities	Aachen, Budapest, Chalmers, DTU, Eindhoven, Florence, Galway, Istanbul, Leeds, Leuven, Milano, Modena, Mondragon, Paris, Warsaw, Zilina
Automotive	Akka, BMW Group, Bosch, Continental, DAF Trucks, Faurecia, FCA, Irizar, JLR, Renault, Valeo, Volkswagen, Volvo Group
ITS	Bestmile, Dinniq, HERE, TomTom, PTV, Swarco, Ubiwhere, TTS Italia
Telecom/IT	ELMOS, Ericsson, EVERIS, Huawei, NXP, Vicomtech
Infrastructure	Asfinag, Sanef, Vinci
Freight & Logistics Services and Users	ALICE, Colruyt Group, Gebruder Weiss, IDIT, Procter & Gamble
Member States	Austria, Belgium, Czech Republic, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, Netherlands, Norway, Spain, Sweden, UK
Regions, cities and public transport operators	Flanders, Gothenburg, Helmond, Paris/Ile-de-France, Madrid, Stuttgart, Vienna
Representative bodies	ALICE, AMICE, ANEC, CEDR, CLEPA, CONEBI, EARPA, ECTRI, EPoS, ERF, ERTICO, ETNO, ETRMA, EUCAR, Eurocities, EuroRap, FEMA, FIA, GSMA, IRU, POLIS, UITP, 5GAA
Cluster and test centres	AIPSS, Aurora Snowbox, Austriatech, CARA, Catapult, Drive Sweden, Moveo, PTCarrereta, Tempere, Vedecom, Zalazone

Huawei is engaged and participates in the new CCAM Partnership. **CONNECT is one of the two project of Cluster 5.**

- We influence the Strategic Research and Innovation Agenda (SRIA) of CCAM which links to the portfolio of R&I and policy strategy of EC
- We participate in an ecosystem where partnerships for new Horizon Europe projects are created

Towards Common European Mobility and ITS/CCAM Data Spaces

Challenges for a common European Mobility Data Space (EMDS)

Key Challenges:

- Access to and sharing of mobility data remain below their potential.
- Mobility and transport ecosystem is particularly complex: Large legacy of initiatives with their own governance, architectures and platforms.
- Different building blocks may fulfill similar functions, but lack of a federated architecture & common standards prevent a true data space.

Legal challenges:

- data protection, liability issues, compliance, intellectual property rights.

Technical challenges:

- interoperability, data sovereignty and trustworthiness.

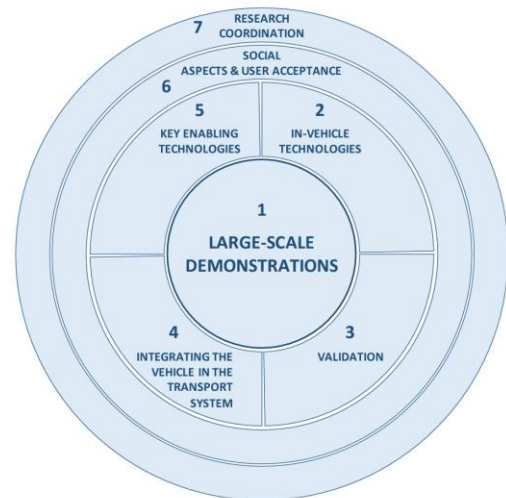
Business challenges:

- convincing organizations that are often competing to exchange some of their data on a voluntary basis requires business models and clear benefits for each involved party including the economic sustainability of intermediaries enabling data sharing

The **CCAM Partnership** aims to promote and facilitate pre-competitive research on Connected, Cooperative and Automated Mobility (CCAM) within the European Research Area, by bringing together the different actors of the CCAM value chain.

Huawei is engaged and participates in the new CCAM Partnership.

CONNECT is one of the two project of Cluster 5. The only for Huawei



Main existing EU mobility data sharing ecosystems and initiatives

Mobility Data Space (Germany):

- Open decentralized ecosystem of data providers, data users and platforms allowing sovereign exchange of mobility data and offering a central directory of data resources & services.
- Operated by Acatech ; funded by the German government.

iSHARE (Netherlands)

- A uniform set of agreements for identification, authentication & authorization enabling organizations to grant each other access to their data.
- Developed by the Dutch transport and logistics sector, it is expanding in new areas through the i4Trust initiative.

Smart Otaniemi (Finland):

- An innovation environment for smart and sustainable urban solutions
- Develops use cases based on cross-sectoral data sharing between transportation and building/energy platforms.

ERTICO

- Plays an important role with a number of initiatives:
 - CCAM test data sharing,
 - TN-ITS for map update exchange,
 - Traffic Management (TM2.0) and
 - FENIX network (trust framework for data sovereignty and sharing in transport and logistics services).

NAPCORE:

- Newly formed organization to coordinate, harmonize and improve the interoperability between the National Access Points established under the ITS Directive all over Europe.

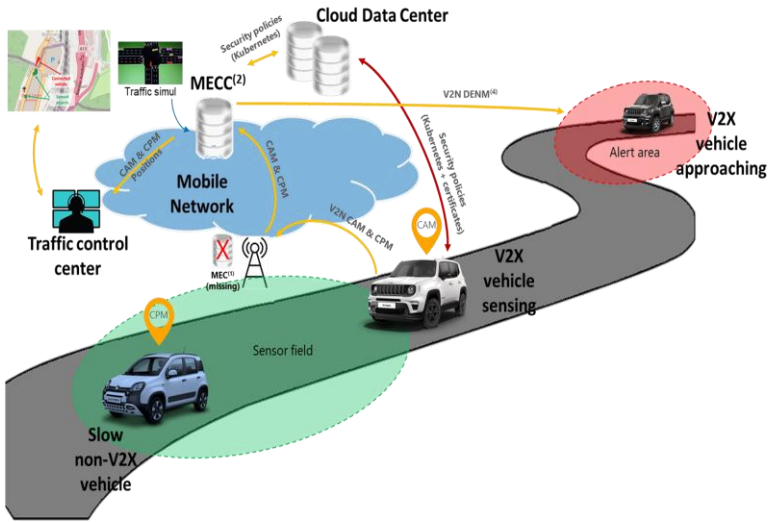
Digital Transport and Logistics Forum (DTLF):

- Commission's expert group defining a common framework to create an interoperable federated environment for data sharing in the freight transport and logistics sector,

PrepDSpace4Mobility is a preparatory action by ERTICO-ITS to support the development of the upcoming common EMDS <https://mobilitydataspace-csa.eu/>

An emerging ITS/CCAM data space paradigm

Horizon Europe CONNECT Use Case: Slow Traffic Detection



The representation of the Slow-Moving Traffic Detection (SMTD) use case.

The slow moving non-V2X vehicle (i.e., the blue one) is detected by a following V2X vehicle (i.e., the white one) thanks to its radar sensor.

As the vehicle ahead is detected, the V2X vehicle creates and sends ETSI-standard CPMs (alongside its own CAMs) towards a MECC server via 5G connection.

The MECC server detects the slow-moving traffic situation and it generates a DENM alert message sent via 5G to all vehicles in a dedicated approaching area (i.e., the black vehicle).

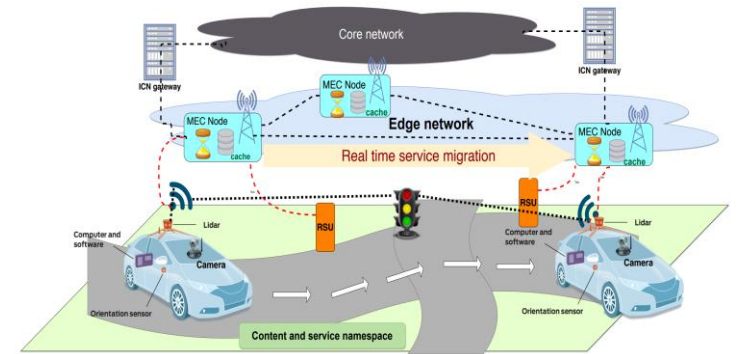
In this way, all the V2X vehicles approaching can be informed of the slow-moving traffic situation ahead of them.

Extending MEC with a novel CCAM connector capability

The MEC architecture can be extended to enable integration with common European Mobility Data Space (EMS) services.

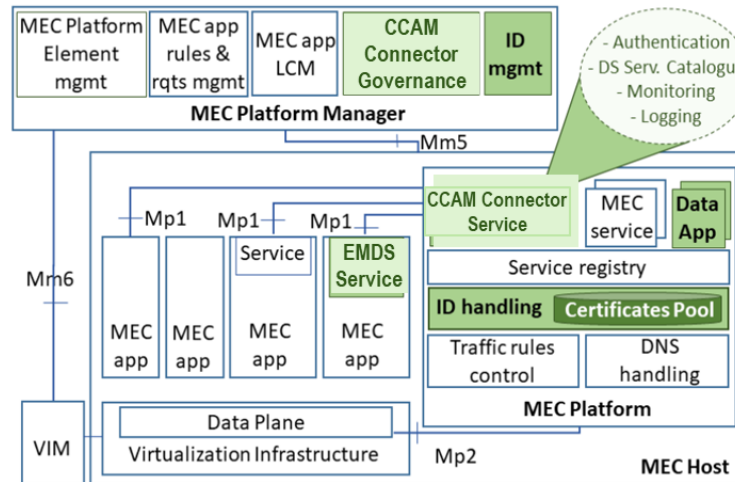
- Each MEC Application (MEC App) can act as a data prosumer. Each application is capable of obtaining a CCAM connector and exchanging data with any application that has a registered CCAM connector inside or outside the MEC host.
- In the general case, the architecture supports the consumption of data services between the MEC Platform and a MEC Application or between two MEC Applications, while any of those exchanging parties can belong to the same or different MEC Host(s).
- In the scenario of two MEC Applications exchanging data, we denote as MEC App2 the application that attempts to receive data and as MEC App1 the one that provides the desired data. After the completion of instantiation for both applications and the assignment of a certified CCAM connector to each of them, the connectors' information are made available through the MEC Platform's relevant API for service discovery and availability.

CCAM data space overlay on ITS/Mobility Data Space



CCAM data space as an overlay on top of mobility data space and ITS edge components (e.g. MEC).

- If vehicle is moving, the **MEC service is migrating from one MEC node to another**
- One possibility may be that we have an overlay, where MEC could be part of EMDS (ITS subsystem) offering a service to a CCAM data space running on top of EMDS.
- The mobility data space being in the lower lever should be able to accommodate the mobility of vehicles, which implies the migration of MEC apps (including the Connector service) from one MEC server to another.
- Therefore the CCAM connectors are not running on a fixed MEC server, but rather migrating as required. The CCAM data space being on the higher level could have connectors that accommodate both the MEC services and the IDS connectors from the mobility data space (EMDS) as well as other cloud services (e.g. the Traffic data server in the CONNECT Slow Traffic Detection use case).

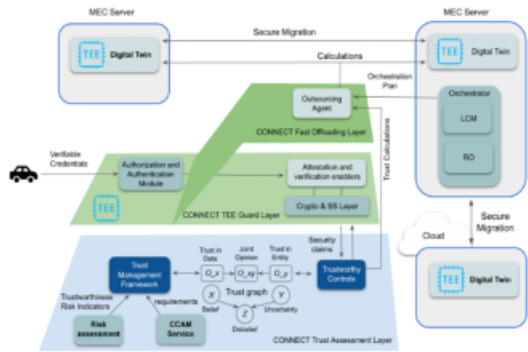


Trust Anchor challenge for CCAM (and other IoT data spaces)

- Trust frameworks for data spaces (e.g. Gaia-X Trust Framework) we have seen so far, including rules about the usage of Trust Anchors and the verification of Credentials attesting claims, are all based on the assumption that Trust Anchors are institutional and trusted to an associated and **verifiable Level of Assurance**.
- However, in emerging CCAM scenarios the verification of assurance of the Trust Anchors or the attesting evidence may not be possible, e.g. because the sources of evidence are untrusted or the evidence is indirect and obtained through a **referral chain**.
- So we need to go beyond authenticating participants key-pair and design / adopt data structures and algorithms that allow presenting attributes in a way that we can assess their correctness and the trustworthiness of their source in the presence of measurable confidence and uncertainty.

Trust Governance Framework in CCAM - The example of the EU Project CONNECT (2022-2025)

The vision of CONNECT is to address the convergence of security and safety in CCAM by assessing dynamic trust relationships and defining a trust model and trust reasoning framework based on which involved entities can establish trust for cooperatively executing safety-critical functions in the presence of uncertainty



- What kind of tools do we need to reason about trust relationships between data sources and data processors in vehicles, the edge and the cloud.
- How to reason about trust relationships between entities that were previously unknown (to each other).
- How to assess the risk of an operation and the level of trust an entity can put on another entity and on the data collected from multiple sources.

CONNECT architecture includes:

- A **dynamic trust assessment framework** that enables trust level evaluation across information referral networks in the presence of uncertainty
- Technological TAs **could be utilized as a trust anchor** to establish a verifiable chain of trust in data sources and data processors by providing verifiable evidence on the correctness of operations, from their trusted launch and configuration to the runtime attestation of execution properties.

Sovereignty Challenge: CONNECT can benefit by a **trust governance framework** that includes policies & rules ensuring transparency, fairness and non-discrimination among eligible participants and providing equitable access for all. These policies should also address **the choice of different technological trust anchors by CCAM entities and conformity to local regulation**

Trust Sources

- Appropriate trust sources are considered to provide evidence for the fulfillment of the corresponding property
- Depending on the trust properties of interest, different trust sources are selected to create the atomic trust opinion of the trust relationship.
- An atomic trust opinion is a trust opinion based only on evidence in the form of trust sources and without fusing or discounting multiple trust opinions
- Some of the trust sources need to be evaluated regularly because the output of these trust sources might change over time. For other trust sources, a one-time assessment at system startup is sufficient because the output does not change.

Some examples

- Trust on Communication**
 - Protection mechanisms of communication
 - Hardware security mechanisms
- Trust on System Integrity**
 - Secure boot
 - Run-time integrity check
 - Known OS-vulnerabilities
- Trust on Application**
 - Run-time operational assurance
 - Known application-vulnerabilities
 - Trusted Execution Environment (TEE)
- Trust on Behaviour**
 - Misbehavior detection
 - Misbehavior Reports
 - Reputation based system
 - Spoofing detection
 - Intrusion detection system (IDS)

Dynamic Trust

Pilot 1 - FIAT CMR
Vehicles provide reliable data for cooperative situation awareness service

Pilot 2 - DENSO
Create resilience in ECU migration of applications

Pilot 3 - SystemX
Trust the Edge for better Misbehavior Detection in Collective Perception Services

17 Partners

Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)

A holistic execution approach is required across the entire ecosystem players:

There are several industry associations on play....

Towards a converging Data Space (Security) Architecture

Reference implementation: OSS on Eclipse foundation

Standardization is going global

Competition is investing heavily

An overview of data space projects in Europe

Emerging architectural variants

Huawei contributions in Hua-X and Digital Sovereignty projects: technical

Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap

Recommendations

Appendix I: Core technologies

Appendix II: Data spaces examples

Hua-X.2.0: Boot-X – a First Open Source Based Data Space as a Service Prototype

Boot-X is developed using **open, interoperable and federated data exchange** standards defined in **Gaia-X specs**

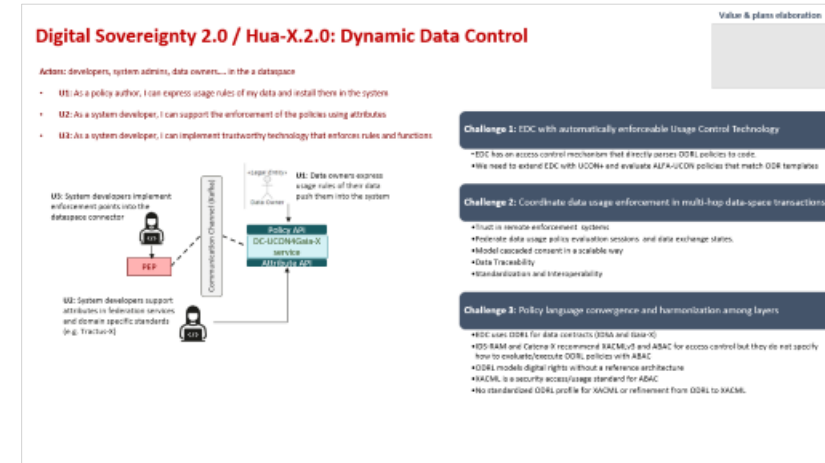
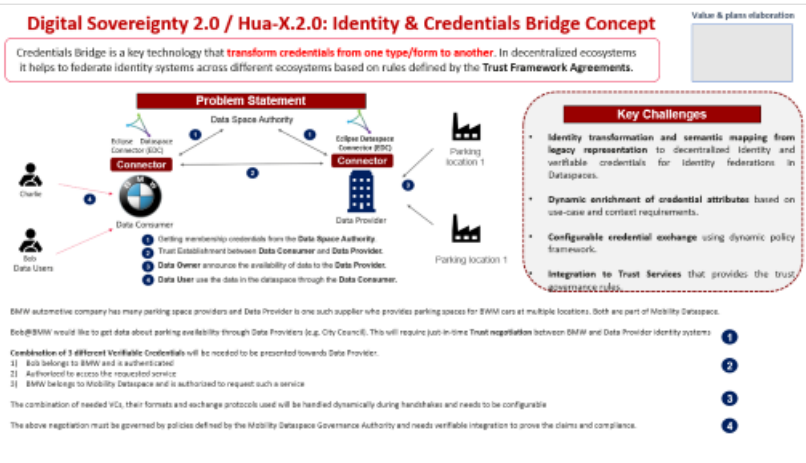
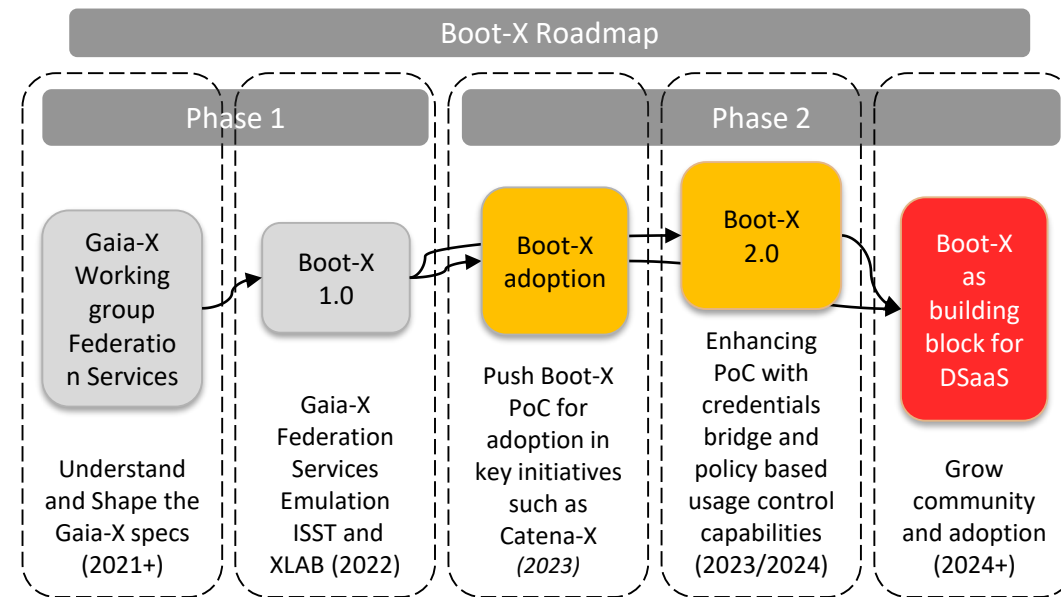
Validation of Supply chain compliance is the first real world use case demonstrated in Boot-X.
Traceability, Circular Economy and Mobility use cases with **multiple data-contributors** are focus for Boot-X

Validation of Supply chain compliance

By law the product/service provider is responsible for the supply chain. He is accountable for non redemptional verification of the standards. In a centralized approach enterprise needs to manage central systems including the user and rights management for all the suppliers to provide needed certificates and proofs for on demand verification. This requires the on-boarding and follow-up with suppliers, limiting the dynamic changes in supply chain. In addition this is incompatible with 1-up 1-down business practices, giving OEM full access to underline sub-contractors. Boot-X offers decentralized, federated compliance validation. Where data is stored decentralized and compliance validation is checked just-in time, and consistent with 1-up 1-down business practices. Datasets are available and are distributed in different servers in the automotive industry value chain.

Technologies:

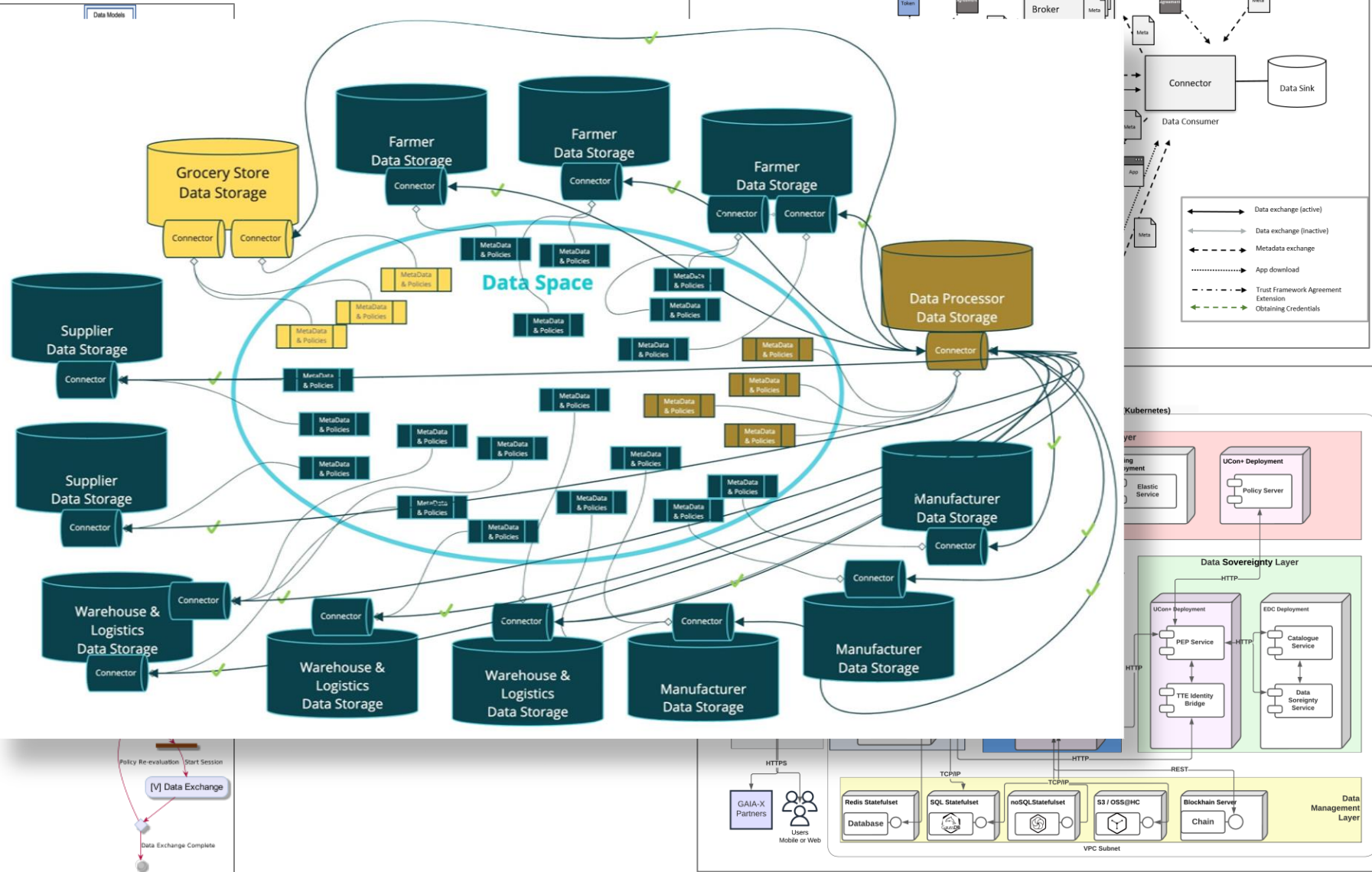
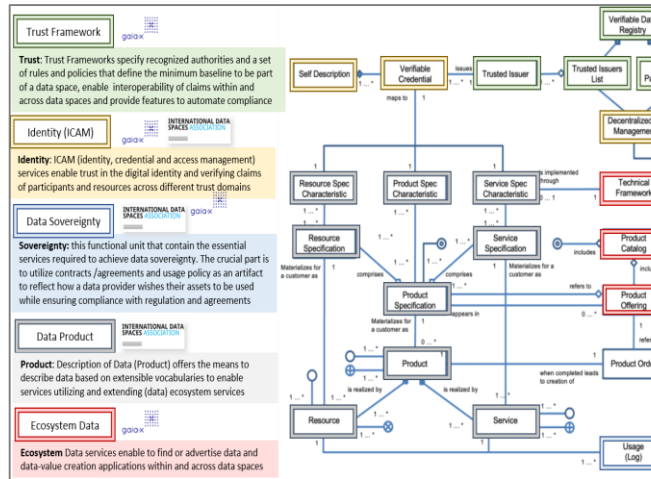
- Open Source projects already developed and reliable. Around 10 open source tools.
- Code developed by Huawei to glue those components together.
- Code developed by Huawei in which Huawei has the IPR rights to implement data governance.



Data space security architecture: 1 - industrial

<https://rmd-confluence-eu-g.huawei.com/display/9EDSRPV/WIP%3A+Towards+a+Security+Reference+Architecture+of+Dataspaces>

PDF snapshot at CRDU_GermanyRC_GE_SVN [LINK]



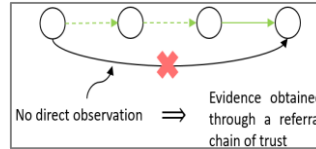
- Comprehensive architecture following the “4+1” model and initial focus on industrial / international data spaces
- Consistent with DSBA convergence paper (especially the unifying conceptual model)
- Builds on top of IDS-RAM4.0 by IDSA
- Consistent with Gaia-X architecture
- Consistent with NIST cloud federation
- Includes additional innovations from Huawei based on Hua-X.2.0 contributions

Dynamic trust assessment

Overarching research problems in trust assessment

Problem 1: Trust levels need to be measured and assessed based on incomplete and/or subjective information provided with uncertainty by potentially untrustworthy sources

- the verification of assurance of trust anchors or attesting evidence is not always possible
- data sources that attest evidence cannot be assured with certainty
- evidence is not direct and is obtained through a referral chain of trust



Problem 2: The referral chains used build trust can change during run-time

Problem 3: No implicit or inherent trust between domains is assumed—Zero Trust principles apply

Gap: Emerging need for **dynamic trust assessment** to assess trustworthiness of data and/or claims taking into consideration **trustworthiness of data sources** and **referral chains** in uncertain and **dynamically** evolving situations.

Solution: Trust Assessment Framework (TAF) that brings together

1. creation and maintenance of trust network models & referral graphs [TMM]
2. trustworthiness evaluation of trust network nodes [TSM]
3. algorithms to compute trust on data/observations according to an agent's trust network model [TDE]
4. agent's policies about assessing trust level against expectation and governing the scope of the trust model [TLEE]

DTA-related research papers

1. **Trust Level Evaluation Engine for Dynamic Trust Assessment with Reference to Subjective Logic**, A. Petrovska,, I. Krontiris, T. Dimitrakos, et al, IFIP Trust Management 2023
2. **Continuous Authorization Architecture for Dynamic Trust Evaluation**, H. Joumaa, A. Petrovska, A. Hariri, T. Dimitrakos, B. Crispo, IFIP Trust Management 2023
3. **In-Vehicle Trust Assessment Framework**, A. Petrovska, et al., eSCAR, 2023

CONNECT deliverables

- D2.1: Operational Landscape, **Requirements and Reference Architecture**
- D3.1: Architectural Specification of **CONNECT Trust Assessment Framework**.

Accepted by **CONNECT consortium & CCN PL**

Dynamic Trust Assessment Framework (TAF)

Trust Sources Manager (TSM) & Trust Sources (TS)

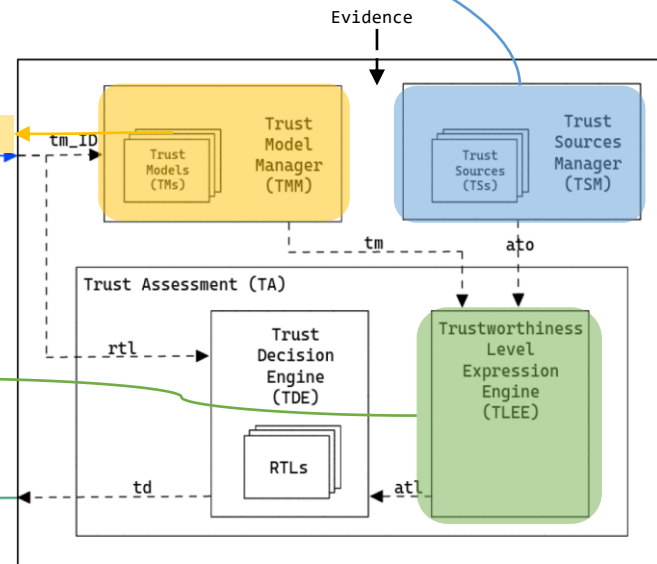
- Selects **trust sources** based on variables under assessment
- Calculates the **trustworthiness** of the relationships from the trust model, based on the **evidence** from the **trust sources**

Trust Model Manager (TMM) & Trust Models

- Deals with creation of the **trust models** – i.e. **trust & referral graphs** – from system models
- Methodology for building and maintaining trust models at design time and maintaining the models at run-time

Trust Level Evaluation Engine (TLEE)

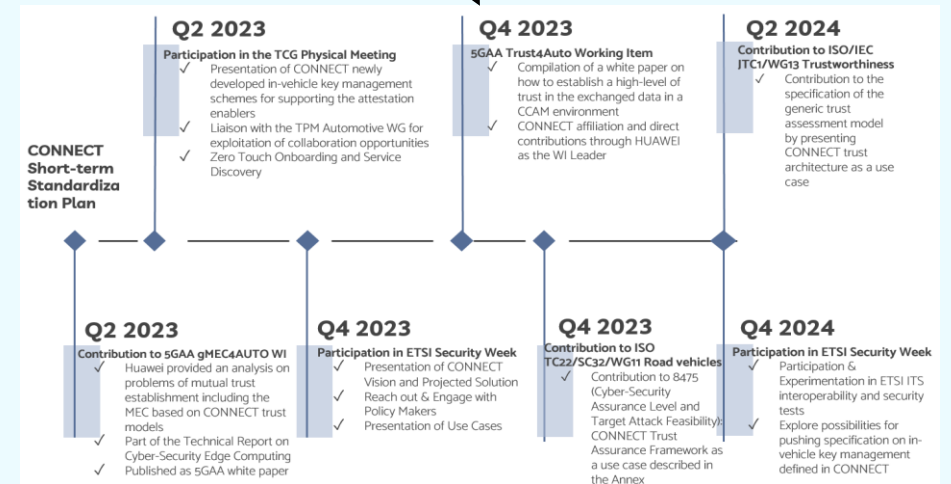
- Applies mathematical algorithm to compute trust level for a given **Trust Model** – i.e. trust & referral graph
- Based on the 1) **advice** by (data) sources and 2) trustworthiness of (data) sources based on both **direct evidence** and **referrals** by trust sources.



TAF High-level Architecture

Standardization efforts overview

Contribution to the 5GAA standardization with definitions on trust and trustworthiness



Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)

A holistic execution approach is required across the entire ecosystem players:

There are several industry associations on play....

Towards a converging Data Space (Security) Architecture

Reference implementation: OSS on Eclipse foundation

Standardization is going global

Competition is investing heavily

An overview of data space projects in Europe

Emerging architectural variants

Huawei contributions in Hua-X and Digital Sovereignty projects: technical

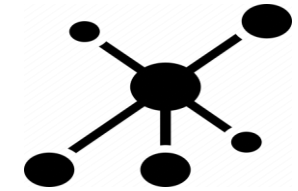
Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap

Recommendations

Appendix I: Core technologies

Appendix II: Data spaces examples

2. Huawei's Industry Research Strategy for Data Spaces Requires 4 Pillars



Regulation

Engagement with relevant industry associations and standardization bodies of the European Commission including ENISA, DGs and DSSC

Work together with PACD and legal experts from CNRS (FR) and Fraunhofer (DE) in order to further analyze regulation for personal and industrial data sovereignty and data spaces as well as related aspects of identity and compliance

Standardization

Participate in GAIA-X and IDSA working groups to shape standards and architecture

Get involved in forthcoming ISO and CEN standardization initiatives

Participate in other relevant standardization initiatives in DIF, W3C, IETF, OASIS, TMF

Implementation

Eclipse Foundation is becoming official open source partner of Gaia-X, Catena-X and IDSA (EDC)

Support Eclipse Open Source project contributions to XFSC and EDC (e.g. via Hua-X2 and DUCA & EU projects)

Bring Open Services Cloud framework and TTE key technologies into XFSC and EDC

Adoption

Leverage and intensify ongoing collaboration with Fraunhofer ISST on industrial data spaces

Establish new collaboration with Fraunhofer SIT and Solid or Prometheus-X community on personal data spaces

Leverage the CONNECT consortium to join EU initiatives in ITS/CCAM data spaces

High-level policy questions

Framing in the current policy debate around digital sovereignty and strategic autonomy

We are trying to distil the key questions from the policy debate which we seek to answer in a white paper

As a first indication, we find the following high-level questions particularly noteworthy:

1. How can we ensure that individuality organizations/states have sovereignty over their digital assets, especially during cross-organizational/international data flow and networks?
2. What policies/regulations can we put in place in order to ensure digital sovereignty in cross-organizational and/or international business workloads?
3. How can a digital sovereignty (virtual) infrastructure enforce the relevant policies/regulations and provide compliance to local regulation and international agreements?

Indicative challenges and topics of interest:

- Typical problems:
 - The difficulty in ensuring territorial sovereignty in the digital realm
 - The difficulty in ensuring (joint) authority across borders
 - The complexity and ambiguity of joint sovereignty, especially between national and operational and operational
- Possible solutions:
 - Rules / standard based framework as a baseline to elaborate the challenge
 - Examples:
 - Gaia-X Trust Framework
 - EU Data Governance
 - CCSP Data Sharing agreement
 - A (virtual) infrastructure to manage the flow of data exchanges (across borders) that underpins digitalization. Examples:
 - International data space: e.g. IDSA, DSSC, etc.
 - European virtual operations and digital ecosystem: e.g. Gaia-X, etc.
 - Personal data spaces, e.g. MyData Global, Digital Garden, etc.
 - CCAM and ITS data sharing: e.g. ECODECO and CONNECT projects
 - Collaborative analysis of Cyber Threat Intelligence: e.g. CCSP projects, etc.

Standardization roadmap: community specifications, open standards & recommendations, international standards

<p>Target Data: ENISA, ENISA, ENISA</p> <ul style="list-style-type: none"> Participate in ENISA's Trust Framework Provide input to ENISA's work on digital sovereignty Participate in ENISA's work on digital sovereignty Participate in ENISA's work on digital sovereignty <p>Background:</p> <ul style="list-style-type: none"> ENISA's work on digital sovereignty ENISA's work on digital sovereignty ENISA's work on digital sovereignty 	<p>Target: ENISA, ENISA, ENISA</p> <ul style="list-style-type: none"> Participate in ENISA's work on digital sovereignty Participate in ENISA's work on digital sovereignty Participate in ENISA's work on digital sovereignty <p>Background:</p> <ul style="list-style-type: none"> ENISA's work on digital sovereignty ENISA's work on digital sovereignty ENISA's work on digital sovereignty 	<p>Target: ENISA, ENISA, ENISA</p> <ul style="list-style-type: none"> Participate in ENISA's work on digital sovereignty Participate in ENISA's work on digital sovereignty Participate in ENISA's work on digital sovereignty <p>Background:</p> <ul style="list-style-type: none"> ENISA's work on digital sovereignty ENISA's work on digital sovereignty ENISA's work on digital sovereignty
---	--	--

Three most important community implementations of data space components: EDC (connector), XFSC (federation), Tractus-X (ecosystem) - all under Eclipse Foundation

<p>EDC (connector)</p> <ul style="list-style-type: none"> Participate in EDC's work on digital sovereignty Participate in EDC's work on digital sovereignty Participate in EDC's work on digital sovereignty <p>Background:</p> <ul style="list-style-type: none"> EDC's work on digital sovereignty EDC's work on digital sovereignty EDC's work on digital sovereignty 	<p>XFSC (federation)</p> <ul style="list-style-type: none"> Participate in XFSC's work on digital sovereignty Participate in XFSC's work on digital sovereignty Participate in XFSC's work on digital sovereignty <p>Background:</p> <ul style="list-style-type: none"> XFSC's work on digital sovereignty XFSC's work on digital sovereignty XFSC's work on digital sovereignty 	<p>Tractus-X (ecosystem)</p> <ul style="list-style-type: none"> Participate in Tractus-X's work on digital sovereignty Participate in Tractus-X's work on digital sovereignty Participate in Tractus-X's work on digital sovereignty <p>Background:</p> <ul style="list-style-type: none"> Tractus-X's work on digital sovereignty Tractus-X's work on digital sovereignty Tractus-X's work on digital sovereignty
--	--	--

Adoption

<p>Leverage existing collaboration for Gaia-X and IDSA</p> <ul style="list-style-type: none"> Leverage existing collaboration for Gaia-X and IDSA Leverage existing collaboration for Gaia-X and IDSA Leverage existing collaboration for Gaia-X and IDSA 	<p>Establish new collaboration on personal data spaces</p> <ul style="list-style-type: none"> Establish new collaboration on personal data spaces Establish new collaboration on personal data spaces Establish new collaboration on personal data spaces 	<p>Leverage the CONNECT consortium to join EU initiatives in ITS/CCAM data spaces</p> <ul style="list-style-type: none"> Leverage the CONNECT consortium to join EU initiatives in ITS/CCAM data spaces Leverage the CONNECT consortium to join EU initiatives in ITS/CCAM data spaces Leverage the CONNECT consortium to join EU initiatives in ITS/CCAM data spaces
---	---	---

High-level policy questions

Framing in the current policy debate around digital sovereignty and strategic autonomy

- We are trying to distill the key questions from the policy debate which we seek to answer in a white paper.

As a first indication, we find the following high-level questions particularly noteworthy:

1. How can we ensure that individuals/ organizations/states have sovereignty over their digital assets, especially during cross-organizational/international data flows and workloads?
2. What policies/regulations can we put in place in order to ensure digital sovereignty in cross organizational and/or international business workloads?
3. How can a digital sovereignty (virtual) infrastructure enforce the relevant policies/regulations and prove compliance to local regulation and international agreements?

- **Indicative challenges and topics of interest:**

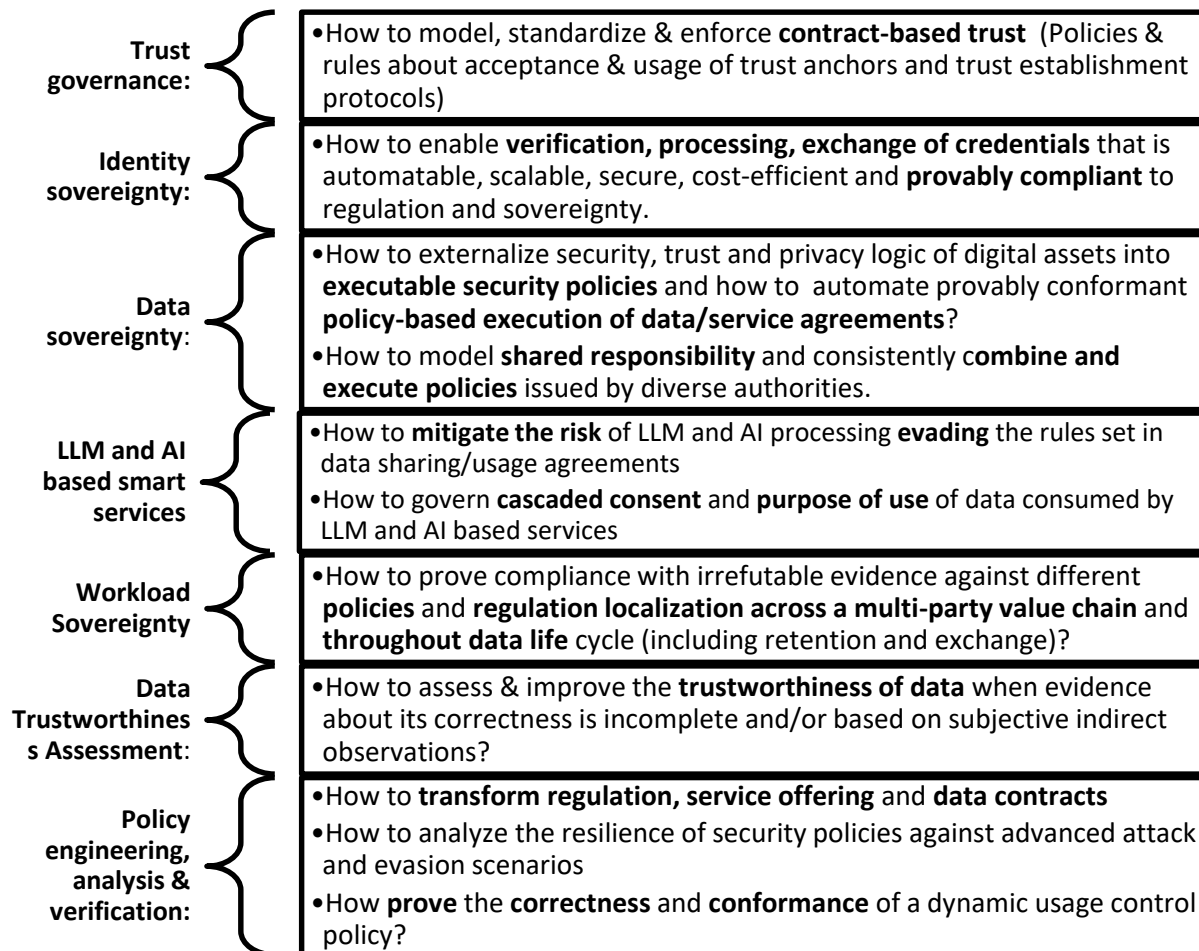
- › Typical problems:
 - » The difficulty in transposing territorial sovereignty to the digital realm
 - » The difficulty to exercise (state) authority across borders
 - » The complexity and inefficiency of joint sovereignty, especially between national and supranational
- › Possible solutions:
 - » **Rule / standard based framework** as a baseline to alleviate the challenge.
Examples:
 - Gaia-X trust framework
 - IDSA data contracts
 - C3ISP Data sharing agreements
 - » **A (virtual) infrastructure to manage the flow of data exchanges (across borders)** that underpins digitalization. Examples:
 - International data spaces - e.g. IDSA, DSSC, etc.
 - Dynamic virtual organizations and digital ecosystems -e.g. Gaia-X, etc
 - Personal data spaces, e.g. MyData Global, Digital Flanders etc
 - CCAM and ITS data sharing -e.g. E-CORRIDO and CONNECT projects
 - Collaborative analysis of Cyber Threat Intelligence - e.g. C3ISP project, etc

High-level socio-technological questions

Furthermore, we would like to address the wider frame of societal and emerging technical issues.

For these issues, we find the following questions relevant:

1. How can we ensure not just technical interoperability across an ever wider range of platforms, interfaces, etc. but also provide practical solutions to manage one's data assets in a sovereign manner?
2. Digital IDs and authentication will become a central building block for future digital ecosystems. How can we ensure that individuals, organizations, and states can obtain, manage and use digital IDs for their purposes whilst remaining compliant to national legal frameworks?
3. How do we manage the trade-off between privacy and user friendliness for digital IDs and authentication?
4. What will be the impact of LLMs and AI in general on digital sovereignty?



Standardization roadmap: community specifications, open standards & recommendations, international standards

Trust Framework Agreement

Target: Gaia-X, DSBA, 5GAA

- Influence / steer the Gaia-X Trust Framework
- Propose guidance for Ecosystem specific extension to other DSBA members such as IDSA and/or BDVA
- Introduce Trust Framework Agreement for CCAM in 5GAA
- Align DIF and ToIP with the above Trust Framework models

Background:

- Gaia-X publishes first Trust Framework specification
- ToIP publishes architecture vision with similar concept
- Strong link (via MS and EU industry) between DIF, EDC, Gaia-X

Data Contracts and Usage Control

Target: Gaia-X, DSBA, DSSC, EDC, DUCA

- Influence Gaia-X, IDSA, EDC to steer the adoption of data contracts and usage control.
- Primary Focus: Gaia-X: Architecture, ICAM, Data Exchange
- Secondary Focus: IDSA-RAM, EDC

Background:

- Usage control and data contracts are recognized as important foundational architectural concepts by Gaia-X and IDSA-RAM
- EC selects DUCA consortium to create an ecosystem for usage control (UCON) and DSA
- EDC recognizes the importance of data contracts and executable usage control policies for enacting data contracts among dataspace connectors

Dynamic Trust Assessment

Target: 5GAA, CCAM, CONNECT

- Introduce dynamic trust assessment to 5GAA for CCAM scenario
- Leverage coordinated standardization effort of CONNECT

Background:

- EC selects CONNECT as a strategic CCAM project
- CONNECT has an ambitious standardization plan for ETSI and ISO/CEN

Gaia-X involvement 

Dataspace Standardization 

Trust Framework Agreement

Target: W3C, OASIS

- Standardize TFA in W3C as an extension of VC
- Standardize TFA in OASIS as an extension of SAML

Background:

- W3C: VC, FIDO2, JSON-LD,
- OASIS Open: WS-Fed, SAML, PKCS#11
- OIDF: OpenID, OIDC
- ODRL is standardized by W3C

DSA, UCON for Cloud Services & C-CTI

Target: OASIS Open

- Standardize UCON as an extension of XACML/ALFA
- Standardize DSA leveraging UCON, LegalXML, etc.
- Standardize DSA and UCON profiles for C-CTI

Background:

- OASIS Open
 - XACML access control
 - SAML identity assertions
 - Contract languages: LegalXML, UBL, etc
 - Cloud: TOSCA, OData, CDP, etc
 - Crypto: PKCS#11
 - CTI: CACAO, STIX, TAXII
- OAuth is standardized by IETF
- ODRL is standardized by W3C

Dataspaces standard

Target: CEN/ETSI

- Participate in Hua-X2.0 team contributing to CEN/ETSI EU-Dataspace standard
- Leverage cooperation with Fraunhofer institutes ISST, SIT, IAO and with CNR and CNRS via DUCA to accelerate impact in Europe (DE, FR, IT, ES, FI, GR, IR)

Background:

- CEN started Data Transaction standardization in 2023 and aims to produce EU standard by 2025

Cloud and Digital Sovereignty Standard

Target: ISO/IEC

- Cloud computing and distributed platforms — Framework and concepts for organizational autonomy and digital sovereignty -- [ISO/IEC AWI TS 10866](#)
- Cloud computing — Concepts for multi-cloud and the use of multiple cloud services based on TFA and ICAM spec - [ISO/IEC DIS 5140](#)
- Cloud computing and distributed platforms — Taxonomy for digital platforms include DSaaS [ISO/IEC DTS 5928](#)

Background:

- CEN started Data Transaction standardization in 2023 and aims to produce EU standard by 2025

TFA and Dynamic Trust Assessment for CCAM

Target: CEN/TC 278, ETSI/TS, ISO/TS and EU-ICIP

- Intelligent Transport Systems by ISO/TS -- [ISO/TS 21177](#)
- Intelligent Transport Systems by ETSI/TS - [ETSI TS 103](#)
- New CCAM standards by CEN / C-ITS

Background:

- EC publishes its strategy and long term vision for C-ITS, CCAM, MaaS convergence
- EC establishes the CCAM Single Platform (2019) and CCAM Partnership (2020)

Adoption

Leverage existing collaborations for Gaia-X and IDSA compliant Industrial / International Data Spaces

Leverage and intensify ongoing collaboration with Fraunhofer ISST on industrial data spaces

- Leverage Horizon Europe DUCA project to establish a community for new data usage control innovation
- Become actively involved in Catena-X and EDC together with the Hua-X team and Boot-X collaboration

Establish new collaboration on personal data spaces

- Target Fraunhofer SIT
- Join Prometheus-X community on personal data spaces
- Alternatively Inrupt/Solid

Exploit opportunities in ITS/CCAM data spaces

- Leverage the CONNECT consortium to join EU initiatives in ITS/CCAM data spaces

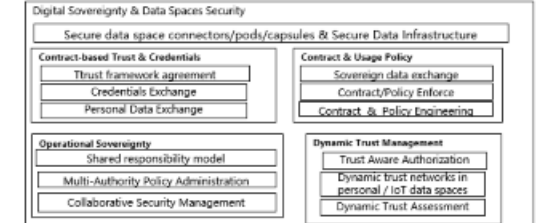
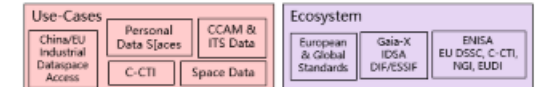
Overview of potential cooperation topics

Cooperation opportunity summary with SIT: regulatory / strategy research priorities

- Analysis of European regulations for data infrastructure
- Analysis of European strategy initiatives and investment plan for data infrastructures
- Analysis of European strategy (regulation and technology innovation investment) in relation to
 - Industry / international data spaces
 - **Personal data spaces**
 - **Data sharing in CCAM & ITS (mobility and integrated transport systems)**
 - Data sharing for Collaborative Cyber Threat Intelligence
 - Digital Sovereignty for Space objects and data
- Analysis of European policy for digital wallets and selective disclosure of credentials
- Analysis of international agreements for data exchange
- Analysis of international agreements about data flow & security in global supply chains
- Analysis of regulation for smart and AI based workloads over sovereign data infrastructures

Cooperation opportunity summary with SIT: technology strategy research priorities

- Threat, security risk and trustworthiness analysis of Huawei's data space architectures
- Comparative analysis of Huawei's data space architectures and European community initiatives
- Use-cases: industrial data spaces**
 - Modelling and engineering of data contracts into data usage policies that can be enacted and monitored by a data space infrastructure
 - Security innovation blue-print of international data space access services for EU / China
 - Security of contract enactment over international data spaces
- Use-cases: Personal data spaces**
 - Overall personal data space architecture analysis
 - Data Linkage and selective disclosure over personal data space
 - Consent management automation
 - Privacy policy enforcement
- Use-cases: IoT data spaces**
 - CCAM & ITS data sharing infrastructure technology analysis and collection of technical requirements for secure data sharing and trustworthiness analysis
 - Proposed data space security architectures for CCAM/ITS
- Use-Cases: Digital sovereignty of space objects and data**
 - Analysis of digital and data sovereignty challenges for space objects and data



Cooperation opportunity summary with SIT: technology stack research priorities

- Contract based trust and credentials: How to model and enforce trust framework agreements to facilitate trust establishment, compliance and credentials exchange in industry/personal/IoT data spaces. Can the concept extend to international data spaces?
- How to optimize and automate consent management and selective disclosure of credentials in personal data spaces?
- How to model, engineer, enforce and audit / attest the enforcement of data (usage/exchange) contracts in data spaces. Bridge the gap between legal text and data space policy
- Security risk analysis of Huawei's data usage control technology and comparison
- User-friendly presentation, authoring and analysis of data sovereignty / data usage policy
- Data usage control policy enforcement aided by MPC / PEC

Proposed cooperation mechanisms

Thematic priority	Proposed mechanisms
<ul style="list-style-type: none"> • Personal Data Spaces • Mobility / ITS Data Spaces 	<ul style="list-style-type: none"> • EU funded projects • National Funded projects • Joint community contributions • Standard contributions



Overview of potential cooperation topics

Cooperation opportunity summary with SIT: regulatory / strategy research priorities

- Analysis of European regulations for data infrastructure
- Analysis of European strategy initiatives and investment plan for data infrastructures
- Analysis of European strategy (regulation and technology innovation investment) in relation to
 - Industry / international data spaces
 - **Personal data spaces**
 - **Data sharing in CCAM & ITS (mobility and integrated transport systems)**
 - Data sharing for Collaborative Cyber Threat Intelligence
 - Digital Sovereignty for Space objects and data
- Analysis of European policy for digital wallets and selective disclosure of credentials
- Analysis of international agreements for data exchange
- Analysis of international agreements about data flow & security in global supply chains
- Analysis of regulation for smart and AI based workloads over sovereign data infrastructures

Cooperation opportunity summary with SIT: technology strategy research priorities

- Threat, security risk and trustworthiness analysis of Huawei's data space architectures
- Comparative analysis of Huawei's data space architectures and European community initiatives

Use-cases: industrial data spaces

- Modelling and engineering of data contracts into data usage policies that can be enacted and monitored by a data space infrastructure
- Security innovation blue-print of international data space access services for EU / China
- Security of contract enactment over international data spaces

Use-cases: Personal data spaces

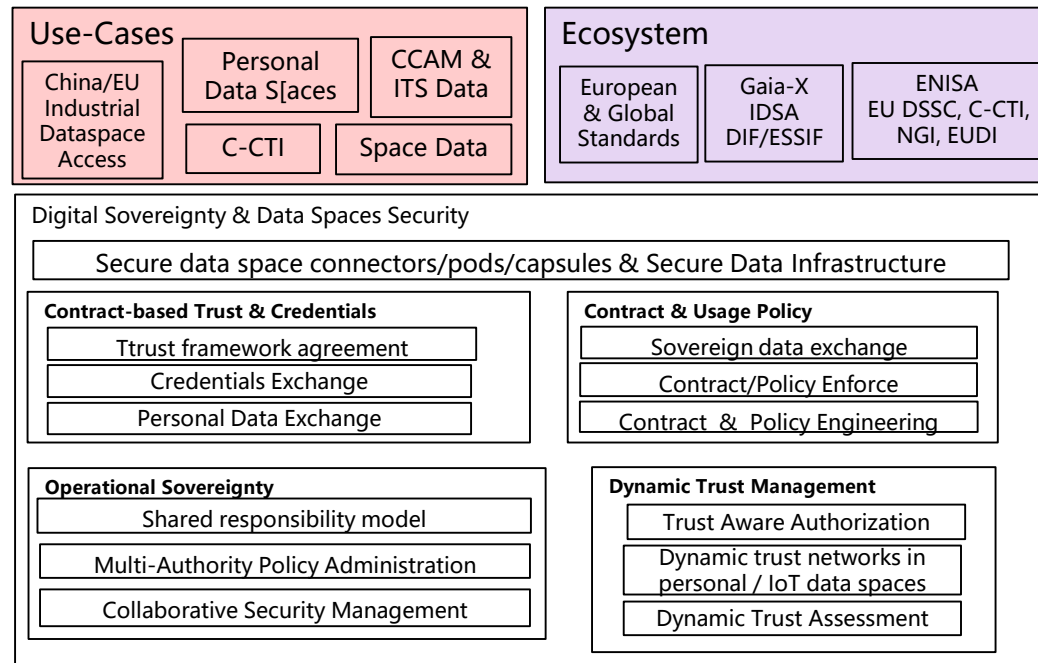
- Overall personal data space architecture analysis
- Data Linkage and selective disclosure over personal data space
- Consent management automation
- Privacy policy enforcement

Use-cases: IoT data spaces

- CCAM & ITS data sharing infrastructure technology analysis and collection of technical requirements for secure data sharing and trustworthiness analysis
- Proposed data space security architectures for CCAM/ITS

Use-Cases: Digital sovereignty of space objects and data

- Analysis of digital and data sovereignty challenges for space objects and data



Cooperation opportunity summary with SIT: technology stack research priorities

- Contract based trust and credentials: How to model and enforce trust framework agreements to facilitate trust establishment, compliance and credentials exchange in industry/personal/IoT data spaces. Can the concept extend to international data spaces?
- How to optimize and automate consent management and selective disclosure of credentials in personal data spaces?
- How to model, engineer, enforce and audit / attest the enforcement of data (usage/exchange) contracts in data spaces. Bridge the gap between legal text and data space policy
- Security risk analysis of Huawei's data usage control technology and comparison
- User-friendly presentation, authoring and analysis of data sovereignty / data usage policy
- Data usage control policy enforcement aided by MPC / PEC

Proposed cooperation mechanisms

Thematic priority	Proposed mechanisms
<ul style="list-style-type: none"> • Personal Data Spaces • Mobility / ITS Data Spaces 	<ul style="list-style-type: none"> • EU funded projects • National Funded projects • Joint community contributions • Standard contributions



Compliance with the upcoming EU Data & Cloud regulations is mandatory but offers market opportunities in EU AND CN (and beyond)

A holistic execution approach is required across the entire ecosystem players:

There are several industry associations on play....

Towards a converging Data Space (Security) Architecture

Reference implementation: OSS on Eclipse foundation

Standardization is going global

Competition is investing heavily

An overview of data space projects in Europe

Emerging architectural variants

Huawei contributions in Hua-X and Digital Sovereignty projects: technical

Huawei contributions in Hua-X and Digital Sovereignty projects: community & roadmap

Recommendations

Appendix I: Core technologies

Appendix II: Data spaces examples

Identity

Capability view:

Thematic view:

Trust agreement model, life-cycle, enactment

Adaptive, compliant, intelligent Credentials exchange

Cascaded, conditional consent Selective disclosure

evidence, proofs (e.g. ZKP), distributed attestation

1 Trust Governance Framework

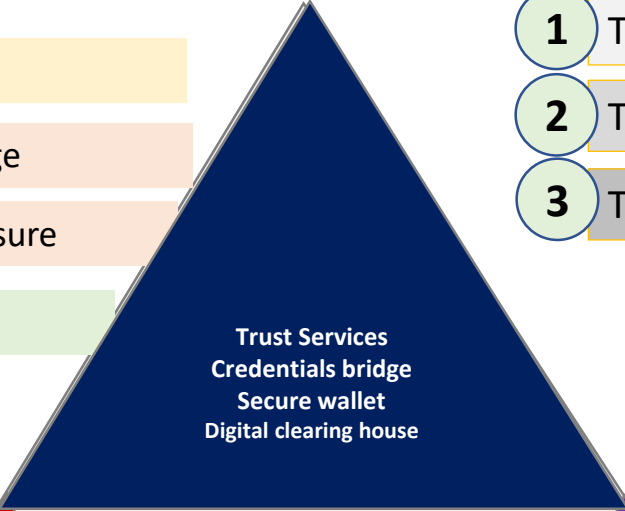
2 Trustworthy Data Exchange

3 Trust Assessment Framework

Dynamic Contract

Dynamic Policy

Dynamic Trust



Trust Services
Credentials bridge
Secure wallet
Digital clearing house

Future digital space

Data Sharing Agreement

Data exchange security policy

Consent, selective disclosure

Trustworthiness (QoT/QoM)
assessment of data exchange

Provenance, Traceability,
Data clearing house

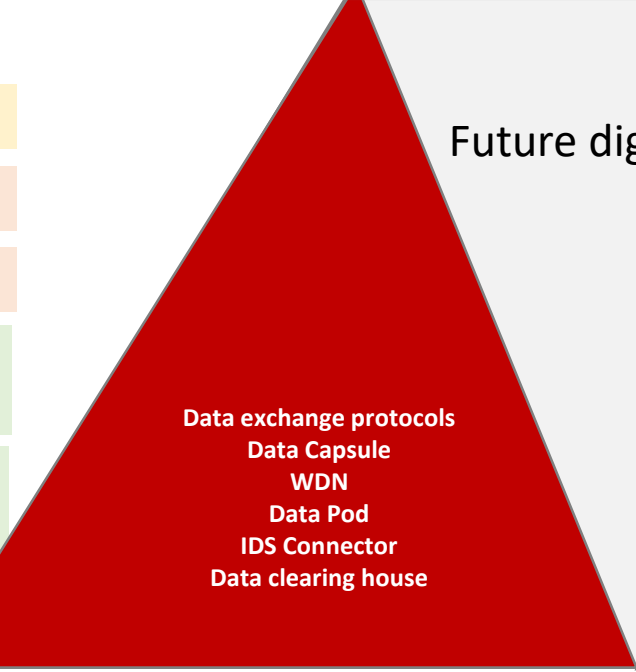
AI/workload Agreement

Compute-to-data

Consent, transparency

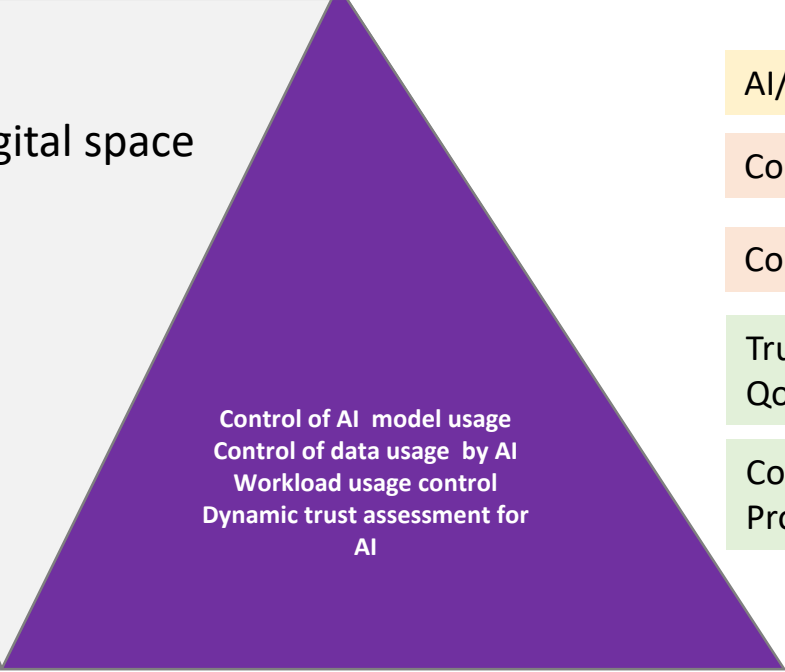
Trustworthiness assessment (QoT,
QoM) of AI data and model use

Compliance, traceability,
Proof of conformity



Data exchange protocols
Data Capsule
WDN
Data Pod
IDS Connector
Data clearing house

Data

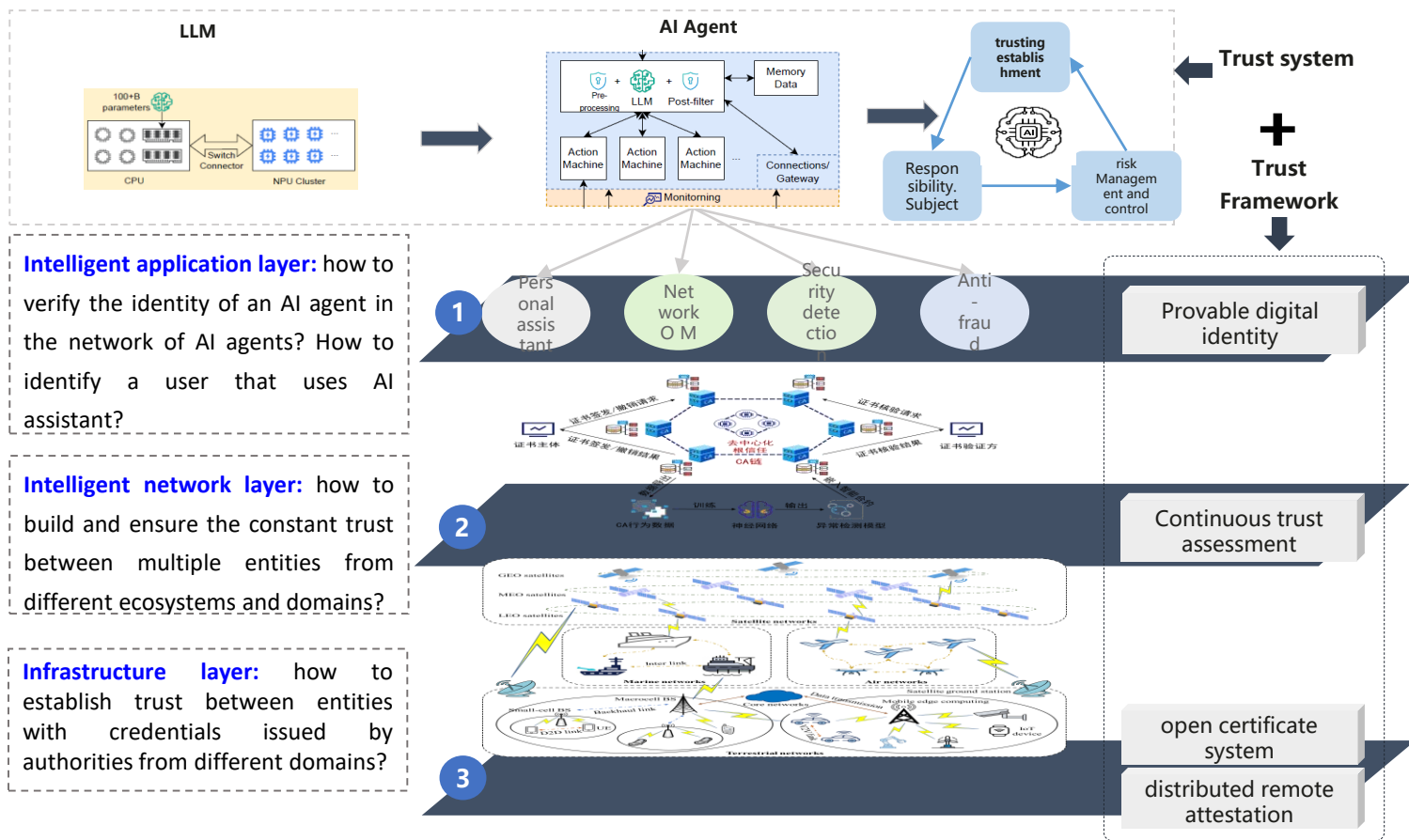


Control of AI model usage
Control of data usage by AI
Workload usage control
Dynamic trust assessment for
AI

Algorithm

Target

1. Research the verifiable digital identities to govern trust within the digital space ecosystem, make breakthroughs in the distributed remote attestation of devices, identities and AI agents, and enable the development of new trust governance services.



Intelligent application layer: how to verify the identity of an AI agent in the network of AI agents? How to identify a user that uses AI assistant?

Intelligent network layer: how to build and ensure the constant trust between multiple entities from different ecosystems and domains?

Infrastructure layer: how to establish trust between entities with credentials issued by authorities from different domains?

Key technology planning

Intelligent application layer

- Use digital signatures to verify the authenticity of messages exchanged between AI agents.
- Each AI agent must have a unique digital signature and the verification process ensures the integrity and origin of the communication.
- Utilize OAuth tokens to facilitate secure authorization and authentication between AI agents, ensuring that only authorized agents can interact with specific functionalities.

Intelligent Data & Network Layer

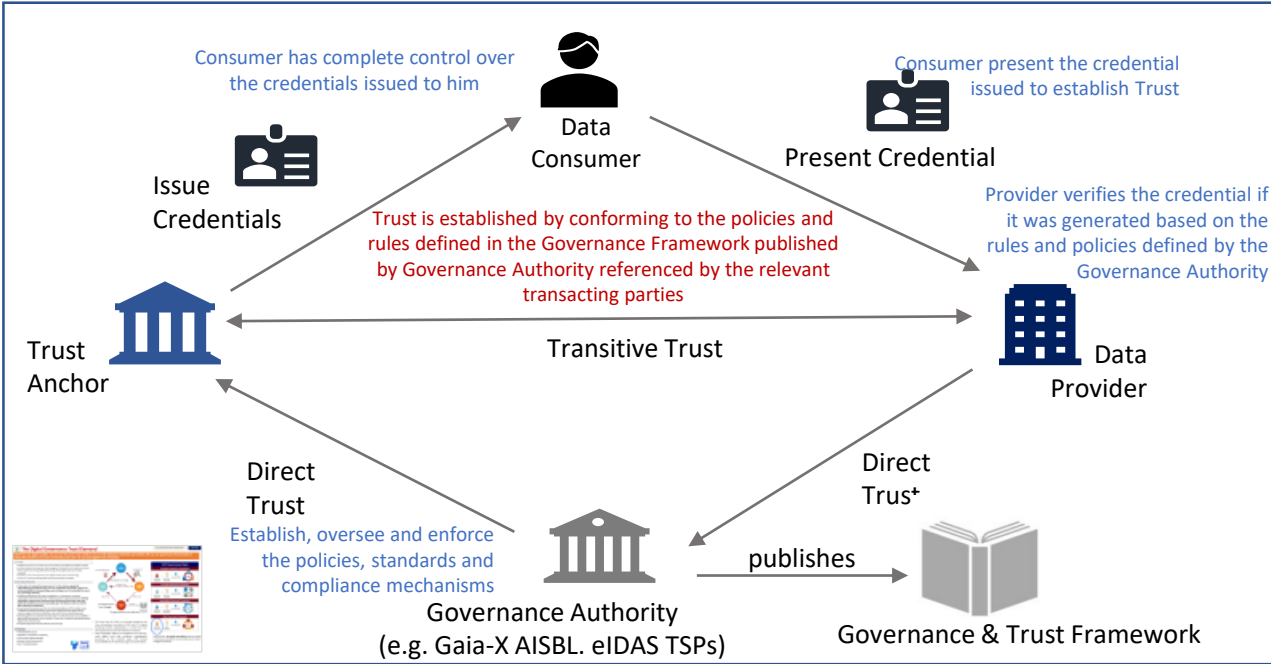
- Leverage decentralized data/digital clearing houses for a tamper-resistant ledger that records interactions and transactions between AI agents, enhancing trust and accountability.
- Establish a comprehensive data governance framework that defines roles, responsibilities, and policies for data management, ensuring consistency and accountability across different domains.
- Incorporate robust consent mechanisms that allow entities to explicitly define the scope and duration of data sharing, promoting transparency and trust in data transactions.

Cloud service and Infrastructure Layer

- Trust Governance Framework facilitates implementation of a secure and standardized cross-domain authentication mechanism to verify the identities of entities from different ecosystems enhancing trust.
- Use of a credential bridge to facilitate interoperability between different authentication systems

1 Trust Governance Framework: Concept

Trust Frameworks specify a set of rules and policies that define the minimum baseline to be part of decentralized ecosystem



Trust Governance Examples



1. GAIA-X:

- Governing Authority: Governed by a consortium of European businesses, research institutions, and government entities
- Focuses on federated trusted statements to reassess the validity of claims, ensuring interoperability and data sovereignty in a cloud-based, decentralized infrastructure. Utilizes verifiable credentials and linked data representations as key components



2. Trust over IP (ToIP):

- The governance is decentralized, with multiple working groups and committees collaborating to develop the standards, policies, and technical frameworks
- Employs a layered architecture combining technical standards (like DID and VC) and governance models.
- Differentiates itself by emphasizing decentralized identity solutions, integrating them with blockchain and distributed ledger technologies for enhanced trust and privacy



3. eIDAS:

- Governing Authority: National supervisory bodies are responsible for overseeing the compliance and enforcement of these standards
- Centers on legal recognition and standardization of electronic identification and trust services in EU.
- Prioritizes the use of Public Key Infrastructure (PKI) for electronic signatures and digital certificates, ensuring legal equivalence and security
- Distinct in its approach to cross-border interoperability



4. Data Spaces Business Alliance (DSBA):

- Focuses on creating a collaborative environment for data governance and standardization across various industries
- Prioritizes interoperable data exchange and management within a legal framework, emphasizing compliance with regional data laws

Trust Governance in Digital Space

Trust Governance Framework with **Trust Framework Agreements** enable **contract-based trust** between participants, support **Policy-based Data Exchange** and scope **Data usage policies**.

Contract-based trust

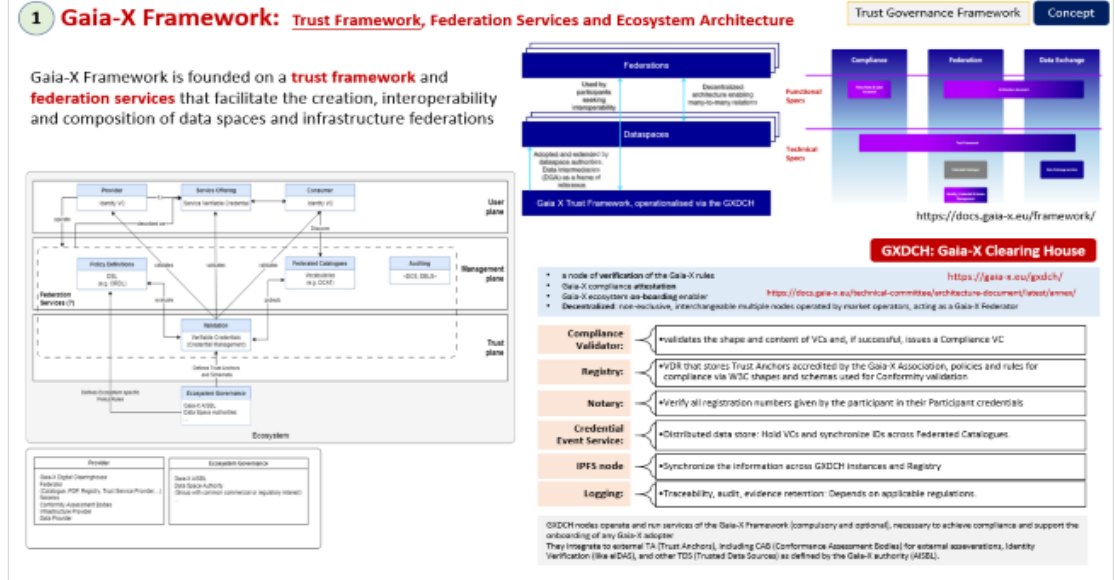
- e.g.
- Industry certifications (ISO, CC, etc.), Gaia-X compliance
 - Employee credentials & professional certification
 - Regional certifications, international association
 - Technological roots of trust and attestation protocols

Policy based Data Exchange

- e.g.
- Geo Data only Anonymized
 - No Exchange of local images
 - Sensor and Maintenance Data OK
 - Exchange of contracts, documentation OK

Data usage policy (enact within scope of DSA + TFA)

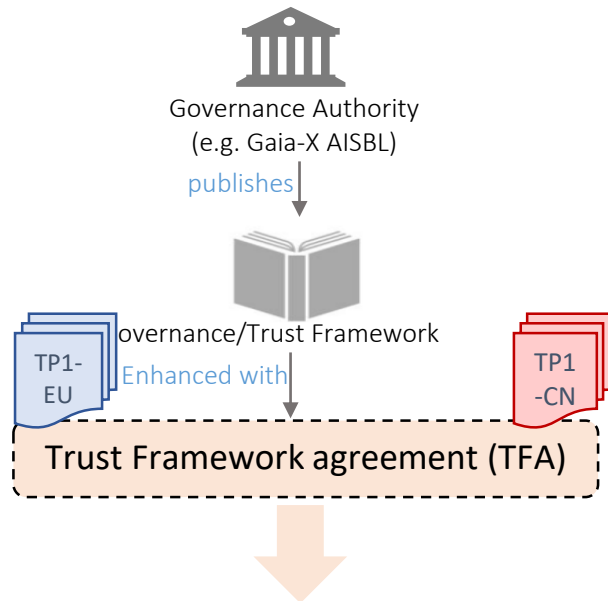
- e.g.
- No disclosure of health condition, income
 - Must inform authorities of every access
 - Cannot forward



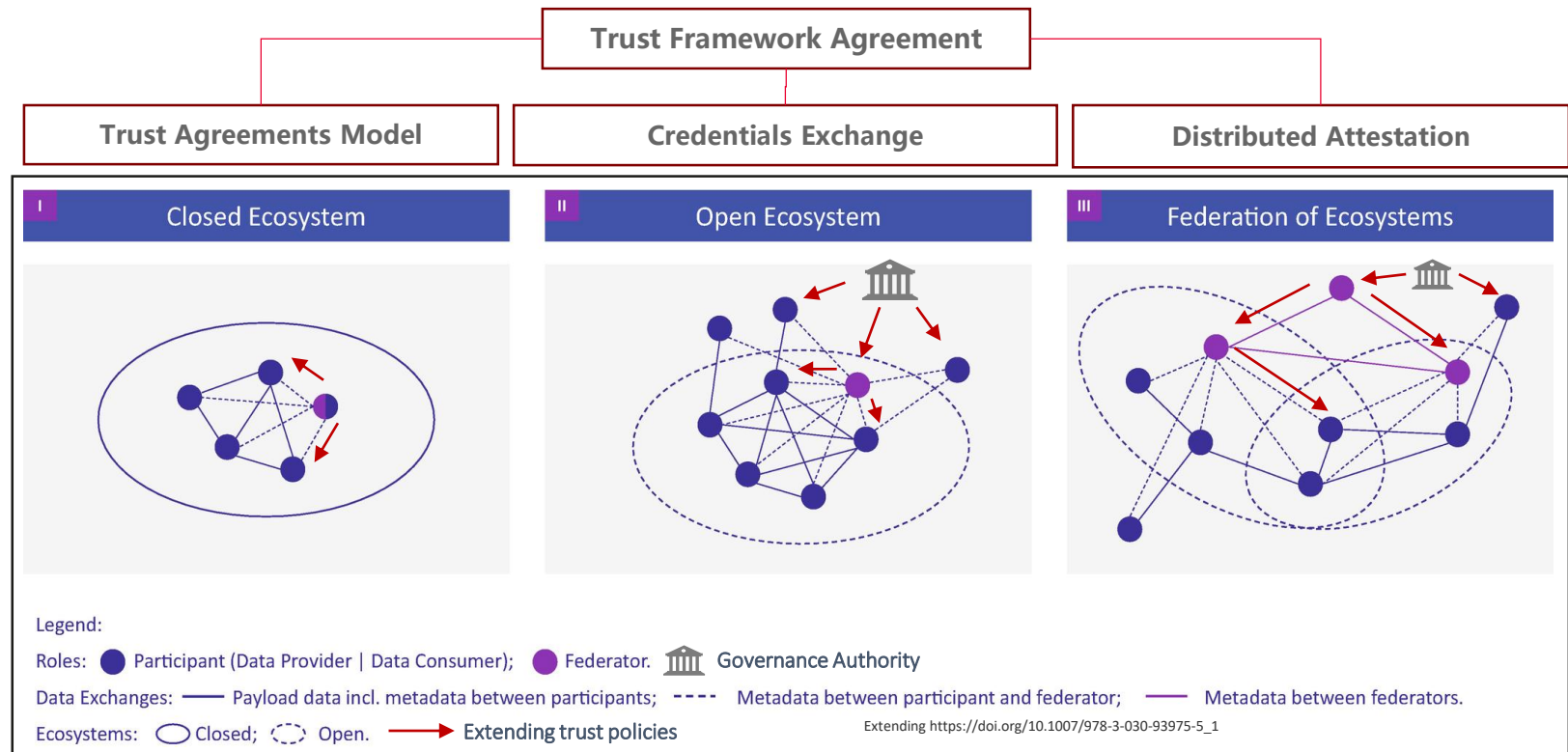
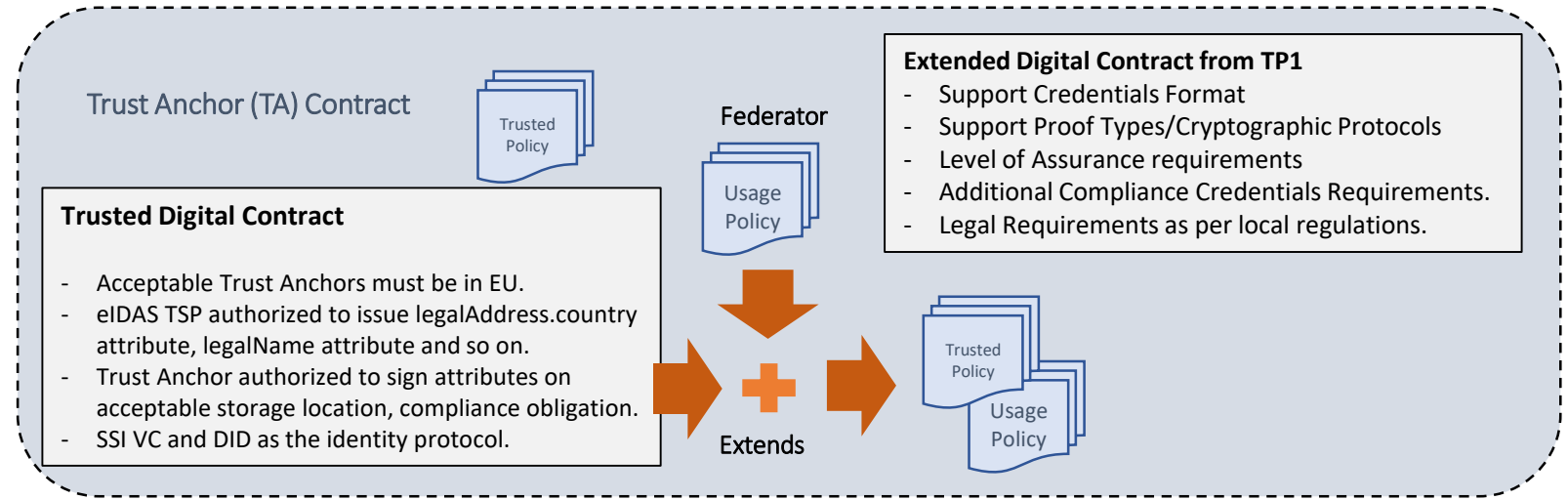
1 Trust Governance Framework

Contract-based Trust (Trust Framework Agreement) enables international and decentralized Ecosystems with

- Transparency & Fairness
- Regional & Ecosystem conformity
- Identity protection & verifiability
- Mitigate the risk of bias and exclusion (through ecosystem-wide agreement)

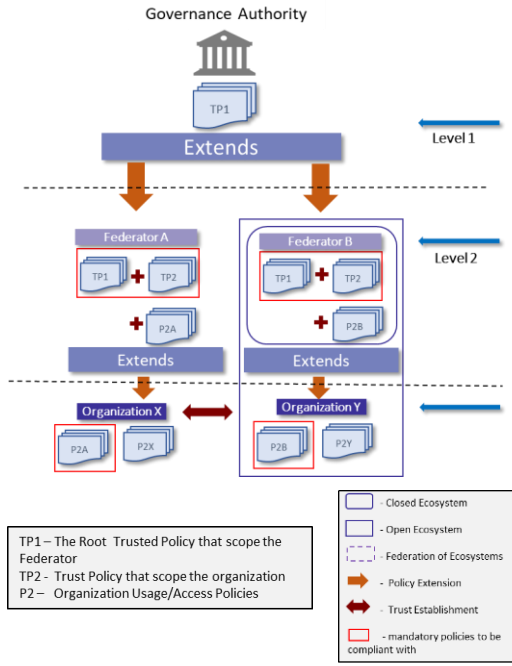


TFAs are **enactable digital contracts** about trust anchors (TAs) that state permissions, prohibitions and obligations in using trust anchors and the credentials they produce. TAs include state, organization, CAB, technological root of trust



1 Trust Agreement Model

The **trust framework** defines extensible policies and rules that govern how participants in an ecosystem or Federation of ecosystems establish trust. TFAs are **enactable digital contracts** about trust anchors (TAs) that state permissions, prohibitions and obligations in using trust anchors and the credentials they produce. TAs include state, organization, CAB, technological root of trust



Problem

- The higher authority set a scope within which the extended policy can operate.
- Federation at **Level 2** (Fed A and Fed B) extends TP1 to ecosystem-trusted policies (TP2 and TP3) that participants must comply with. Trusted Policies ensure fairness of the Federator by scoping their capabilities concerning the higher authority.
- Example, the Federation cannot define policies that will exclude any participant due to geopolitical reasons since the Federator operates within the scope defined by the governance body using TP.

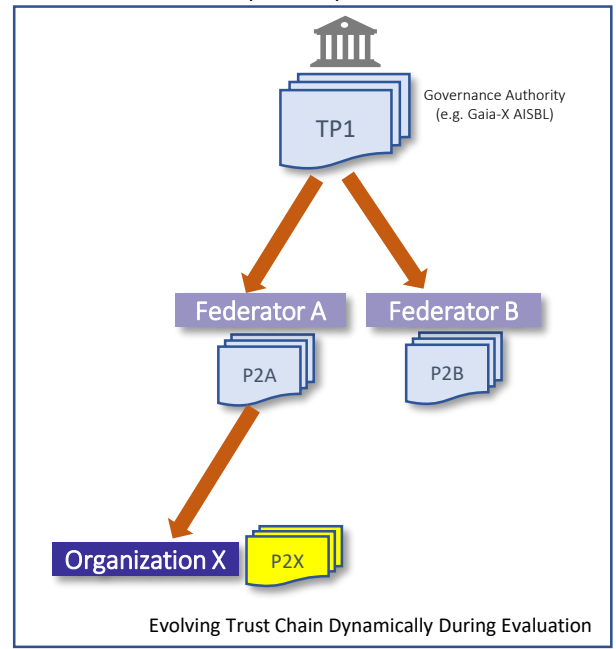
Research questions

- The policies are distributed among different entities. The challenge lies in evaluating these policies during runtime, posing an architecture/protocol challenge.
- The scope of Trust Policies (TP) can indeed encompass rules that determine whether a series of cascading data exchanges is trustworthy.
- The TP policies between federators and organizations are interconnected, forming dynamic rules. A framework is required to evaluate these policies collectively: monitoring policy compliance chain wise (e.g. **P2Y-> P2B -> TP2->TP1**)

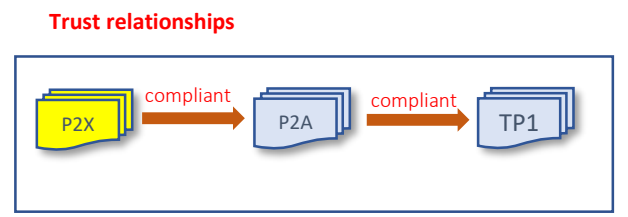
Trust Chain

- Concept:**
- The **trust framework** evaluates whether an organization/entity with local policies is trusted by assessing its compliance with multiple trust policies.
 - A **trust chain** represents a sequential link of trust relationships between entities. In this chain, entities or components establish and verify trust with one another, forming a hierarchical structure. Each link in the trust chain relies on the reliability of the preceding link, ultimately leading back to a trust anchor. The system propagates trust, providing the foundation for trust establishment.
 - Policy Constraint on Another Policies:** The trust policy may impose scope or requirements on another policy, creating a tree of interdependencies. These constraints serve as a mechanism to coordinate and align policies together.
 - Multi-Author Policies:** The trust policies involve multiple authors and multiple federations. Managing multi-author policies during run time evolution requires effective coordination, explicit dependencies, and enforcement mechanisms.

The trust chain among multi-author trust policies forms a dynamic tree created based on constraints and attributes, with explicit dependencies and robust enforcement mechanisms ensuring a harmonized and secure trust framework. The dynamically evolving tree, assessed during runtime evaluation, shapes the trust relationship.



TP1, P2A, P2B – Trusted Policies
P2X – Organization policy



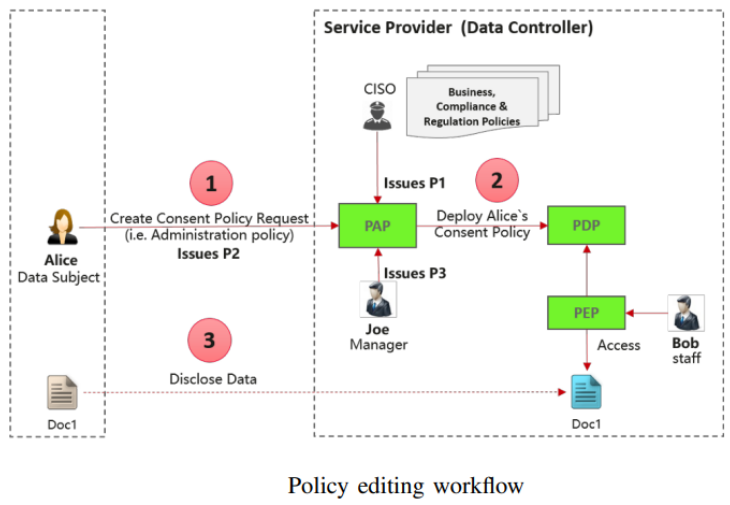
1 Trust Agreement Model

Administration and Delegation Profile (ADP) - Background

- The ADP allows administrators to write policies about other policies forming trees that start with top level policies designated as root of trust.
- Usage Policy will not be enforced unless it is explicitly authorized by Administrative Policies. Thus, a Usage Policy can be Admissible if its enforcement is authorized by all upper layer policies, or **NotAdmissible** if one of the Administrative Policies in the hierarchy cannot be considered.
- The policy evaluation flow can be summarized in two different steps: **reduction** and **combination**

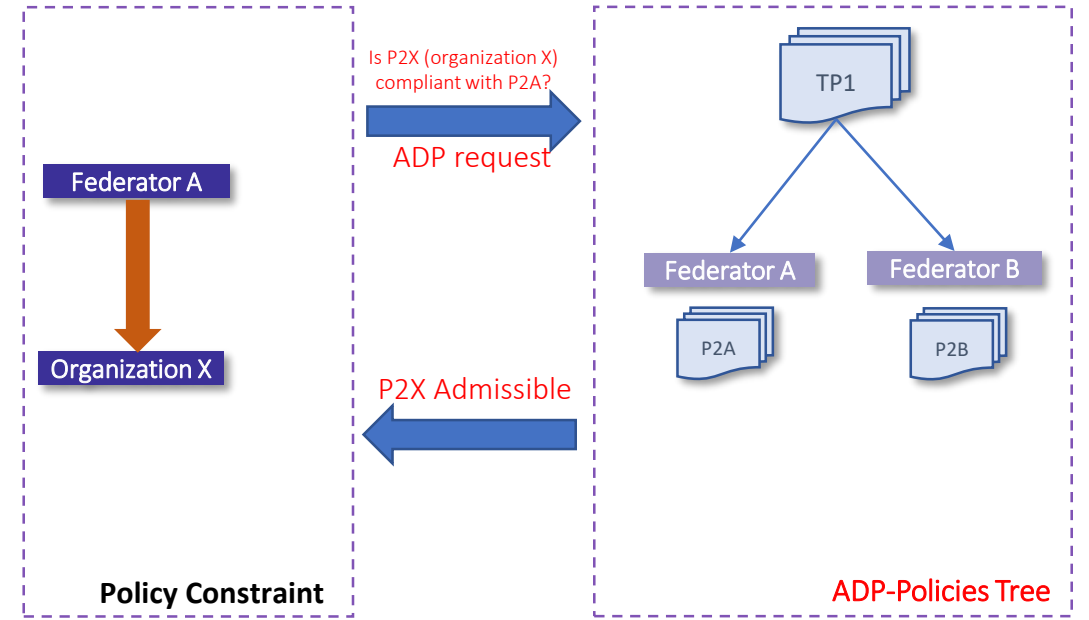
Reduction determines whether a usage policy was written by an authorized personnel and whether the evaluation outcome can be considered or not. This is achieved by creating an evaluation tree having as root node a **root-of-trust** policy and as edges the results of applicable policies, then finding the branches that can reach the root-of-trust.

Combination step, the PDP combines all valid results using combining algorithms defined in the policies



Trust Agreement Model using ADP

- The Trust Policies (TP) between entities can be viewed as Administrative and Delegation Policies (ADP), where each participant defines the scope of the agreement and delegates it to the federators/participants.
- ADP enables administrators to craft policies about other policies, creating trees that begin with top-level policies designated as the root of trust.
- ALFA policy uses "PolicyIssuer," "Attributes.delegate attribute", and "Attributes.delegation-info", which are used to create an administrative request.
- The higher authority set a scope within which the extended policy can operate.
- Root-of-trust policies that encode regulations defining the actions data owners and data processors can take regarding the data.

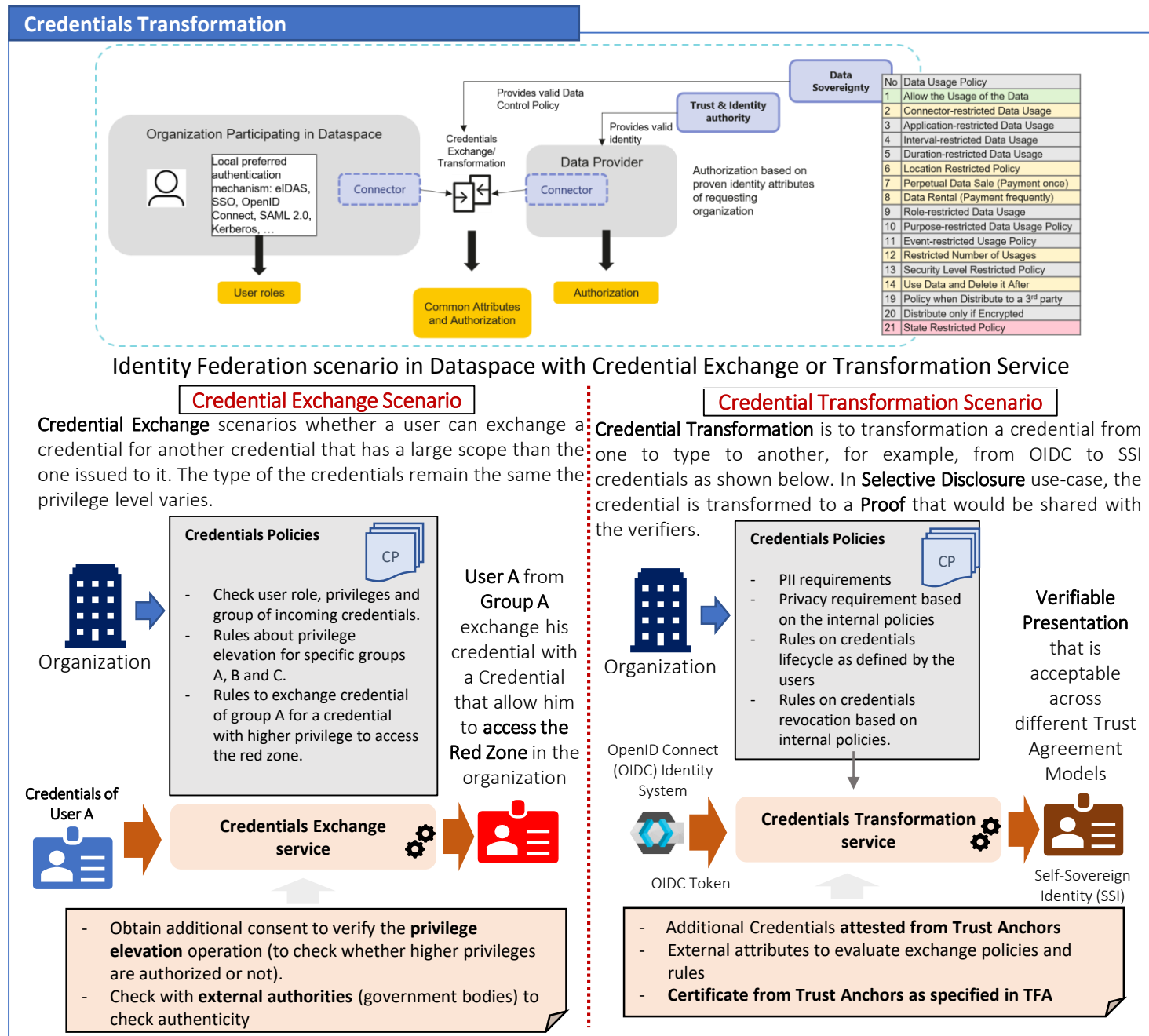


TP1, P2A, P2B – Trusted Policies
P2X – Organization policy

- The baseline technology that does a policy-based transformation or exchange of credentials from one type to another.
- The technology is **Adaptive** to different use-cases and trust models due to the policy-based approach. The business logic of how the credentials need to be transformed or exchanged are encoded as policies.
- The integration with Trust Governance Framework enable transformation or exchange credential in **Compliance** with Trusted Policies that scopes the usage of the new Credential.
- The Credentials Transformation or Exchange service technology can be adopted to different contextual changes and operate in an intelligent manner enabling it provider better services with minimal intervention.
- Enabling **selective disclosure** to minimize identity footprint, granular consent

Challenges

- Collecting the evidence of credentials exchange
- Integrating with different Trust Frameworks and being compliant with multiple policy systems.
- Improving the Trustworthiness of the credential exchange services
- Building trust between parties involved in the exchange and ensuring the validity and authenticity of exchanged credentials.
- Implementing effective mechanisms for managing the revocation and expiration of exchanged credentials to maintain data accuracy and security.
- Overcoming the technical complexities of implementing zero-knowledge proofs for credential exchange to enable verification without revealing sensitive information
- Resolving the challenges associated with translating and mapping credentials between different formats and schemas to ensure seamless interoperability.
- Dynamic consent management, cross-domain consent handling, legal harmonization while establishing selective disclosure

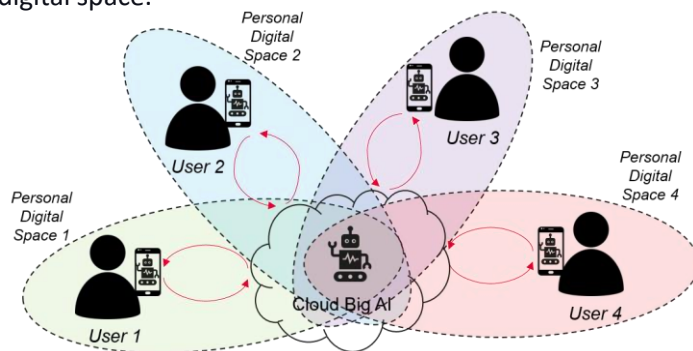


1 Delegation of an Action from entity to entity

A user relies on an AI assistant to delegate authority for online services. The AI assistant, equipped with the user's preferences and budget constraints, autonomously performs tasks defined by a user reducing the user's direct involvement in the decision-making process.

Problem

- Multiple user accounts may share AI agents. Ensuring that each user has appropriate permissions while interacting with AI agents is essential in maintaining security and integrity for each account.
- The AI agents perform actions beyond the scope of the original query, which necessitates a mechanism for user consent and authority delegation. Applications may require the AI agent to perform delegated tasks without compromising the user.
- Define the scope of a delegated authority to an AI assistant for managing personal digital space.



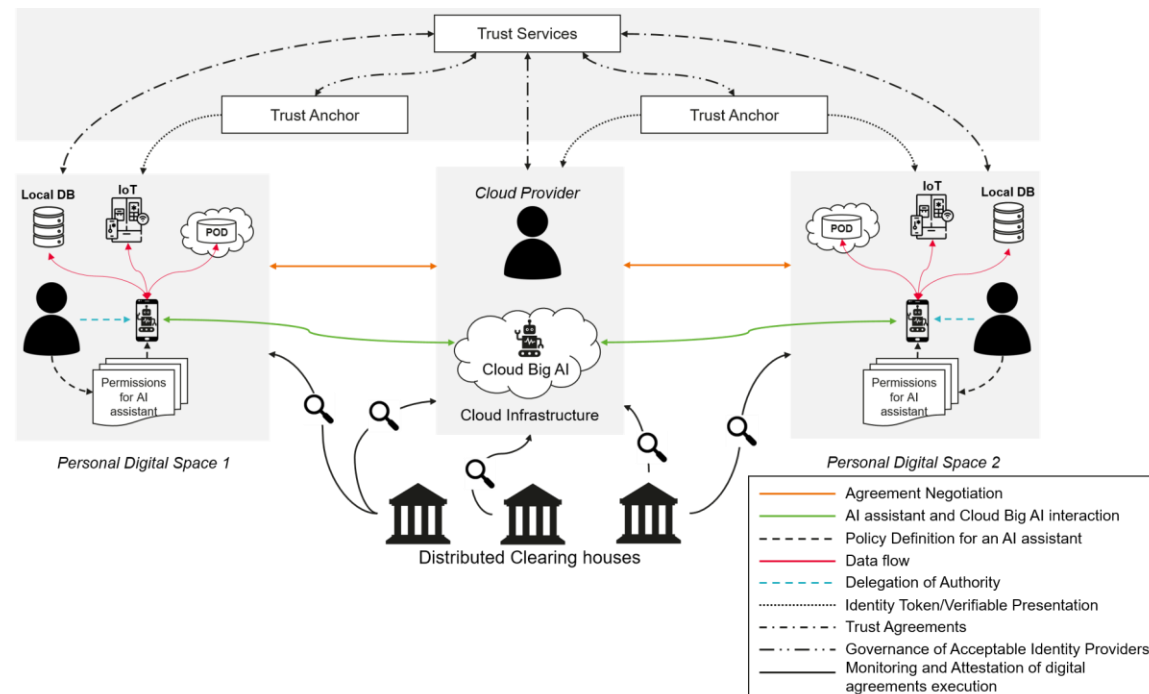
Research questions

- Investigate the potential bias in the decision-making algorithms of the AI assistant to ensure fair and unbiased choices, especially when dealing with diverse user preferences and socio-economic backgrounds.
- Research methods to enhance the security and privacy aspects of the AI assistant's autonomous decision-making, addressing issues such as data protection, secure communication, and preventing unauthorized access to sensitive user information.
- Explore ways to empower users with greater control over the AI assistant's decision-making process, allowing them to easily intervene, modify, or override decisions to align with their evolving preferences or unexpected changes in circumstances

Delegation of Actions

Trust framework and distributed data and digital clearing houses are used to enhance trust through the accountability and traceability of operations and data flows between different AI agents and user's AI assistant:

- The digital space emphasizes enforcing access control privacy obligations to ensure that data exchange between client AI agents and the cloud is accompanied by the correct fulfillment of privacy obligations, such as anonymization.
- Research explores techniques related to the Trust Level Evaluation Engine for ensuring data integrity and authenticity in distributed systems. The focus is on robust mechanisms to verify the trustworthiness of data exchanged with the cloud.
- Examine methods for implementing secure access controls and authorization mechanisms, particularly in cloud environments, to ensure that only authorized entities can handle and process sensitive data securely.
- Investigate decentralized trust services protocols and techniques for building mutual trust between entities.
- Digital Spaces can support the commercial AI model provider with evidence collected from clearing houses and ensure that the digital ecosystem consists only of trustworthy stakeholders



Distributed Remote Attestation

The **distributed remote attestation** is a crucial security service that allows a *remote verifier* to assess the state of an *untrusted remote prover* (device). As the number of *Internet of Things (IoT)* devices continues to rise, ensuring their security becomes increasingly important.

The remote attestation ensure the reliability of evidence such that the participants in a digital space can check the trustworthiness of credentials issued by the Trust anchors.

Types:

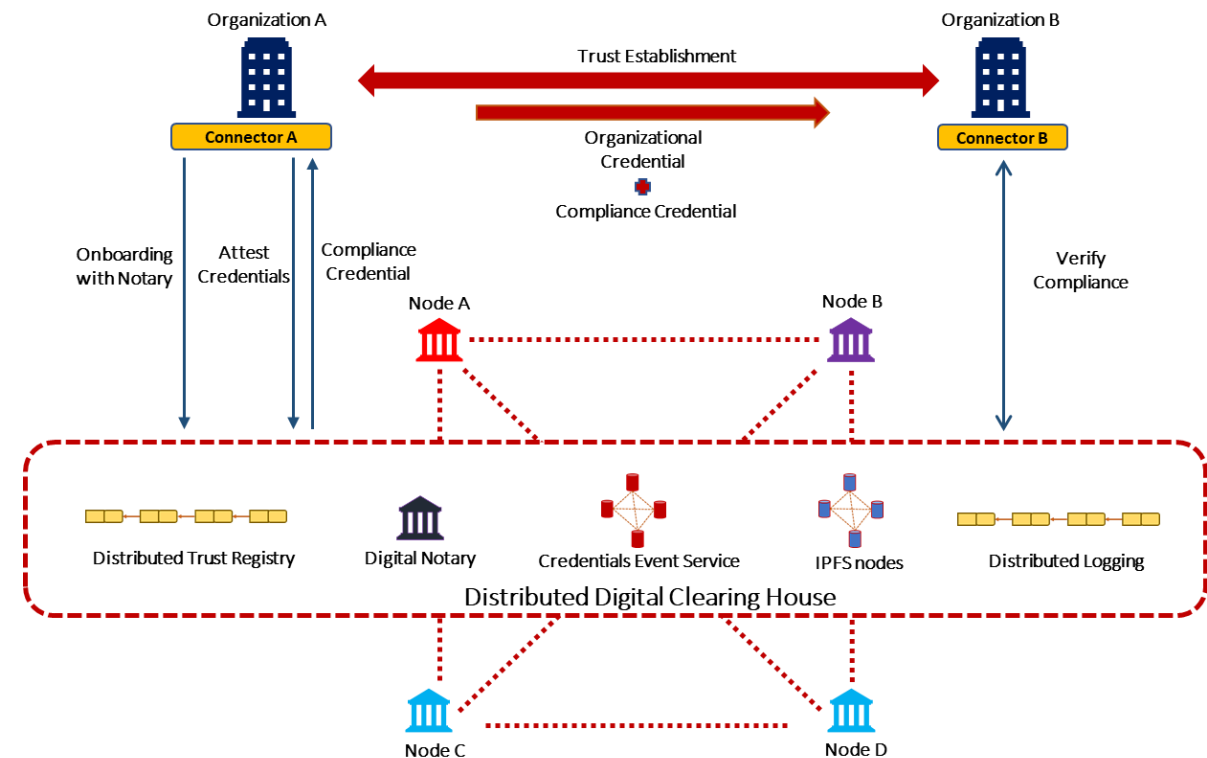
- **Paradigms of Remote Attestation:** *Software-Based Attestation, Hardware-Based Attestation, Hybrid Attestation*
- **Traditional Remote Attestation Protocols** - focus on reasoning about the state of a prover device.
- **Swarm Attestation** - as interconnected IoT devices form swarms, attesting their collective state becomes essential

Challenges

- **Scalability:** Traditional challenge-response remote attestation protocols between the verifier and a single prover face a severe scalability challenge when they are applied to large scale IoT systems 2.
- **Trustworthiness:** The measurement, quote generation, and reporting done by trustworthy TCB (Trusted Computing Base) is critical for remote attestation 1.
- **Constrained disclosure:** Attester can decide what information can be sent to verifiers without revealing confidentiality and privacy 1.
- **Technical capabilities:** Technical capabilities for updating whitelists, validating, verifying, and evaluating attestation reports are necessary for

Delegation of Actions

- **Distributed Trust Registry:** Manages the list of Trust Anchors in an immutable manner. The Trust Anchors are decide based on policies that is scoped by the governance authority defined Trust Governance Agreements. There are various technology that could be used to implement this such as Blockchain, DLT or TRAIN.
- **Digital Notary:** The notary helps with onboarding by attesting the registration number of the organization. The attestation from the notary is necessary to ensure compliance.
- **Credentials Event Service:** A distributed storage solution that holds compliant credentials usually in the form of Verifiable Credentials (VCs) and helps with publishing compliant services through federated catalogues. This is usually implemented using Interplanetary File System (IPFS) nodes.
- **Distributed Logging:** Logs the credentials issuance events for the purpose of traceability, audit and evidence retention.



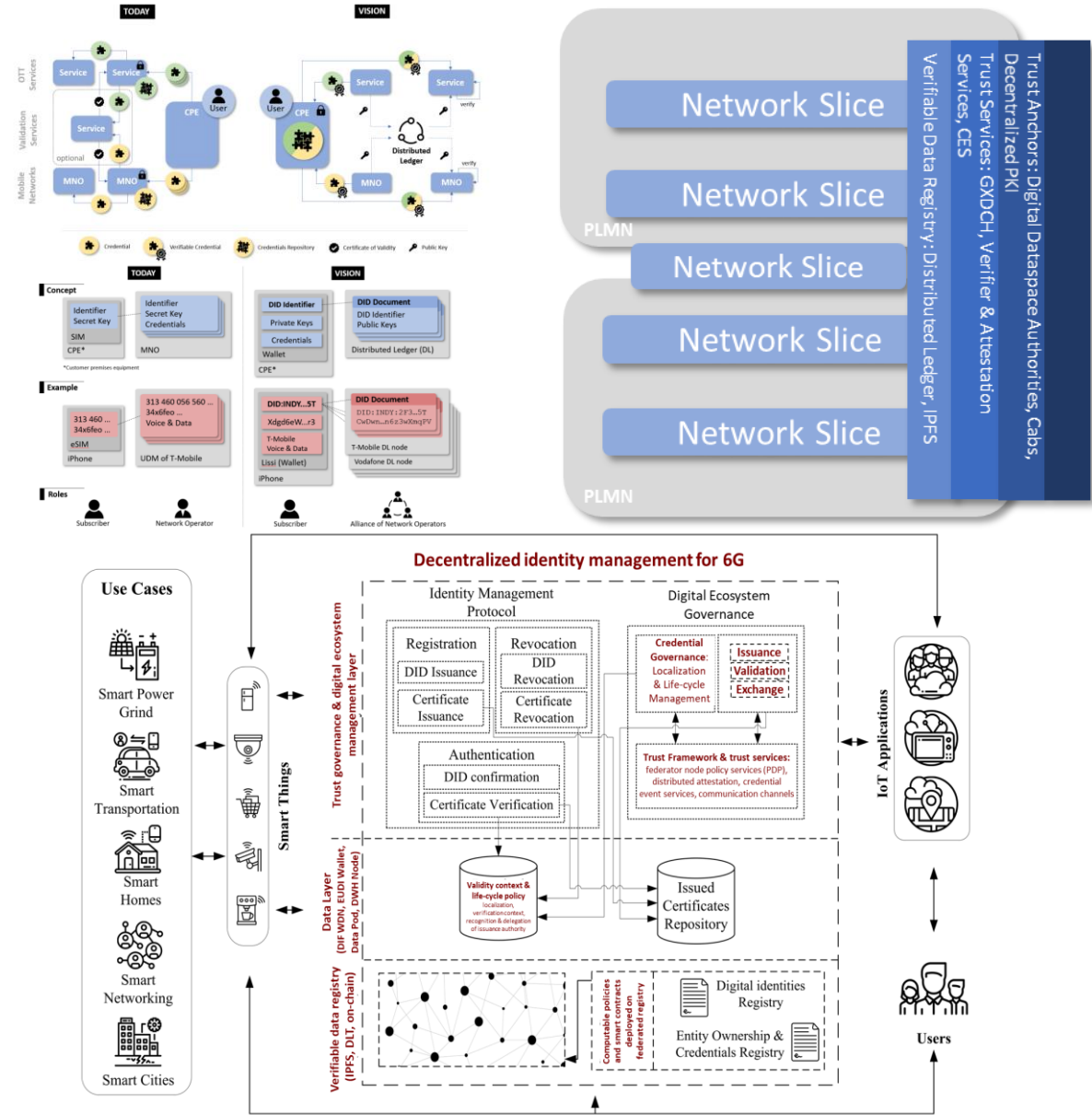
1 Decentralized Identity in 6G

Distributed Remote Attestation

- **Self-sovereign Identity:** Users own and control their digital identities, granting access to specific data or services only to trusted parties
- **Edge Computing Integration:** Integrating decentralized identity solutions with edge computing in 6G networks to support distributed, low-latency identity verification and authentication processes at the network edge
- **Federated Authentication:** Users authenticate different services using single, decentralized identity provider
- **Privacy-Preserving Data Sharing:** Users control how their personal data is shared with third parties, ensuring responsible data usage
- **Dynamic verification:** Ensuring the validity of provided verifiable credentials/claims
- **Multi-Domain Identity Management:** Enabling seamless management of decentralized identities across diverse 6G domains, including IoT, augmented reality, virtual reality, while ensuring interoperability and security

Challenges

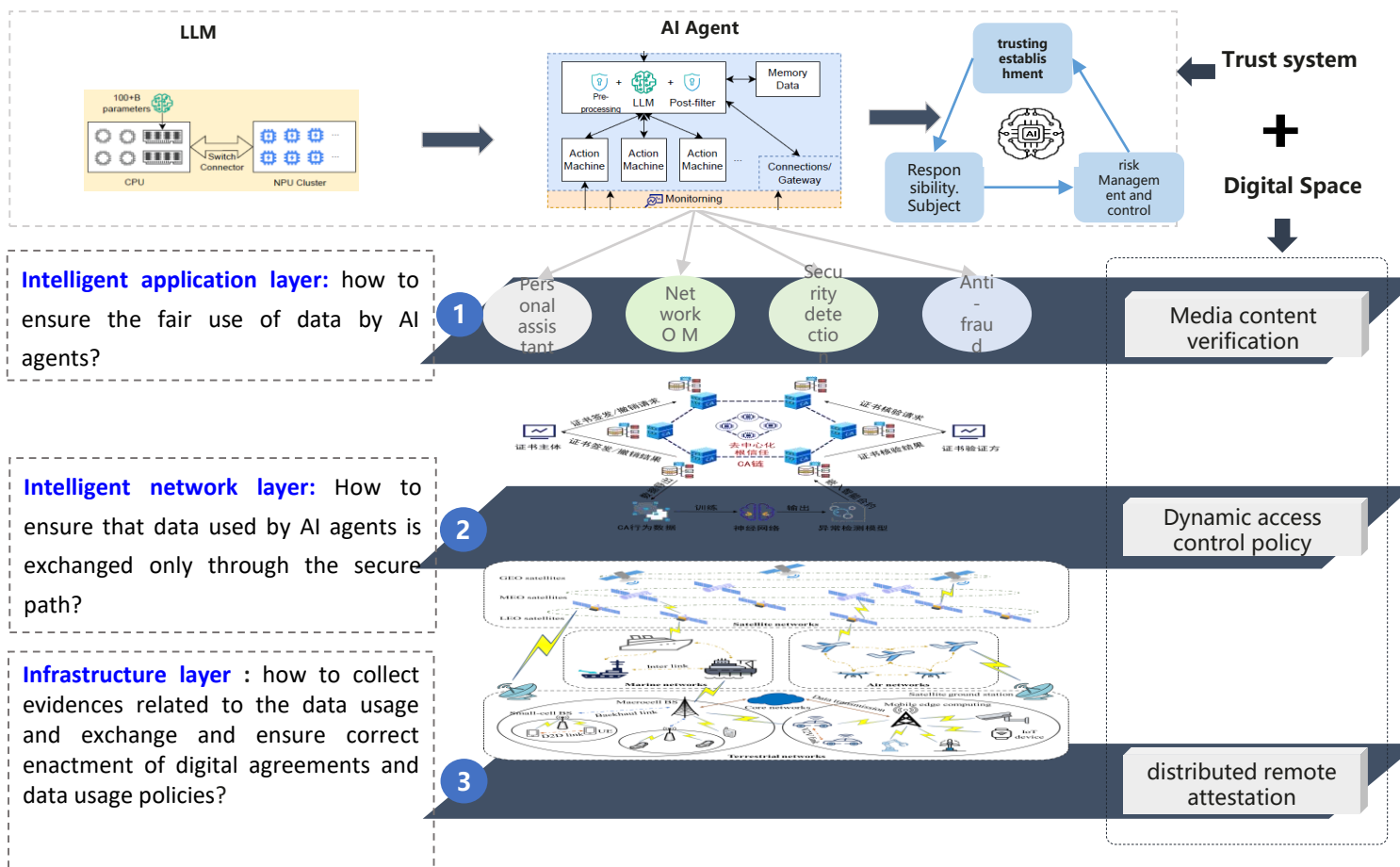
- **Dynamic Network Slicing:** Adapting decentralized identity solutions to support dynamic network slicing in 6G, allowing for personalized network configurations while maintaining identity management integrity
- **Cross-Domain Trust:** Ensuring secure and trustful cross-domain access control
- **Cross-Domain Identity Management:** Enabling seamless and secure management of decentralized identities across diverse 6G domains, such as IoT, augmented reality, virtual reality, and tactile internet, while upholding privacy and security standards
- **Data Ownership and Control:** Addressing the complexities of data ownership and control within decentralized identity systems, particularly in the context of 6G's data-intensive and distributed computing paradigms
- **Identity Lifecycle Management:** Managing the lifecycle of decentralized identities, including issuance, revocation, and updating, within the dynamic and fast-paced 6G network environment
- **Trust Anchor Distribution:** Establishing secure and efficient methods for distributing trust anchors and decentralized identifiers across 6G networks to ensure trustworthiness and reliability



Research on Digital SpacesTrust: Cascaded end-to-end data exchange

Target

1. Research the cascaded and verifiable enactment of digital agreements and data usage policies, make breakthroughs in digital space technologies, and enable the development of new digital space services.
2. Build a digital space ecosystem to enable secure, cascaded end-to-end data exchange ensuring verifiable data ownership with delegation of authority and traceability of data at each phase of data life-cycle.



Key technology planning

Trust System

- Policy enforcement ensures that only authorized users can interact with AI agents.
- Digital Spaces can support the commercial AI model provider with evidence collected from clearing houses and ensure that the digital ecosystem consists only of trustworthy stakeholders
- Data sharing agreements specify rules and conditions for data sharing based on data type as well as the location of data in case of cross-border sharing.

Intelligent application layer

- Sharing agreements enable reliable data and service sharing across different domains.
- Policy enforcement ensure a secure and privacy-preserving data exchange among applications for collaborative AI.
- Enable federated learning and cross-domain data exchange enabling AI models to learn from distributed sources without compromising data ownership and privacy.
- Create data marketplaces governed by contracts and agreements.

Intelligent network layer

- Policy enforcement at ensures network security and compliance with regulations and mitigates threats.
- Different domains exchange network-related data to analyse network traffic and events and improve network configurations and services using AI.
- Contract-based governance facilitates collective decision-making among network participants and domains.
- Contracts and agreements enable dynamic provisioning and sharing of network resources and ensure fair and transparent allocation.

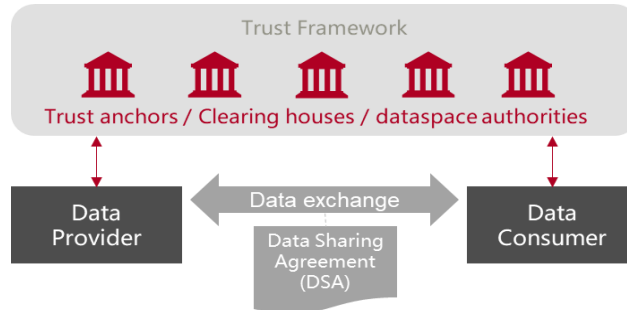
Infrastructure layer

- Cloud infrastructure enable virtualized data sharing networks allowing secure and controlled data exchange.
- Clearing houses can be used to generate, collect and maintain tamper-proof records of network events and usage patterns, which enables trust and accountability.
- Cyber-physical systems help with the distribution of clearing house and with the generation and collection of evidences and proofs.
- Policies must be enforced upon the generation and collection of data by cyber-physical systems to ensure compliance with regulations and to protect data ownership starting from its collection.

Existing digital space concepts focus on one-to-one data exchange only in a single ecosystem with a single trust framework.

Data sharing agreements concern two parties only

Trustworthiness of the data exchange is guaranteed through the digital space authorities (e.g., trust anchors, clearing houses, etc.).



Problem

Future digital spaces incorporate many data sharing nodes belonging to different federations or trust frameworks.

Therefore, data exchange is not necessarily one-to-one sharing but rather a cascaded sharing among many nodes.

Data sharing agreements must concern multiple parties instead of two only.

Trustworthiness of the data exchange must be guaranteed through a share responsibility among several authorities belonging to different trust frameworks

Research questions

How to model data sharing agreements to consider both single nodes as well as the end-to-end path of data?

How to generate policies to be enforced at each node throughout the path?

How to manage conditional cascaded consent throughout the path of the data? (each node may have its own conditions and consent for data sharing, and such condition must propagate and be enforced throughout the path).

How to synthesize monitors to track the data usage and ensure the enforcement of the agreement throughout the end-to-end path? How to generate and collect evidence of compliance across several nodes and several trust frameworks.

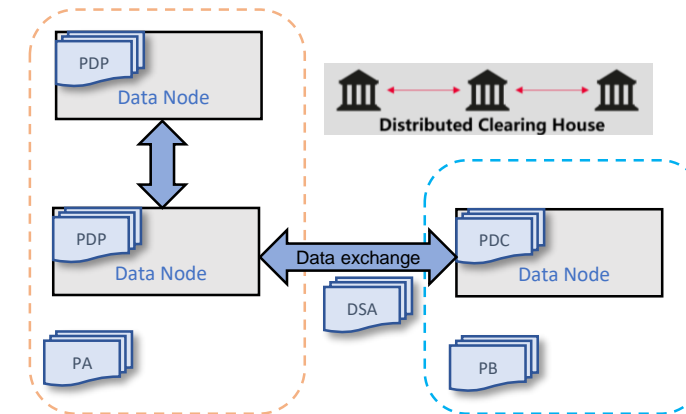
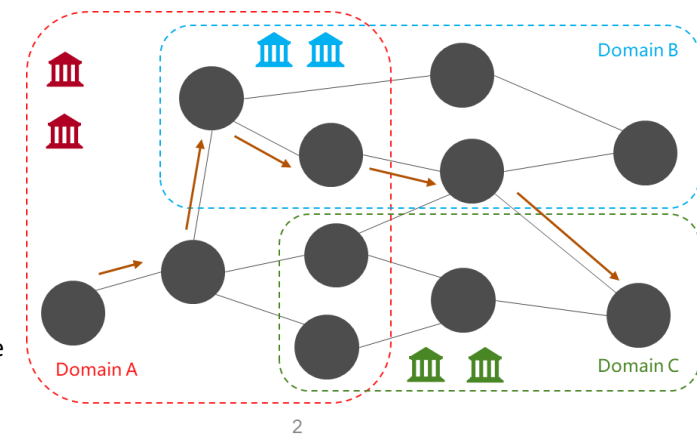
end-to-end data exchange

Concept:

- A clear expectations and guarantees should be clarified regarding what each party/node can offer during negotiation.
 - This negotiation process is integral and should be a standard practice at every edge within the domain.
 - The domain itself operates under specific policies that must be enforced, ensuring that agreed-upon conditions are met.
 - This enforcement can be observed at different levels, including:
 - The negotiation level between nodes,
 - Node-level policies
 - Policies across domain nodes.
 - The policy scoping ensures that policies of different levels are consistent.
 - The contracts across domains, whether they represent a network, enterprise, or data space, a comprehensive consideration of these agreements is essential for seamless operations and interconnectivity.
- Clearing house can facilitate secure evidence collection and storage for compliance in negotiation and policy enforcement processes when data is shared within a single/different domains
1. Enforcement within a single domain can adopt either centralized or decentralized approaches, offering flexibility in implementation. However, when extending across different domains, only decentralized enforcement is feasible.
 2. Technologies such as blockchain or DAA play a crucial role in securely collecting and storing evidence to ensure compliance with the negotiation and policy enforcement processes.
 3. The Clearing houses can efficiently resolve issues by referring to the securely stored evidence.

Examples:

- A scenario of a supply chain system where, internally, before any data is moved, a thorough check is conducted to ensure compliance of contractual agreement.
- The compliance include check of local policies, negotiation-level policies, and across domain policies



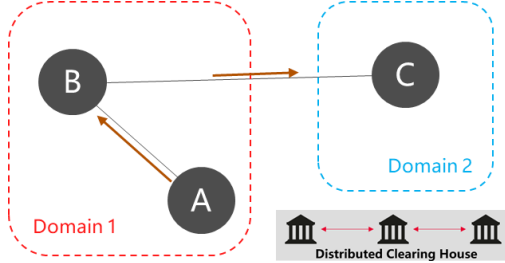
PDP, PDC – Local Usage Policies of DC and DP
 PA, PB – Cross domain usage policies
 DSA – Agreement Usage Policies

2 Distributed Data Clearing House

A **distributed clearing house** is a decentralized authority that facilitates the exchange of data among multiple parties, ensuring compliance with established agreements while upholding data privacy and security.

A- Role of Data Clearing House:

- **Agreement Management and Enforcement.** The clearinghouse manages data exchange agreements, including the terms of data usage, pricing, and any relevant contractual obligations.
- **Provenance and traceability** of data, enabling participants to verify the origin, transformations, and ownership history of the data they exchange.
- **Resolving disputes** between data providers and consumers regarding data exchange agreements.



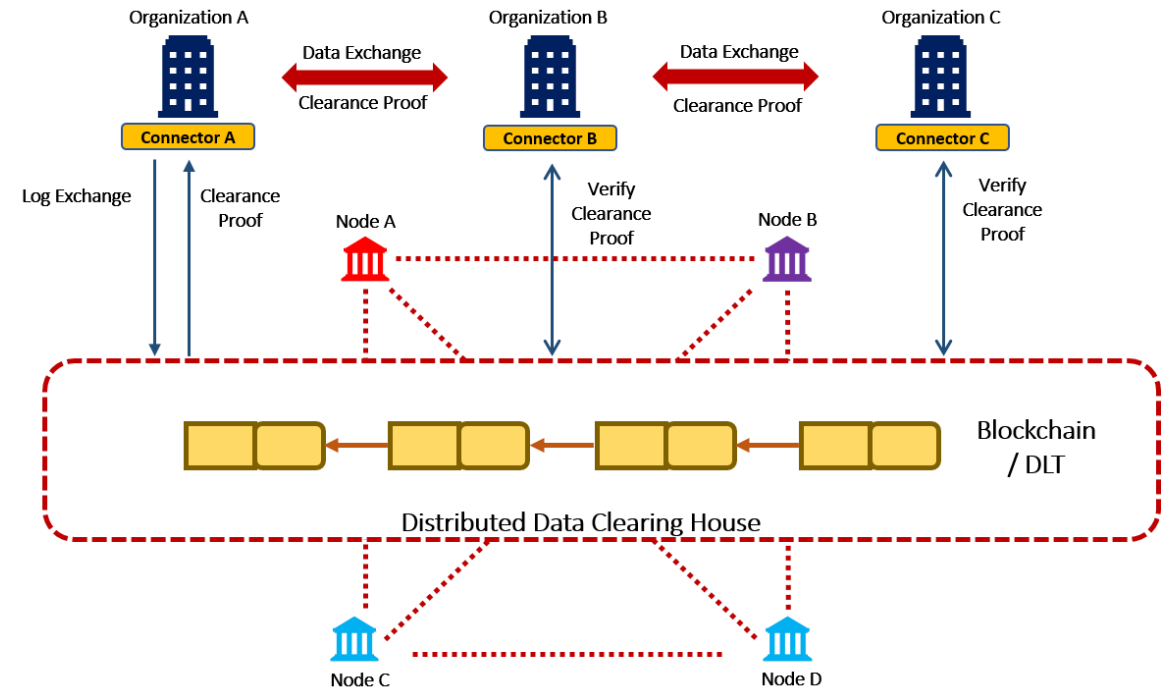
B- Distributed Clearinghouse Scenario:

- In a distributed clearinghouse scenario, the CH1, CH2, and CH3 clearinghouses operate in a network of interconnected nodes spanning different domains.
- The clearinghouse facilitates data exchange between nodes A and B across domain 1, overseeing their data exchange agreements and maintaining the provenance and traceability of shared data.
- Meanwhile, an agreement enables node B (in domain 1) to share data received from A with node C in domain 2.
- The clearinghouse should monitor and collect logs of node B's activities within domain 1 and node C within domain 2, ensuring compliance with data exchange agreements.
- A standardized protocol and trust establishment are essential to ensure integrity and adherence to agreements across the distributed clearinghouse network. This protocol should enable seamless communication and verification of data exchanges between distributed clearinghouses, confirming that shared data between domains complies with the agreed-upon terms.

Distributed Data Clearing House

Concept:

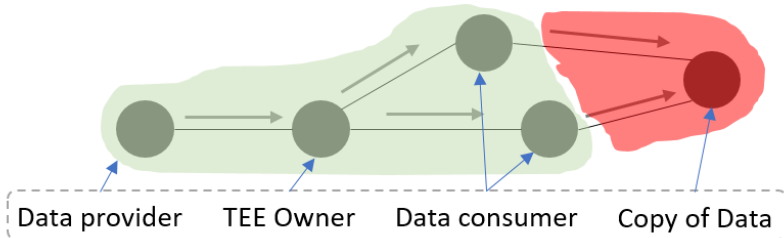
- **Interoperability and Standards:** Clearinghouses can implement interoperability standards to facilitate seamless data exchange across different platforms and domains. This involves using standard protocols to ensure consistency in data formats and communication between diverse systems.
- **Trust:** Establishing trust between clearinghouses and between them and participating nodes involves developing robust authentication and identity verification protocols.
- **Decentralized Identity Systems:** Clearinghouses can explore decentralized identity systems to give participants more control over their identities and credentials.
- **Dynamic and Adaptive Clearinghouse Monitor:** A dynamic clearinghouse monitoring framework that can adapt to changes in agreements and monitor usage access logs, accommodating evolving requirements and emerging technologies.
- **Security in Cross-Domain Data Exchanges:** Addressing security challenges in cross-domain data exchanges involves considering diverse regulatory environments and data protection requirements. This includes compliance with data protection regulations, addressing liability issues, and considering ethical considerations in data sharing.
- **Distributed Ledger:** Clearinghouses can leverage blockchain and smart contracts or other DLTs to collect events and automate the enforcement of data exchange agreements within clearinghouse frameworks.



2 Data Capsule

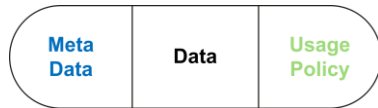
Current situation:

- Existing digital space concepts focus on data exchange between two entities and modification on the original data are out of the scope.
- Data capsule** facilitates data exchange and modification, however, without taking into account **traceability record**.
- The exchange of data capsule is considered between **trusted entities**, i.e., **data owner** and **Trusted Execution Environment Owner**
- Third parties can read data without any further changes



Challenges:

- In future digital spaces, numerous parties will consume and share the same data acting as **data consumer** and **data provider** simultaneously;
- Entities will consume data and share its modified version with other participants after implementing modifications of that data;
- Current data capsule implementation partially support traceability and data ownership statement without any records of authority delegation;
- Any modifications and delegation of ownership are not traceable and trustworthiness of shared data is not fully achieved;



Current Data Capsule structure

Research questions

- How to collect and register any usage and/or modifications of data?
- How to collect, manage and associate data usage consent issued by multiple parties, yet enforcing data usage and obligation policies?
- How to verify data ownership and keep track of authority delegation?
- How to collect and combine the data usage control policies defined by different parties across the cascaded data exchange environment?

Data Capsule Execution Environment

Current scenario for TEE and data capsule:

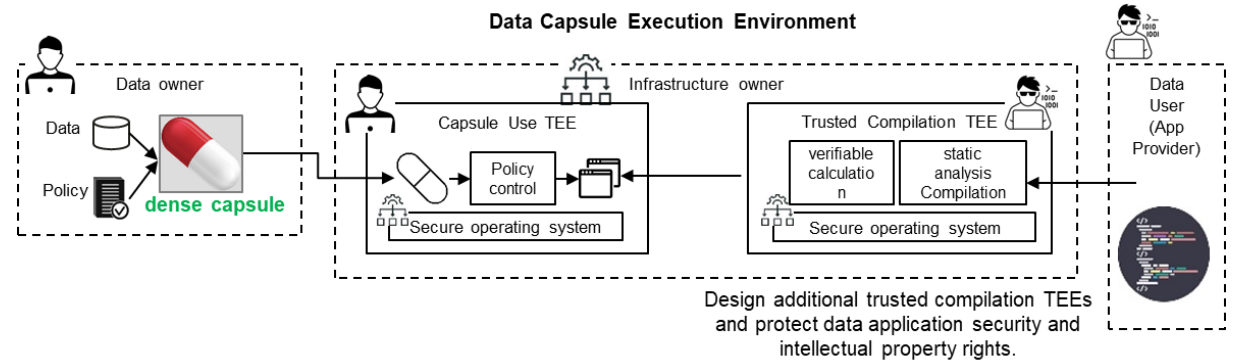
Trusted Execution Environment provides secure area that protects data loaded inside it from unauthorized access or modification.

Data capsule is a self-contained and self-enforcing data model that contains sensitive data, a policy restricting how the data may be processed, and metadata relevant for data privacy concerns.

TEE and data capsule are used to enable a **self-expiring data capsule**. Sensitive data is encapsulated into a data capsule that has an **access policy** and an **expiring condition**.

The **access policy** specifies which functions are eligible to access the protected data and its expiry conditions.

The **expiring condition** dictates when the data should become inaccessible to anyone, including the previously eligible functions.



Involved Stakeholders:

Data owner (provider) – an entity that has legal ownership of the data or acts as a delegee by providing data on behalf of the data owner;

Infrastructure Owner – an entity that provides secure infrastructure for the TEE deployment and execution of operations requested by data consumer. Infrastructure owner may act on behalf of data owner in accordance to the delegation policy by offering data as a service;

Data Consumer – an entity that uses data in accordance to the policies defined by the data owner and enforced by the Data Capsule Execution Environment

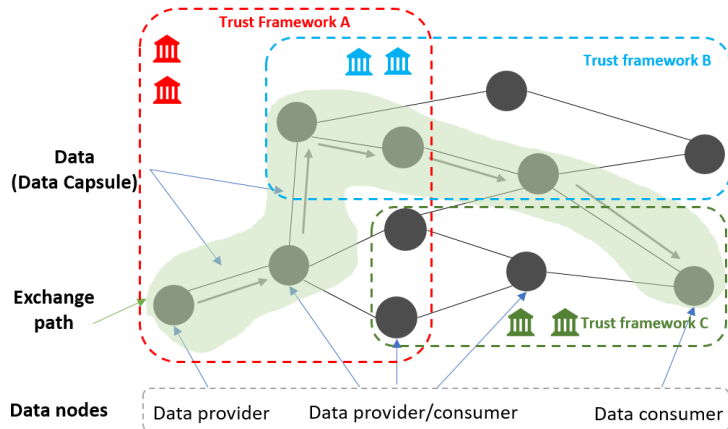
2 Advanced Provenance Capsule for cascaded end-to-end data exchange

Current situation

- Existing digital space concepts focus on data exchange between two entities and data modification is out of the scope

Challenges:

- In future digital spaces, numerous parties will consume and share the same data acting as data consumer and data provider simultaneously;
- Entities will consume data and share its modified version with other participants after implementing modifications of that data;
- Current data sharing approaches partially support traceability and data ownership statement without any records of authority delegation;
- Any modifications and delegation of ownership are not traceable and trustworthiness of shared data is not fully achieved;



The technical solutions of the concept are applicable to the use cases:

- AI Assistant** – secure communication with other agents that perform different tasks;
- AI and LLM Training** – exchange traceable data for AI agent and LLM training;
- Media Content Right Verification** – secure exchange of media content with the traceable changes and prof of ownership;

Advanced Data Provenance Capsule

Concept:

Advanced Data Provenance Capsule – is a self-contained and self-enforcing data container that tracks the origin and changes of data throughout its life-cycle. It consist of **5** components:

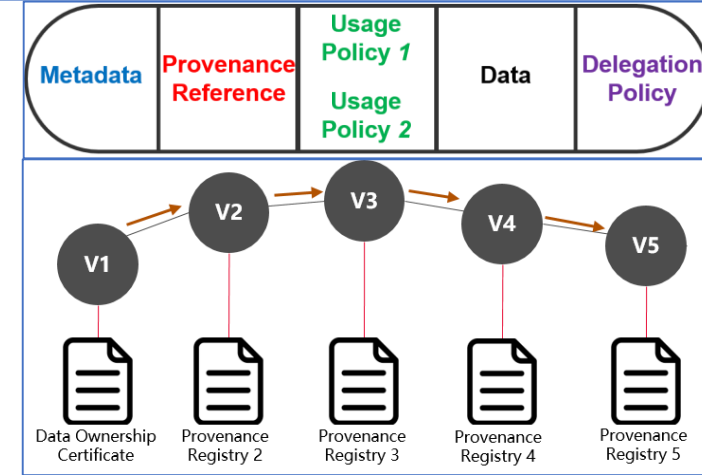
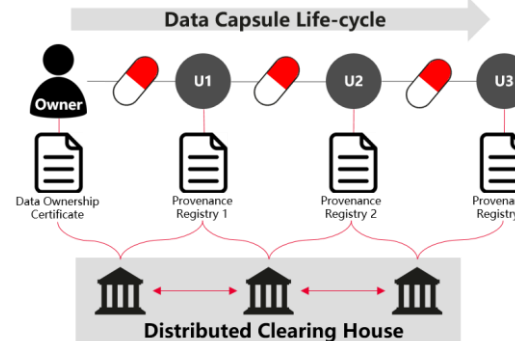
- Metadata** – provides information about data, including creation date, hash value, etc.
- Provenance Reference** – is a reference to the statement that describes the history, ownership and registry of every change done to the data.
- Data Usage Policies** - a set of policies defined by the data creator and the delegated entity.
- Data** – defines an information asset provided by the data creator.
- Delegation Policy (ADP)** – a set of delegation policies defined by the data creator (*in some cases could be defined by the delegated entity*) to scope delegated activity

Data Owner (delegator) creates a data capsule with:

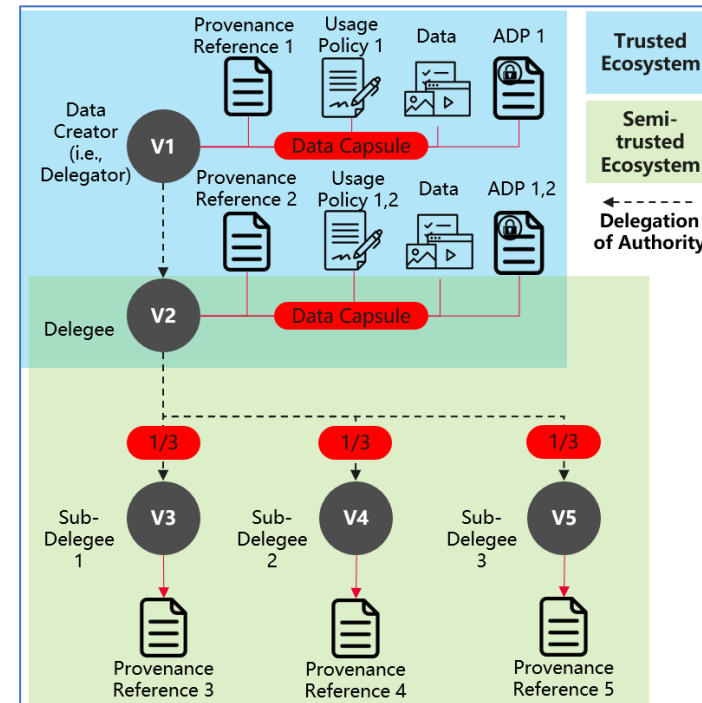
- Provenance Reference 1** – reference to the initial capsule information available on the request at the **Clearing House**;
- Usage Policy 1** – permits delegee to read/write data;
- Data** – original data asset with no modifications;
- ADP 1** – specifies the scope of delegation for the delegee

Delegee acts on behalf of **Data Owner**:

- Provenance Reference 2** – reference to the data usage registration statement;
- Usage Policy 2...n** – allows sub-delegee to access parts of the original data;
- Data** – original data asset for selective disclosure;
- ADP 2** - specifies the **scope of delegation** for each sub-delegee



Delegation of Authority and Selective Disclosure

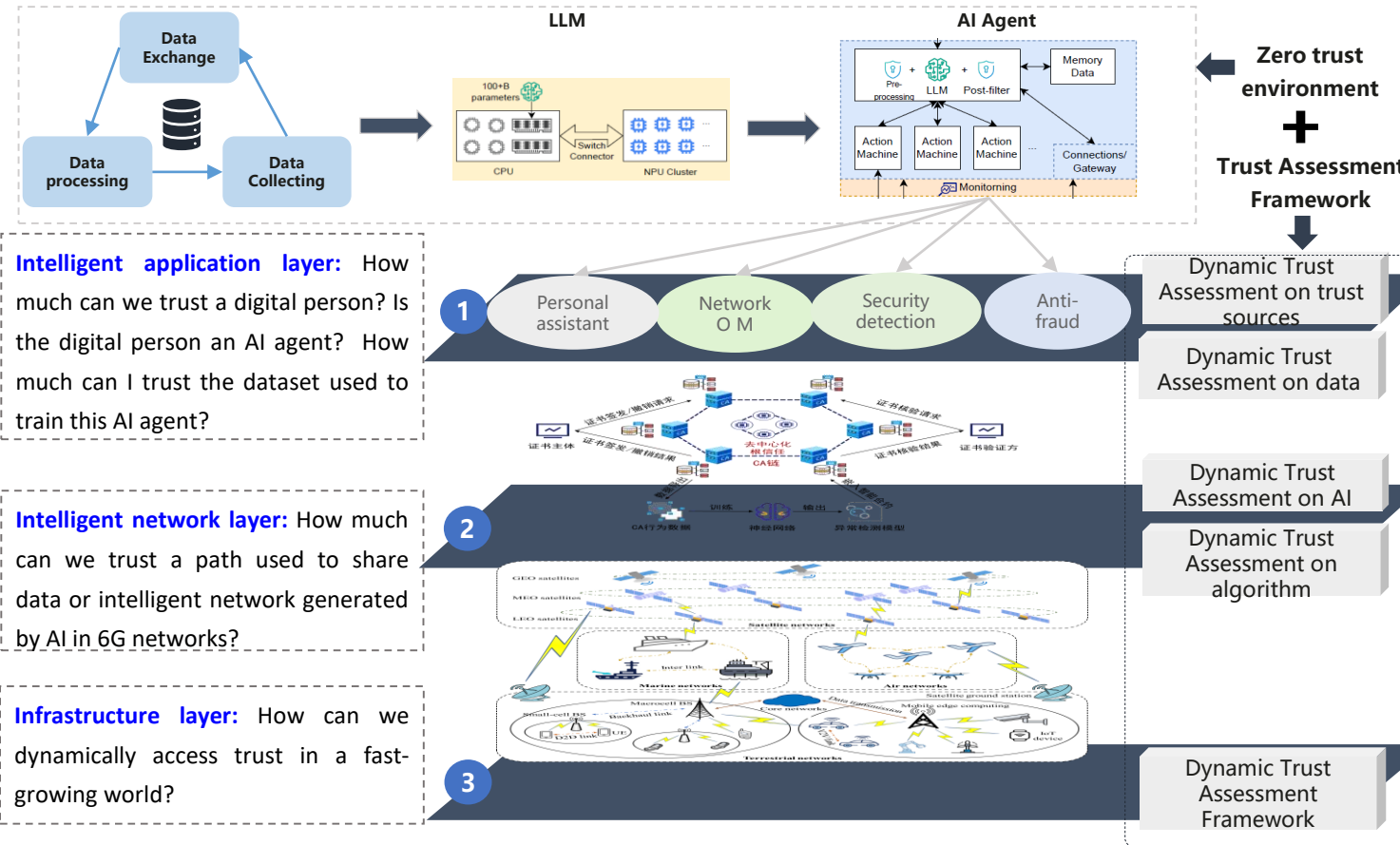


Research on Digital Spaces Trust: Constructing Dynamic Trust assessment for Data, Algorithm and AI

3

Target

1. Build a reason opinion in a uncertain world (zero trust environment) where uncertainty comes from devices, services
2. Build a **Trust Assessment Framework that is endogenous to AI** and promote the standardization of an open and neutral intelligent network trust assessment mechanism in ITU-T.



Intelligent application layer: How much can we trust a digital person? Is the digital person an AI agent? How much can I trust the dataset used to train this AI agent?

Intelligent network layer: How much can we trust a path used to share data or intelligent network generated by AI in 6G networks?

Infrastructure layer: How can we dynamically access trust in a fast-growing world?

Key technology planning

Intelligent application layer

- A Trust Assessment framework (TAF) that can evaluate trustworthiness in entities and data using a reasoning framework such as Subjective logic.
- Design an agnostic TAF in order to support any uncertainty reasoning framework (Subjective logic, Dempster Shafer Theory ...) and should be able to choose the right operator for a given task.

Intelligent network layer

- A Trust Assessment framework (TAF) that can evaluate trustworthiness in Algorithm and AI based on the trustworthiness in the training dataset.
- Design a sufficiently agnostic TAF for trustworthiness in AI in order to support any scope of Trust such as privacy, fairness.

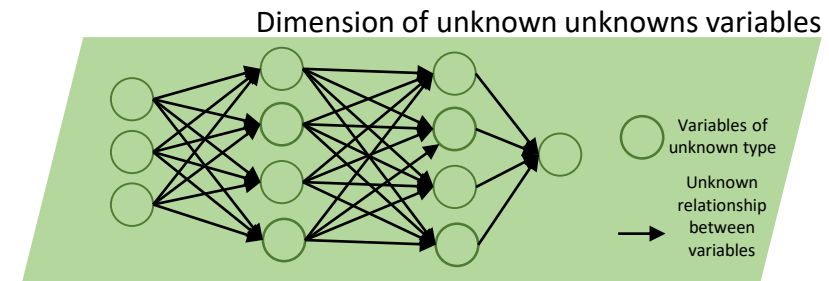
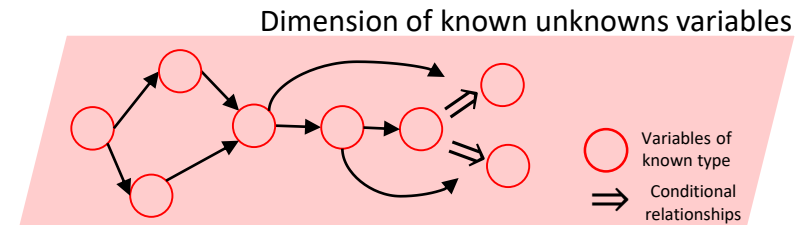
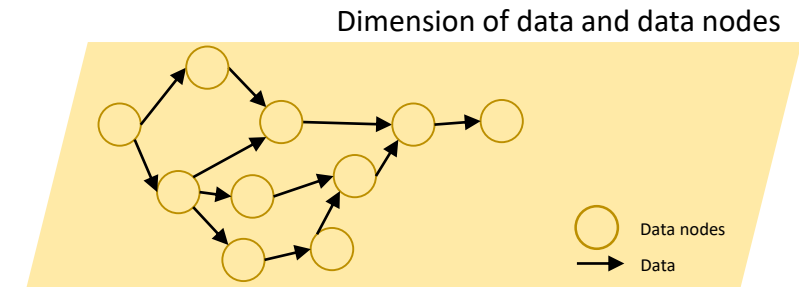
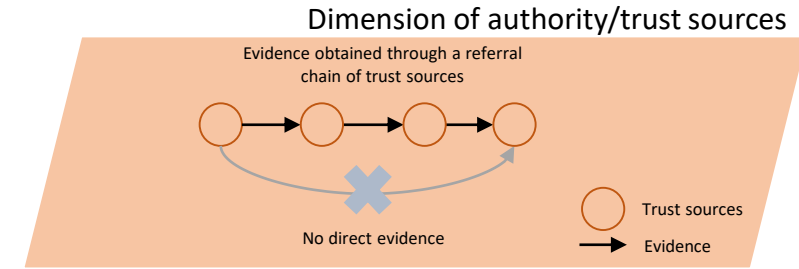
Infrastructure layer

- Design a dynamic TAF that will not depend on the environment such that it will not require some changes for some specific use cases.

3 Dynamic Trust Assessment concept

Complexity Levels of Trust Assessment

Uncertainty and subjectivity	<p>CL1</p> <p>Level of Assurance</p> <ul style="list-style-type: none"> Well-defined claims Known trust authorities Complete evidence Clear verification algorithms <p><i>The level of assurance is related to the level of quality of the requirements that are met in the process.</i></p>
	<p>CL2</p> <p>Dynamic Trust on chains of Trust Sources</p> <ul style="list-style-type: none"> Well-defined claims to verify The rules of the trust framework are clearly specified Verification algorithms can cope with uncertainty Untrustworthy trust anchors Cannot prove trust chain Evidence obtained indirectly <p><i>Dynamic Trust Assessment of the trust authorities.</i></p> <p>Subjective Trust Networks (STNs)</p>
	<p>CL3</p> <p>Dynamic Trust on chains of Data and Data Nodes</p> <ul style="list-style-type: none"> The data and the data nodes that produce need to be assessed for quality The evidence about the data is undirect Missing information about how to validate the claim, or the claim is about something subjective The claim requires a subjective trust assessment, because there is no evidence about the data in the claim <p><i>Dynamic Trust Assessment of the 1) data, 2) the data nodes (data providers/consumer) and 3) the end-to-end data exchange (paths).</i></p> <p>Subjective Trust Networks (STNs)</p>
	<p>CL4</p> <p>Dynamic Trust including Known Unknowns</p> <ul style="list-style-type: none"> Known unknowns assertions about variables Predictive analysis and reasoning are needed (e.g., probabilistic reasoning, stochastic analysis, Bayesian reasoning, Subjective Networks) <p><i>Dynamic Trust Assessment that includes reasoning without learning.</i></p> <p>Subjective Networks (SN): STN + Bayesian Reasoning</p>
	<p>CL5</p> <p>Dynamic Trust including Unknown Unknowns</p> <ul style="list-style-type: none"> Unknown unknowns assertions about variables Learning is needed (e.g., training, ML, reinforcement learning, big AI) <p><i>Dynamic Trust Assessment that includes learning.</i></p> <p>Neural Networks (NNs) Big AI</p>



3 Dynamic Trust Assessment

of cascaded exchange paths

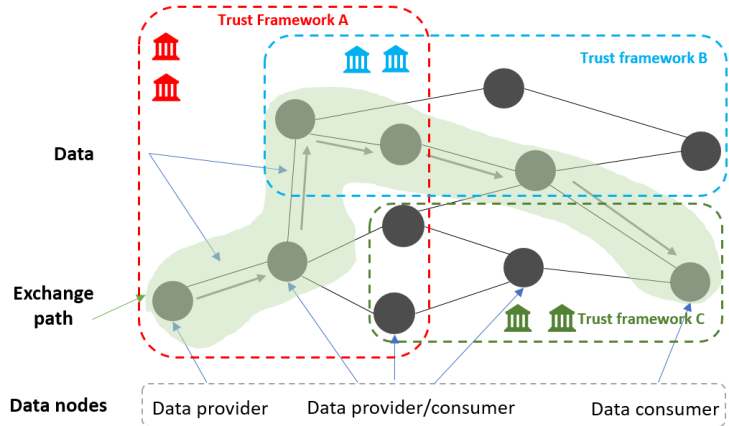
Challenges

- Existing digital space concepts focus on one-to-one data exchange



However:

- data exchange is not necessarily one-to-one sharing but rather a cascaded sharing among many **data nodes** that produce (**data providers/consumer**), use or forward the **data**
- the **data** and the **data nodes** could be unknown and untrustworthy (following the Zero Trust principle)
- missing information about how to validate the claim, or the claim is about something subjective



TAF: Dynamic Trust Assessment On Chains on Data and Data Nodes

The technical solutions of the concept are applicable to all the use cases:

- AI Agent Assistant** – trust assessment of the AI assistant interaction with services;
- AI and LLM Training** – trust assessment of data used for AI and LLM training;
- Data Warehouse and Data Capsule** – trust assessment of data exchange path;
- Media Content Right Verification** – trust assessment of the media content exchange path;
- 6G** – trust assessment of heterogeneous devices communication

That include 1) **data**, 2) the **data nodes** and 3) the **end-to-end data exchange (paths)**.

TAF: Dynamic Trust Assessment for data exchange paths

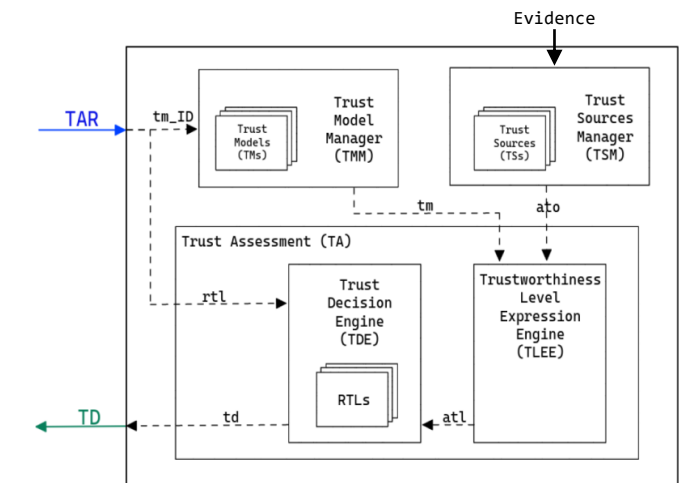
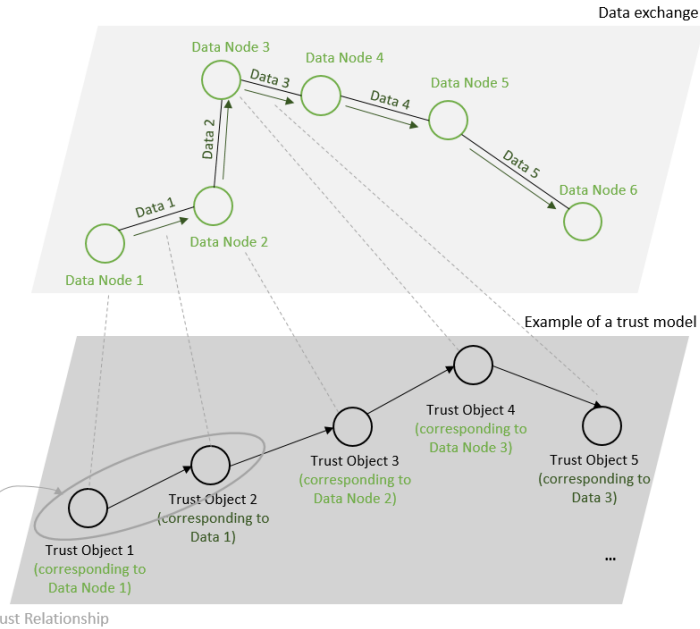
Concept

Dynamic Trust Assessment Framework (TAF) is running in parallel with the execution of the concrete system under consideration (concretely the cascaded exchange paths)

- TAF assesses the trustworthiness on the 1) data and 2) the data nodes (that produce, use or forward the data) as part of the end-to-end data exchange (paths) in relation to a certain property

The TAF brings together:

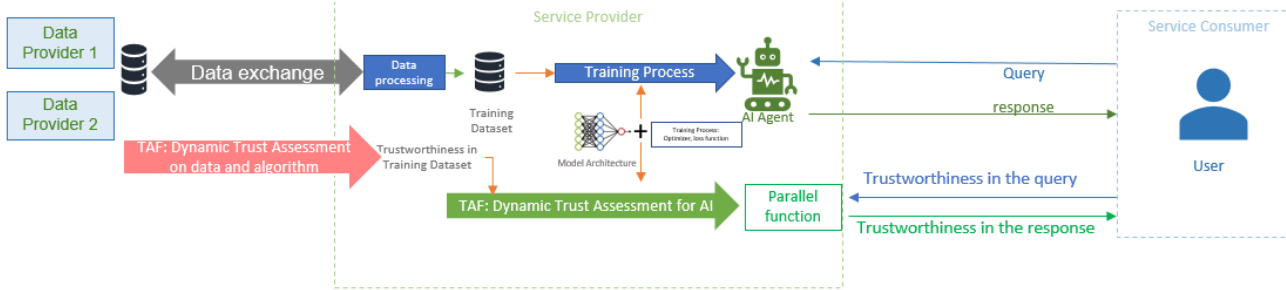
- creation and maintenance of trust network models [TMM]
 - The trust model is a graph that is build based on the underlying data exchange path/graph topology
 - Depending on the concrete use case and the objectives of the trust evaluation, the vertices in the trust model can depict different aspect from the data exchange (e.g., a vertex in the trust model can represent a 1) data node or 2) the data itself)
 - The trust model is dynamic and it needs to be updated at run-time during the operation of the system (models@RT)
- quantifying the trustworthiness of trust relationships [TSM]
 - Select trust sources for each trust relationship based on variables under assessment
 - The trust sources can also form dynamic chains (see L2)
 - Algorithms and methods are needed for calculating the trustworthiness of each trust relationships from the trust model, based on the evidence from the trust sources
- quantifying the trustworthiness of the trust model [TLEE]
 - Algorithms and methods needed to compute the trust level of the overall trust network
 - Uses the input from TMM and TSM to calculate the level of trust (i.e., the trustworthiness)



TAF High-level Architecture

3 Dynamic Trust Assessment

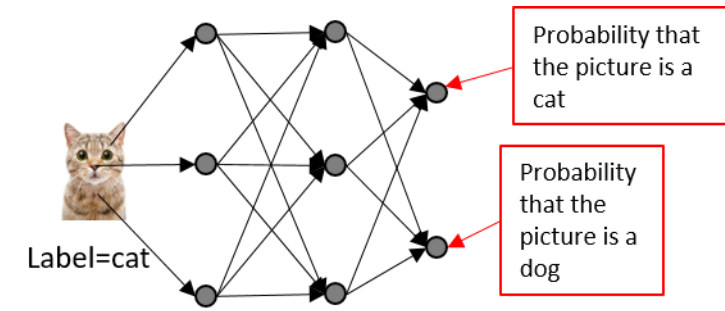
for NNs/LLMs (e.g. Q*) <https://www.xda-developers.com/artificial-general-intelligence-q-star/>



- Depending on the source of the training data, the path used to share the data, the actor of the processing, the TAF can be used to derive trust in the dataset
- The trust (for a given scope) in the dataset intuitively impact the trust (for the same scope) in the NN trained using this dataset
- The trust in the data X and the label Y is used as evidence to create a parallel function that will be used only to propagate trust opinion(like the trained Neural Network with X and Y)
- This parallel function can be used during operational/reinforcement learning phase to calculate trustworthiness in the output of the Neural Network
- During reinforcement learning if the parent model is updated/improved, the parallel function should also be updated accordingly
- Using zero trust concept, initialization of the parallel function is done by mean of full uncertainty (vacuous opinion for SL)

TAF: Dynamic Trust Assessment for AI

- Training dataset consist of Picture of cat/dog and label of each picture, and trust opinion on each picture and label.
- How does this trust opinion impact trustworthiness of the Neural Network?



- Create a parallel function (during training of the model) on trustworthiness data
 - Propagate trustworthiness in the data during forward propagation (of standard training process) using reasoning framework to multiply, fuse and discount trust opinions
 - Calculate the trust opinion on weights and bias using conditional relationship (apply operators relevant for that) between variable during backpropagation
 - The resulting parallel function could be neural network with the same architecture as the original one but where weights are distribution/opinion instead of value

3 Dynamic Trust Assessment

for NNs/LLMs

During training process we can distinguish two main subprocesses:

- **Feed forward:** this process is the one used for inference (**but it is also used during training**). It starts with the first layer and uses the input data X as input. For each layer we compute the output as following: $\sigma(X \times \theta_{L1} + B)$ where σ is the activation function, θ_{L1} is the weights matrix of first layer and B_{L1} the bias. The output of this layer will be used as input of next layer and so on. The final output y' will be the output of the last layer
- **Back Propagation:** This process is the one used to learn(to update the weights) based on feedback based on the error. It starts with the last layer and uses as input the error $\delta_y = y - y'$. For each layer we update the weights and bias using the error and compute the new error to forward to the next layer in the process

The goal here is to map both processes to a corresponding one at the opinion level.

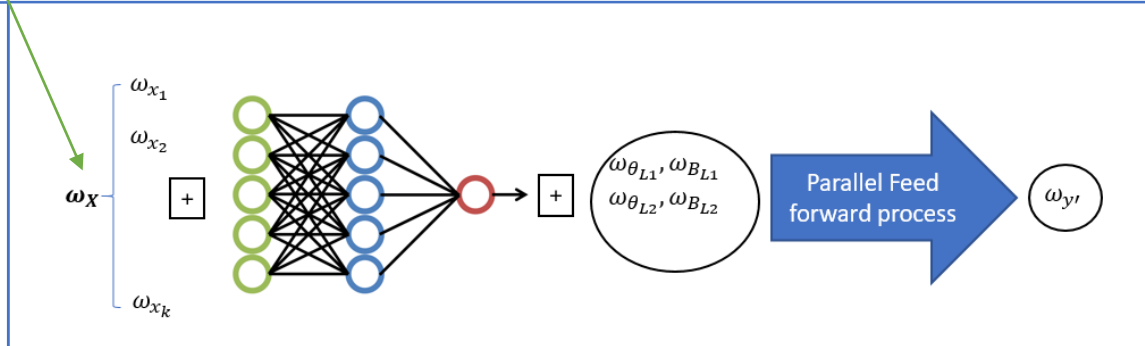
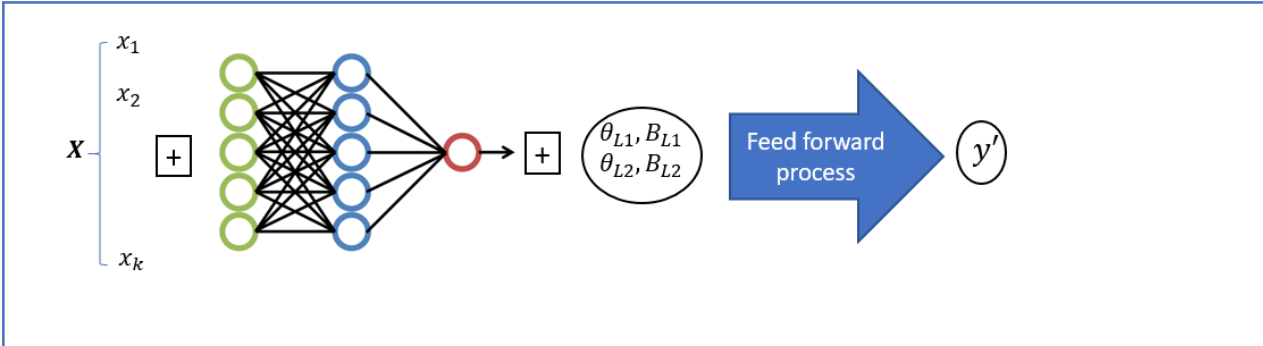
NOTE: the parallel function is not derived by the mean of a training process

Neural Network

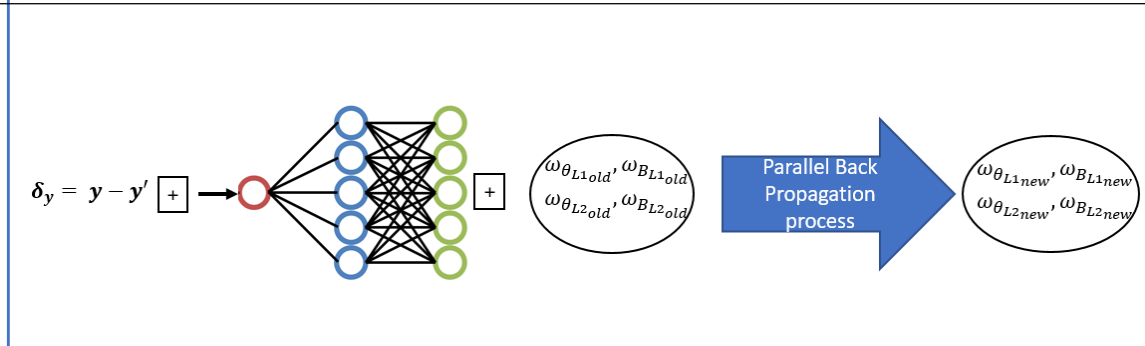
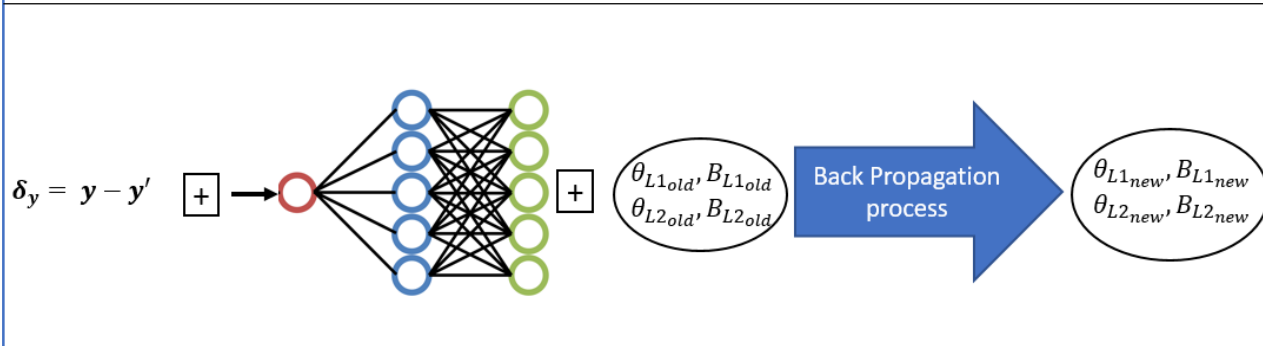
Opinion on the data X

Corresponding parallel dynamic trust function

Feed Forward

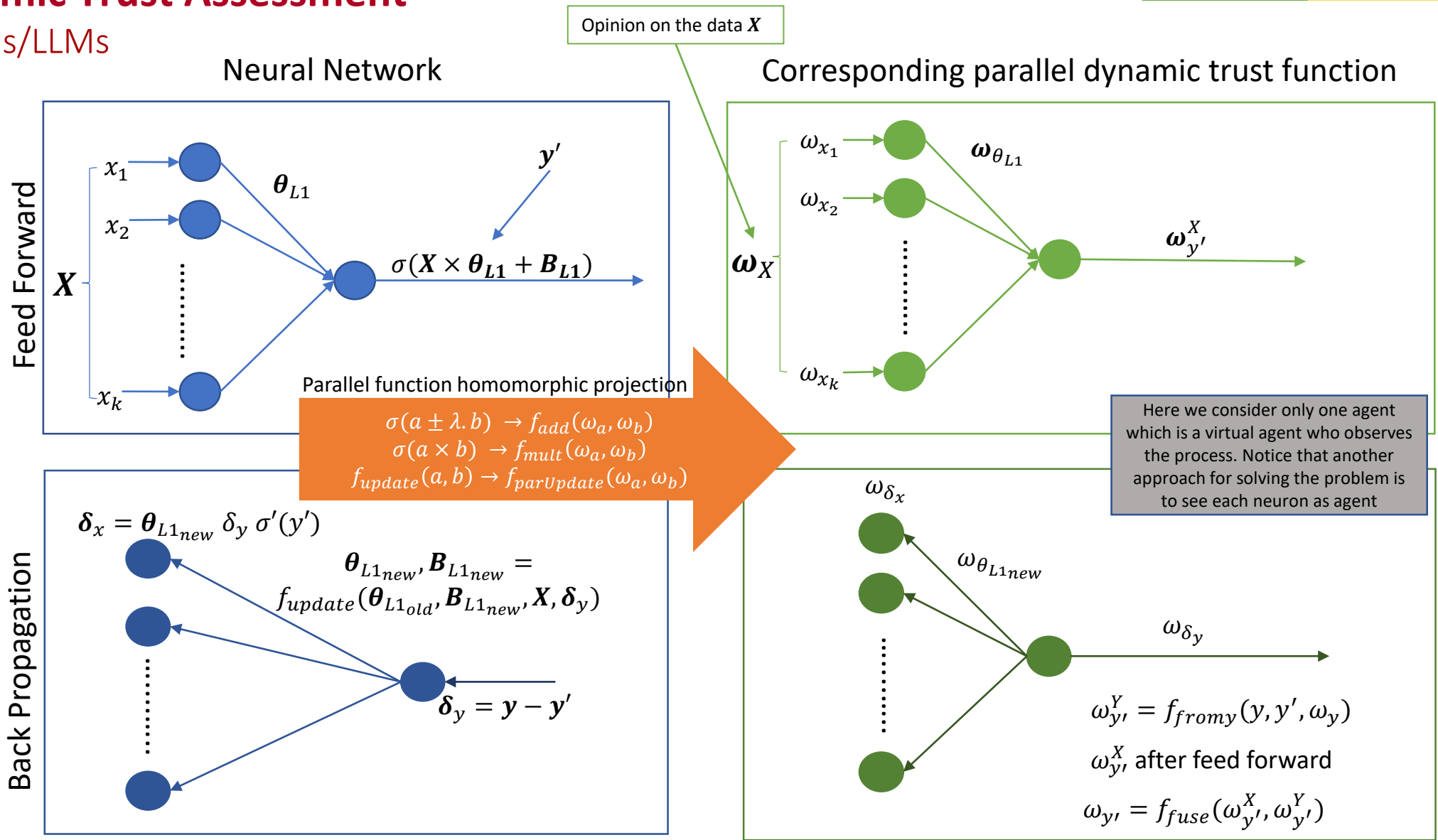


Back Propagation



3 Dynamic Trust Assessment

for NNs/LLMs

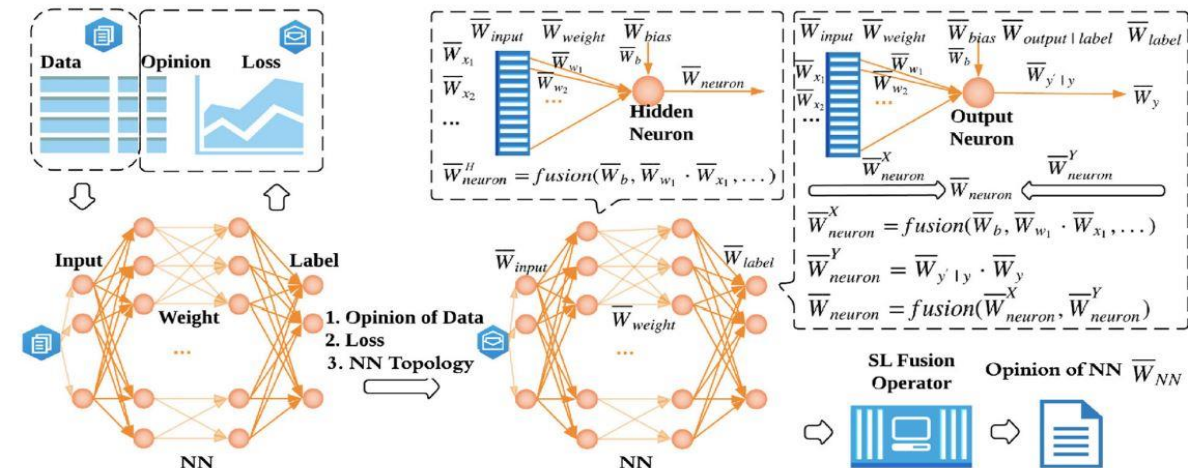
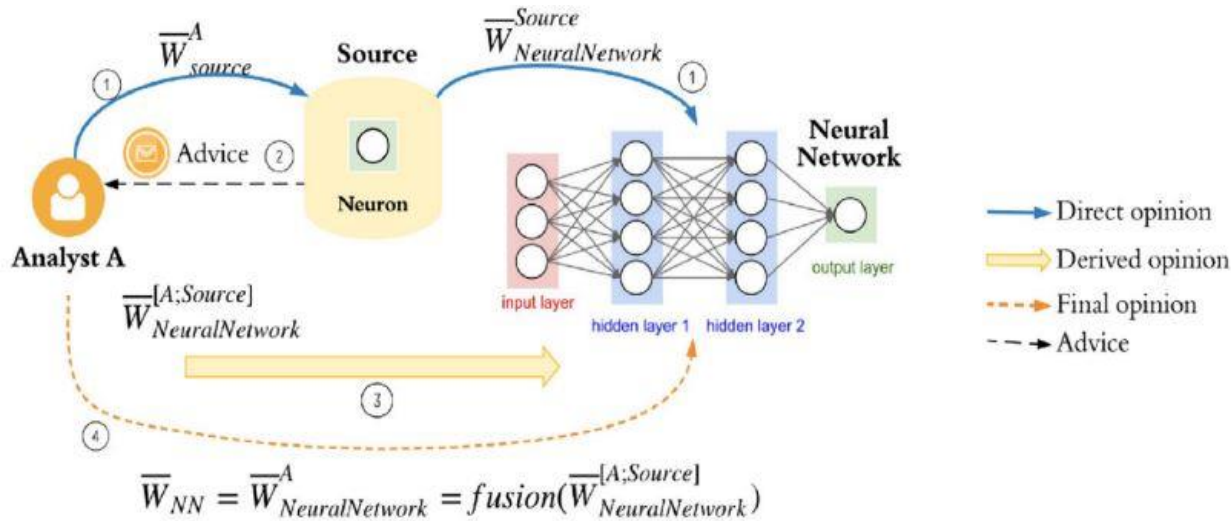


Challenges consist in finding appropriate function for the parallel function based on a reasoning framework (Subjective Logic for example) and (maybe) some of the neural network features (is it a neural network for computer vision or natural language processing?)
 $f_{add}, f_{mult}, f_{fromy}$ and $f_{parUpdate}$ as well as each fusion operator (f_{fuse}) to use

3 Dynamic Trust Assessment

for NNs/LLMs. Example of existing framework: DeepTrust <https://www.frontiersin.org/articles/10.3389/frai.2020.00054/full>

- **DeepTrust** is a framework for quantifying trust in a neural network based on trust in the training dataset.
- DeepTrust does not create a **parallel function**, however during the process of DeepTrust, there is a need for quantifying trust opinion on all data (and variable) exchanged/used during feed forward and back propagation.
- Therefore DeepTrust also needs **parallel function homomorphic projection**:
 - f_{add} : Subjective Logic Average fusion
 - f_{mult} : Subjective Logic Multiplication operator
 - $f_{parUpdate}$: Based on f_{add} and f_{mult}
 - f_{fuse} : Subjective Logic Average fusion
 - f_{fromy} : Using an ϵ to count **positive** and **negative** evidence

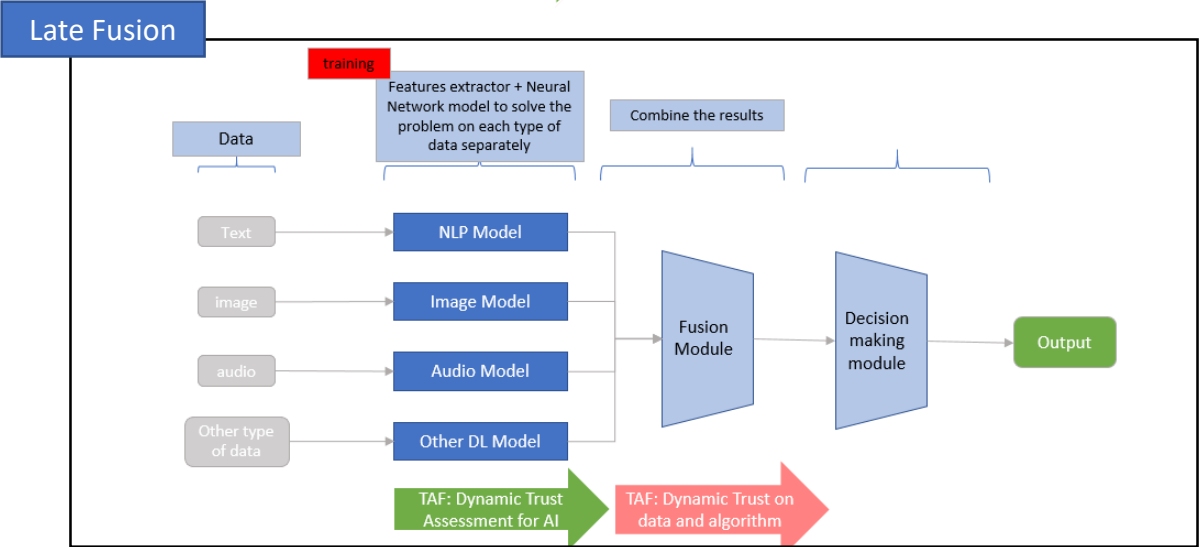
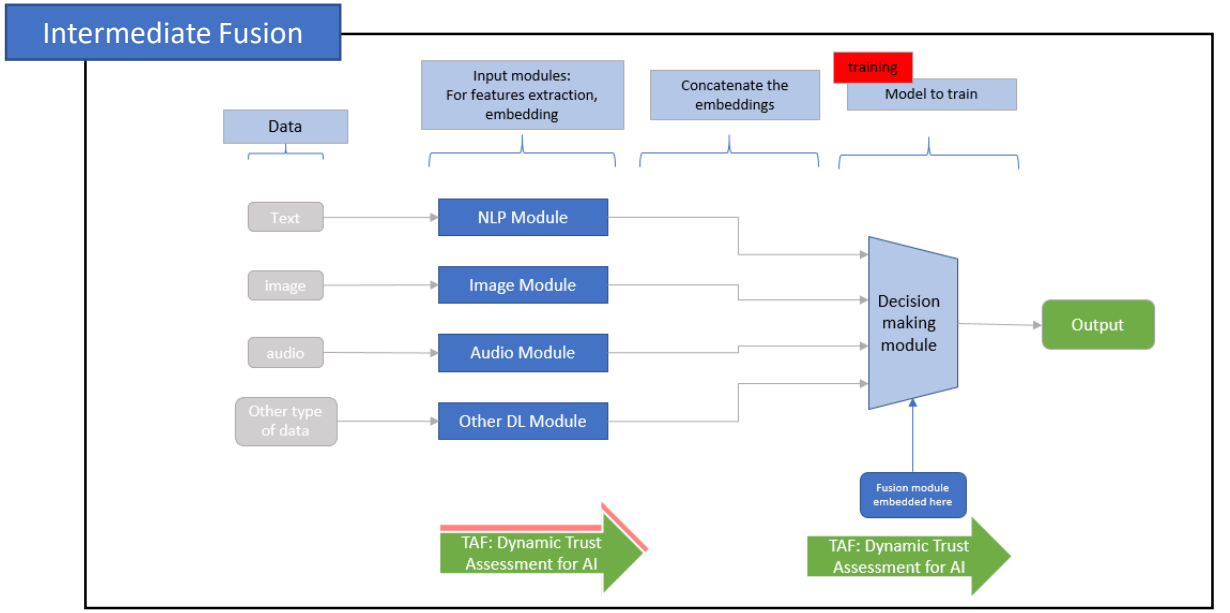
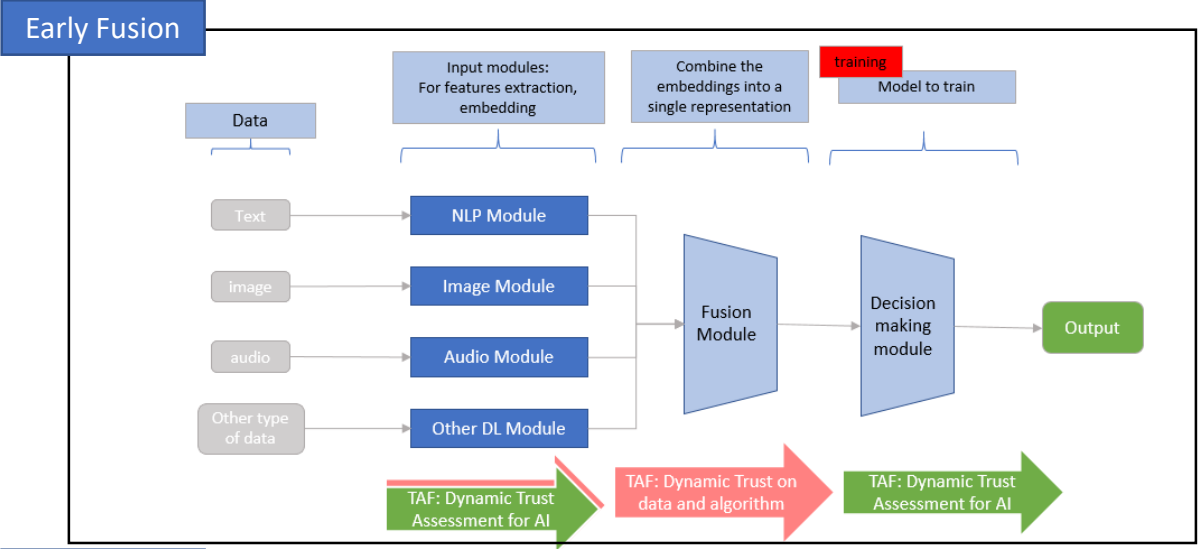


3 Dynamic Trust Assessment

for Multimodal AI (e.g. Gemini AI) <https://www.unite.ai/googles-multimodal-ai-gemini-a-technical-deep-dive/>

- Benefits of Multimodal AI compared to single modal AI (classic one):
- Multimodal AI take different type of data as input
 - Multimodal AI more closely simulates human perception through senses
 - Multimodal AI Learns relationships and dependencies between different types of data for better prediction

- We can distinguish 3 types of architecture:
- **Early Fusion:** the fusion is done before the training. The single modalities are processed individually for feature extraction then fused before training/making decision
 - **Intermediate Fusion:** concatenate each feature representations before Late Fusion
 - **Late Fusion:** solve the problem separately using each type of data, then fuse the output using average or majority vote ...



- Depending on the architecture of the Model, we might need to apply dynamic trust assessment on algorithm or for AI
- The goal will be to derive a big parallel function that will be a concatenation of the parallel function for the training part and the TAF process for evaluating trust

End slide

THANK YOU FOR YOUR ATTENTION