# arsys

The Role of Verifiable Credentials in Gaia-X

- Part of IONOS Group SE, Europe's leading digitalization partner and trusted cloud enabler, with more than 10 brands in the IT market.

- IONOS Group SE is a publicly traded group with more than 6 million customers, a global network of 29 datacenters in Europe and the United States and more than 1,400 million euros in sales (2023 FY).

- Arsys leads the Spanish professional market for Internet presence services, cloud computing and IT infrastructure solutions. It specializes in designing fully-customized cloud projects (public, private & hybrid cloud, DaaS, cloud backup, cloud storage, managed kubernetes and managed security) with maximum guarantees of availability, performance and security.

- It holds these certifications: Tier III, Conformity with the Spanish National Security Scheme (level: high), ISO 9001, ISO 14001, ISO 27001, ISO 27018, ISO 50001, AENOR good practices in e-commerce... Arsys belongs to the European Alliance for Industrial Data, Edge and Cloud, Gaia-X, IDSA, BDVA, among others.

- Experience in EU-funded projects.

Source: https://gaia-x.eu/gaia-x-framework/
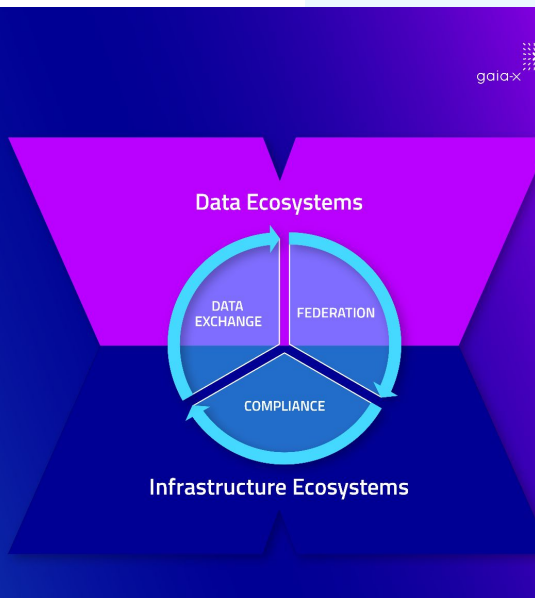
The Gaia-X initiative

Defining the guidelines to build a federated and secure data infrastructure, Gaia-X aims to boost the creation of data spaces that stimulate growth, innovation and competitiveness of the data economy.

Throughout the definition of three pillars (**Compliance**, **Federation and Data Exchange**), Gaia-X establishes common rules of behavior to generate a trusted environment where data can be shared, connecting different application and service providers with the owners of this data (**Ecosystems**) and facilitating secure, transparent sharing, reliable and interoperable information (**Infrastructure**).

Depending on its objectives, each Gaia-X pillar implements its own **functional** and **technical** specifications, which are translated into the development of different software components.

arsys

Compliance

Establishes and defines the necessary mechanisms to ensure compliance with common rules of behavior in data spaces, based on European values of trust.
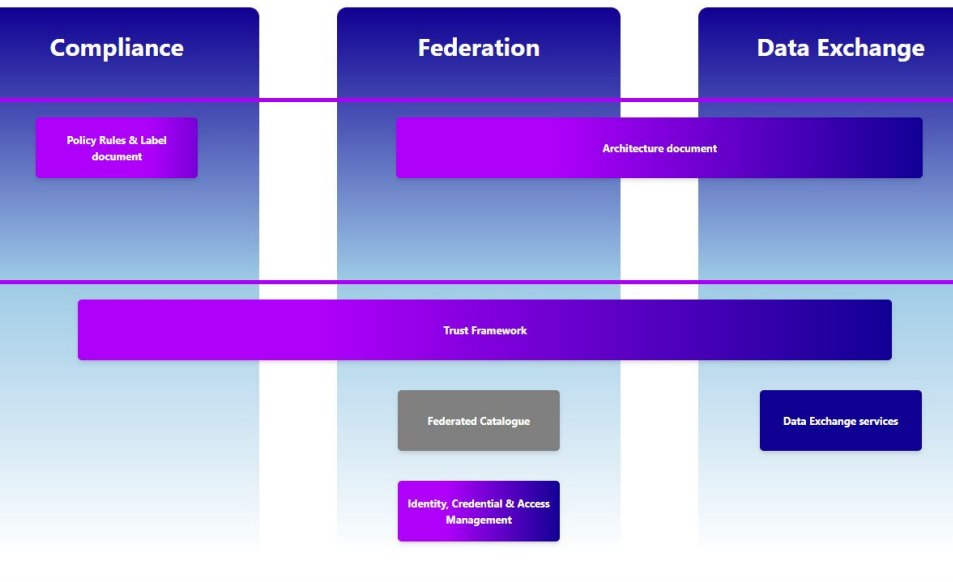
Federation

Facilitates the secure and reliable exchange of data and services, not only among the members of the data space themselves but also between different sectors or ecosystems.

Data exchange

Provides the means to carry out the data exchange itself and keep records of the negotiation of data and use contracts at the infrastructure layer.

arsys

Compliance

Policy Rules & Label document

Federation

Architecture document

Data Exchange

Trust Framework

Federated Catalogue

Data Exchange services

Identity, Credential & Access Management

Source: https://gaia-x.eu/services-deliverables/deliverables/

The Trust Framework

The Gaia-X Trust Framework collects the evolution in the development of the specifications documents and components defined in the three pillars of Gaia-X.

The **functional specifications** describe concepts at a high level. The technical architecture document describes what a federation is, while the policy rules document contains the common set of policies and rules which a federation has to comply with.

The **technical specification** documents describe the minimum set of attributes and rules that participants must provide to act according to the framework defined by Gaia-X, as well as how the software components within the different areas behaves.

According to these specifications, the Gaia-X development teams themselves, with the help of the community, implement software artifacts that, executed at the infrastructure layer, offer the necessary functionalities to work in a Gaia-X compliant data space.

arsys

Verifiable credentials

- The **Trust Framework** is based on the use of **verifiable credentials** as a mechanism to achieve the objectives proposed by the initiative regarding the secure, transparent, trustworthy, and interoperable sharing of information.

- Its use is defined by the **World Wide Web Consortium** (W3C), which develops internationally accepted standards and guidelines for building an Internet based on the same values of security and transparency pursued by Gaia-X.

- Verifiable credentials are a **set of claims or assertions** about something, signed by the entity providing the information using **digital certificates** and validated by a **trusted entity** accepted by all participants in the data-sharing ecosystem.

- Once generated, the credentials are used to provide security and trust in the exchanges of information and processes that occur within the data space. According to the Trust Framework, we can distinguish between **Participant** credentials and **Service Offering** credentials.

- The software components (also known as **Compliance Services**, and operated in the so-called **Gaia-X Digital Clearing Houses**) developed in each work area are responsible for validating the correctness of these credentials and ensuring they comply with the specifications described in the areas of Compliance, Federation, and Data Exchange that make up the Gaia-X framework.

Participant Verifiable Credential

Participants in a data exchange process need to be identified by providing their participant verifiable credential. In this process, we can define two main actors:

Provider: manages resources within the ecosystem, which can be combined to create a service offering. These services are offered and made accessible to other participants.

Consumer: a participant who seeks out service offerings in the ecosystem and consumes them according to their needs.

Participant credentials must contain basic information about the company, as a legal identifier, as well as the acceptance of certain terms and conditions.
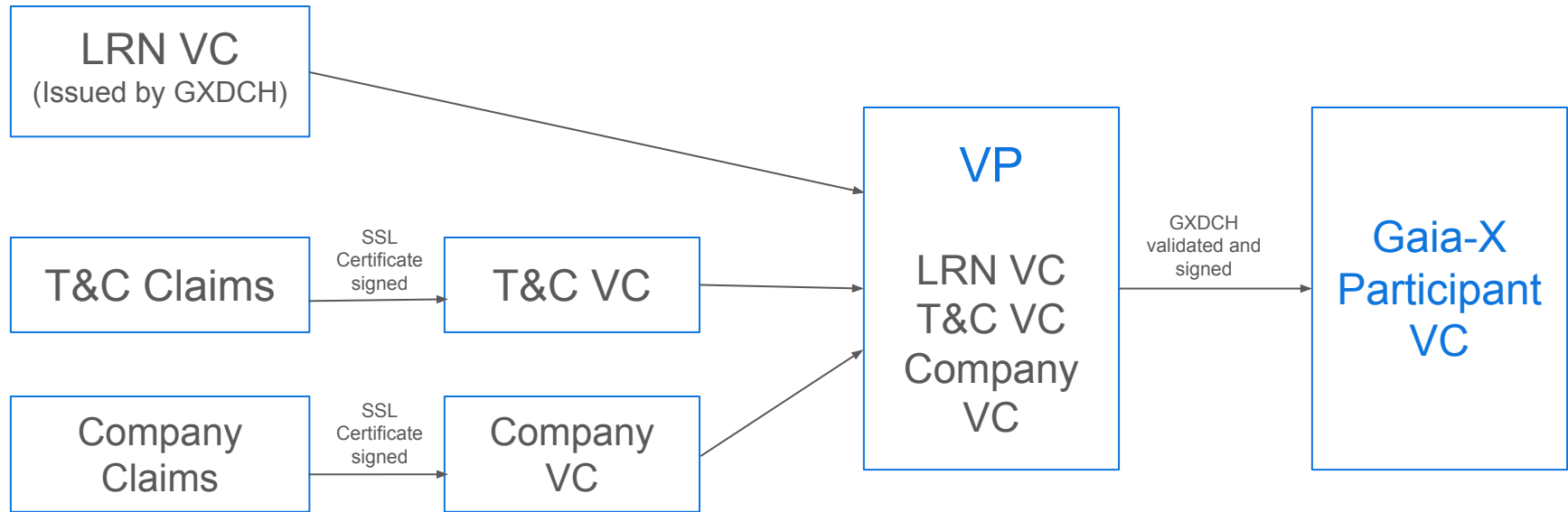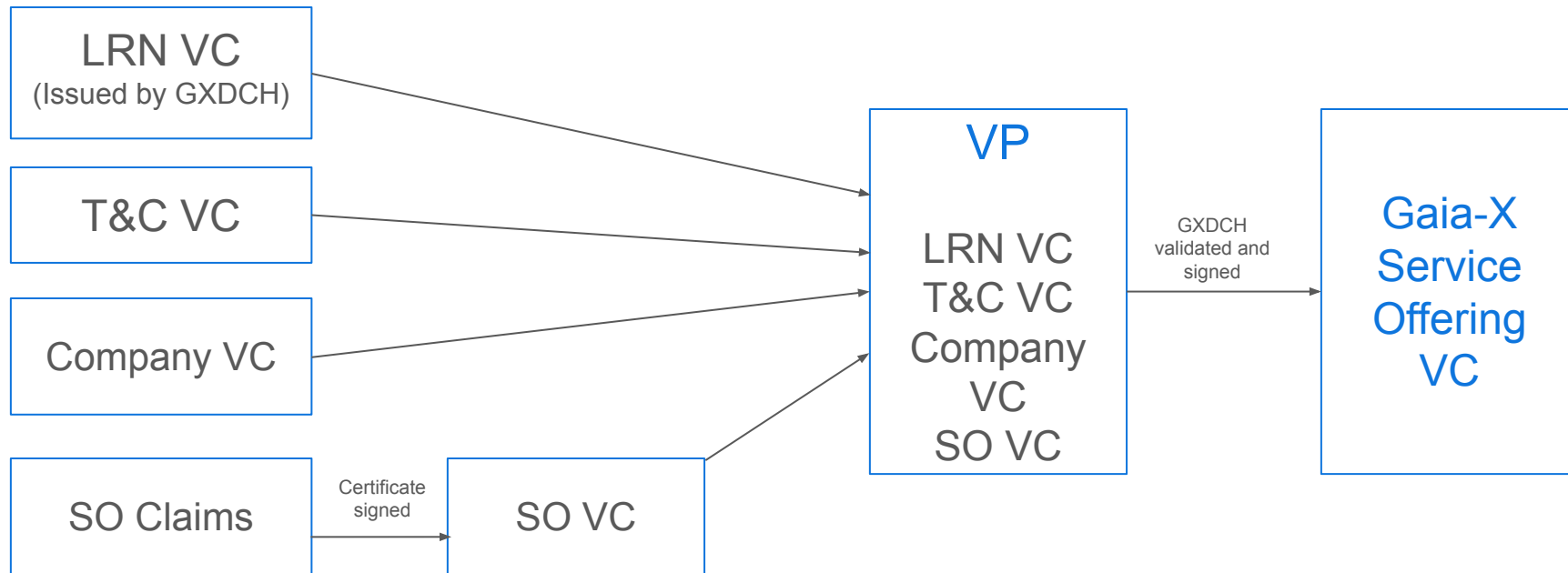
arsys

Service Offering Credential

A **service offering** is made up of a set of resources that a provider manages and publishes in a service catalogue so that it can be consumed by the rest of the participants in the data ecosystem.

Each service offered **must have** an associated verifiable credential, which contains both the statements describing the service itself and the terms and conditions of use, as well as information about access rules and policies.

Participant VC

arsys

LRN VC (Issued by GXDCH)		

| T&C Claims | →SSL Certificate signed→ | T&C VC |

| Company Claims | →SSL Certificate signed→ | Company VC |

VP

LRN VC
T&C VC
Company VC

→ GXDCH validated and signed →

Gaia-X Participant VC

Service Offering VC

arsys

GXDCH: Gaia-X Digital Clearing House

- They are nodes where **software components** developed by the working groups - according to the specification documents and rules formulated within the framework of the Trust Framework - are run, enabling the generation and verification of the validity of verifiable credentials that identify both participants in the data space and the service offerings that are part of it.

- Each node is operated by a **service provider** according to rules defined by the Gaia-X AISBL Association, which delegates its governance to the different providers. This decentralized, open, and transparent operational approach allows for the creation of data spaces that ensure the sovereign, secure, and trustworthy sharing of information.

- The software components running on the nodes that make up the GXDCH network are the result of the work carried out in Gaia-X, and they evolve as development phases are completed, offering **new functionalities and services** to the participants in the ecosystem.

- In the version called "Tagus" (completed in the fourth quarter of 2023), there are three mandatory components (**Gaia-X Compliance, Gaia-X Registry, and Gaia-X Notarisation Service**) responsible for providing the minimum necessary functionality to generate and verify the validity of participant and service descriptions, as well as the information contained within them.

- In addition to the three aforementioned services, the GXDCH can also offer additional functionalities and tools, such as the Wizard Service, a catalog for making our service offerings available in the ecosystem, or a Wallet to store our verifiable credentials.

arsys

Certificates

Validate the chain of certificates used to sign the credential.

Proof

Verify that the claims have not been altered after the credential was generated.

Structure

The information of the credential must be structured according to the definitions of the Trust Framework.

Rules

Other validations: terms and conditions, legal registration number...