Gaia-X
IAM Framework

- Version 1.3 -

WP Identity & Trust (IAM Community) Contact Information

- Gebhard Marent, gebhard.marent[at]capgemini.com
- Martin Matthiesen, martin.matthiesen[at]csc.fi

Released versions of this working document on Nextcloud:

- https://community.gaia-x.eu/s/P23ZJNLyjf7n7Zp?path=%2FReleases

Version Information

Version	Date	Changes	Reason	Editors
1.0	18.02.2021	First release aligned with Gaia-X IAM Community	-	Gebhard Marent for the Gaia-X IAM Community
1.01	19.02.2021	Document name simplified	TAD References	Gebhard Marent, Martin Matthiesen
1.1	01.04.2021	Processed the Gaia-X feedback received	Finalizing our current state in order to become an official reference	Gebhard Marent, Martin Matthiesen for the Gaia-X IAM Community
1.2	15.07.2021	Secure Identifiers, Service Identities	-	Gebhard Marent, Martin Matthiesen for the Gaia-X IAM Community
1.3	17.02.2022	Federated Trust Model, sharpened focus on high level topics	Aligned content with TAD 2112 and I&T mission statement, removed obsolete/expired content	Gebhard Marent, Martin Matthiesen for the Gaia-X IAM Community and I&T SWG.

Table of contents

1. IAM Framework (HLD/DLD) Document

This document represents the results of the community contributions of the *Open Work Package Identity and Trust* to Gaia-X, now *Sub Working Group Identity and Trust.* It is intended as further input to the Gaia-X Architecture Document. The requirements and recommendations in this document are non-normative for Gaia-X, in case of contradictions between this document and the Architecture Document the Architecture Document is relevant.

Commenté [1]: To make the relation to the TAD clear.

1.1. Motivation

This document will show how Trust is applied in IAM within the Gaia-X Ecosystem.
The following table maps the general Gaia-X architecture objectives to the objectives of Identity & Trust, presented in this document.

Architecture Objectives	**IAM Rationale**	**IAM Implication**
Openness and Transparency	Increases acceptance	Open Standards and Specifications. Open Source and Open Software is preferred.
Interoperability	See Machine-Processability	Standardized APIs (OIDC, SSI), Gaia-X Identifier
Federated Systems	1:1 trust relationships do not scale.	Federated Trust Model
Authenticity and Trust	Inherent	Federated Trust Model
Security-by-design[1]	Company and citizen data protection	Threat Modeling / Mitigations, inherent verifiability.
Privacy-by-design[2]	Partly required by EU regulation	Our Framework must be implementable following GDPR, ISO27001
Usage-friendliness and simplicity	Increases security, adoption	OpenSource reference implementation
Machine-Processability	Quality and automation	Identifier, enforced protocols, standardized APIs

The developed/designed framework supports a layered approach, which is described more in detail in chapter 5. Layered Identity Management.

[1] For a detailed overview see for example Ross, Ronald S., McEvilley, Michael, Oren, Janet C. (2018), "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [including updates as of 1-03-2018]," Special Publication (NIST SP)-800-160). doi:10.6028/NIST.SP.800-160v1 or Paul A. Grassie, Michael E. Garcia, and James L. Fenton.2017.Digital identity guidelines. Technical Report. NISTSpecial Publication 800-63-3. doi:10.6028/NIST.SP.800-63-3

[2] See for example George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea and Stefan Schiffner. "Privacy and Data Protection by Design – from policy to engineering". Report. ENISA, December 2014. doi:10.2824/38623

The “Federated Identity Model” in the Executive Whitepaper 2020 (Driver of digital innovation in Europe) is the baseline for a further developed one, which relies on a Federated Trust Model using two layers, we call them Participant Layer and Principal Layer. In practice, this means that Participants use a selected few Identity Networks for mutual verification and trust establishment, SSI being the recommended option for interoperability. After trust is established, underlying existing technologies already in use by Participants (on the “Principal layer”) can be federated and reused, for example Open ID Connect or domain specific x509-based communication protocols.

In this document we consider only B2B use cases. B2C Identity Management Systems might be considered in a future release of this document. Presently Participants do not need to change their existing B2C Identity Systems to participate in Gaia-X.

This version of this document was created between July 2021 and February 2022. Sources:

- GAIA-X IAM Framework v1.2.pdf
- Community alignment sessions twice a week, prepared by Gebhard Marent and Martin Matthiesen

Unless explicitly mentioned graphics are created by this group.

1.2. Contributors

The following Contributors have actively contributed to this release. For older releases see sources URL above.

Name	**Organization**
Inés Atug	HiSolutions AG
Gernot Boege	FIWARE Foundation e.V.
Florian Bühr	Hewlett Packard Enterprise
Theo Dimitrakos	Huawei Technologies Co., Ltd
Mohamed Amine Essifi	BMW
Hannes Hahkio	CGI
Peter Koen	Microsoft
Nicolas Liampotis	GRNET/EGI Foundation
Boris Lingl	DATEV eG
Petteri Kivimäki	Nordic Institute for Interoperability Solutions
Gebhard Marent	Capgemini Deutschland GmbH
Martin Matthiesen	CSC - IT Center for Science

Valeri Parshin	Fujitsu TDS GmbH
Anne-Marie Praden	Thales
Augusto Sansoni	Aruba S.p.A.
Sergiu Stejar	1&1 IONOS SE
Bastien Vigneron	Outscale

1.3. Definitions

For better understanding, the following terms, aligned with the Glossary chapter of the Technical Architecture Document (TAD 2109) from September 2021, are listed here again.

Other Terms/Definitions	**Description**
Conformity Assessment Body (CAB)	Body that performs Conformity Assessment services[3].
Claim	An assertion made about a subject within Gaia-X.[4]
Credential	A set of one or more Claims made and asserted by an Issuer.
Federated Catalogue	Federated Catalogue is a Gaia-X Federation Service. It enables the discovery and selection of Providers and Service Offerings in a Gaia-X Ecosystem.
Self-Description	A Self-Description expresses characteristics of an Resource, Service Offering or Participant and describes properties and Claims while being tied to the Identifier.
Service Offering	A Service Offering is a set of Resources, which a Provider bundles into an offering. A Service Offering can be nested with one or more Service Offerings.
Verifier	Is used in the TAD. Definition from W3C: “A role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation for processing.”

[3] DIN EN ISO/IEC 17000
[4] https://www.w3.org/TR/vc-use-cases/#terminology

Other Terms/Definitions	Description
Holder	Is used in the TAD. Definition from W3C: “A role an entity might perform by possessing one or more verifiable credentials and generating presentations from them. A Holder is usually, but not always, a subject of the verifiable credentials they are holding. Holders store their Credentials in credential repositories.”
Issuer	Is used in the TAD. Definition from W3C: “A role an entity can perform by asserting Claims about one or more subjects, creating a verifiable credential from these Claims, and transmitting the verifiable credential to a holder.”

The following definitions are used in the context of the IAM Framework.

Terms/Definitions	Description
Chain of Trust	If trust is derived from a root of trust through an intermediary, we have a chain of trust. Examples are Gaia-X conformant CABs and Principals of Participants.
Consumer	A Consumer is a Participant who consumes Service Instances in the Gaia-X Ecosystem to enable digital offerings for End Users.
Credential Manager (CredMgr)	In this document the name of the credential repository used by a Holder.
End User	A natural person or process not being a Principal, using a digital offering from a Participant. Participants manage their relations with End-Users - including identities - outside of the Gaia-X Ecosystem scope
Federated Trust Component	A Federation Service component, which ensures trust and trustworthiness between Gaia-X and the interacting Identity System of the Participant. This component guarantees Identity proofing of the involved Participants to make sure that Gaia-X Participants are who they claim to be.
Federation Plugins	Different Identity System Technologies used by Participants can be federated using Federation Plugins. The Federation Plugin transfers an established Participant Trust to the Principal Layer.
Gaia-X Verifiable Data Registry	The Gaia-X Registry is the single source of truth for the Ecosystem, it is a public distributed, non-reputable, immutable, permissionless database with a decentralized infrastructure and the capacity to automate code execution.
Identity	An Identity is a representation of an entity (e.g. Participant/Resource) in the form of one or more attributes that allow the entity to be sufficiently distinguished within context. An Identity may have several Identifiers..

Identity Networks	Identity Networks enable trusted Identity transactions of Gaia-X Participants. Before taking on any role (i.e. Provider, Consumer, CAB, Federator) in Gaia-X, all Participants need to be part of a compliant Identity Network first.
Identity Network Client	The Identity Network Client is the interface to the Identity Network. The client sends/receives requests to the Network using the specific protocol.
Identity Resolver Service	The Identity Resolver Service resolves Identities using the Identity Network Client.
Identity System (IDS)	The Identity System represents the existing identity system used by a Participant. An example would be a corporate identity network.
Participant	A Participant is an entity which is identified, onboarded and has a Gaia-X Self-Description. A Participant can take on one or multiple of the following roles: Provider, Consumer, Federator, CAB.
Principal	A Principal is an entity which is a member of a Participant. A Principal can be either a natural person or a digital representation of a Participant's Resource.
Principal@Provider	Principal of a Gaia-X Participant in the context of the Provider role.
Principal@Consumer	Principal of a Gaia-X Participant in the context of the Consumer role.
Provider	A Participant who provides Resources in the Gaia-X Ecosystem.
Root of Trust	Root of Trust is a concept that starts a chain of trust. It is a source that can be trusted in a given context. Examples for roots of trust can be: The Gaia-X AISBL, an Ecosystem like Catena-X, non-Gaia-X conformant CABs, a certificate.
Verification Service	The Verification Service can verify credentials provided by Participants.
Visitor	Anonymous, non-registered entity (natural person, bot, ...) browsing a Gaia-X Catalogue.
Provider AM	The Provider Access Management is a component owned by the Provider that will grant access during the Service ordering process, for the Consumer to the Service Instance created by the Provider.
Service Delivery Layer	The Service Delivery Layer realizes the Service Offerings as Service Instances.

Service Contract	A Service Contract is an agreement (contract) between a Consumer and a Provider, to allow and regulate the usage of one or more Service Instances. It is related to a specific version of a Service Offering from which it derives the attributes of the Service Instances to be provisioned. The Service Contract has a distinct lifecycle from the Service Offering and additional attributes and logic.
Service Instance	A Service Instance is the instantiation of a Service Offering at runtime, strictly bound to a version of a Self-Description. The Service Instance has a unique Identity and can be composed of one or more atomic building blocks which must be identifiable as they associate to a Service Contract.
Gaia-X Tag	A Gaia-X Tag is an attribute which is obtained through a process. This process confirms conformance or compliance to a standard or certification scheme with a level of assurance in accordance with Gaia-X rules. The Tag can be proven using e.g. verifiable credentials. Tags can contain additional information about the intended scope and visibility. On the level of Service Offerings, Gaia-X Tags are called Gaia-X Labels.

2. Functional Model of Identity Identifiers

Gaia-X Participants use Identifiers which need to be unique and interoperable. This chapter lists the aligned characteristics of the Identity Identifier, the Identifier format across the supported technologies and the IAM Identifier requirements. For IAM, we agreed to have an Identifier format for both Participants and Principals.

2.1. Requirements for Identity Identifiers Participant/Principal

There SHALL NOT be Gaia-X issued Identifiers, we will reuse existing identifiers. Identifiers in Gaia-X MUST fulfill the following requirements.

RI1	Identifiers used for Identities shall be unique within its context.
RI1a	The context of an identifier must be uniquely identifiable within Gaia-X.
RI1b	There must be a mechanism to guarantee uniqueness based on an existing identifier and its context.
RI2	Identifiers are generated and controlled by the Identity System of a Participant.
RI3	It is solely the responsibility of a Participant to determine the conditions under which the Identifier will be issued.
RI4	Identifiers can be referenced without publishing the Identifier beforehand in a separate system.
RI5	Identifiers shall be derived from the native identifiers of an Identity System without any separate attribute needed. The Identifier shall provide a clear reference to the Identity System technology used. OpenID Connect and DID shall be supported. Any scheme for

	Identifiers must permit future extensions to the scheme.
RI6	It is intended that the lifetime of an Identifier is permanent. That is, the Identifier will be globally unique forever, and may be used as a reference to a resource well beyond the lifetime of the resource it identifies or of any naming authority involved in the assignment of its name [RFC1737]. Reuse of an Identifier for a different entity is forbidden.
RI7	An Identifier should support resolution. There must be a mechanism that enables authorized entities to obtain associated contextual information from an identifier such as Participant, location, ecosystem, contract and linkable address (e.g. URL) in the case of computational resources. For Identifiers that have corresponding URLs or other resource access protocols, there must be some feasible mechanism to associate an Identifier with an address of the resource [RFC1737].
RI8	The Identifier shall be comparable in the raw form. It shall not be needed to make any transformation to compare two Identifiers and tell whether they are the same.
RI9	Identifiers should not contain more information than necessary (including Personal Identifiable Information).
RI10	The identifier needs to express the identity system it was issued with.

2.2. Secure Digital Identity Identifier requirements

A 'Secure Digital Identity' is a unique Identity with additional data for robustly trustworthy authentication of the entity (i.e. with appropriate measures to prevent impersonation).

Requirements:

SDI1	Resolvable Identifiers MUST support verifiable Claims[5] as defined by W3C.
SDI2	The integrity MUST be verifiable (for example using cryptographic algorithms).
SDI3	The Identity MUST be traceable to its Issuer.
SDI4	Issuers MUST be identified using Gaia-X compliant Identifiers.
SDI5	Identifiers MUST be immutably bound to a tamper-proof Credential.
SDI6	The process of identifying the holder of an Identity MUST be publicly verifiable and the process owner itself MUST be trustworthy.
SDI7	It MUST be possible to invalidate a Secure Identifier (for example using revocation lists).

[5] https://www.w3.org/TR/vc-use-cases/#:~:text=A%20verifiable%20claim%20is%20a,home%20address%2C%20or%20university%20degree

2.3. Principal Identifier format

Identifiers used for Principal Identities shall be URIs following the [RFC3986] and re-using the existing schemas if possible.

Generally, the format should indicate the protocol, i.e. in URI form if supported by the used standard. If the identity standard does not provide this, the identifier must resolve to a Self-Description containing this information.

Alternatively a private URI schema *org.gaia-x.<protocol>* can be defined where necessary [BCP35[6]]. The schema shall define additional semantics to indicate the underlying protocol. The generic structure of the Identifier would take the form: *<schema>:<protocol specific identifier>.*

Following the recommendations above will ensure interoperability within and between Ecosystems.

2.4. Participant Identifier format

The Participant Identifier format essentially follows the Principal Identifier format with the exception that all Participants need to support all possible formats of other Participants. For interoperability reasons the number of supported formats should be limited to an absolute minimum.

[6] https://www.rfc-editor.org/info/bcp35

3. Functional Identity Management Requirements

3.1. General Assumptions

Trust of Identities for the verification of the verifiable identity document/token is inherited from the Participants:

> *Provider X Service or Principal A and Consumer Y Service or Principal B trust their respective identities because Provider X and Consumer Y trust each other as Gaia-X Participants (result: successful mutual authentication).*

Participants can verifiably demonstrate that they are members of a Gaia-X compliant Ecosystem and that they fulfill the membership criteria.

3.2. General IAM requirements for the Principal Layer

R1	Existing Identity System solutions should be capable of being integrated into Gaia-X compliant Ecosystems.
R2	Identity management is done in a fully decentralized manner, thus not relying on a centrally managed component.
R3	Gaia-X Principals are uniquely identified by an Identifier.
R4	The disclosure of identity attributes is minimal according to relevant policies (e.g. user consent, Gaia-X compliance, Participant policies).
R5	Traceability requires agreement of the involved Participants.
R6	Participants are responsible to decide on and enforce trust. This is supported by trust anchors like TSPs/CABs acknowledged by the Gaia-X Association.
R7	Identity management also supports technical components.
R8	Identity management supports means for tracking Claims that are signed by third parties (such as certification results signed by evaluation facilities or certification facilities).
R9	Information associated with Identities support authorization.
R10	The authentication mechanism must comply with relevant policy and regulations, like e.g. eIDAS.

3.3. Service Identity requirements

In this chapter a Service as defined by ISO 20000[7] is described by using its parts. The Service is offered using a Service Offering, ordered using a special type of contract, which we call

[7] A Service is the “means of delivering value for the customer (3.2.3) by facilitating outcomes the customer wants to achieve”.

Service Contract and utilized using a defined Service Instance. Note that the term service itself is not strictly defined below and not used on its own[8]. The refinement of these concepts is out of scope for this document and is currently (February 2022) in scope for the Service Composition WG.
The following requirements for the Service Identity are needed in order to achieve interoperability, trustworthiness from the perspective of SWG I&T.

1. All requirements for Identifiers in chapter 2.1 apply.
2. We recommend using Secure Identifiers as described in chapter 2.2.
3. Service Offerings, Service Contracts and Service Instances have unique Identifiers and one respective distinct Identity and thus a respective Self-Description[9].
4. Service Instance Identities are associated with Service Offerings and Service Contract. This association needs to be reflected in the relevant attributes.
5. There must be a separate functionality for
    a. attestation
    b. authentication & identification
    c. access control.
6. In order to enable Service Composition, every Service Instance MUST provide its output in standardized machine readable way.

Further information regarding scope and use cases can be found in Appendix 6.3. Use Case "Sensor Data" (service-centric).

https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-10:ed-1:v1:en:term:3.2.15
In Gaia-X terms, this customer is a Consumer.

[8] "A Provider offers a Service, which the Consumer orders and the Provider then provides", means in Gaia-X terms: A Provider creates a Service Offering. A Consumer orders a Service Instance using a Service Contract. The Provider makes the Service Instance available to the Consumer.

[9] The Self-Description of a Service Offering describes the range of options for a later Service Instance. The Self-Description of a Service Contract links the Service Offering to a Service Instance, and can have additional information like the duration of the contract and individual pricing. The Self-Description of the Service Instance inherits most of its properties from the Service Offering, some from the Service Contract and has some possible runtime properties of its own, like an IP address.

4. Federated Trust Model

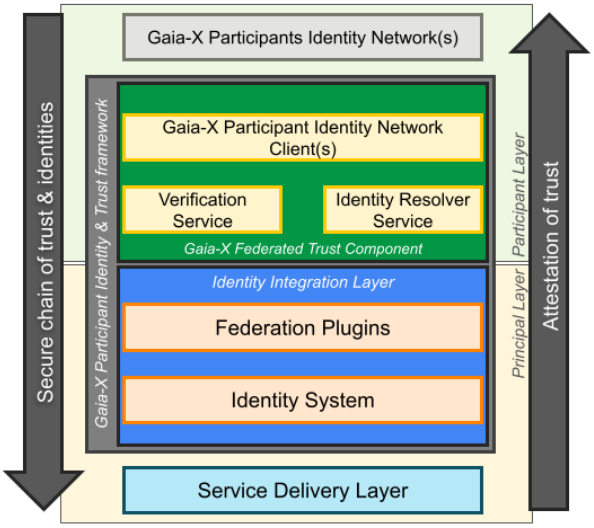
Trust in Gaia-X covers identification, authentication and authorization, credential management, decentralized Identity management as well as the verification of analogue credentials.

4.1. Federated Trust Model - High Level View

This chapter describes the components required to provide an attested secure Chain of Trust & Identities[10].
Service implementations and the corresponding service delivery layer may include End-User services, distributed microservice architectures across multiple Participant domains, and/or cross domain data or digital service delivery.

4.1.1. Architecture principles for this approach

Mutual trust based on mutually verifiable Participant identities between contracting Participants, Provider and Consumer, is fundamental to federating trust and identities in the Principal layer. Participants are responsible for issuing credentials for their Principals.
Heterogeneous ecosystems across multiple identity networks in the Participant layer must be supported as well as heterogeneous environments implementing multiple identity system standards.
The high degree of standardization of Participant layer and Principal layer building blocks of the Gaia-X Federated Trust framework must ensure that there is no lock-in to any implementation of identity network and identity system likewise.



[10] Please refer to chapter 1.3. Definitions where some elementary concepts and components of the Federated Trust Model are defined.

4.1.2. Chain of trust and identity

The Gaia-X Participant Identity & Trust framework delivers a secure chain of trust and identities to the service delivery layer.

Mutual participant verification
In the Participant layer, the Gaia-X Federated Trust Component implements the functionality to resolve and verify the identity of the contracting Participants. The Consumer verifies the Provider identity, the Provider verifies the Consumer identity.
Successful mutual Participant verification results in a verified Participant Token representing the trust between Provider and Consumer.

Identity System federation
In the Principal layer, the Federation Plugin implements the functionality to federate trust between the Identity Systems of the contracting Participants based on the successful mutual Participant verification described above.
The federation of trust between the identity systems is based on the identity system standard implemented for the service delivery layer. Required for the federation is a secure mutual exchange of the required federation metadata and an agreement on the duration of the federation.

Exemplary Identity Systems standards supporting federation are: OIDC/OAuth2 (draft), SAML, SPIFFE/SPIRE.
Identity System federation may also include federating the trust between certificate authorities supporting X.509 for Principals.

Identification and Authentication
Once successfully federated, the Identity Systems are enabled to identify and authenticate the Principals in the Service Delivery Layer of the contracting Participants. Federated Principal identities are mutually trusted based on the federation of the Identity Systems of the contracting Participants.

4.1.3. Attestation of trust

In addition to providing a secure chain of trust and identity, the Gaia-X Federated Trust framework attests the chain of trust from service delivery layer to the Participant identity.
The attestation may include according to required trust policies of the service delivery:

- resolving the Participant identity
- checking the relevant attributes of the Participant identity
- attesting the mutual Participant verification
- attesting the exchanged federation metadata

4.1.4. Integration of the framework

The Gaia-X Federated Trust framework is in essence agnostic to implementations of identity network, verification method as well as identity system standard.

Gaia-X Participants Identity Network integration

Different networks are supported by corresponding implementations of the Gaia-X Federated Trust Component serving as a client component of the Gaia-X approved Participant identity network. Provider and Consumer do not need to be registered on the same network. On each side the respective Gaia-X Federated Trust Components need to integrate with the network the contracting partner is registered with.

Principal Identity Integration Layer

While the interface to the Gaia-X Federated Trust Component is standardized, the federation mechanism of the Federation Plugin is specific to the implemented Identity System supporting current and future standards like OIDC/OAuth2 (draft), SPIFFE/SPIRE, PKI.
Furthermore, multiple Identity Systems required for complex service offerings, e.g. OIDC for user Principals, SPIRE for service Principals, are perfectly supported meaning that multiple Identity Systems on either side can be federated by corresponding plugins based on the very same mutual Participant identity verification if required for the service delivery.

5. Layered Identity Management

The Gaia-X IAM Framework supports two layers, the Participant layer and the Principal layer. Both approaches are described in the following subchapters. The next version of this document will have more details on how to integrate these two Layers.

5.1. Participant Layer - Decentralized Approach

For the Identity Management of the Participant Layer as described in chapter 4, we strongly recommend a decentralized identity model, for example self-sovereign identity (SSI[11]) implementations. The implementation may need to be extended to conform to the Trust Model outlined in chapter 4, for example to enable Participants sovereignty in exercising the recognition of authority relative to other Participants, like CABs.

Participant Identities are represented by Decentralized Identifiers (DIDs) and a DID document. A Participant DID is in control of the related Participant that it identifies. A DID connects the subject with a DID document allowing trustable interactions and resolving additional metadata. A DID document consists of different parts like cryptographic material for verification or service-endpoints for interaction.

Reference: https://www.w3.org/TR/did-core/

This combination of resolvable DIDs and public keys allow the verifiable attestation of Participant attributes, so-called Verifiable Credentials (VC), giving the Participant complete control of it's digital identity. This is the second key element of SSI. A Verifiable Credential is comparable to a physical credential in a digital world with the addition to be automatically verifiable through signatures and the DPKI (Decentralized-PKI).

Reference: https://www.w3.org/TR/vc-data-model/

5.2. Principal Layer

Participants in Gaia-X will start with various technologies on the Principal Layer, like for example OIDC, X509, SAML2, Spiffe, LDAP and others. See chapter 6.2 for examples.

[11] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=379913698

6. Appendix

6.1. Examples for Identifier formats

For currently envisioned technologies the following schema and protocol specific identifier specification can apply:

6.1.1. OpenID Connect

Since the Identifier needs to indicate the underlying protocol with which it was issued, we propose the following structure for Identifiers issued using OpenID Connect:

org.gaia-x.openid:<iss>;<sub>
";" is chosen as a separator because it is not a part of URL (iss), nor a part of the email address specification (sub) and also not a part of the base64 character set

Example:
org.gaia-x.openid:https://myidp.org/auth/realms/master;YWxpY2VAZm9vLmNvbQ

6.1.2. DID

DID URI schema is defining the relevant structure already (did:<method>:<identifier>), so there is no need to define it in the Gaia-X context.

Example:
did:web:foo.com

6.2. Examples of Principal Layer Technologies

These examples are not complete. A further revision of this document will include more specific examples on how to integrate relevant technologies.

6.2.1. OpenID Connect

Identity System Providers should implement the following OpenID Connect Profiles[12]. These profiles are:

- Hybrid Relying Party

6.2.2. DID and DID methods

DID can be supported natively and via the OpenID Connect SIOPv2 DID Profile.
Some additional information can be found here:
https://github.com/WebOfTrustInfo/rwot8-barcelona/blob/master/final-documents/did-auth-oidc.md

DID methods requirements

[12] https://openid.net/wordpress-content/uploads/2018/06/OpenID-Connect-Conformance-Profiles.pdf

The requirements need to be derived from other working groups like Compliance.

Existing DID methods
There will be a list of supported DID methods maintained by the Gaia-X Federated Trust Component.
For all available methods see https://www.w3.org/TR/did-spec-registries/#did-methods.

6.2.3. Other Technologies

We do not recommend to federate SAML2 directly for the following reasons:

- All potential SAML2 participants will likely have to support OIDC
- Interconnect between SAML2 and OIDC is possible, there are bridge solutions available on the market.
- SAML2 significantly increases the complexity.

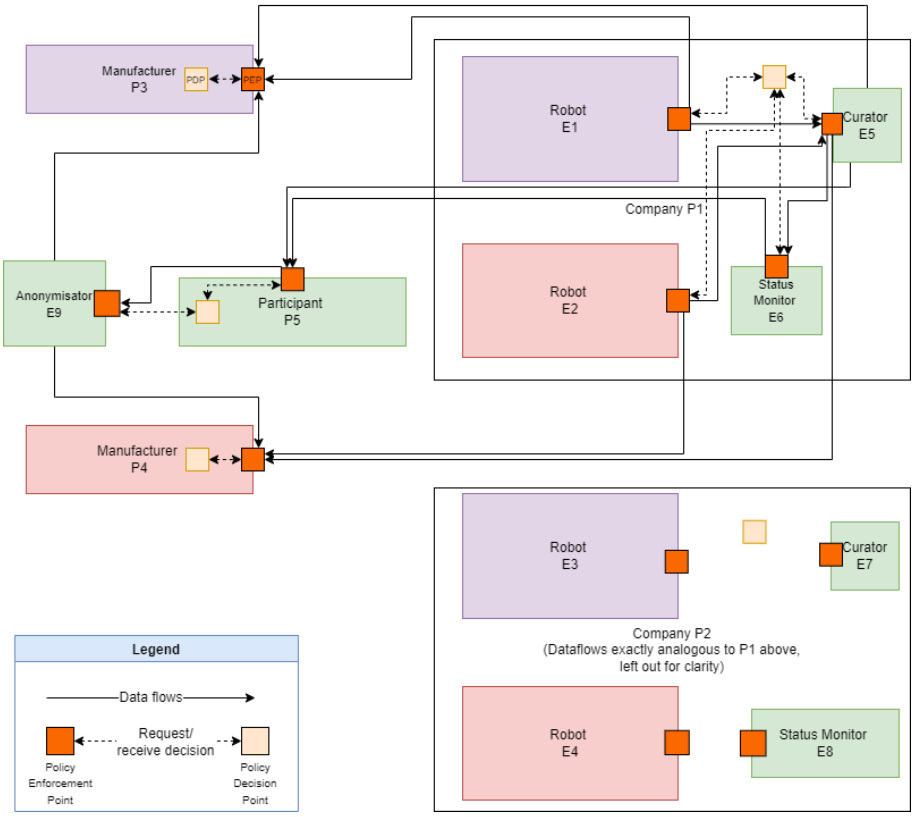
6.3. Use Case “Sensor Data” (service-centric)

For clarification purposes, we defined the following scope for our use case example:

	Service Offering	**Service Contract**	**Service Instance**	**Provider Internal Subcomponent of Service Instance**
Gaia-X compliant Identity/Identifier and Self-Description	Yes	Yes	Yes	No
Scope of	Provider	Provider/ Consumer	Provider	Out of scope for Gaia-X

Use Case Description:
The use case consists of five Participants (**P1-P5**) and nine Service Instances (**E1-E9**, each having an Identity and a corresponding Identifier). Of the Participants four are manufacturers:

- The Robot Manufacturers **P3** and **P4** provide **robots.**
- The robots are used by the Companies **P1** and **P2** which are manufacturers of products for End-Users, like cars, washing machines or TVs. In this scenario they produce similar products.
- The robots provide sensor data which is curated by the Participant **P5** and prepared for display on the **status monitor** on the shop floor.
- The companies **P1** and **P2** also provide Participant **P5** with aggregated selected data.
- Data ownership (Robot Manufacturer P3/4 vs. Company P1/2, P5) is defined in contracts.
- When the data is processed by Participant **P5** it is anonymised and offered to the robot manufacturers to improve their products.



The graphic above shows possible data flows, for simplicity only the flows regarding **P1** are shown, the flows in **P2** are similar. Data is only passed on to the next recipient if a clear policy allows it, using **policy enforcement points,** which are in this case logically separated from the **policy decision points**.

7. Meeting Minutes / Backlog

The I&T meeting minutes / backlog can be found here:
https://docs.google.com/document/d/1_PMuHPcj0-h1gRwIgxKkiC_z2buNboUqjrV14pS52M0/edit