# About GAIA-X

With Gaia-X, representatives from business, science and politics on an international level create a proposal for the **next generation of data infrastructure**: an open, transparent and secure digital ecosystem, **where data and services can be made available, collated and shared in an environment of trust**.

Gaia-X is a project initiated by Europe for Europe and beyond. Representatives from business, politics, and science from Europe and around the globe are working together, hand in hand, to create a federated and secure data infrastructure. Companies and citizens will collate and share data – in such a way that they keep control over them. **They should decide what happens to their data, where it is stored, and always retain data sovereignty**.

The architecture of Gaia-X is based on the **principle of decentralisation**. Gaia-X is the result of a multitude of individual platforms that all follow a common standard – the Gaia-X standard. Together, we are developing a data infrastructure based on the values of openness, transparency, and trust. So, what emerges is not a cloud, but a networked system that links many cloud services providers together.

## Targeted Domain

1. Agriculture
2. Energy
3. Finance
4. Geoinformation
5. Health
6. Industry 4.0/SME
7. Mobility
8. Public Sector
9. Smart City/Smart Region
10. Smart Living

The Gaia-X Hub Germany contributes to the goals of the European data strategy, especially regarding the development of European data spaces and ecosystems. In addition, it supports the user side in the development of use cases and contributes to the scaling of the Gaia-X services. It supports the establishment and further development of a sovereign data infrastructure based on [Federation Services](https://gaia-x.eu/what-is-gaia-x/federation-services) and [Policy Rules & Standards](https://gaia-x.eu/what-is-gaia-x/standards). The local Gaia-X actors can network within the Gaia-X Hub Germany and are supported in their endeavours to promote a sovereign data infrastructure.

Gaia-X promotes federations, a new model of cloud data exchange that is orthogonal to the existing dominant model of hyper-concentration of data. Data are acquired in all sectors across the globe. **They shall no more be concentrated in single places**. **The new way of computing is a continuum from the edge**, i.e., from devices and data sources in the field directly to the cloud. This minimises the need for data bandwidth, bringing the computing processes to the data and adapting to the phenomenon of data-gravity.

Through Gaia-X federations and federated services, **several data owners can exchange data amongst each other minimising data transfers and leveraging services for data that are guaranteed in terms of identity, description, service characteristic, service controllability and, more in general, can be trusted.**

Through Gaia-X federations, several technology providers can create and offer a network of services with common identity, common self-description, common controllability, and interoperability across their nodes. This creates the necessary trust, the quality of services and the critical mass necessary to create value out of data and to deal with data-gravity and data distribution.

Through a federated model, Gaia-X providers offer a value that is not possible to obtain from highly centralised, proprietary, closed, non-federated and non-interoperable technologies that currently dominate the market and, as a matter of fact, do not provide for the level of trust requested by users.

Gaia-X facilitates the interlinking of all participants in the digital economy – in accordance with European values and standards. For the portability, interoperability and interconnection of the infrastructure, the applications and the data, a set of policy rules and an architecture of standards is defined.

Specification

<https://www.gxfs.de/federation-services/overview-specification-documents/>

The following technical specifications have been drawn up in Spring 2021 and were awarded in an EU-wide tender. Starting in December 2021 the winning bidders are now going to implement the first set of Federation Services, which will create an GXFS open-source reference implementation.

| Lot # | Name | Description | Specification document |
| --- | --- | --- | --- |
| 1 | Authentication/ Authorization | [Lot 1: Authentication/ Authorization](https://www.gxfs.de/public-tender/lot-1-authentication-authorization/) | [SRS\_GXFS\_IDM\_AA](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_IDM_AA.pdf) |
| 2 | Personal Credential Manager | [Lot 2: Personal Credential Manager](https://www.gxfs.de/public-tender/lot-2-personal-credential-manager/) | [SRS\_GXFS\_IDM\_PCM](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_IDM_PCM.pdf) |
| 3 | Organization Credential Manager | [Lot 3: Organization Credential Manager](https://www.gxfs.de/public-tender/lot-3-organizational-credential-manager/) | [SRS\_GXFS\_IDM\_OCM](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_IDM_OCM.pdf) |
| 4 | Trust Services API | [Lot 4: Trust Services API](https://www.gxfs.de/public-tender/lot-4-trust-services-api/) | [SRS\_GXFS\_IDM\_TSA](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_IDM_TSA.pdf) |
| 5 | Core Catalogue Functions | [Lot 5: Core Catalogue Functions](https://www.gxfs.de/lot-5-core-catalogue-features/) | [SRS\_GXFS\_FC\_CCF](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_FC_CCF.pdf) |
| 8 | Data Contract Service | [Lot 8: Data Contract Service](https://www.gxfs.de/public-tender/lot-8-data-contract-service/) | [SRS\_GXFS\_SDE\_DCS](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_SDE_DCS-1.pdf) |
| 9 | Data Exchange Logging Service | [Lot 9: Data Exchange Logging Service](https://www.gxfs.de/public-tender/lot-9-data-exchange-logging-service/) | [SRS\_GXFS\_SDE\_DELS](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_SDE_DELS-1.pdf) |
| 10 | Continuous Automated Monitoring | [Lot 10: Continuous Automated Monitoring](https://www.gxfs.de/public-tender/lot-10-continuous-automated-monitoring/) | [SRS\_GXFS\_CP\_CAM](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_CP_CAM.pdf) |
| 11 | Onboarding & Accreditation Workflows | [Lot 11: Onboarding & Accreditation Workflows](https://www.gxfs.de/public-tender/lot-11-onboarding-accreditation-workflows/) | [SRS\_GXFS\_CP\_OAW](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_CP_OAW.pdf) |
| 12 | Notarization API | [Lot 12: Notarization API](https://www.gxfs.de/public-tender/lot-12-notarization-api/) | [SRS\_GXFS\_CP\_NOTAR](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_CP_NOTAR.pdf) |
| 13 | Portal | [Lot 13: Portal](https://www.gxfs.de/public-tender/lot-13-portal/) | [SRS\_GXFS\_IP\_POR](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_IP_POR.pdf) |
| 14 | Orchestration | [Lot 14: Orchestration](https://www.gxfs.de/public-tender/lot-14-orchestration/) | [SRS\_GXFS\_IP\_ORC](https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_IP_ORC.pdf) |
|  | Reference Document Identity and Access Management | GaiaX Community Document IAM | [GX\_IDM\_AO](https://www.gxfs.de/wp-content/uploads/2021/08/annex_GX_IDM_AO.pdf) |

## Architecture

<https://www.gaia-x.eu/sites/default/files/2021-10/Gaia-X_Architecture_Document_2109.pdf>

<https://www.gxfs.de>

**6.1.2 Organisation Credential Manager (OCM)**

The OCM establishes trust between the different Participants within the Gaia-X ecosystem by offering credentials to company

Participants and managing credentials of the organisation.

**6.1.3 Personal Credential Manager (PCM)**

PCM acts as a user representative, securely holding the acquired distributed identity credentials and identity attributes, providing the

technical means to selectively disclose the attributes for authentication and service consumption. The PCM as a Gaia-X component

is used by a natural person – typically in the form of a personal wallet for a user. The PCM enables users to interact with the SSIbased

ecosystem through VC’S and DID’s in a privacy-preserving way. The PCM form factors are smartphone-based applications and

browser-based applications/add-ons for stationary PCs and notebooks.

**6.1.4 Trust Services (TRU)**

The Trust Services are the technical implementation to enforce policies for the usage of the decentralised and self-sovereign

components of Gaia-X. The Trust Services work through cryptographic validation of the provided credentials. The Trust Services’

scope covers the technology functionalities to ensure a consistent level of trust between all Participants in Gaia-X. Further features

are verification by applying standards like LD Proof Chains/Sets, establishing policy-driven trust, providing the required trust anchors,

and ensuring trust chains between multiple Participants.

Trust Service Features

<https://www.gxfs.de/wp-content/uploads/2021/06/SRS_GXFS_IDM_TSA.pdf>

1. Verifying digital signatures of VCs
2. Signing and verifying JSON-LD proof-chains and proof-sets
3. Managing JSON-LD policies via GitOps
4. Policy evaluation to ensure policy driven trust
   1. <https://www.cncf.io/blog/2020/08/13/introducing-policy-as-code-the-open-policy-agent-opa/>
   2. <https://www.kubermatic.com/blog/opa-rego-in-a-nutshell/>
   3. <https://marketplace.visualstudio.com/items?itemName=tsandall.opa>
   4. <https://play.openpolicyagent.org/>
5. DID resolving endpoint to resolve DID documents
6. Derived verifiable credentials should be supported in further release

The creation and validation of digital signatures plays a particularly important role here. The product scope includes signing and verifying of necessary data, enabling policy driven trust, ensuring trust-chains between participants and validating eIDAS compliant signatures

Policy Management:

provides **functionalities around the signing, validation, import, export, and merge of policies from internal and external policy repos**. This is necessary to ensure that only trusted policies are imported from trusted resources

Task Controller:

To handle async policy execution

Trust Chain Verification:

Verify chain of trust

JSON-LD Signing and Verification

Signing and verification of policies and

Trusted Caching

Store securely in memory data for identities and related information

Trusted Information Exchange:

Import and export of trusted information data

Policies example for reference:

* PrincipalCredentialRequest
* GetTrustedConnectionState
* TrustedConnectionCredentials
* CredentialIssueRequest
* PresentationRevokationState

Policies Flow:

GDPR/ Federal Policy Rules -> general Gaia-x Policy -> Resource Policy -> Provider/Consumer Policy

Personal Credential Manager

Features:

1. Principal (Natural user) Onboarding/ Registration

| User Story Title | Principal user to get onboarded on Gaia-x ecosystem |
| --- | --- |
| Description | This user story will allow the principal user to get onboarded to the AISBL and allow the user to do further operations like login to the portal and be a member of Gaia-x eco system. Principal credential is also issued on registration. |
| Interface Dependent Modules | NA |
| Internal Dependent Module | OCM (AISBL) |
| Functional Requirement Ids | IDM.PCM.00008, IDM.PCM.00012, IDM.PCM.00013, IDM.PCM.00038 |
| Prerequisite | Install Gaia-x app from playstore/app store User email should not be registered for SSI wallet |
| Flow Diagram | Diagram: PCM.Flow.PrincipalOnBoard |
| Scenarios | Success:   1. Principal user should able to securely store email address on device 2. Principal user able to create wallet 3. Principal user able to create DID 4. Principal user able to connect AISBL Org 5. Principal user able to receive and accept Principal credential 6. Notification for connection established 7. Notification for credential acceptance 8. View connection details under org list 9. View issued credentials   Failure:   1. Wallet creation failed. Allow recreating of wallet for same email address 2. Mediator connection failure, It should allow to reconnect later 3. Failure to connect with AISBL, should allow the re-initiate connection and issuance flow. 4. Notification not received, resent from mediator |
| Acceptance Criteria | PCM user and wallet has been created and protected, so that only the allowed entity (user) can access their own PCM. |
| Comments |  |

2. PCM app login

| User Story Title | Principal user gets logged into PCM app |
| --- | --- |
| Description | This user story will allow the principal user to get login into PCM app |
| Interface Dependent Modules | NA |
| Internal Dependent Module | NA |
| Functional Requirement Ids | IDM.PCM.00039 |
| Prerequisite | User registration should have been successful. PCM should have indy wallet and secure store with email |
| Block Diagram |  |
| Flow Diagram | Diagram: PCM.Flow.PrincipalOnBoard |
| Scenarios | Success:   1. Enter valid emailId and wallet pin. Same will be verified from the secure store. 2. Email and pin should be secured.   Failure:   1. Combination of email and wallet pin failure. 2. Multiple failures should not lock the wallet. |
| Acceptance Criteria | PCM user can make use of protected PCM functions if authentication is successful |
| Comments |  |

1. Passwordless Login (TODO)

| User Story Title | Principal user will provide verifier with proof |
| --- | --- |
| Description | This user story will allow the principal user to produce proof using VC when requested by other GAIA-X participants. |
| Interface Dependent Modules | OCM (Proof Manager) |
| Internal Dependent Module | Trust Services |
| Functional Requirement Ids |  |
| Prerequisite | Existing Connection, Existing VC |
| Block Diagram |  |
| Flow Diagram |  |
| Scenarios | Success:   1. User should able to request for Credentials 2. User should get a Verified Credential in PCM   Failure:   1. Request is rejected |
| Acceptance Criteria | A PCM user can propose an issue credential request and receive VC in PCM. |
| Comments |  |

1. Issue Credential

| User Story Title | Principal user will get a credential |
| --- | --- |
| Description | This user story will allow the principal user to get a VC, which he can produce as proofs when required |
| Interface Dependent Modules | OCM (Attestation Manager) |
| Internal Dependent Module | Trust Services |
| Functional Requirement Ids | IDM.PCM.00008, IDM.PCM.00012, IDM.PCM.00013, IDM.PCM.00038 |
| Prerequisite | Existing Connection, Existing Schema |
| Block Diagram |  |
| Flow Diagram |  |
| Scenarios | Success:   1. User should able to request for Credentials 2. User should get a Verified Credential in PCM   Failure:   1. Request is rejected |
| Acceptance Criteria | A PCM user can propose an issue credential request and receive VC in PCM. |
| Comments |  |

1. Accept credential
2. Store Credential
3. Generate VC Presentation
4. Wallet backup
   1. Store on physical device (Decentralised as this will be under holder control)
   2. Store on cloud wallet (Custodial wallet on cloud)- This will support browser and cloud based wallet

| User Story Title | Principal user can make a secured backup of wallet on personal device |
| --- | --- |
| Description | This user story will allow the principal user to backup a wallet, using a mnemonic phrase for encryption on drive of choice. |
| Interface Dependent Modules |  |
| Internal Dependent Module |  |
| Functional Requirement Ids | IDM.PCM.00035 |
| Prerequisite | Wallet on device. |
| Block Diagram |  |
| Flow Diagram |  |
| Scenarios | Success:   1. Wallet is backed up   Failure:   1. Wallet is backed up, but incompatible to import. |
| Acceptance Criteria | A PCM user is able to backup the wallet that can be imported on any device. |
| Comments |  |

1. Wallet Restore

| User Story Title | Principal user can Restore the Pre-existing wallet |
| --- | --- |
| Description | This user story will allow the principal user to restore a pre-existing wallet, using mnemonic and wallet backup on any smartphone device. |
| Interface Dependent Modules |  |
| Internal Dependent Module |  |
| Functional Requirement Ids | IDM.PCM.00036 |
| Prerequisite | Existing Backup and Mnemonic |
| Block Diagram |  |
| Flow Diagram |  |
| Scenarios | Success:   1. Wallet is restored   Failure:   1. Wallet is not restored because of wrong mnemonic or incorrect backup |
| Acceptance Criteria | A PCM user is able to restore his wallet on any mobile device. |
| Comments |  |

Library

Open Source Module

Dependencies

High Level Diagram

Flow Diagram

Constraint

Next Phase ( Iteration -2 )

Organization Credential Manager

Features:

1. Participant Onboarding

| User Story Title | Participant (organisation) gets onboarded on Gaia-X ecosystem |
| --- | --- |
| Description | This user story will allow the participant (organisation) to get onboarded to the gaia-x ecosystem. |
| Interface Dependent Modules | NA |
| Internal Dependent Module | OCM, AISBL, TSA, Notary, Certifier |
| Functional Requirement Ids | IDM.AO.5.2.3 |
| Prerequisite | AISBL, Notary and Certifier modules should be ready to serve |
| Flow Diagram |  |
| Scenarios | Success:   1. Accept organisation data with eIDAS certificate and store in the DB 2. Notarize eIDAS VC 3. AFJ spin up successfully(Part of agent spinup process) 4. Create auto acceptance connection with AISBL 5. Auto accept Participant Credential from AISBL 6. Store connect and participant credential records in gaia-x database   Failure:   1. Handle agent spin up crash and failure. 2. Retry connection with AISBL 3. Notification failure on connection and issue credential 4. Retry issue credential on failure |
| Acceptance Criteria | A Participant/ Organization will get onboarded and verified as a valid GAIA-X recognised organisation. |
| Comments |  |

1. AISBL onboarding