

Gaia-X Lab — Onboarding Presentation

Kai Meinke – Gaia-X Lab Development Team

Pierre Gronlier – Gaia-X CTO

Friday, 08 April 2022





Mission of the Gaia-X Lab

Friday, 08 April 2022

What is the Gaia-X Lab?



- The Gaia-X Lab is a **development team** under the Gaia-X CTO office.
- The Gaia-X Lab team writes prototypes to technically validate functional and technical hypothesis made by the Gaia-X Working Groups, when working on the Gaia-X specifications.
- The team demonstrates working prototypes.
- The Lab accelerates the development of external open-source software (OSS) project.
- The Lab identifies missing functional components in the Gaia-X Specifications

Deliverables of the Gaia-X Lab?



- All results of the prototyping activities are shared with the Gaia-X Working Groups and the Gaia-X Lighthouses projects for their own considerations.
- The Gaia-X Lab doesn't contribute to the Gaia-X specs.
- The Gaia-X Lab doesn't release any official Gaia-X deliverables.
- All working activities are publicly done in the current repository.

Public Repository: https://gitlab.com/gaia-x/lab

Public Backlog: https://gaia-x.atlassian.net/browse/LAB

What happens with the Code?



Туре	Use Case	Action
Accelerator	The prototype is a feature of an existing OSS project.	It's contributed back to the OSS project.
Filler	The prototype identified a missing Gaia-X Component.	It's released as a new OSS project under the Eclipse Foundation.
Demonstrator	The prototype showcases a workflow for educational purpose	It's released as a new OSS project under the Gaia-X OSS rules.

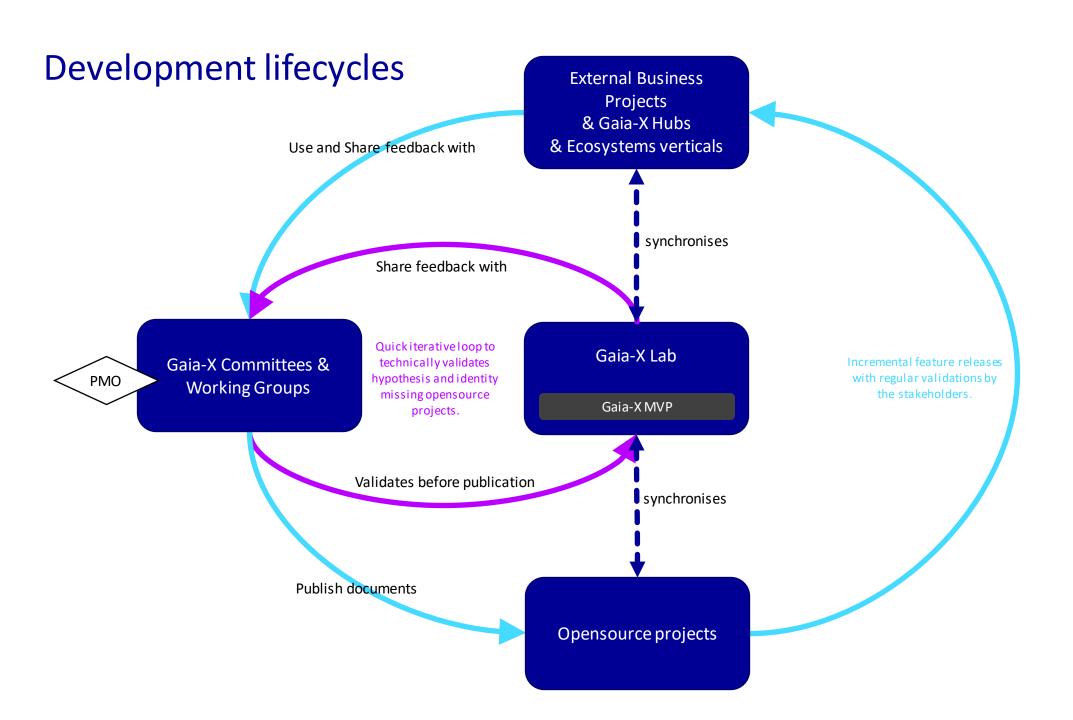
All Gaia-X Lab projects follow the Gaia-X OSS rules.

The license is either **Apache License Version 2.0** or **Eclipse Public License - v 2.0**.





Context of the Gaia-X Lab



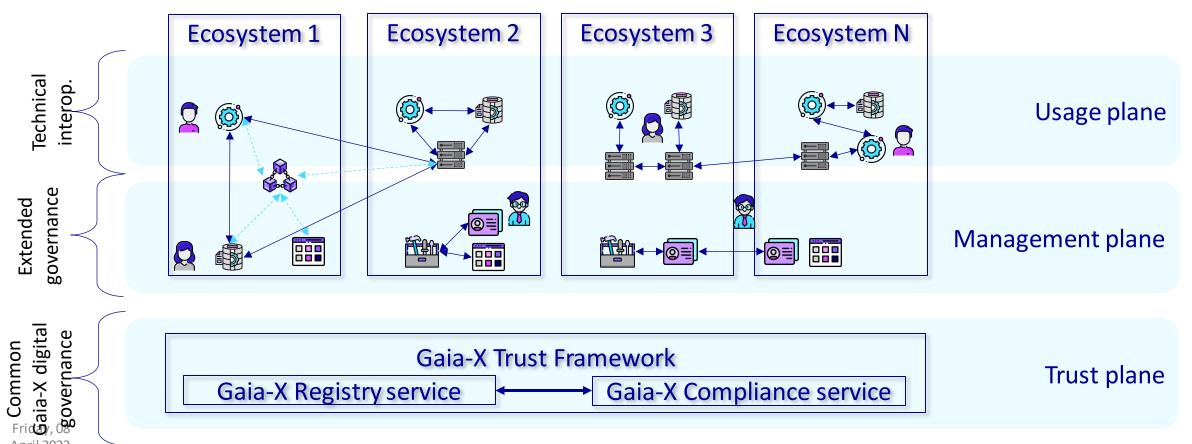
gaia-x

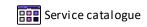
ST 500-332:Cloud Federation Reference Architecture ({

One Gaia-X Ecosystem, federating interoperable autonomous ecosystems.



Gaia-X Ecosystem: the virtual set of Participants, Service Offerings, Resources fulfilling the requirements of the
 Gaia-X Trust Framework.







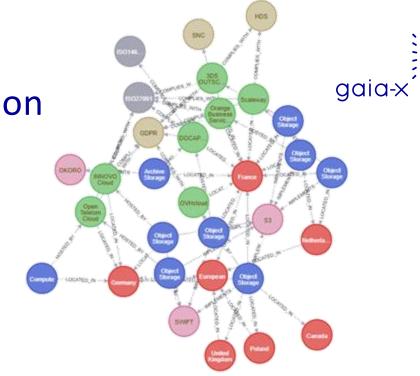




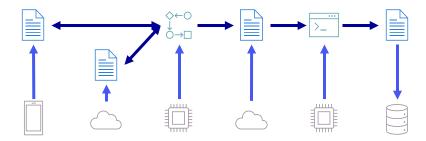


Gaia-X Trust Framework 1/2 from fragmented market to service composition

- composite services from atomic or elementary
 services as well as complex services.
- Ensuring composability and hence substitution
- Creates Transparency with portability across
 providers and hosting platforms



Knowledge graph of verifiable and composable signed claims (Catalogue demonstrator - March 2020)



Data pipeline example, from edge (mobile) to cloud

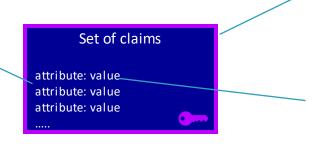
Gaia-X Trust Framework 2/2

To ensure **Trust** the Gaia-X Trust Framework is:

- Automated by Gaia-X specific components part of decentralized technology framework
- Versioned, i.e. bound to a specific version in time of the Compliance rules set
- Applied to the self-description file of all entities implied in the Gaia-X conceptual model (*)
- Aimed to verify the existence and veracity of the attributes and not judging their value

(*) as defined as part of the Gaia-X Conceptual model described in the Gaia-X Architecture document

The content
Verify if the mandatory attributes are filled in and if the values are verified.



The envelop

Verify the keypair issuers and cryptographic signatures

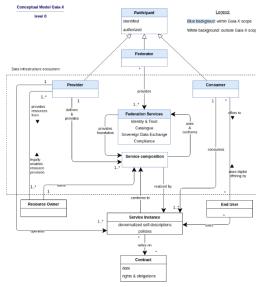
Claims

Machine readable or plain English

- Trust Framework example:
 - All cars must have a color
 - All Datasets must have a location.
 - All Services must identify their provider with its legal country of jurisdiction.

- Label examples:
 - cars level 1 are red, cars level 2 are blue, ...
 - My dataset must be located in EU
 - My services must be non-subject/immune to non-EU laws



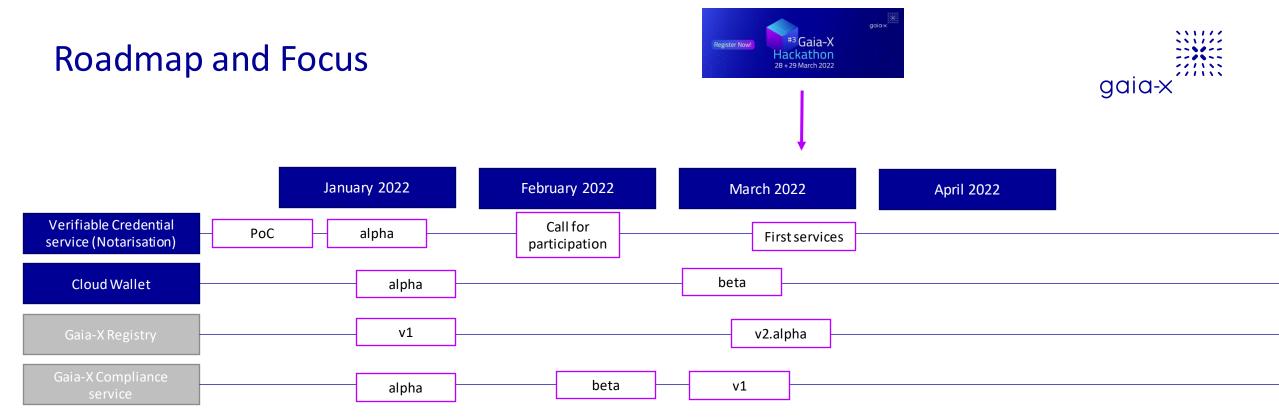








Roadmap



• Demonstration of the **Trust Framework**, Self-Sovereign Identity (SSI) & Verifiable Credentials

Gaia-X defined

Gaia-X owned

- Alpha Version of Gaia-X Registry
- First verification of Gaia-X Compliance
- Trust Framework: https://gaia-x.gitlab.io/policy-rules-committee/trust-framework/



Gaia-X Lab Onboarding Demonstrator

Gaia-X Lab Onboarding Demonstrator



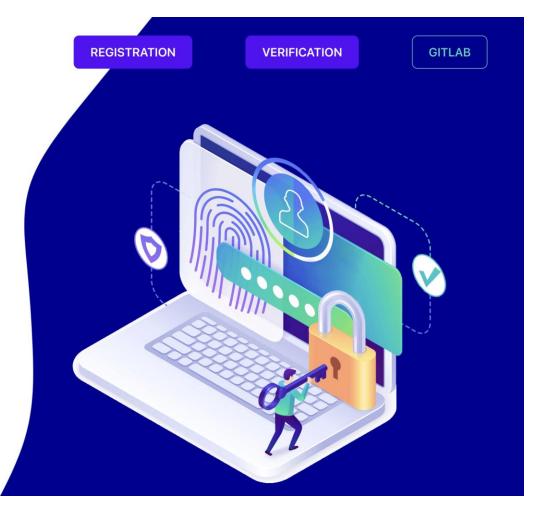
Gaia-X Lab

Onboarding Portal

This web app demonstrates how SSI could be used to issue Gaia-X participation credentials in a way that is cryptographically secure, privacy-respecting, and machine-verifiable.

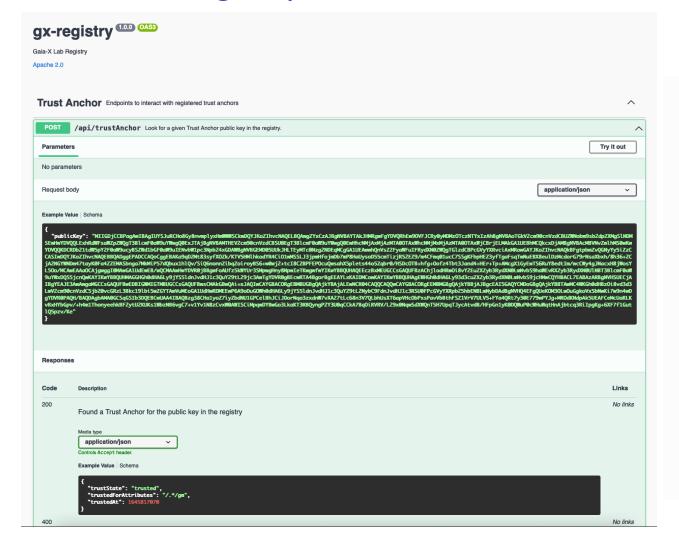
REGISTER CREDENTIAL

VERIFY CREDENTIAL



Demonstrator: https://onboarding-portal.lab.gaia-x.eu/Repositories: https://gaia-x.atlassian.net/browse/LAB

Gaia-X Lab Registry





3. List of defined trust anchors

Name	Defined as
State	The Trust Service Providers (TSP) must be a state validated identity issuer. - For participant, if the legalAddress.country is in EEA, the TSP must be eiDAS compliant. - Until end of 2022 Q1, to ease the onboarding and adoption this framework DV SSL can also be used. - Gaia-X association is also a valid TSP for Gaia-X association members.
eiDAS	Issuers of Qualified Certificate for Electronic Signature as defined in eIDAS Regulation (EU) No 910/2014 (homepage: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home) (machine: https://ec.europa.eu/tools/lotl/eu-lotl.xml)
DV SSL	Domain Validated (DV) Secure Sockets Layer (SSL) certificate issuers are considered to be temporarily valid Trust Service Providers. (homepage: https://wiki.mozilla.org/CA/Included_Certificates) (machine: https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReportPEMCSV)
Gaia-X	To be defined after 2022Q1.
EDPB CoC	List of Code of Conduct approved by the EDBP (homepage: https://edpb.europa.eu/our-work-tools/documents/our-documents_fr?f%5B0%5D=all_publication_type%3A61&f%5B1%5D=all_topics%3A125)
gleif	List of registered LEI issuers. (homepage: https://www.gleif.org/en/about-lei/get-an-lei-find-lei-issuing-organizations) (machine: https://api.gleif.org/api/v1/registration-authorities)

Demonstrator: https://registry.gaia-x.eu/api-docs/#/Trust%20Anchor/post_api_trustAnchor
Repositories: https://gaia-x.atlassian.net/browse/LAB

Features of the Gaia-X Onboarding Demonstrator



- Demonstrates working prototype of the Trust Framework
- Validates functional and technical hypothesis made by the Gaia-X Working Groups
- Accelerates the development of free open-source software (FOSS)
- Issues and verifies Gaia-X Participant Credentials, based on Self-Descriptions
- Leverages Gaia-X Participants Credentials for Access Control
- Provides a first Version of the Gaia-X Registry

Technology



- SSI Kit provided by walt.id under Apache 2.0 License, extended for Gaia-X
- Communication via HTTPS
- Using Decentralized IDentifiers (DIDs), JSON LD-based Credentials, based on DID:WEB
- Using Open ID Connect for Verifiable Presentations (OIDC4VP)
- Using Self-Issued Open Identity Provider v2 (SIOPv2)
- Cryptosuite (RSA and ED25519, SECP256K1 and others also possible)
- Registry can be used to find and verify the keys of Trust Anchors



Demonstration and Flows

Actors





• Gaia-X Participant undergoing a demo KYB process to receive a Gaia-X Credential



Gaia-X Federator / Gaia-X AISBL providing Identity Services and Credentials



• Gaia-X Service Provider offering a service to accredited Gaia-X Participants

Documents & Tools





• Self-Description Generator



• Self-Description of a Participant



Verifiable Credentials signed by the Participant and the Federator / AISBL



• Set of Credentials held by the Participant in a Credential Manager / Wallet

Infrastructure





• Private Database containing information about participants



Public Webserver to provide frontends



• Issuer / Signatory



Verifier



Credential Manager / Wallet

Gaia-X AISBL / Federator









AISBL provides Trust Framework, Federator follows Trust Framework



Federator / AISBL public key is listed in the **Gaia-X Registry** as Issuer



Federator provides **Onboarding Portal** for Accreditation



Identification via public key in DID:WEB via public Webservice



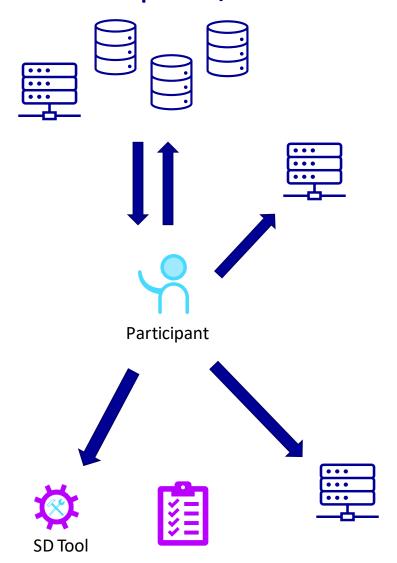
Federators provide Credential Issuer / Signatory



Federators provide Credential Validator Service / Verifier

Participant / Service Provider

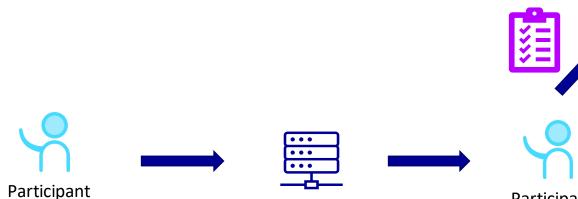




- Participant is registered with Trusted Data Sources
- Participant public key is NOT listed in the Gaia-X Registry
- Participant creates Self-Description using SD Toolkit
- Participant uses Onboarding Portal for Accreditation
- Participant operates a public Webservice (optional)
- Participant has access to a Credential Manager







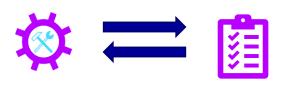


Federator / AISBL



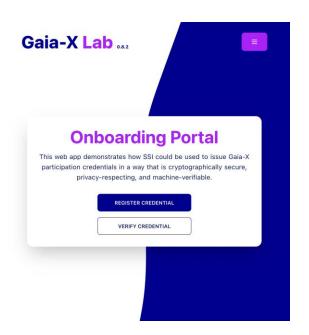
Participant (OpenID Provider) visits the Onboarding Portal to receive a Credential

Onboarding Portal requests email address to verify the Participant The participants receives access to the Onboarding Service



This represents a full KYB process in which the AISBL / Federator checks the provided information (SD) with Trusted Data Sources and verifies the integrity of the SD & identity.

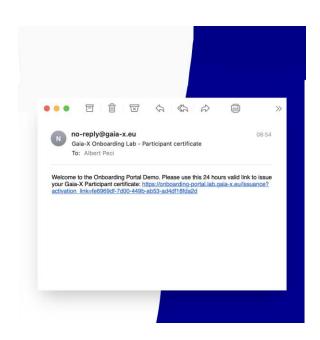




1. Visit the Gaia-X
Lab Onboarding Portal and select Register Credential.
This will start the onboarding flow.

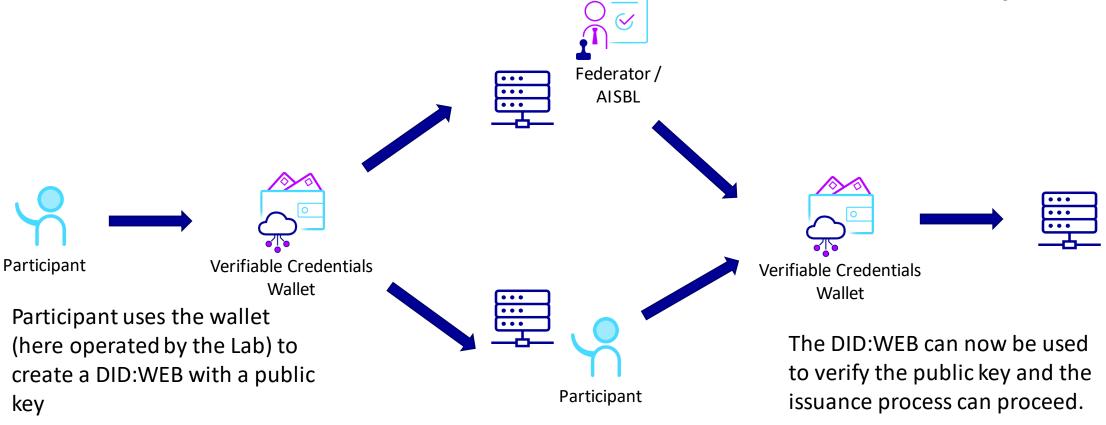


2. Type your email that you also used to register on GitLab. If your email is not registered, you will not get an email and cannot issue a Participant Credential. Click on *Submit*.



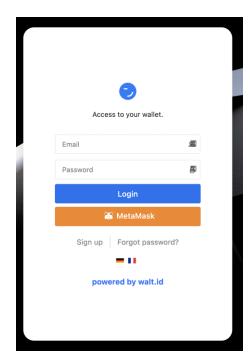
3. Check your emails. You will receive a registration link that is valid for 24 hours. Click on the link to initiate the issuance of your credential.

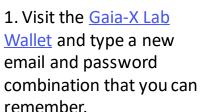


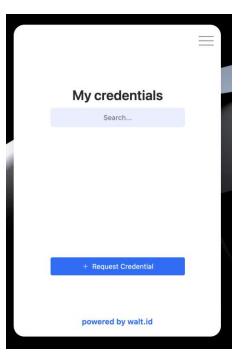


Participant exposes the DID:WEB Document via Lab Registry or an own webservice under the own domain

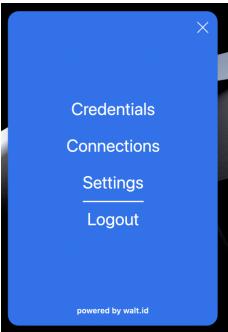




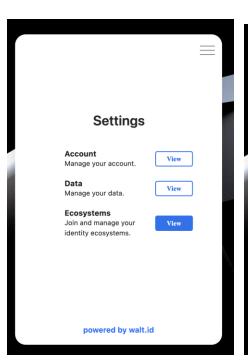




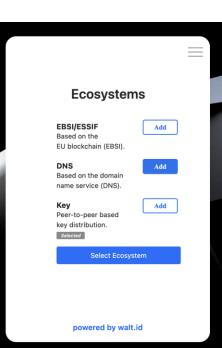
2. If you used a new account, an empty credential page will be shown. Click on the hamburger menu in the top right corner.



3. The menu opens. Select *Settings* to setup your account.

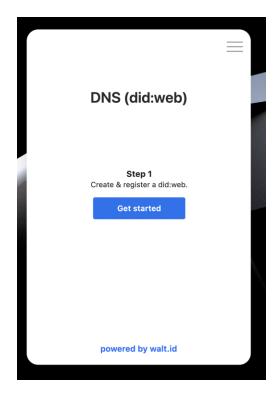


4. There are different aspects that you can manage in your wallet. We are interested in the Ecosystem setting for now.

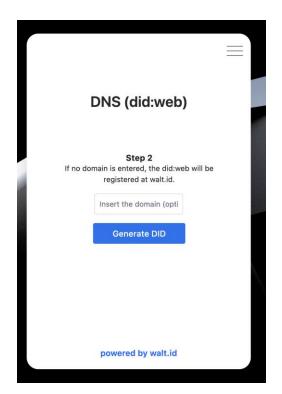


5. We want to use did:web, so we click on *Add* for the *DNS* option.

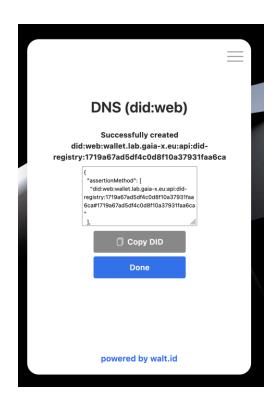




1. The Setup Wizard begins. Click on *Get Started* and follow the steps.

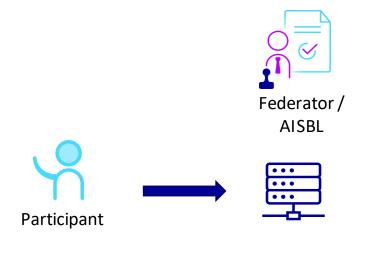


2. You can now enter a domain that you control. If you do not enter a domain a default domain of the demonstrator will be used. Click on *Generated DID*.

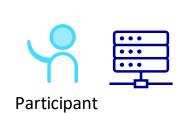


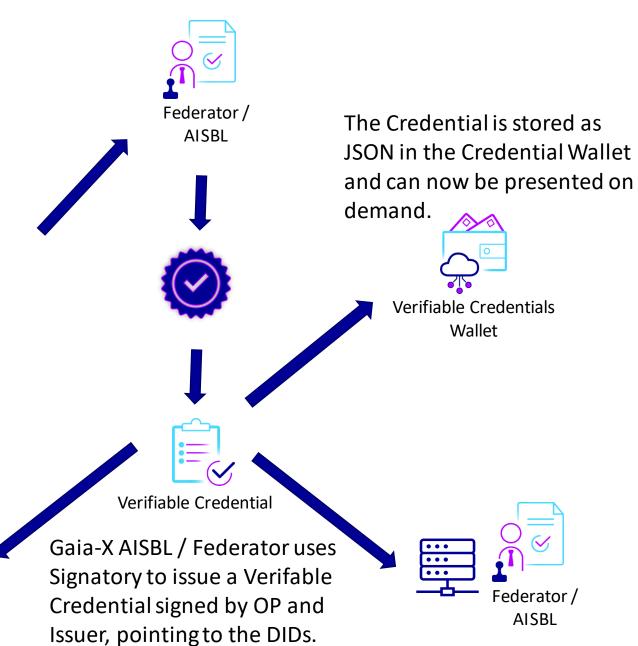
3. Your did:web was successfully created. You can now copy the DID to inspect it in detail, use it somewhere else or just close the window.



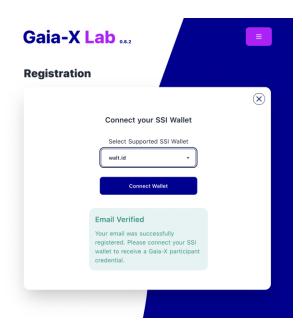


Participant (OpenID Provider - OP) requests a Participant Credential from Federator/AISBL





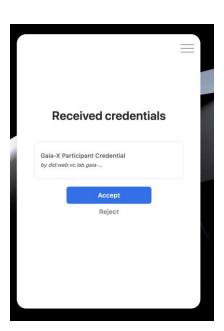




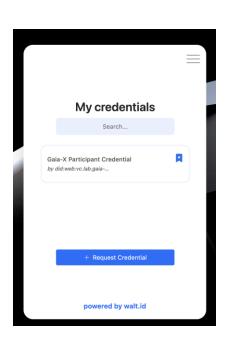
1. Click on the link from the email that you received. If your token is considered valid you can choose your wallet and click on *Connect Wallet*.



2. You can now issue your credential. Click on Issue Credential and the onboarding API will prepare a new credential for you. You will be redirected to your wallet to accept the credential.



3. You received a credential. Click on the credential to view its content first. Click on *Accept* next if you want the credential in your wallet.



4. Your credential was successfully added to your wallet. You can use it now to create verifiable presentations.

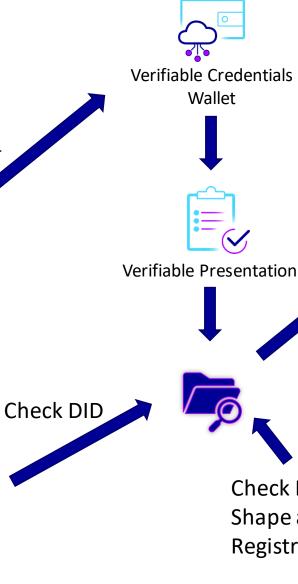


Participant wants to access a Service offered by a Service Provider requiring the Credential.





Participant is the OpenID Provider (OP), the Service is the Requesting Party (RP).



If the Credential has been successfully verified the Service Provider grants access to the Service Offering.





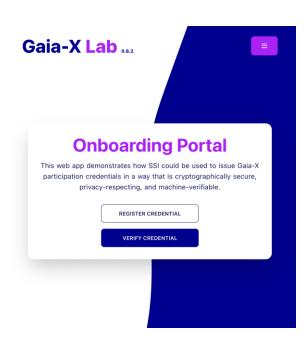




Service Provider





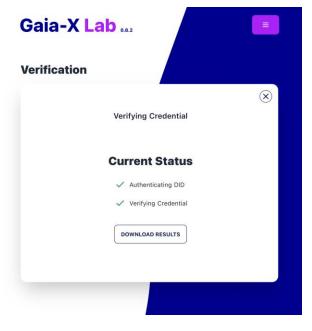




Presentation request

Gaia-X Participant Credential

Share
Reject



1. Visit the Gaia-X
Lab Onboarding Portal and select Verify Credential.
This will start the verification process.

2. Select your wallet and click *Connect Wallet*. This will open a new tab with your wallet.

3. Your wallet allows you to select which credential you want to present to the requester. Select your credential and click on *Share*.

4. The Onboarding Portal will verify your credential if your credential is valid, you can download the results to share it with others.

What has not been shown?

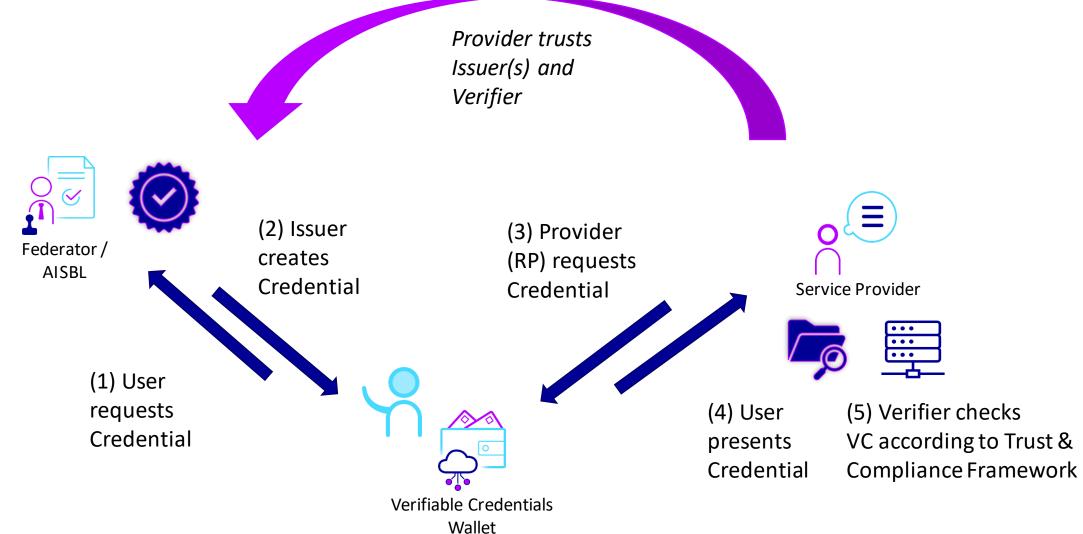


- The Participant would have checked the Credentials of the Service Provider
- The Credentials will be used to increase trust in Service Providers and Service Offerings
- Many Verifiable Credentials can be combined to Verifiable Presentations
- The Verifiable Presentations will be part of the Service Offerings in the Catalogue
- The Registry can be used to revoke, i.e. the rights of an issuer, and this would lead to invalid Credentials

• The Issuer and the Verifier are the parties the Trust has been delegated to.

Summary – Triangle of Trust





Gaia-X Lab Onboarding Demonstrator



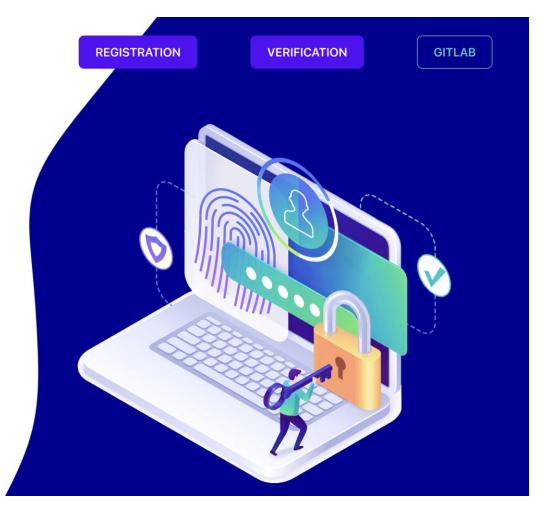
Gaia-X Lab

Onboarding Portal

This web app demonstrates how SSI could be used to issue Gaia-X participation credentials in a way that is cryptographically secure, privacy-respecting, and machine-verifiable.

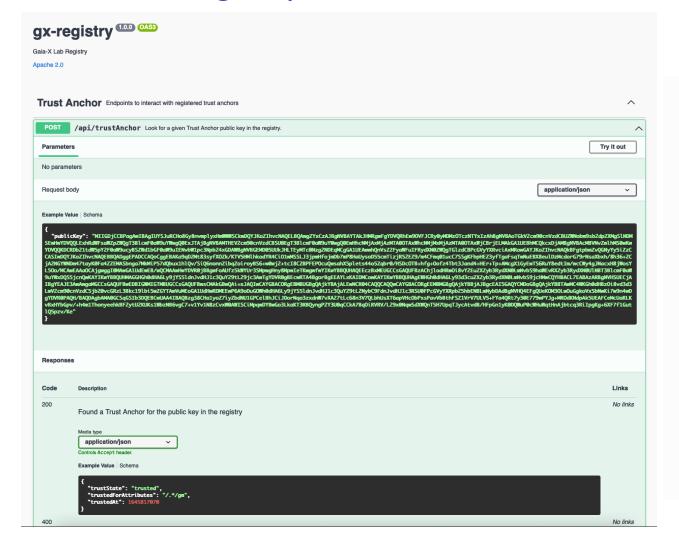
REGISTER CREDENTIAL

VERIFY CREDENTIAL



Demonstrator: https://onboarding-portal.lab.gaia-x.eu/ Repositories: https://gaia-x.atlassian.net/browse/LAB

Gaia-X Lab Registry





3. List of defined trust anchors

Name	Defined as
State	The Trust Service Providers (TSP) must be a state validated identity issuer. - For participant, if the legalAddress.country is in EEA, the TSP must be eiDAS compliant. - Until end of 2022 Q1, to ease the onboarding and adoption this framework DV SSL can also be used. - Gaia-X association is also a valid TSP for Gaia-X association members.
eiDAS	Issuers of Qualified Certificate for Electronic Signature as defined in eIDAS Regulation (EU) No 910/2014 (homepage: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home) (machine: https://ec.europa.eu/tools/lotl/eu-lotl.xml)
DV SSL	Domain Validated (DV) Secure Sockets Layer (SSL) certificate issuers are considered to be temporarily valid Trust Service Providers. (homepage: https://wiki.mozilla.org/CA/Included_Certificates) (machine: https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReportPEMCSV)
Gaia-X	To be defined after 2022Q1.
EDPB CoC	List of Code of Conduct approved by the EDBP (homepage: https://edpb.europa.eu/our-work-tools/documents/our-documents_fr?f%5B0%5D=all_publication_type%3A61&f%5B1%5D=all_topics%3A125)
gleif	List of registered LEI issuers. (homepage: https://www.gleif.org/en/about-lei/get-an-lei-find-lei-issuing-organizations) (machine: https://api.gleif.org/api/v1/registration-authorities)

Demonstrator: https://registry.gaia-x.eu/api-docs/#/Trust%20Anchor/post_api_trustAnchor
Repositories: https://gaia-x.atlassian.net/browse/LAB

Gaia-X Lab Registry



• Use the eIDAS Trusted Service Provider List and TSP Services Public Keys provided Example: https://www.signatur.rtr.at/currenttl.xml for Austrian eIDAS TSPs

A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH

MIIEOTCCA7mgAwIBAglCApMwDQYJKoZlhvcNAQEFBQAwgc8xCzAJBgNVBAYTAkFUMYGLMIGIBgNVBAoegYAAQQAtAFQAcgB1AHMAdAAgAEcAZQBzAC4AIABmAPwAcg
AgAFMAaQBjAGgAZQByAGgAZQBpAHQAcwBzAHkAcwB0AGUAbQBIACAAaQBtACAAZQBsAGUAawB0AHIALgAgAEQAYQB0AGUAbgB2AGUAcgBrAGUAaAByACAARwBt
AGIASDEYMBYGA1UECxMPQS1UcnVzdC1RdWFsLTAxMRgwFgYDVQQDEw9BLVRydXN0LVF1YWwtMDEwHhcNMDIwMjA2MjMwMDAwWhcNMDUwMjA2MjMwMDAw
WjCB0TELMAkGA1UEBhMCQVQxgYswgYgGA1UECh6BgABBAC0AVAByAHUAcwB0ACAARwBIAHMALgAgAGYA/AByACAAUwBpAGMaaABIAHIAaABIAGkAdABzAHMAeQ
BzAHQAZQBtAGUAIABpAG0AIABIAGwAZQBrAHQAcgAuACAARABhAHQAZQBuAHYAZQByAGSAZQBoAHIAIABHAG0AYgBIMRkwFwYDVQQLExBUcnVzdFNpZ24tU2InLTA
xMRkwFwYDVQQDExBUcnVzdFNpZ24tU2InLTAxMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3vqE78j1NAIAT8GC1kqNk6qL+jn1dLTADCiQVlyct01vk00zINk
Ug2x6k7E2xnmyDPg4ihayczDYcuzzQMMms63MFDIONMZ180CxFsZpOYK8SctdTWdH0tGJFJF00BWI6ROykMxo3knPLMDMTS586MgPdKxmihk5OjyZvqiEH1SdmuFR4UT
ke81cisUkM6+hh4v/AYrPShXOIEmNmFILMw9iQST5aeyImgfWwixCZgnmS7fr3j65gezxhPN56qRyndgu97/9VsKMASYTsaD8pZEZ230TlopuwGb4AeO7CUrU22scpnreHLW
1ZX4hldJYJXzFpBH2pAnHfiQgADs4CwIDAQABo4GyMIGvMA8GA1UdEwEB/wQFMAMBAf8wEQYDVR0OBAoECEeMFJHO+gwZMBMGA1UdIwQMMAqACEs8jB2F6W+tM
A4GA1UdDwEB/wQEAwIBBjBkBgNVHR8EXTBbMFmgV6BVhINsZGFwOi8vbGRhcC5hLXRydXN0LmF0L291PUEtVHJ1c3QtUXVhbC0wMSxvPUetVHJ1c3QsYz1BVD9jZXJ0a
WZpY2F0ZXJIdm9jYXRpb25saXN0PzANBgkqhkiG9w0BAQUFAAOCAQEAS1Ch3C9IGqX4c/PCp0Hp93r+07ftu+A77EW7w5kDQ6QhuuXAJgVk4Vyp4D+wIJMxQpvDGkBnaS
YcRyT5rT7ie/eImbHi+ep6AD/mcKs8D2XXDDEy/UxuvEe7pDqrAZc93LID8HnrMf2OFqXbmBggN/TvD20s2CBnEgP+QCm9asttMCg1FLIAIeDL/JstH3ddTIIQNPgUCCaUmATP
80Onh2eon7Fn5+dnKDUY4j6IRDPSDzu0wU0s9VWiyS9Lay0f7P9h3LcYHtAYZg2BPIEAqpOVNVXZ+4JdjRKvhHh9pgadnGNkunrenDiekHgbABop0s2yj5EDAkqYIosnp4bOCQ

Demonstrator: https://registry.gaia-x.eu/api-docs/#/Trust%20Anchor/post_api_trustAnchor

Example: https://www.signatur.rtr.at/currenttl.xml





Appendix

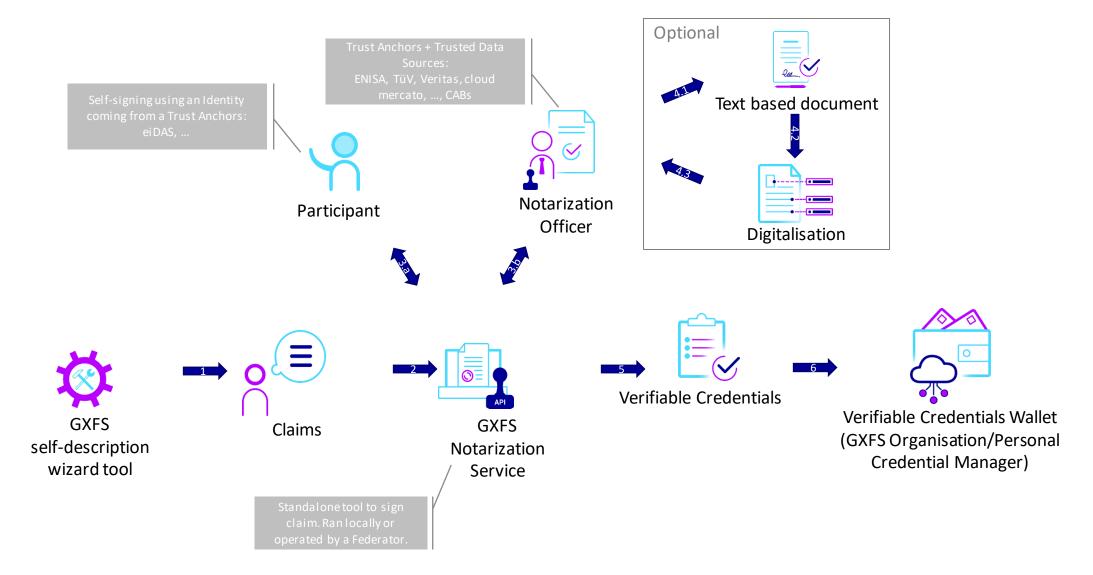
Useful Resources



- Gaia-X <u>Architecture Document 21.12.</u>
- W3C OIDC Core OpenID Connect Core 1.0
- W3C IDC4VP <u>OpenID Connect for Verifiable Presentations</u>
- W3C OIDC Core <u>OpenID Connect Core 1.0</u>
- W3C DID Core <u>Decentralized Identifiers (DIDs) v1.0</u>
- Self-Issued <u>OpenID Provider v2 (SIOPv2)</u>
- walt.id SSI Kit Website

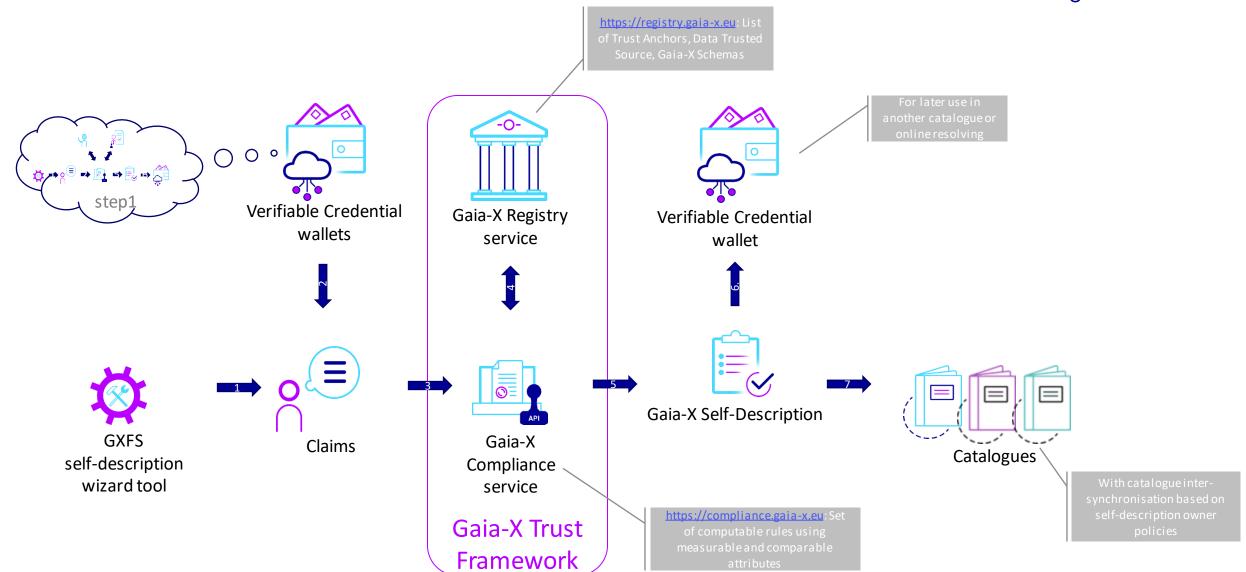
Step1/3: Collect signed claims





Step2/3: Create Gaia-X Self-Descriptions





Step3/3: Ecosystem governance extension



