

Digital Collaboration by Federation

info@facis.eu
www.facis.eu

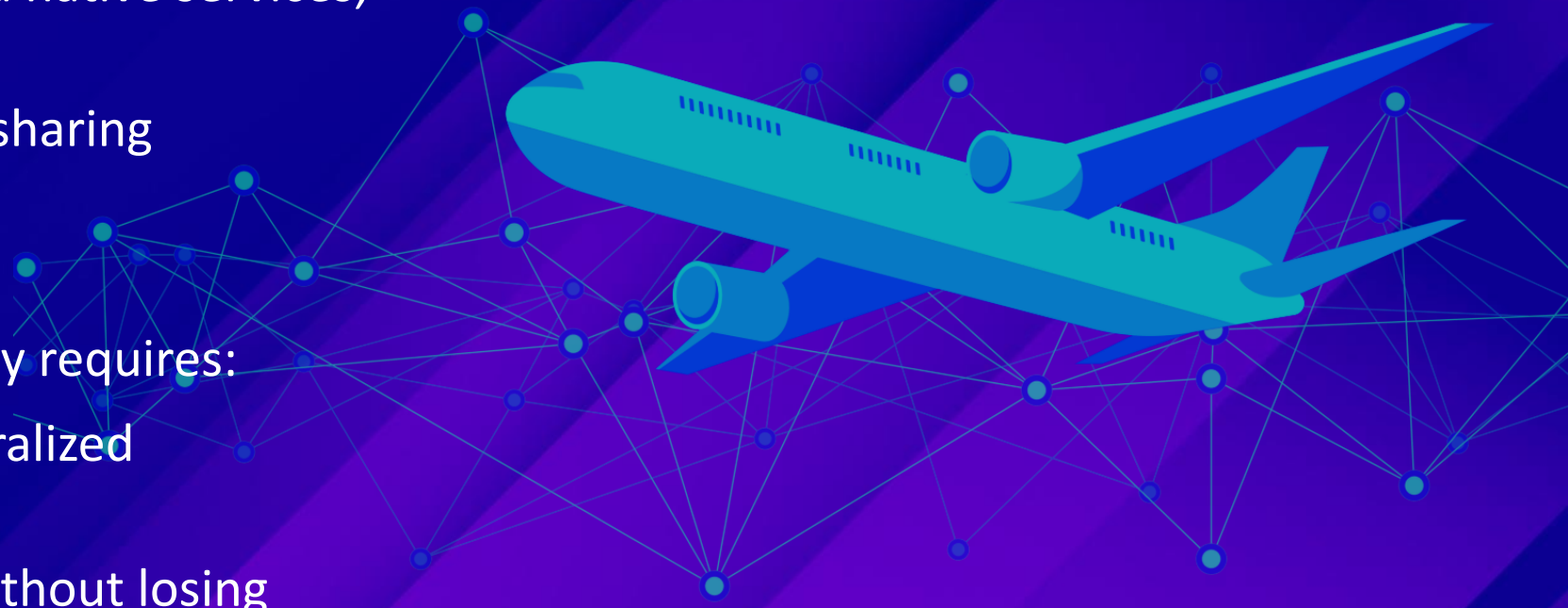
8ra CLOUD·EDGE CONTINUUM

Funded by the European Union
NextGenerationEU

Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag

Introduction

- Aviation enters a new digital era:
  - Digital twins, IoT, cloud native services, AI
  - Cross-enterprise data sharing for *efficiency & safety*



- To fully benefit, the industry requires:
  - Open, trusted, decentralized collaboration
  - Secure data sharing without losing control
  - No vendor lock-in

Purpose of this PoC & Steps Taken

Purpose:



Demonstrate **secure, trusted, and interoperable collaboration** in the aviation sector using **federated architecture** principles and **Gaia-X Trust Framework** as sample for Trust Anchoring and Compliance Assessment.

Key objectives:



- Enable **cross-stakeholder data sharing** without losing data control.
- Apply **Zero Trust security** & **ABAC.**
- Use **SSI** & **VCs** for authentication and verification up to **VPs** for interconnected governance.
- Show real-world scenarios in **Aircraft on Ground** procedures.

Process Overview

Use Case Definition

1. Axis Use Case

Specification

1. Defined **functional & security requirements** based on AXIS / Airbus 8ra
2. Use of W3C, Gaia-X & interoperability standards

Technical Design

1. Designed **Aviation Federation**
2. Mapped **Zero Trust architecture** & ABAC policy model

Implementation

1. Deployed **modular cloud-native components** on 8ra-compliant platforms
2. Integrated **Federation Services** & **Trust Orchestration**

Demon-stration

1. Partners onboarded with digital IDs & VCs
2. Executed scenario with **granular, secure data exchange**
3. Validated **policy-driven access decisions** across systems

Outcome:

A functioning **federated aviation demonstrator** proving that **secure, sovereign, and interoperable collaboration** is possible without centralizing sensitive data with SSI and cross-enterprise trust mechanism

Why Focus Here?

Challenges to cross-enterprise collaboration:

- **Data Silos** – Legacy systems are proprietary and not accessible
- **Lack of Trust** – No universal, verifiable digital credentials
- **Security Risks** – Increased attack surface
- **Regulatory Barriers** – GDPR, data sovereignty, compliance
- **Business Protection** – Collaboration without losing competitive edge

PoC Technical Highlights

- Orchestration of scenarios, using mature **low-code technology**
- Modular, cloud-native service components
- Federated identity onboarding via **SSI and VCs**
- Connection to **Gaia-X Digital Clearing Houses** as trust service for Partner and Services accreditation
- Dynamic, policy-driven access with trust service rule engine
- Standardized interoperability and security measurement
- Aligned with **W3C & Gaia-X** and other common specifications

Security Model

- Zero Trust Principles:
  - Continuous verification (users & systems)
  - Least-privilege, per-request access
  - Authentication: SSI + VCs for identities and qualifications
  - Authorization: ABAC policies define precise access
  - Minimized attack surface – no implicit trust

Demonstrator Implementation

- Partners onboard with verified digital identities
- Publish services to a shared catalogue
- ABAC-managed access
- Runtime VC evaluation for authorization
- Secure, auditable, and compliant cross-ecosystem interactions

Key Outcomes



Faster incident resolution via automated, trusted data exchange



Interoperable collaboration with full data control

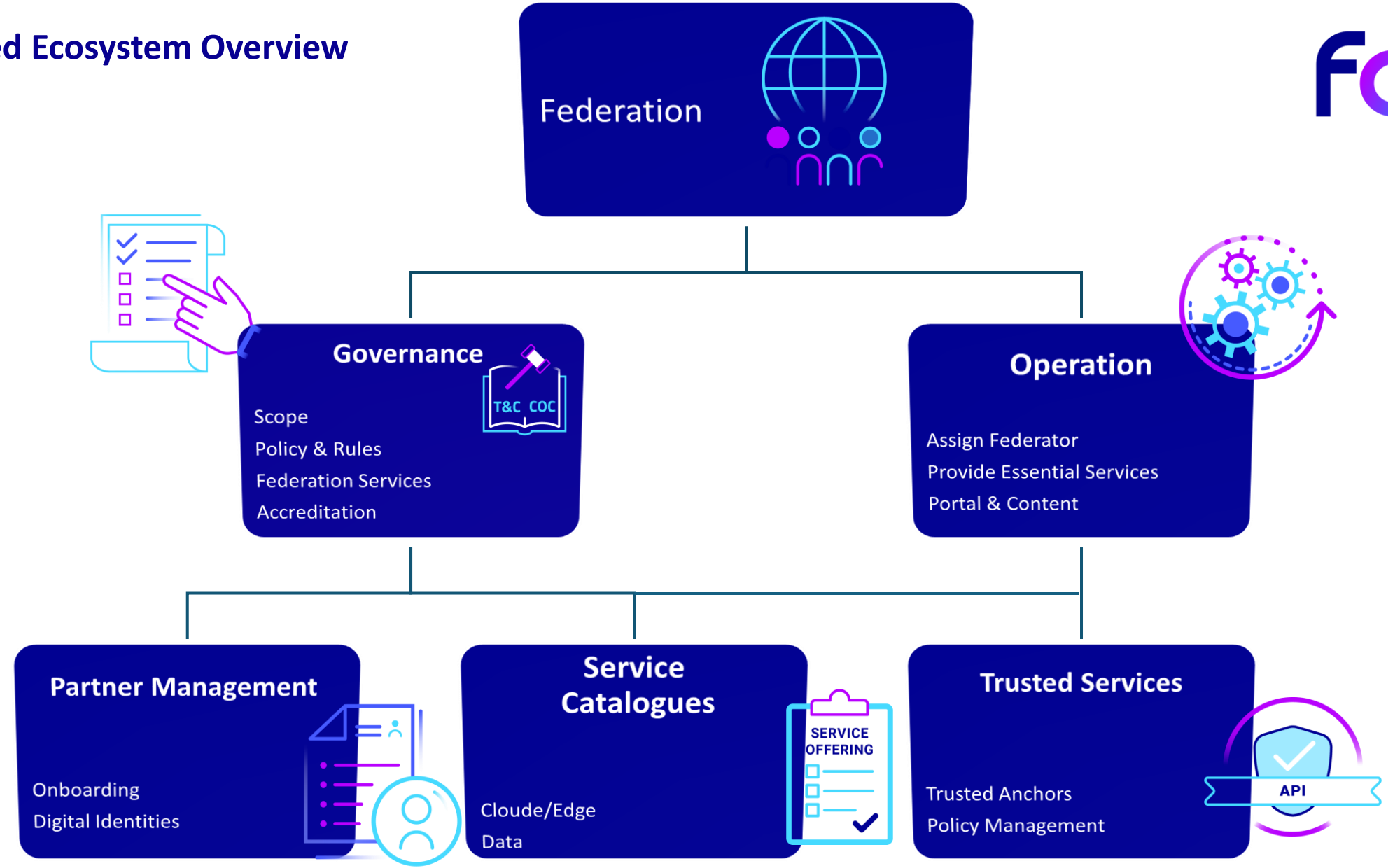


Stronger security via Zero Trust and federated governance



Compliance by design with European data sovereignty principles

Federated Ecosystem Overview



Federated Approach – FACIS PoC / Aviation Federation

Aviation Portal



Apply as new partner

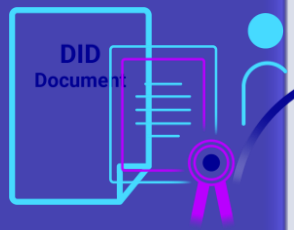
Partner Data & Verification



AI tool for data collection

JSON-LD output

DID & Certificates



Preparation for verification from the trust anchor

Verification



Request to the trust anchor

(GXDCH – option to choose)

Trust Anchor Verified Credentials



VC issuance

Aviation Compliance Statement



Policy & rules agreement

Aviation VC



Partner accreditation



Partner Onboarding in a Federated Ecosystem – Storyline

Goal:

Seamlessly onboard partners into the Aviation Federation by

- creating a compliant organizational profile,
- issuing a verifiable membership credential,
- and making it accessible via the federation portal and the organization's wallet.

Key components:

- **Portal:** User interface for onboarding, uploading documents, and displaying status.
- **ORCE:** Orchestration engine that runs onboarding workflows and connects services.
- **TSA (Trust Service API):** Validates compliance, checks schemas, and enforces rules.
- **OCM (Organizational Credential Manager):** Stores verified profiles and issues onboarding VCs.
- **PCM Cloud (Personal Credential Manager)**: Principal core digital wallet responsible for the secure storage, lifecycle management, and presentation of VCs required for access to the requested service.

1. AI-Assisted VC Collection – Auto-gather credentials for compliance

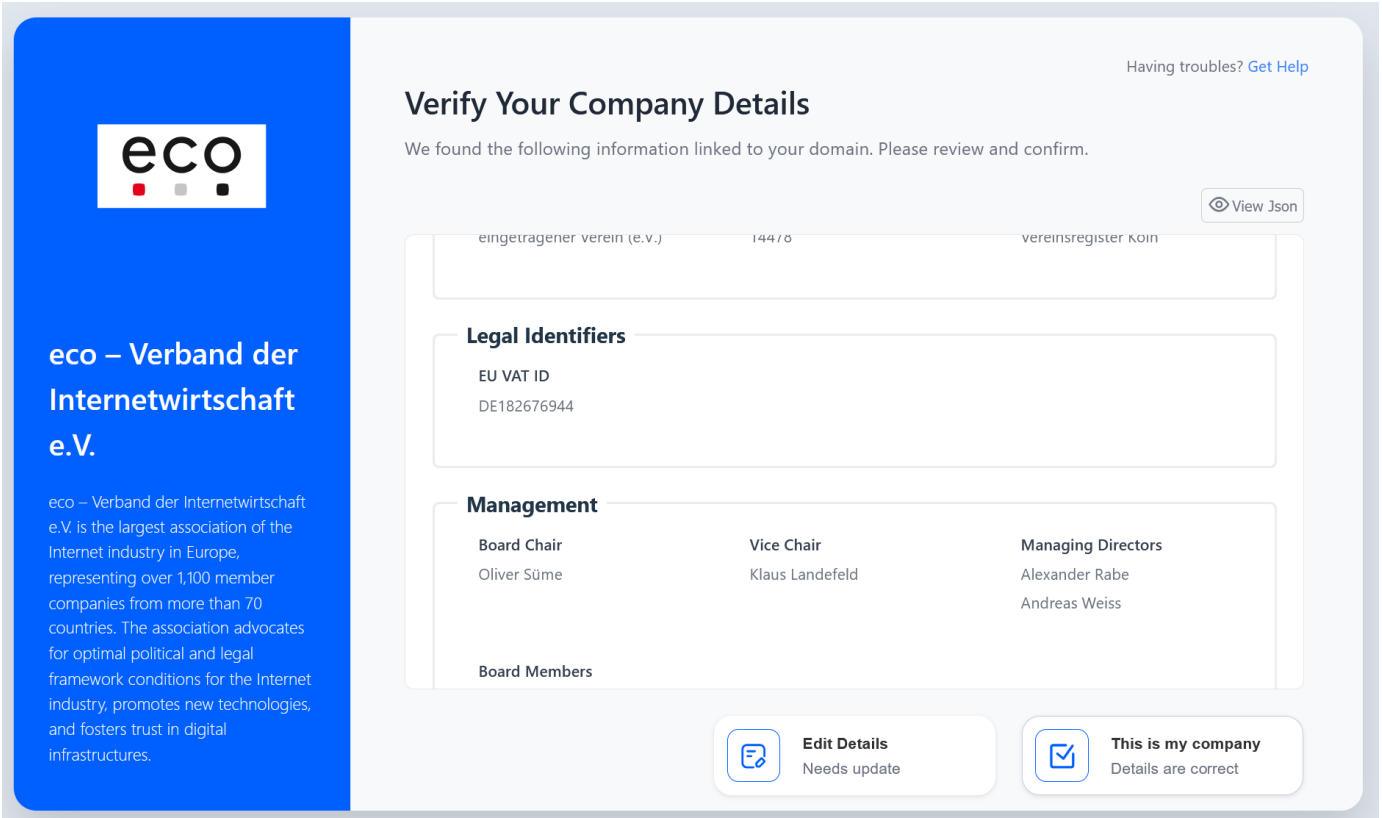
Onboarding new participants into a federated ecosystem requires both **compliance and efficiency**.

- An advanced, locally deployed AI tool supports the process by discovering and collecting available public information, reducing manual effort and accelerating compliance validation.



My company's website or public information on the internet is **available** our website URL is **eco.de** The domain I choose for registering in the Gaia-X ecosystem is **facis.cloud** Great, you are all set 🚀

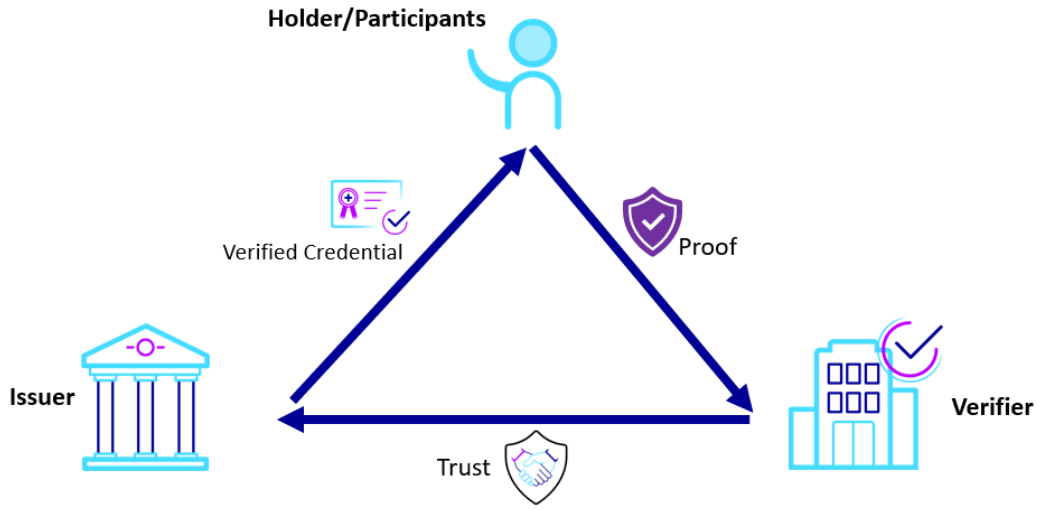
CONFIRM & NEXT



How does SSI work?

Triangle of Trust

- **Issuer**
  - Issuance of credentials & verifiable digital credentials
- **Holder**
  - Users, organizations, or technical devices that have legitimate credentials
- **Verifier**
  - e.g., consumer in the form of an application or person who needs the credentials



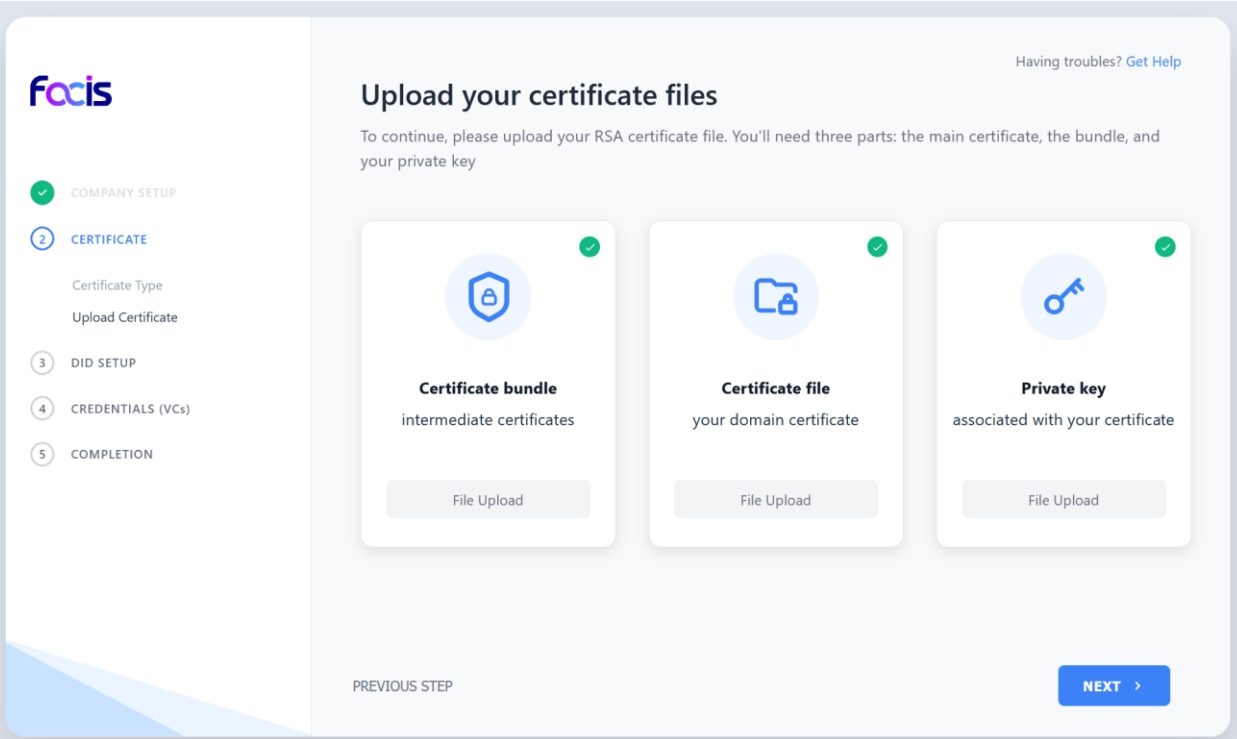
2. Submit Legal Data – Apply for membership

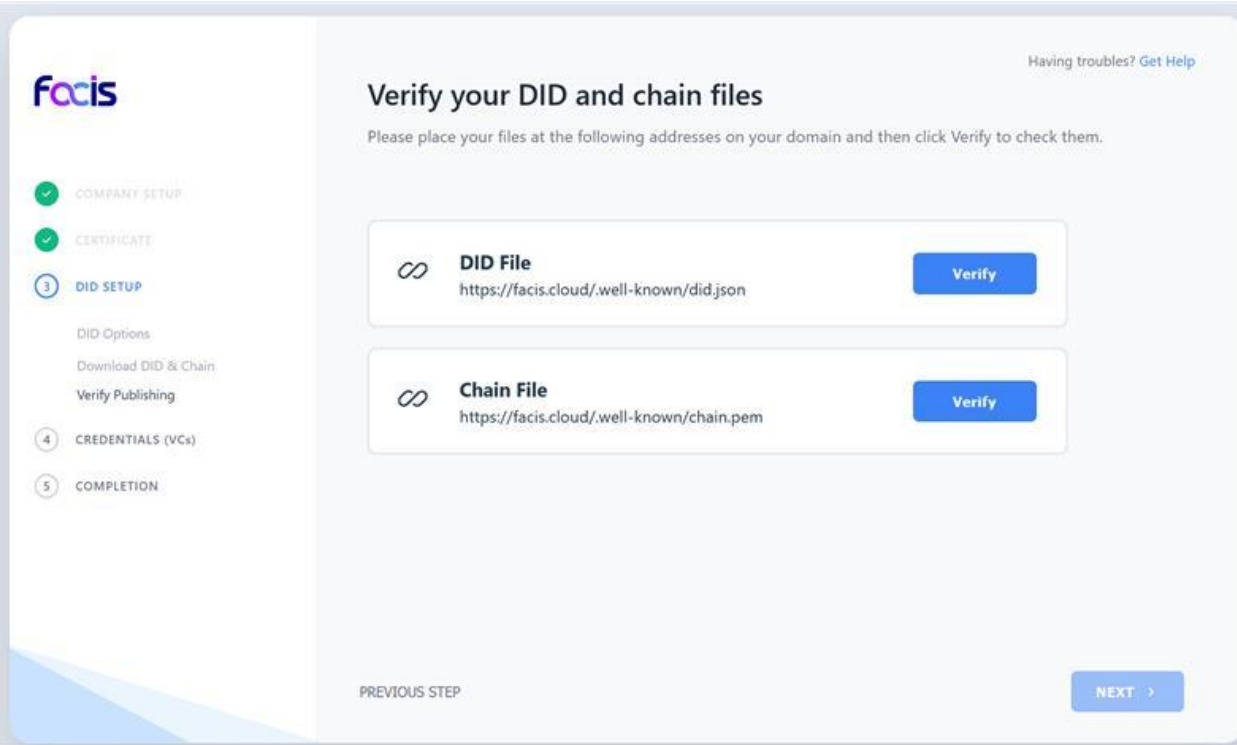
Holder/Participants

The participant submits the required legal data to apply for membership in the federation.

The participant provides:

- **Company's legal data:** a self-description (JSON-LD),
- **Compliance certificates** (e.g., ISO 27001),
- **and a DID (Decentralized Identifier).** The system allows to create or confirm a DID – a secure, partner-controlled digital identity used for onboarding, credential issuance, and trusted participation in the federation.





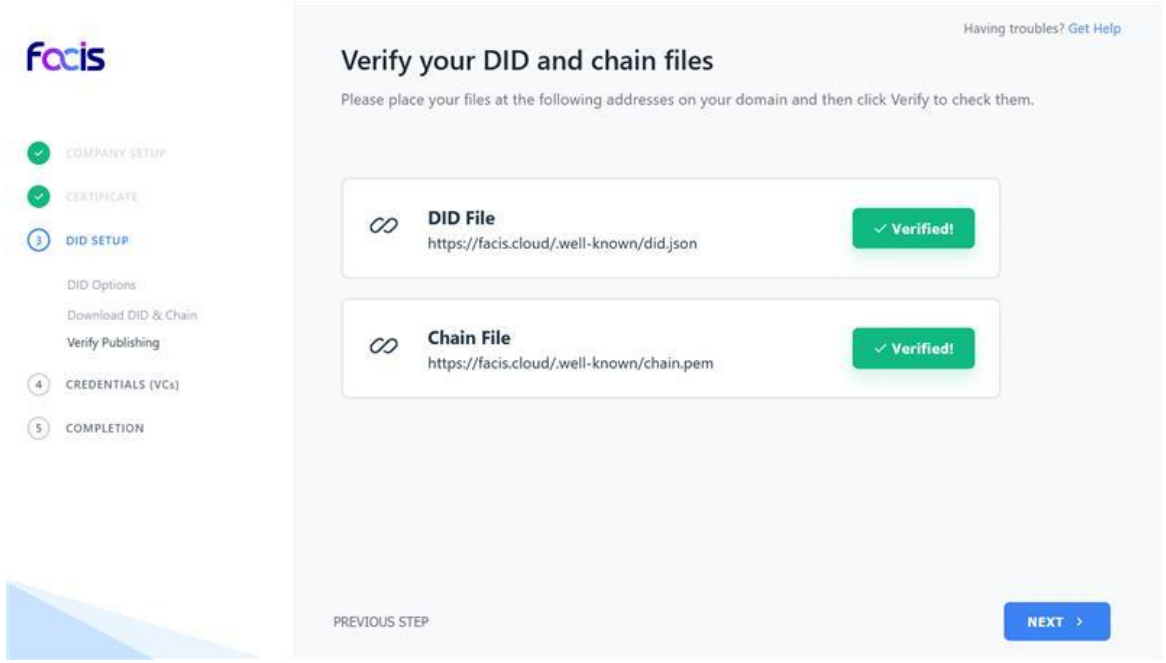
3. Verification

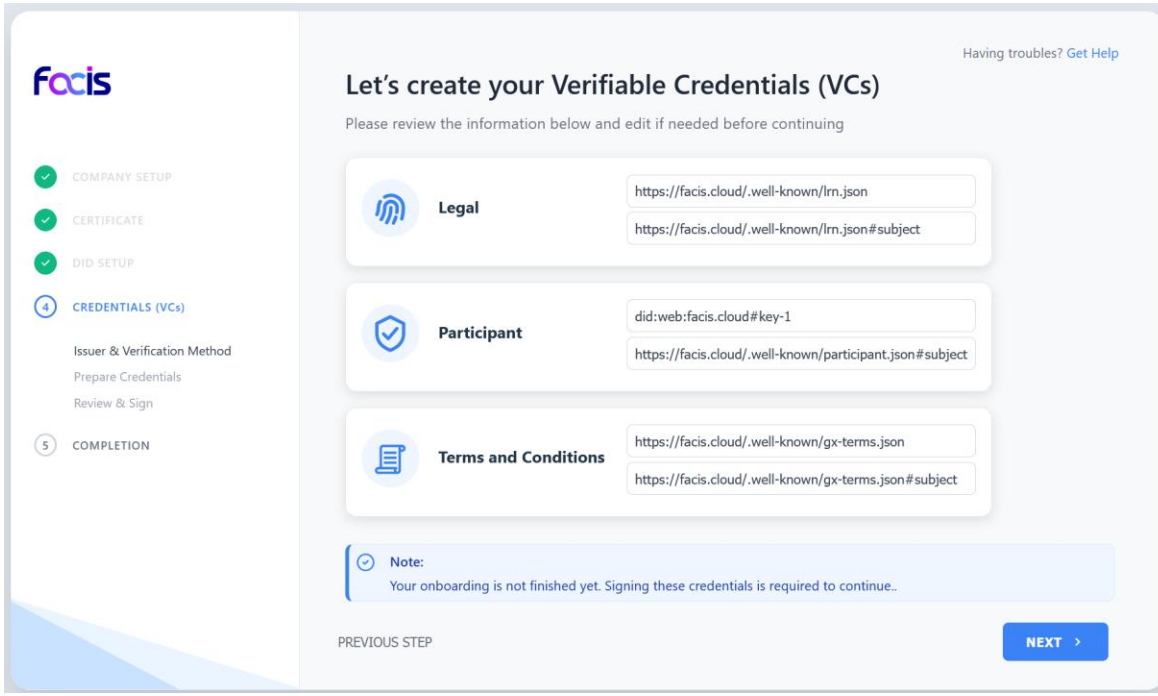
The system verifies that the submitted data is valid by checking the issuer's authenticity and ensuring the verifier trusts that issuer.

System actions:

- validates the partner's data, stores a provisional profile,
- and triggers ORCE to route artifacts to the Trust Services.

The Trust Service checks compliance (schema, signatures, validity).



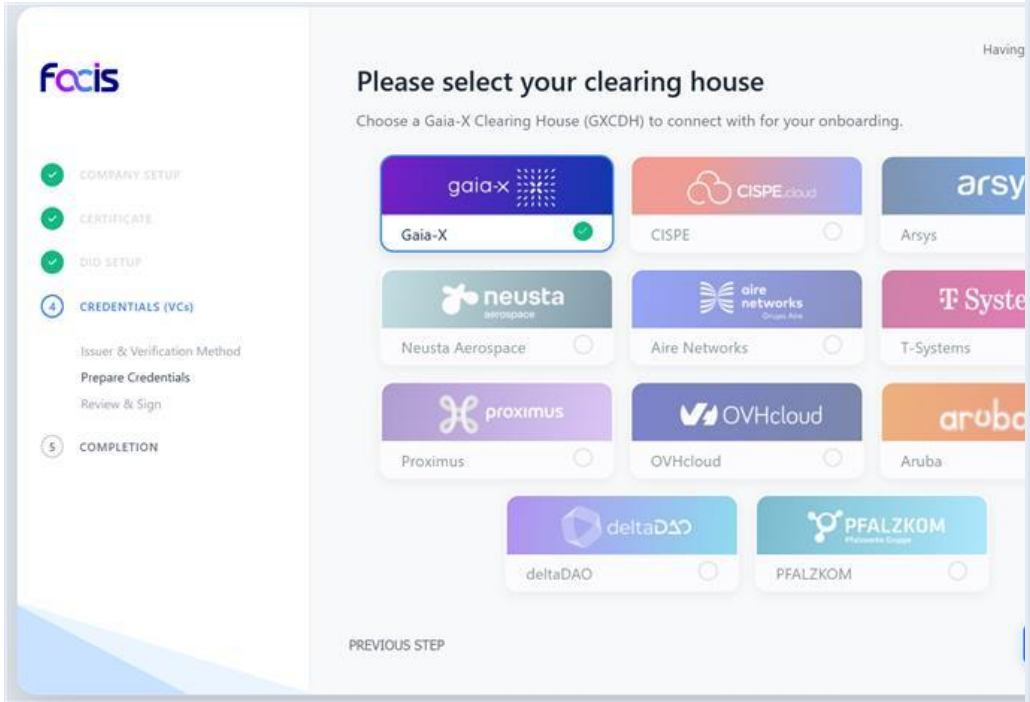


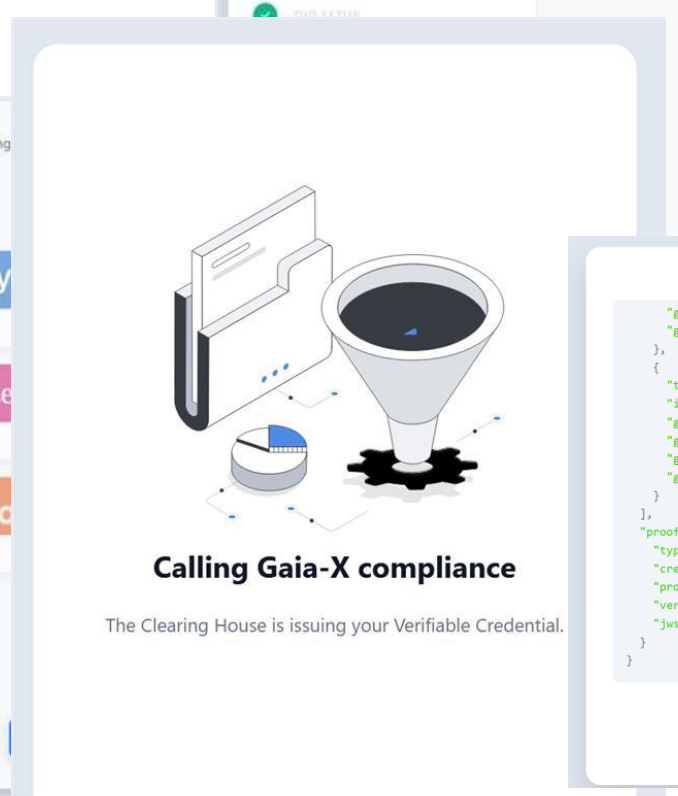
4. Issue Trust Anchor’s VC (e.g. Gaia-X)

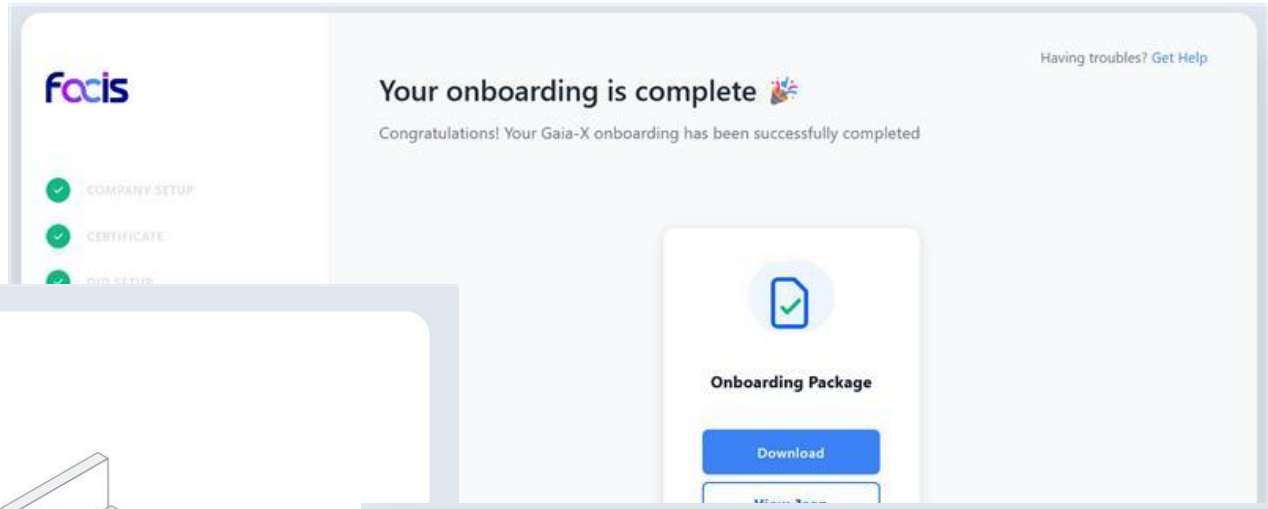
The system performs all validations, and once the **trust anchor** (in this case the GXDCH) verifies the data, the system approves the Gaia-X onboarding and issues the Gaia-X-compliant VC to the participant.

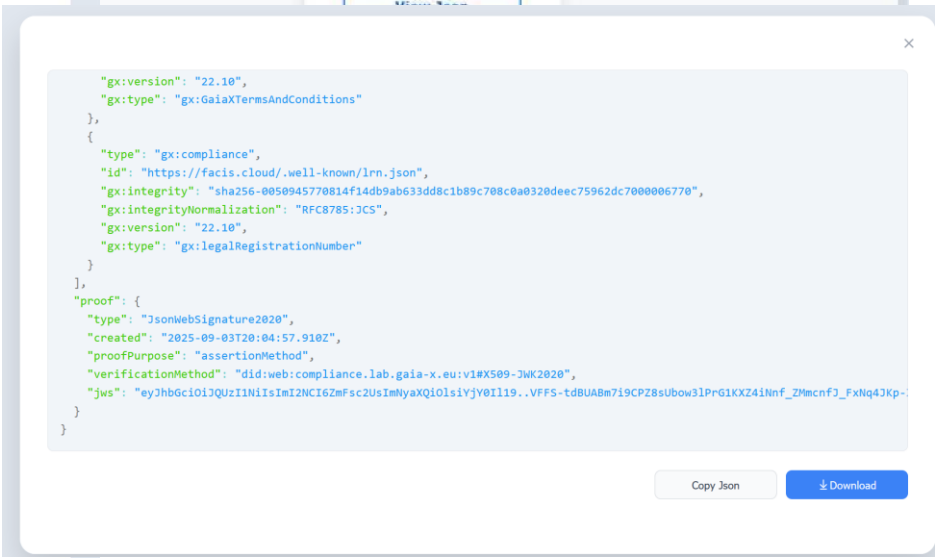
System actions:

- Allows the participant to choose the desired clearing house (GXDCH).
- Approves onboarding and issues a Gaia-X-compliant Onboarding VC which will be linked to the partner’s





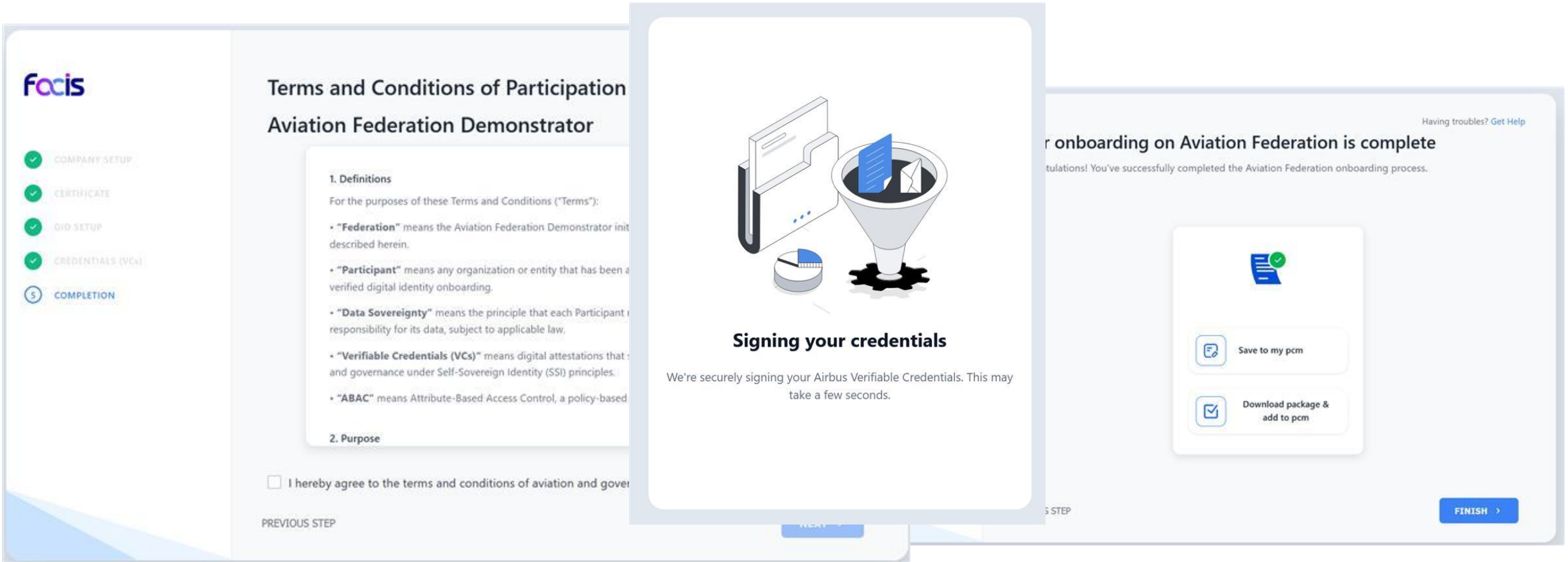




5. Finish Aviation Onboarding

System actions:

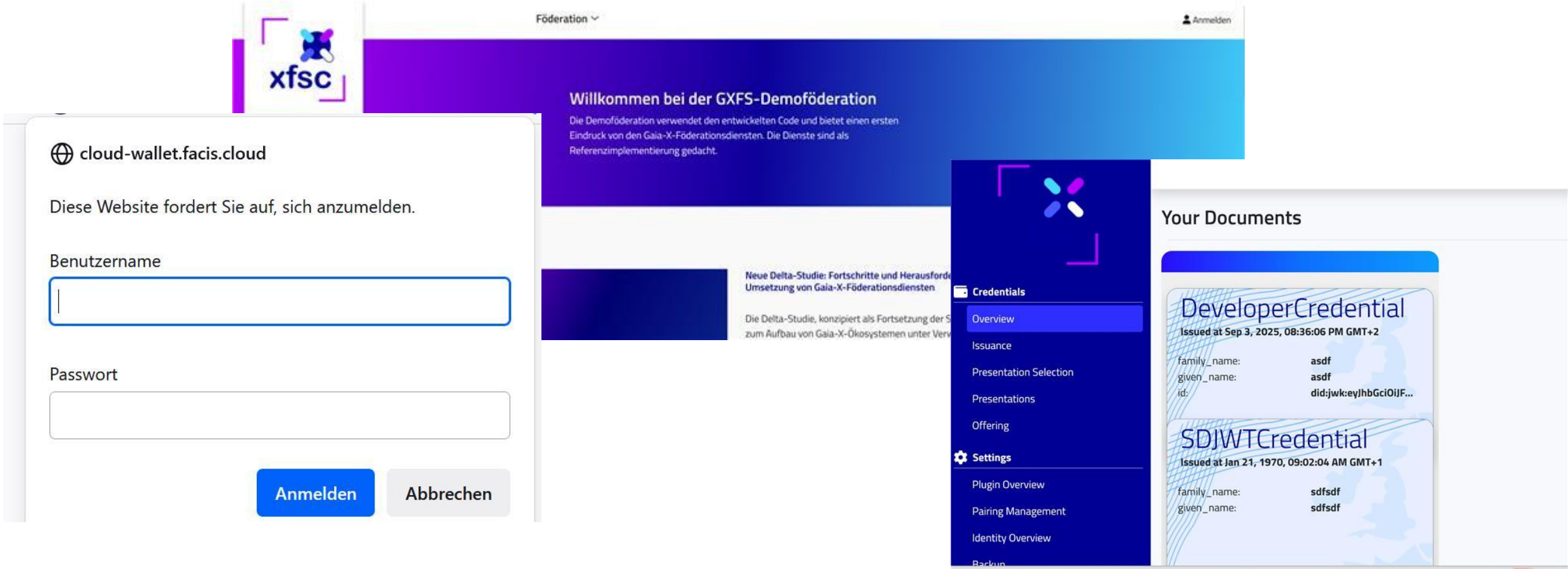
- The Participant agrees to the Aviation Policies and Rules
- Approves onboarding and issues a Aviation-compliant Onboarding VC which will be linked to the partner's DID and wallet.



5. VC Issuance to the Participant Wallet (PCM Cloud)

System actions:

- The system generates and cryptographically signs an Aviation-compliant Onboarding VC linked to the participant’s DID.
- The VC is securely stored in the Personal Credential Manager (PCM Cloud) for future authentication and access to aviation services.



XFSC Technology Stack & AI Integration

- **Portal, ORCE, TSA, OCM, PCM Cloud from the XFSC Toolbox**



- **IONOS AI Model Hub**
  - https://cloud.ionos.com/managed/ai-model-hub

- **Open-source technology (no vendor lock-in)**
  - Choose from high-performance large language & text-to-image models
  - Access to the latest and most reliable open-source models
  - No licensing fees for using deployed models

Trust Anchor Integration



https://gaia-x.eu/services-deliverables/digital-clearing-house/

FACIS Project Overview

- **FACIS (Federation Architecture for Composed Infrastructure Services)**
  - Tackling fragmentation through federation of services across providers without losing autonomy
  - Provide open-source, reusable components deployable across industries (manufacturing, mobility, aerospace, etc.)
- Key Deliverables:
  - **SLA Governance Framework**
    - Base Taxonomy for multi-provider SLAs and representation of maschine-readable SLAs
    - Playbook enabling consistent, transparent, and enforceable SLA governance across complex service ecosystems
  - **Digital Contracting Service**
    - Tool to support bilateral and multilateral contract management
    - Combines eSigning with qualified electronic signatures such as EUDI
  - **Federation Architecture Patterns**
    - Modular blueprints/ orchestrated templates for building and operating trusted, federated digital ecosystems.

Real-world applications

- **Proof-of-Concept for Aviation Federation**
  - Collaboration with AXIS project (Airbus Operations GmbH) to showcase how decentralized (Gaia-X) principles and XFSC technologies can work in real, highly-regulated industrial settings
- **Focus**
  - Integrating aircraft as «Flying Edge Device» into a federated cloud infrastructure
  - Show how scalable trust chains, federated catalogues, and digital wallets enable collaboration
    - E.g. Aircraft Maintenance, Passenger Service, Fueling Processes
  - Not just about technical IT integration, but about demonstrating the transformative potential of federated services for trusted, identity-based business processes in aviation

Key Tools and Standards for Practical Interoperability

- **Federation Architecture Patterns (FAPs):** Open-source, resuable templates orchestrating services for operating digital ecostystems
- **Orchestration Engine:** OSS Low-code engine based on Node-Red, adjusted and developed based on XFSC features
- **XFSC Toolbox as basline components:** https://projects.eclipse.org/projects/technology.xfsc
- **Standards applied:**
  - W3C VC/VP – credentials for organizations/users
  - OID4VC – standardized issuance and presentation of veribale credentials
  - DIDComm v2 – secure communication between participants of a federation
  - Gaia-X Trust Framework – compliance, trust anchor, catalogue integration
  - eIDAS – legal identity alignment where required
  - SSI – Self-Sovereign Identity
  - JSON-LD – Linked data for standardized service metadata
  - OpenAPI/ GraphQL – service discovery and integration APIs
  - Etc.

Federation Architecture Patterns (FAPs)

Deliverables

- Development of 5 basic FAPs that cover generic functions for federated ecosystems
- Development of 4 vertical FAPs as special adaptions of FAPs for specific domains such as Industry 4.0
- Open-Source Repository: All FAPs are published as free open-source components to promote use and further development by the community

Goals

The main objectives of the FAPs are to simplify and harmonize processes in the development of federated ecosystems. They are intended to:

- Promote interoperability between different providers and services
- Reduce complexity in the implementation of infrastructures
- Enable rapid adaption and scaling of digital services

Approach

FAPs are provided as low-code templates to simplify implementation and enable customization to specific requirements. They are developed based on FOSS components such as the XFSC Orchestrator.

FAP Concept Paper


FAP | A Practical Pre-built Blueprint for Operating Federated Digital Ecosystems

FAP in a Nutshell

Federation Architecture Pattern (FAP) is a modular, extensible, and standards-based reference architecture for operating secure, interoperable, and policy-compliant federated digital ecosystems.

FAP addresses critical trust and interoperability challenges that often arise when setting up federated ecosystems by defining a **federation-native architecture**. Under this model, each actor operates independently but adheres to shared protocols, trust models, and policy enforcement standards. Such an approach promotes **modularity, trust by design, and interoperability at the edge** – enabling dynamic collaboration between autonomous entities without surrendering control. This is indispensable in trust-based ecosystems like **federated healthcare systems or cross-organizational supply chains.**

Get in touch with us

Homepage

Newsletter

info@facis.eu
www.facis.eu

CLOUD·EDGE CONTINUUM

Funded by the European Union
NextGenerationEU

Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag