Second Phase of the XFSC specification

The second Phase of the XFSC specification builds upon the groundwork laid in GXFS specification Phase 1 and aligns with the principles of the Gaia-X Trust Framework 22.10.

The recently defined specifications and supplementary requirements apply to these specific components and are currently subject to a tendering procedure:

TRAIN

We are introducing a new component into the XFSC Toolbox called "Trust Management Infrastructure" (TRAIN). TRAIN supports with establishing and verifying the trust basis (root of trust) for participants in the Gaia-X distributed ecosystem and the credentials issued by those entities. Thus, TRAIN plays a pivotal role in building trust within the Gaia-X ecosystem, providing a flexible and interoperable infrastructure for entities to establish and manage trust relationships.

This is achieved through the introduction of trust lists combined with anchoring of pointers in the DNS. Gaia-X Federations and other entities are supported in the sovereign publication and administration of trust lists for their specific trust frameworks. Verifying entities are supported in their sovereign trust decisions. To achieve this, the following functionalities will be developed:

- Trust Framework Configuration
- Trust List Management
- Zone Manager Handler
- Trusted Content Resolver (Extended Universal Resolver) + Libraries
- DNS Zone Manager

Please note that the libraries are intentional for different languages such as GO, Java, Python and JavaScript. It's also intentional to create the libraries as helpers for using the extended universal resolver, by adding content resolver steps, validation routines for VC and other assistive functionalities.

OCM Extension

The purpose of this extension is to provide changes to the OCM components to enhance the OCM in its functionality and adopt the latest Gaia-X requirements (e.g. Support of did:web method and VC with JsonWebKey2020 https://docs.gaia-x.eu/technical-committee/identity-credential-access-management/22.10/credential_format/), enabling secure interactions within the Self-Sovereign Identity (SSI)-based ecosystem. The Organization Credential Manager Extension 1 (OCM.E1) enhances the participant's interaction with the SSI-based ecosystem in a trustful and secure environment. This comprises the utilization of the participants digital identity for different functionalities:

- Extended management of secure and trustable connections with other parties (Connections in this context are private, secured, and persistent channels between entities)
    - Blocking of Connections
    - Handling of blocked connections
- Refreshing and Revocation of verifiable credentials from attesting parties (e.g., Gaia-X Membership credential from a verified notary)
- Utilization of AIP v2.0 alongside AIP v1.0 by updating the AFJ Framework
- Provision of verifiable Public Profile (service endpoints within OCM DID Document)
    - Configuration of Private Custom Endpoints (with DID-Auth/OIDC)
    - Configuration of Endpoint Mappings to internal/external functionality

OCM W-Stack

The purpose of the OCM W-Stack is to provide all necessary components for the extension of the administration of the digital identity of a participant in the Gaia-X context. The OCM W-Stack enhances the participant's interaction with the SSI-based ecosystem in a trustful and secure fashion. This comprises the utilization of the participants digital identity for different functionalities:

- Implementation of Full W3C DID/VC/VP Support for Credential Exchange and Trust
- Implementation of OpenID Standards
    - OpenID4VC/VP
    - SIOP
    - VC Issuance Protocol Extension
- Establishment of secure and trustable connections with other parties
- Request and reception of verifiable credentials from attesting parties (e.g., Gaia-X Membership credential from a verified notary) in JSON-LD Format
- Attestation of attributes to principals in the form of verifiable credentials (e.g., employees, technical assets)
- Validation of received verifiable presentations from other parties (e.g., validation of Gaia-X membership of other participants)
- Maintenance of the verifiable Public Profile
- Scalable VC/VP Storage
- Graph Indexing for Linking VC/VP

Same as the OCM the OCM W-Stack prioritize W3C compatibility, but technologically the OCM W-Stack will be a non-Indy implementation to become independent of Hyperledger Indy and maximize interoperability.

PCM Cloud

We are also introducing a PCM that can be interacted with by computer browser, thus giving you an alternative to the existing PCM App. The purpose of the PCM Cloud is the same as the existing PCM App - to provide all necessary components for the self-sovereign administration of the digital identity of a principal in the Gaia-X context. The PCM Cloud enables a natural person to act as a principal of an organization within the SSI-based Gaia-X ecosystem in a privacy-preserving, trustful and secure way from a computer browser. This comprises the following main functionalities:

- Remote Management of a Cloud Wallet or multiple Wallets which are connected to the PCM Cloud
- Reception and management of verifiable credentials from other parties (e.g., a principal credential from a Gaia-X participant) by using the web frontend
- Presenting Verifiable Presentations to other parties in an automated or manual manner by using plugins
- Secure storage and management of respective secrets
- Consent Management
- Policy Based Decisions about Issuing/Presentations
- Plugin System which extends the Holder Capabilities

The PCM Cloud is designed as a cloud-based component offering a user-friendly web interface for managing OCM, OCM W-Stack, and TSA. It serves as an integration layer, facilitating various Holder use cases. The PCM Cloud orchestrates these use cases through plugins, such as the "ID Card Proof Plugin," enabling functions like automatic ID card verification.

PCM Extension

The purpose of the PCM is to provide all necessary components for the self-sovereign administration of the digital identity of a principal in the Gaia-X context on a mobile device. The PCM enables a natural person to act as a principal of an organization within the SSI-based Gaia-X ecosystem in a privacy-preserving, trustful and secure way. The extension comprises the following main functionalities:

- AIP 2.0 Support
- Reception and management of updated W3C verifiable credentials
- Presenting W3C and AIP 2.0 Verifiable Presentations to other parties in a proved manner
- Secure storage and management of respective secrets
- Remote Management of the PCM Cloud Solution
- Support of the PCM Cloud functionality
- Enhancements in QR Code Support Reading and Presentation

Furthermore, the scope includes the provision of the developed software in a usable format for end users including the respective distribution channels (e.g., App Stores).

TSA Extension

The aim of the Trust Services API Extension is to ensure a consistent level of trust between Gaia-X participants and components. The Trust Services API can be used by all other XFSC components. 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.

The scope also includes necessary tools (e.g., Command Line Scripts) to operate and maintain the created software components in an enterprise environment with focus on high-availability, security and monitoring and logging based on common standards.

The main updates/extensions are:

- Extended policy management
- Component is made more "manageable" for deployment
- Signature services are designed for eIDAS compliant signatures and verifications
- TSA gets integration interface via cloud events and web hooks
- Configurability is extended
- JSON schema validation is added

NOT Extension

The scope is to extend the existing component “Notarization API”, with the following new features:

- Protocol agnostic issuances depending on the incoming DID and format definitions
- New issuance and verification protocols
- Business validation flow for the notary
- Documentation for using NOT as the compliance service for memberships
- Dynamic schema configuration
- Enrollment of organization to certain trustlists
- Trust verification with the TRAIN module before the issuance process
- Automatic Notarization Verification

The product extension will also include interfaces (API’s) to integrate the notarization component smoothly in external software for Non-IT operator usage (e.g., lawyers, notaries, governments, certifiers ...).