Zweite Phase der XFSC-Spezifikation

Die zweite Phase der XFSC-Spezifikation baut auf den in Phase 1 der GXFS-Spezifikation gelegten Grundlagen auf und orientiert sich an den Prinzipien des Gaia-X Trust Framework 22.10.

Die kürzlich definierten Spezifikationen und ergänzenden Anforderungen gelten für diese spezifischen Komponenten und sind derzeit Gegenstand von Ausschreibungsverfahren:

TRAIN

Wir führen eine neue Komponente in die XFSC Toolbox ein, die "Trust Management Infrastructure" (TRAIN). TRAIN unterstützt den Aufbau und die Verifizierung der Vertrauensbasis (Root of Trust) für die Teilnehmenden des verteilten Gaia-X-Ökosystems und die von diesen Entitäten ausgestellten Credentials. TRAIN spielt somit eine zentrale Rolle beim Aufbau von Vertrauen innerhalb des Gaia-X-Ökosystems, indem es eine flexible und interoperable Infrastruktur für Entitäten bereitstellt, um Vertrauensbeziehungen aufzubauen und zu verwalten.

Dies wird durch die Einführung von Vertrauenslisten in Kombination mit der Verankerung von Pointern im DNS erreicht. Gaia-X Föderationen und andere Entitäten werden bei der souveränen Veröffentlichung und Verwaltung von Vertrauenslisten für ihre spezifischen Trust-Frameworks unterstützt. Verifizierende Entitäten werden bei ihren souveränen Vertrauensentscheidungen unterstützt. Um dies zu erreichen, werden die folgenden Funktionalitäten entwickelt:

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

Bitte beachten, dass die Bibliotheken für verschiedene Programmiersprachen wie GO, Java, Python und JavaScript gedacht sind. Es ist auch beabsichtigt, die Bibliotheken als Hilfsmittel für die Verwendung des extended universal resolver zu erstellen, indem Schritte zur Inhaltsauflösung, Validierungsroutinen für VC und andere unterstützende Funktionen hinzugefügt werden.

OCM Extension

Der Zweck dieser Erweiterung ist es, Änderungen an den OCM-Komponenten vorzunehmen, um den OCM in seiner Funktionalität zu verbessern und die neuesten Gaia-X-Anforderungen zu übernehmen (z.B. Unterstützung der did:web-Methode und VC mit JsonWebKey2020 https://docs.gaia-x.eu/technical-committee/identity-credential-access-management/22.10/credential_format/), was sichere Interaktionen innerhalb des Self-Sovereign Identity (SSI)-basierten Ökosystems ermöglicht. Die Organization Credential Manager Extension 1 (OCM.E1) verbessert die Interaktion des

Teilnehmenden mit dem SSI-basierten Ökosystem in einer vertrauensvollen und sicheren Umgebung. Dies umfasst die Nutzung der digitalen Identität des Teilnehmers für verschiedene Funktionalitäten:

- Erweitertes Management von sicheren und vertrauenswürdigen Verbindungen mit anderen Parteien (Verbindungen sind in diesem Zusammenhang private, gesicherte und dauerhafte Verbindungen zwischen Entitäten)
    - Blockierung von Verbindungen
    - Handhabung von blockierten Verbindungen
- Refreshing und Revocation von Verifiable Credentials von attestierenden Parteien (z.B. Gaia-X Membership credential von einem verifizierten Notar)
- Nutzung von AIP v2.0 neben AIP v1.0 durch Aktualisierung des AFJ Frameworks
- Bereitstellung eines verifiable Public Profile (Service-Endpunkte im OCM DID Dokument)
    - Konfiguration von Private Custom Endpoints (mit DID-Auth/OIDC)
    - Konfiguration von Endpoint Mappings zu internen/externen Funktionen

OCM W-Stack

Der Zweck des OCM W-Stacks ist es, alle notwendigen Komponenten für die Erweiterung der Verwaltung der digitalen Identität eines Teilnehmenden im Gaia-X-Kontext bereitzustellen. Der OCM W-Stack verbessert die Interaktion des Teilnehmenden mit dem SSI-basierten Ökosystem in einer vertrauensvollen und sicheren Weise. Dies umfasst die Nutzung der digitalen Identität des Teilnehmers für verschiedene Funktionalitäten:

- Implementierung einer vollständigen W3C DID/VC/VP Unterstützung für Credential Exchange and Trust
- Implementierung von OpenID-Standards
    - OpenID4VC/VP
    - SIOP
    - VC Issuance Protocol Extension
- Aufbau von sicheren und vertrauenswürdigen Verbindungen mit anderen Parteien
- Anforderung und Empfang von Verifiable Credentials von attestierenden Parteien (z.B. Gaia-X Membership Credential von einem verifizierten Notar) im JSON-LD Format
- Attestierung von Attributen zu Principals in Form von Verifiable Credentials (z.B. MitarbeiterInnen, techn. Assets)
- Validierung empfangener Verifiable Presentations von anderen Parteien (z.B. Validierung der Gaia-X-Mitgliedschaft anderer Teilnehmenden)
- Pflge des Verifiable Public Profile
- Skalierbare VC/VP Speicherung
- Graph Indexing für Verknüpfung von VC/VP

Wie der OCM legt auch der OCM W-Stack Wert auf W3C-Kompatibilität. Technologisch wird der OCM W-Stack jedoch eine Nicht-Indy-Implementierung sein, um von Hyperledger Indy unabhängig zu werden und die Interoperabilität zu maximieren.

PCM Cloud

Außerdem führen wir ein PCM ein, das über einen Webbrowser genutzt werden kann und somit eine Alternative zur bestehenden PCM-App darstellt. Der Zweck des PCM Cloud ist derselbe wie der der bestehenden PCM App - die Bereitstellung aller notwendigen Komponenten für die selbständige Verwaltung der digitalen Identität eines Principals im Gaia-X-Kontext. Der PCM Cloud ermöglicht es einer natürlichen Person, als Principal einer Organisation innerhalb des SSI-basierten Gaia-X-Ökosystems datenschutzkonform, vertrauensvoll und sicher über einen Computerbrowser zu agieren. Er umfasst die folgenden Hauptfunktionalitäten:

- Remote Management einer Cloud Wallet oder mehrerer Wallets, die mit dem PCM Cloud verbunden sind
- Empfang und Verwaltung von Verifiable Credentials von anderen Parteien (z.B. ein Principal Credential von einem Gaia-X Teilnehmer) über das Web-Frontend
- Automatisiertes oder manuelles Präsentieren von Verifiable Presentations für andere Parteien unter Verwendung von Plugins
- Sichere Speicherung und Verwaltung von jeweiligen Secrets
- Consent Management
- Policy-basierte Entscheidungen über Issuing/Presentations
- Plugin-System zur Erweiterung der “Holder Capabilities”

Die PCM Cloud ist als Cloud-basierte Komponente konzipiert und bietet eine benutzerfreundliche Webschnittstelle für die Verwaltung von OCM, OCM W-Stack und TSA. Sie dient als Integrationsschicht, die verschiedene Anwendungsfälle von “Holdern” erleichtert. Die PCM Cloud orchestriert diese Anwendungsfälle durch Plugins, wie z. B. das "ID Card Proof Plugin", das Funktionen wie die automatische ID-Kartenprüfung ermöglicht.

PCM Extension

Der Zweck dieses Produkts ist es, alle notwendigen Komponenten für die selbständige Verwaltung der digitalen Identität eines Auftraggebers im Gaia-X-Kontext auf einem mobilen Endgerät bereitzustellen. Das PCM ermöglicht es einer natürlichen Person, innerhalb des SSI-basierten Gaia-X-Ökosystems auf datenschutzfreundliche, vertrauenswürdige und sichere Weise als Prinzipal einer Organisation zu agieren. Die Erweiterung umfasst die folgenden Hauptfunktionalitäten:

- AIP 2.0 Support
- Empfang und Verwaltung von Verifiable Credentials basierend auf dem aktuellen W3C Standard
- Präsentation von W3C and AIP 2.0 Verifiable Presentations für andere Parteien in überprüfter Weise
- Sichere Speicherung und Verwaltung von jeweiligen Secrets
- Remote Management der PCM Cloud
- Unterstützung der PCM Cloud Funktionalität
- Erweiterung in QR Code Support Reading und Presentation

Darüber hinaus umfasst der Leistungsumfang die Bereitstellung der entwickelten Software in einem für den Endnutzer nutzbaren Format unter Einbeziehung der jeweiligen Verbreitungskanäle (z.B. App Stores).

TSA Extension

Das Ziel der Trust Services API Extension ist es, ein einheitliches Vertrauensniveau zwischen Gaia-X-Teilnehmenden und Komponenten zu gewährleisten. Die Trust Services API kann von allen anderen XFSC-Komponenten genutzt werden. Die Erstellung und Validierung von digitalen Signaturen spielen dabei eine besonders wichtige Rolle. Der Umfang umfasst das Signieren und Verifizieren notwendiger Daten, das Ermöglichen von policy-gesteuertem Vertrauen, das Sicherstellen von Vertrauensketten zwischen Teilnehmenden und das Validieren von eIDAS-konformen Signaturen.

Der Umfang umfasst auch die notwendigen Werkzeuge (z. B. Command Line Scripts) für den Betrieb und die Wartung der erstellten Softwarekomponenten in einer Enterprise-Umgebung mit Schwerpunkt auf High-Availability, Security sowie Monitoring und Logging auf der Basis gängiger Standards.

The wichtigsten Aktualisierungen/Erweiterungen sind:

- Erweitertes Policy Management
- Komponente wird „benutzbarer“ gemacht fürs Deployment
- Signaturdienste werden für eIDAS compliant Signaturen und Verifikationen ausgelegt
- TSA erhält ein Integrationsinterface über Cloud Events und Web Hooks
- Konfigurierbarkeit wird erweitert
- JSON Schema Validation wird hinzugefügt

NOT Extension

Die bestehende Komponente “Notarization API wird um folgende neue Funktionen erweitert:

- “Protocol agnostic issuances” in Abhängigkeit von der eingehenden DID und Formatdefinitionen
- Neue Ausstellungs- und Verifizierungsprotokolle
- Business validation flow für den Notar/Beglaubiger
- Dokumentation für die Verwendung der NOT API als Compliance-Dienst für Mitgliedschaften
- Dynamische Schemakonfiguration
- Eintragung der Organisation in bestimmte Vertrauenslisten
- Vertrauensüberprüfung mit dem TRAIN-Modul vor dem Ausstellungsprozess
- Automatische Notarization Verification

Die Erweiterung wird auch Schnittstellen (API's) enthalten, um die Notarization-Komponente reibungslos in externe Software für die Nutzung durch Nicht-IT-Betreiber (z.B. Anwälte, Notare, Behörden, Zertifizierer ...) zu integrieren.