FACIS FAP PCI (Principal Credential Issuance)

Credential management by Participants for Principals

Version / Date 21-NOV-2025

Status: Idea **/ Draft /** In Review / In Implementation / Released

1. Purpose & Value

The **Principal Credential Issuance FAP** provides an end-to-end, interoperable pattern for defining, configuring, and issuing verifiable principal credentials within a federated ecosystem.
It connects organisational administrators, data APIs, and wallets through a secure and standardised issuance process based on SSI and federation principles.

Purpose

- To allow organisations to define credential types (schemas, branding, definitions) and securely issue them to verified employees.
- To standardise credential administration and issuance workflows across ecosystems.
- To enable decentralised trust and cross-domain interoperability, avoiding centralised control.
- To provide an easy to use frame for credential issuance

Value

- Reduces complexity and cost of credential setup and issuance.
- Ensures compliance with federated trust frameworks (e.g., Gaia-X, eIDAS).
- Enables employees to carry portable, verifiable credentials in digital wallets (especially OID4VCI compatible one)
- Supports scalability across domains such as education, health, mobility, supply chain, etc.
- On Top Integration for existing OAuth2 Systems (e.g. Keycloak)

2. Scope & Boundaries

In Scope

- Provision of SaaS Toolstack for Issuance including ORCE Basic Workflows

- Multi Account Usage
- Credential definition and configuration via Administration Page (schemas, images, definitions)
- Metadata storage for credential templates and issuance parameters.
- Integration with OAuth2-based authentication and employee data APIs.
- Issuance workflow orchestration through ORCE and Issuing Plugins.
- credential delivery for OID4VCI compatible Wallets via QR codes, deep links and offering links.
- Credential verification and revocation

Out of Scope

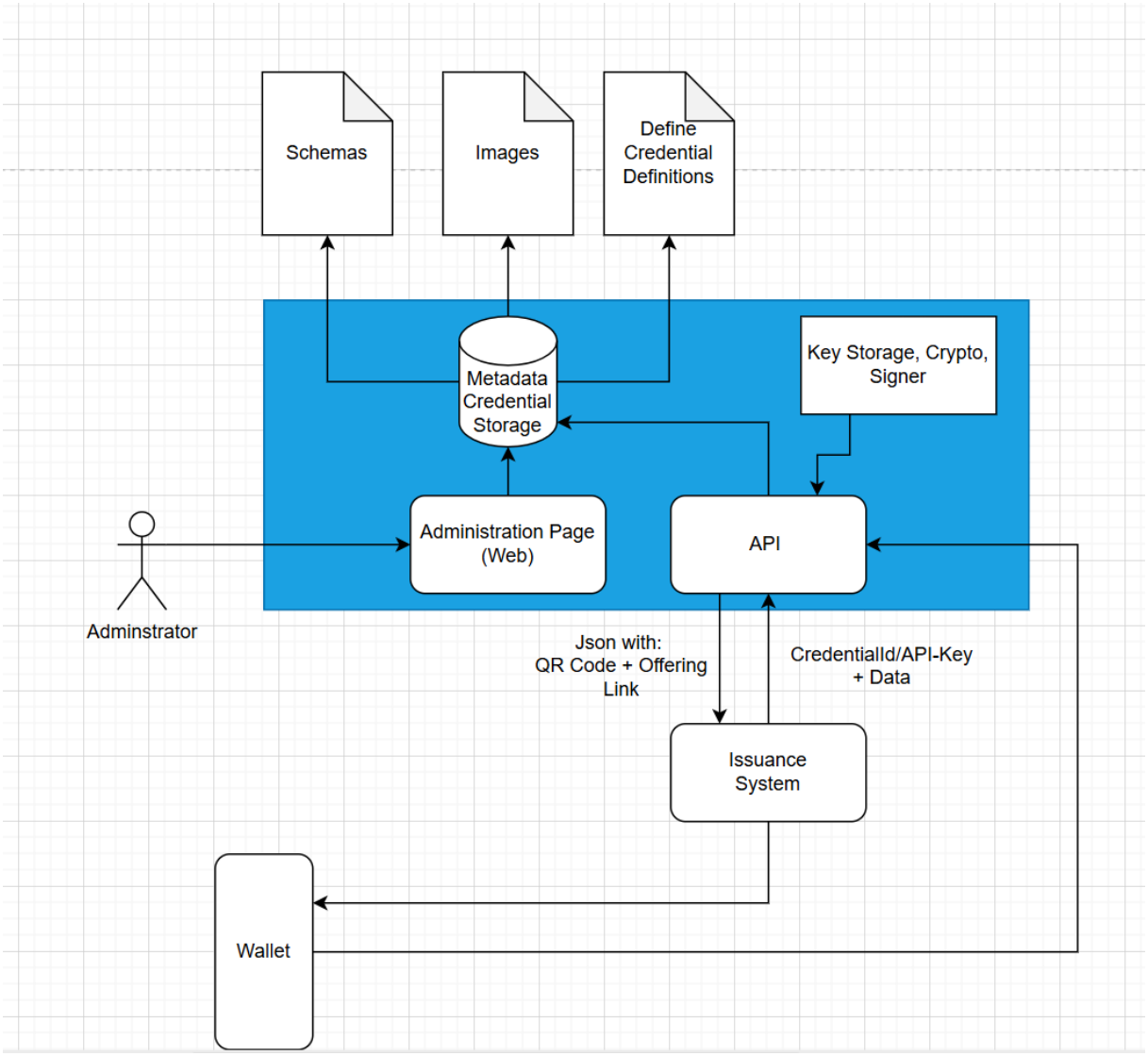
- Full HR or data system management.
- Legal identity validation beyond trusted SSI/eIDAS providers.
- Wallet Implementation
- OCM W-Stack Deployment (will be provided)

3. Architecture Building Blocks

This FAP combines two main sub-patterns:

1. **Credential Administration & Configuration Workflow**
2. **Principal Issuance Workflow**

3.1 Credential Administration & Configuration



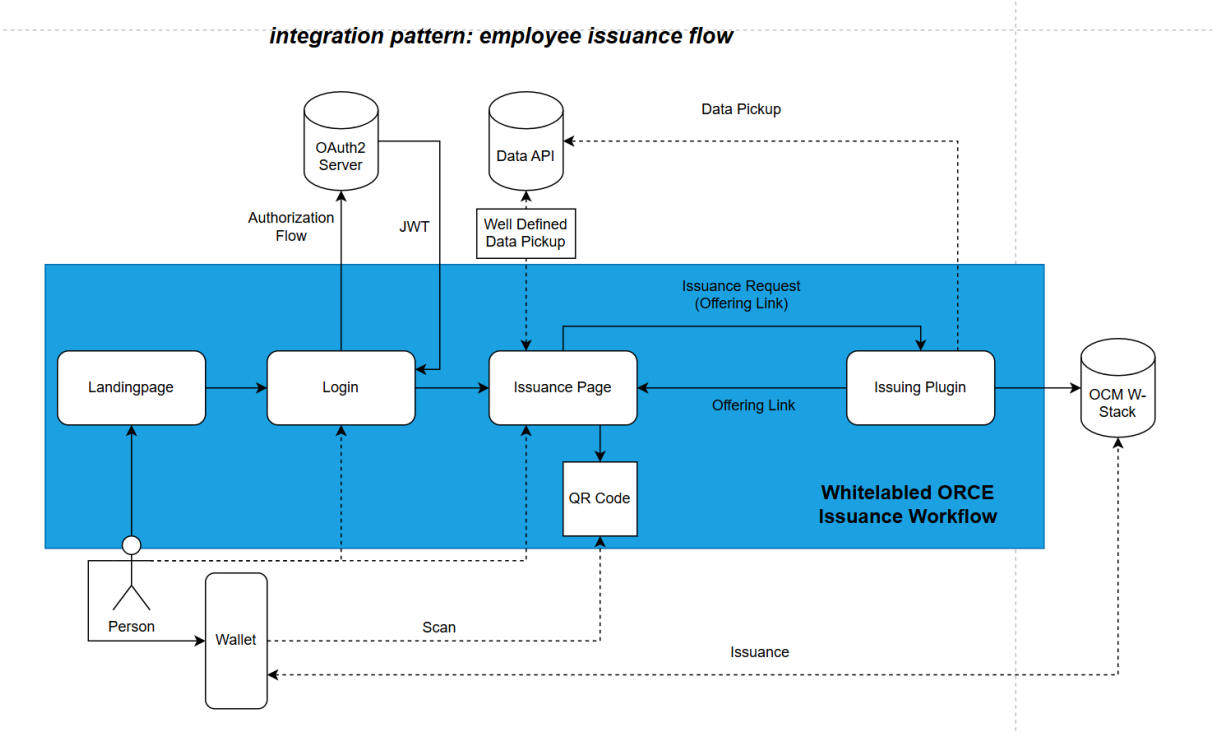
Administrators manage credential metadata, templates, and issuance rules used later in the issuance process.

Key Components:

- **Administrator:** Configures and manages credential templates.
- **Administration Page (Web):** UI for defining schemas, uploading images, and setting credential definitions.
- **Metadata Credential Storage:** Repository holding credential schemas, branding, and definitions.
- **Key Storage, Crypto, Signer:** Manages cryptographic material for secure credential signing.

- **API:** Exposes credential templates and metadata to issuance systems.
- **Issuance System Connector:** Consumes credential definitions to produce offering links or QR codes.

3.2 Employee Issuance Workflow



Once credential templates are defined, the issuance workflow securely issues credentials to employees.

Key Components:

- **Landing Page:** Entry point for employees.
- **Login (OAuth2):** Authenticates users and obtains JWT.
- **Data API:** Provides verified employee data for issuance.
- **Issuance Page:** Displays issuance offer (QR code or link).
- **Issuing Plugin:** Creates and sends issuance offers to wallets, integrated with OCM W-Stack.
- **Wallet:** Employee's digital wallet where credentials are stored.
- **OCM W-Stack:** Manages credential creation, signing, and issuance.
- **ORCE Workflow:** Orchestrates the end-to-end process.

4. Standards & Protocols

- **W3C Verifiable Credentials (VC/VP)** – credential data and exchange model.
- **OIDC4VCI** – standard issuance interaction between issuer and wallet.
- **OAuth2 / OpenID Connect** – user authentication and authorization.
- **JSON-LD / JSON Schema** – schema and metadata definitions.
- **DIDComm v2** – secure messaging channel between issuer and wallet (optional).
- **Gaia-X Trust Framework** – compliance, trust anchors, and federation governance.
- **eIDAS 2.0** – legal identity and qualified trust alignment.
- **GDPR** – consent and data minimisation during issuance.

5. Reuse & Variants

Cross-domain Use Cases:

- **Education:** Student or faculty ID credential issuance.
- **Health:** Healthcare professional credentials.
- **Supply Chain:** Employee or supplier authorisation credentials.
- **Mobility:** Driver or fleet operator credentials.

Reusable Modules:

- Credential Definition & Metadata Storage.
- OAuth2 Authentication Flow.
- Issuance Page + Issuing Plugin integration.
- QR Code / Offering Link Generation.

Variants:

- **Self-Service Issuance:** Employee initiates issuance via landing page.
- **Automated HR Integration:** Batch issuance triggered by HR or IAM systems.
- **Federated Issuer Networks:** Shared credential definitions across organisations.

7. Expected Outcomes

- Operational SaaS prototype of a federated employee issuance system.
- Reusable issuance and configuration components (admin UI, API, ORCE workflow).
- Verified compliance with SSI standards (VC, OIDC4VCI, GDPR).
- Foundational building block for broader **Federated Identity & Trust Ecosystem**.