Interoperable Trust Frameworks for Digital Identity: OpenID Federation, X.509, Trust Lists and Wallet Attestations

Tunji Durodola
Secure Identity Alliance

tunji.d@trustvault.eu
+372.5.452.0624

Introduction

Moving from Technical Standards to Sovereign Ecosystems

SECURE IDENTITY ALLIANCE

Introduction

From trust anchors to attestations: the machinery behind interoperable digital trust

Overview

1. Exploring how interoperable trust frameworks combine federation metadata, PKI, trust lists and wallet attestations to establish verifiable trust relationships across digital identity ecosystems, with emphasis on technical interoperability, governance boundaries, validation paths and cross-border assurance.
2. **Session focus:** mechanisms for trust establishment rather than high-level policy aspirations
3. **Framing question:** how relying parties, wallets and issuers decide which entities to trust and why
4. **Scope:** OpenID Federation, X.509, trust lists, wallet attestations and their interplay

ITU

SECURE IDENTITY ALLIANCE

Why Trust Management Is the Real Interoperability Problem

Why Trust Management Is the Real Interoperability Problem

Standards are not solutions; they are tools. The gap between a protocol and a trusted ecosystem is where policy must lead.

- Interoperability breaks down when trust anchors, authority boundaries and validation rules are not machine-processable.
- Cross-jurisdiction ecosystems require machine-processable trust, not bilateral manual onboarding
- Wallet ecosystems introduce additional actors: issuers, wallets, verifiers, trust registries, scheme authorities and supervisory bodies
- Technical trust management must answer who is trusted, for what role, under which policy, and for how long?

ITU

SECURE IDENTITY ALLIANCE

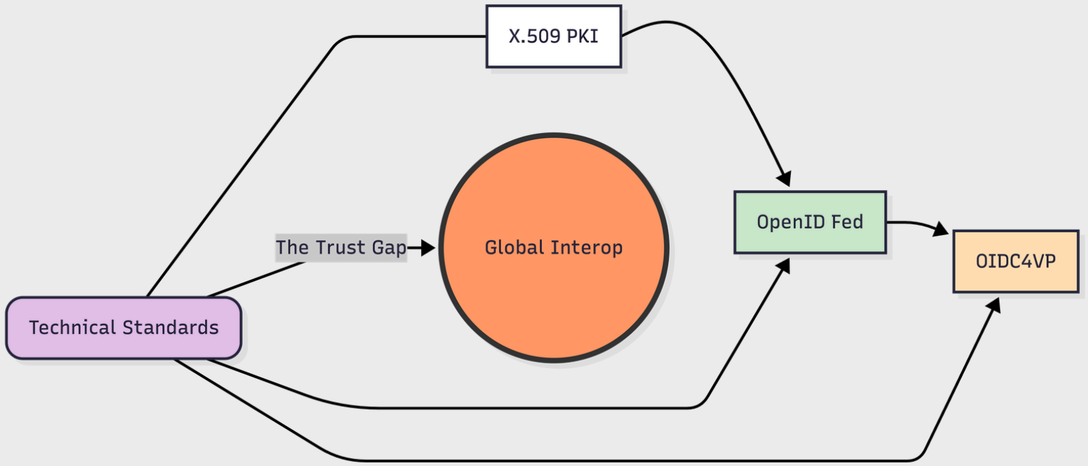
Trust Models and Trust Anchors

- **Hierarchical trust model:** classic PKI with certificate chains rooted in trusted certification authorities
- **Federated trust model:** signed metadata statements chaining authority through federation entities and trust anchors
- **List-based trust model:** explicit inclusion of trusted entities through signed or governed trust lists
- **Attestation-based model:** cryptographic statements about wallet instance, device, key provenance or certification status
- Real-world deployments commonly blend these models rather than choosing only one

ITU

SECURE IDENTITY ALLIANCE

The Multi-Protocol Paradox



The Multi-Protocol Paradox:
X.509 vs. OpenID Federation

- **X.509 PKI:** The "Hard" Root. Ideal for static, high-assurance governmental CAs where long-term legal non-repudiation is the primary requirement.
- **OpenID Federation 1.0:** The "Agile" Layer. Specifically designed for dynamic metadata exchange and reducing the massive administrative overhead of traditional PKI.
- **The Hybrid Reality:** Modern architectures must support X.509 for the Root of Trust while utilizing OIDCFED for the scalable distribution of those trust anchors to verifiers.
- **Technical Friction:** The difficulty of mapping X.509 certificate policies to OIDC metadata statements without losing semantic meaning.

ITU

SECURE IDENTITY ALLIANCE

X.509 and PKI Still Matter

- X.509 remains foundational for identity binding, key management, transport security and qualified trust services
- Certificate chains provide well-understood validation semantics, revocation mechanisms and auditability
- PKI is particularly strong where legal identity, hardware protection and regulated issuance are required
- Limitations appear when role semantics, ecosystem metadata and dynamic authorisation need richer expression than certificates alone
- In many architectures, PKI secures the keys while federation or trust registries express ecosystem relationships

ITU

SECURE IDENTITY ALLIANCE

Interoperability vs. "Intra-operability"

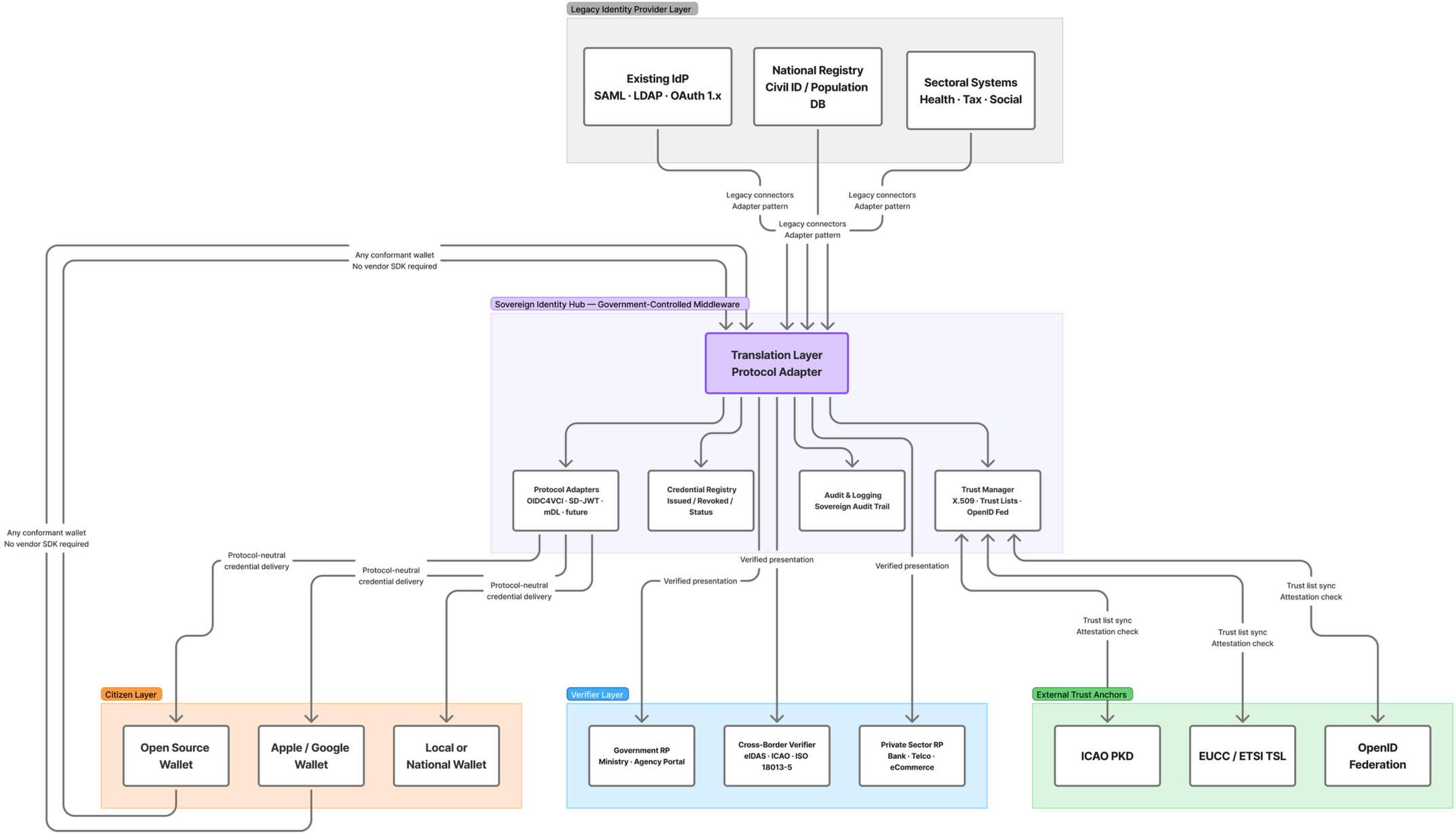
Interoperability vs. "Intra-operability"

- **The Illusion of Choice:** A vendor may use OpenID protocols but implement proprietary "extensions" that effectively lock a government into their specific verifier suite.
- **Schema Mismatch:** The "Standard" protocol (OIDC4VP) doesn't guarantee the "Standard" payload. (e.g., mDL vs. W3C Verifiable Credentials).
- **The Verifier Onboarding Bottleneck:** If a verifier must manually integrate with every issuer's specific "flavor" of a standard, the ecosystem fails to scale.
- **Data Minimization Hurdles:** Ensuring that Selective Disclosure (SD-JWT) is actually supported by the "off-the-shelf" verifiers pushed by major tech players.

ITU

SECURE IDENTITY ALLIANCE

The "Sovereign Identity Hub"


Legacy Identity Provider Layer
Existing IdP
SAML · LDAP · OAuth 1.x
National Registry
Civil ID / Population DB
Sectoral Systems
Health · Tax · Social
Legacy connectors
Adapter pattern
Legacy connectors
Adapter pattern
Legacy connectors
Adapter pattern
Any conformant wallet
No vendor SDK required
Sovereign Identity Hub — Government-Controlled Middleware
Translation Layer
Protocol Adapter
Protocol Adapters
OIDC4VCI · SD-JWT · mDL · future
Credential Registry
Issued / Revoked / Status
Audit & Logging
Sovereign Audit Trail
Trust Manager
X.509 · Trust Lists · OpenID Fed
Any conformant wallet
No vendor SDK required
Protocol-neutral
credential delivery
Protocol-neutral
credential delivery
Protocol-neutral
credential delivery
Verified presentation
Verified presentation
Verified presentation
Trust list sync
Attestation check
Trust list sync
Attestation check
Trust list sync
Attestation check
Citizen Layer
Open Source Wallet
Apple / Google Wallet
Local or National Wallet
Verifier Layer
Government RP
Ministry · Agency Portal
Cross-Border Verifier
eIDAS · ICAO · ISO 18013-5
Private Sector RP
Bank · Telco · eCommerce
External Trust Anchors
ICAO PKD
EUCC / ETSI TSL
OpenID Federation

The "Sovereign Identity Hub" (Modular Middleware)

- **Decoupling Strategy:** Separating the Identity Provider (IdP) from the Wallet and the Verifier.
- **The Middleware Layer:** A government-controlled "Identity Hub" that acts as a translation layer between legacy systems and modern OIDC flows.
- **Wallet Agnosticism:** The architecture must allow any conformant wallet (Open Source, Apple/Google, or Local) to receive credentials without vendor-specific SDKs.
- **Protocol Neutrality:** Building the backend so that switching from OIDC4VCI to another future protocol doesn't require a total system overhaul.

ITU

SECURE IDENTITY ALLIANCE

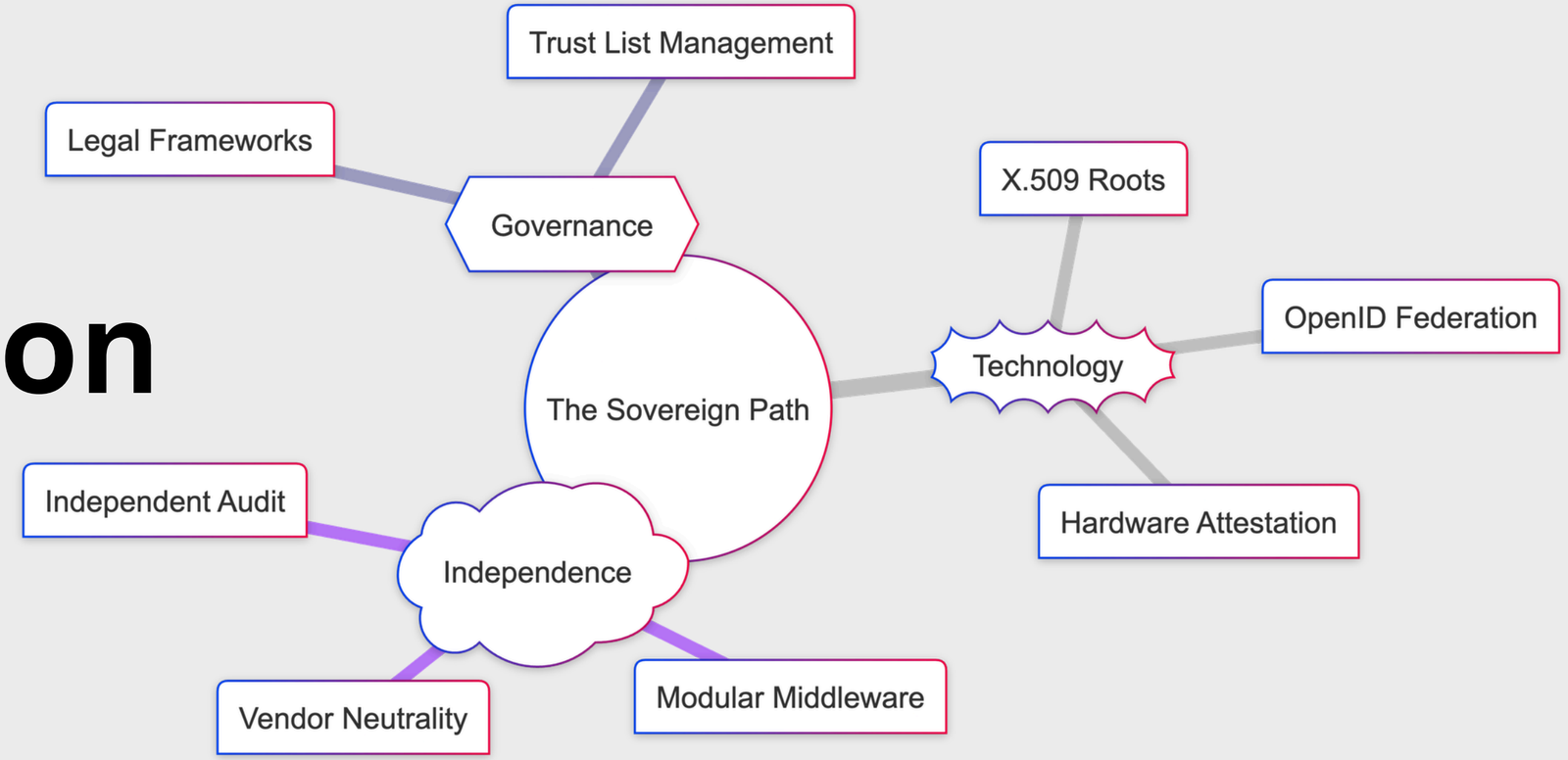
The "Sovereign Identity Hub" (Modular Middleware)

- **The Hardware Anchor:** Why software-only wallets are insufficient for national ID. Requirement for Secure Enclave / TEE integration.
- **Proof of Association:** Mechanisms to ensure the credential is bound to the device and the holder, preventing "Credential Stuffing."
- **Dynamic Attestation:** Using OIDC4VCI to request a fresh "Wallet Attestation" at the moment of issuance to prove the app hasn't been tampered with (Root/Jailbreak detection).
- **The Verifier's Dilemma:** How a verifier in a foreign jurisdiction can trust the hardware attestation signature from a device they don't manage.

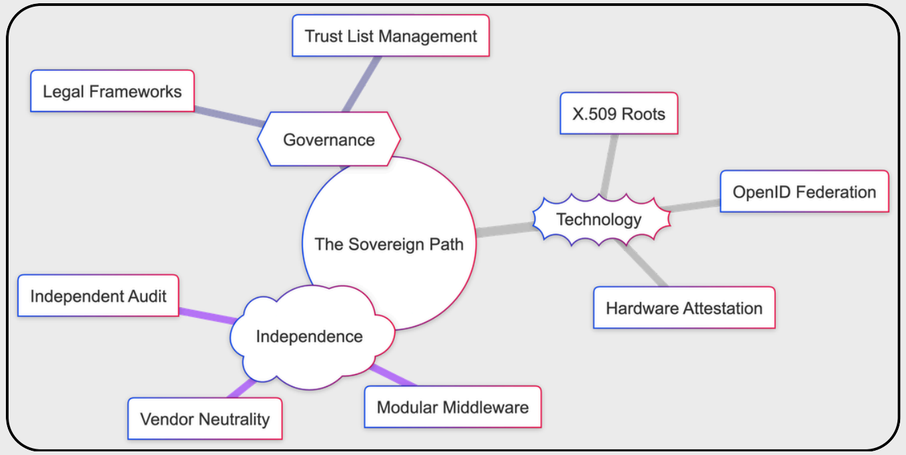
ITU

SECURE IDENTITY ALLIANCE

Conclusion


Trust List Management
Legal Frameworks
Governance
X.509 Roots
OpenID Federation
The Sovereign Path
Technology
Hardware Attestation
Independent Audit
Independence
Vendor Neutrality
Modular Middleware

Building for the Citizen, Not the Vendor



- **Identity as Infrastructure:** Digital ID is a public utility, much like roads or water; it cannot be "owned" by a single vendor.
- **Sovereignty by Design:** A jurisdiction must be able to swap any component (Issuer, Hub, Wallet) without starting over.
- **Interoperability is a Choice:** It is a policy decision to be open, and a technical decision to enforce it.
- **Bottom line:** Use open standards, demand modularity, and never trust a "Black Box."

ITU

SECURE IDENTITY ALLIANCE

SECURE IDENTITY ALLIANCE

Thank You

Tunji Durodola
Secure Identity Alliance

tunji.d@trustvault.eu