

# Trust Framework Mapping & SIDI Hub

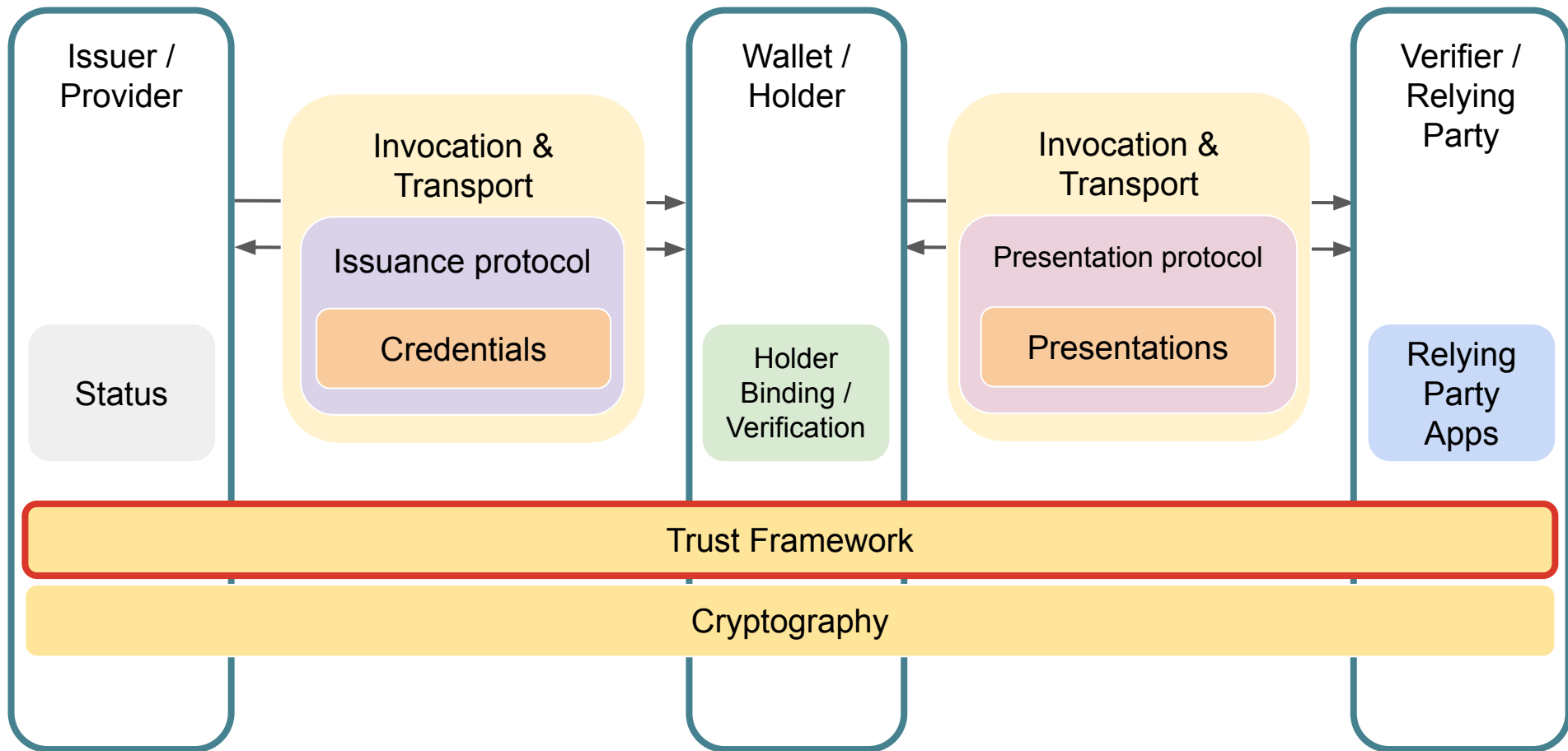
Gail Hodges

Executive Director, OpenID Foundation

[director@oidf.org](mailto:director@oidf.org)



# The Building Blocks for the Digital Credentials Stack





We are building a “**Digital Commons**” of open tools – from policy to technology – that help countries implement **safe, interoperable Digital Identity.**

# Founding Principles

1

Human Centricity & Human Rights

2

Domestic Sovereignty

3

Multi-Lateral Engagement

4

Grounded in Use Cases & Benefits

5

Technology & Policy Normalization



## 2023 Guide to Trust Frameworks

“

**Trust Frameworks create an ecosystems in which users, organizations, services, and devices can trust each other because they are following a common set of rules and policies.**

”

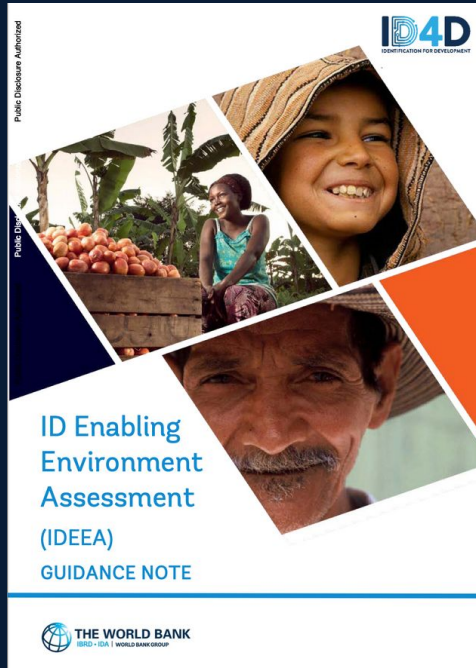


## Trust Framework Original Analysis of 10+ Countries





## Existing frameworks for trustworthy ecosystems



Source: SIDI Hub Summit, Paris December 2024, TrustTech.

<https://sidi-hub.community/>

## Trust Frameworks need to reflect

- Purpose
- Scope
- Enabling Environment



**Ecosystem Purpose & Scope**

**Rule of Law**

**Accountable Institutions**

**Users and Access**

**Trust Management**

**Trust Services Rules**

**Proofing and Assurance**

**Data Protection & Management**

## Ecosystem Purpose & Scope

- Legal Identity
- Legal Status
- Functional Uses

## Rule of Law

- Legal Authority & Mandates
- Privacy & Data Protection Law
- Cybersecurity Law
- Rights & Civil Protections
- Judicial Oversight
- Correction, Remedy, Redress

## Accountable Institutions

- Institutional Arrangements
- Contracts and Liability
- Managing Ecosystem Actors
- Capacity
- Procurement
- Data & Monitoring

## Users and Access

- Accessing Services
- Enrollment & Inclusion
- Account Management

## Trust Management

- Trusted Actors
- Trust Between Actors

## Trust Services Rules

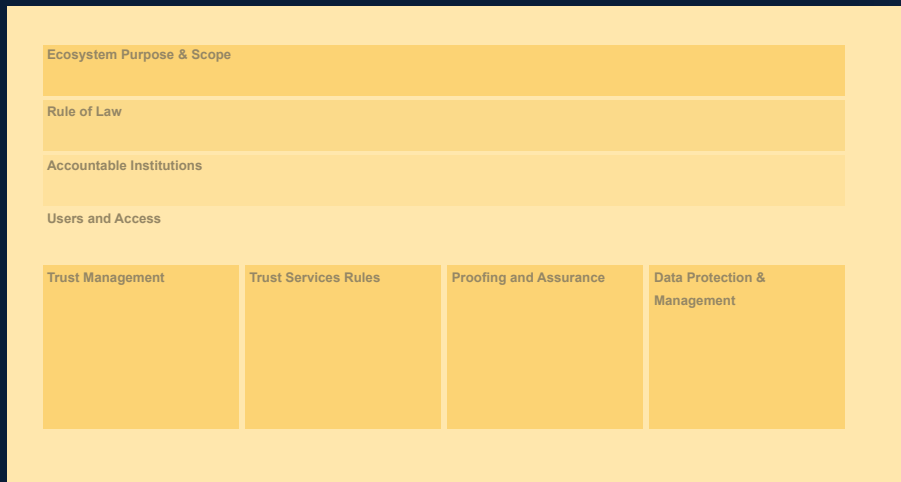
- Authentication
- Verification
- Electronic Signatures

## Proofing and Assurance

- Proofing & Binding
- Credential Types
- Assurance Rules

## Data Protection & Management

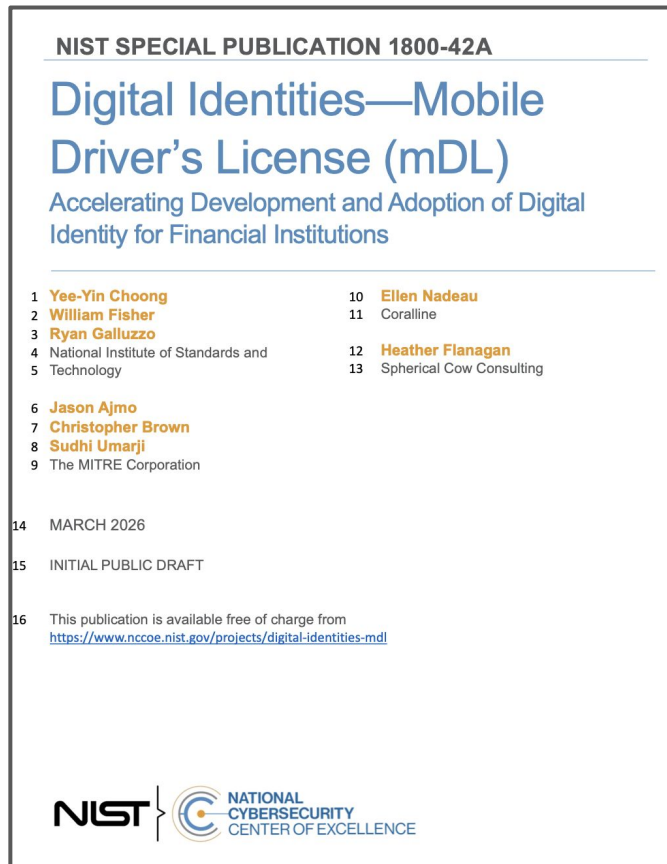
- Privacy & Consent Rules
- Data Storage & Retention Rules
- Risk Management
- Incident Management
- Data Standards
- Data Exchange



## Use Case Rulebooks

- Trust Framework components profiled to the ecosystem
- Metadata requirements
- Schema libraries

# FI Use Case: NIST NCCoE mDL Accelerating FI adoption



- NIST NCCoE Phase 1 with state issuers, leading banks, digital platforms, OIDF
  - Proved out interoperability of OpenID4VC/ DC API/ IETF/ ISO/IEC specs + “NIST verifier” in 11 interop events
  - Report feedback by May 5th 2026
- Learnings from FIs needing more visibility to assurance and authentication metadata
  - OIDF eKYC reports with US, Australia, NZ, EU for global standards approach
- Engaging FI consortia to support governance, scale deployment

# FI Use Case: Compliance via protocol/ format

## 6.1 Assurance Context URIs ( context\_uri )

Defines the specific legal or regulatory trust framework governing the verification event.

| Jurisdiction | Parameter Value ( context_uri ) | Governing Framework  | Description                                            |
|--------------|---------------------------------|----------------------|--------------------------------------------------------|
| US           | urn:openid:assurance:us:real_id | DHS REAL ID Act      | Federal standards for state-issued driver's licenses.  |
| EU           | urn:openid:assurance:eu:eidas   | eIDAS 2.0 Regulation | European digital identity framework (EUDI Wallet).     |
| AU           | urn:openid:assurance:au:tdif    | TDIF                 | Australian Trusted Digital Identity Framework.         |
| NZ           | urn:openid:assurance:nz:distf   | DISTF                | New Zealand Digital Identity Services Trust Framework. |
| Global       | urn:openid:assurance:global:iso | ISO/IEC 29115        | Global entity authentication assurance framework.      |

## 6.2 Assurance Classifications ( assurance\_classification )

Values are dependent on the associated context\_uri and define the specific level of assurance achieved.

| Associated Context | Parameter Value ( issuance_assurance_classification ) | Definition                                                           |
|--------------------|-------------------------------------------------------|----------------------------------------------------------------------|
| *:real_id          | status:full_compliance                                | Credential meets highest mandated federal standards.                 |
| *:eidas            | loa:high                                              | Cryptographic hardware binding verified; equivalent to face-to-face. |
| *:eidas            | loa:substantial                                       | Strong authentication, but lower initial proofing requirements.      |
| *:tdif             | ip:3                                                  | Identity Proofing Level 3 (High Confidence) under AU TDIF.           |
| *:distf            | level:high                                            | High assurance identity proofing under NZ DISTF.                     |

## 6.3 National Identifier Types ( identifier\_type )

Standardized values for the national\_identifier\_match object.

| Jurisdiction | Parameter Value ( identifier_type ) | Jurisdictional Target                  |
|--------------|-------------------------------------|----------------------------------------|
| US           | ssn                                 | Social Security Number                 |
| US           | tin                                 | Taxpayer Identification Number         |
| EU           | pid                                 | Personal Identification Data (eIDAS)   |
| AU           | tfn                                 | Tax File Number                        |
| AU           | crn                                 | Customer Reference Number (Centrelink) |
| NZ           | ird                                 | Inland Revenue Department Number       |

## 6.4 Authoritative Organizations ( organization )

Specifies the entity that performed the freshness or revocation check.

| Jurisdiction | Parameter Value ( organization )      | Entity Type / Example                                              |
|--------------|---------------------------------------|--------------------------------------------------------------------|
| US           | urn:issuing_authority:us:aamva        | American Association of Motor Vehicle Administrators (DTS)         |
| EU           | urn:issuing_authority:eu:es:fnmt      | Fábrica Nacional de Moneda y Timbre (Spain - National Mint/Issuer) |
| EU           | urn:issuing_authority:eu:member_state | Generic routing for EU Member State national registries            |
| AU           | urn:issuing_authority:au:dvs          | Australian Document Verification Service                           |
| NZ           | urn:issuing_authority:nz:dia          | New Zealand Department of Internal Affairs                         |
| NZ           | urn:issuing_authority:nz:nzta         | New Zealand Transport Agency (Waka Kotahi)                         |

Protocol, format, and jurisdiction-agnostic framework for identity claims that extends the: [OpenID Identity Assurance Schema Definition 1.0](#) and [OpenID Connect for identity Assurance Claims Registration 1.0](#) to directly support Relying parties (RPs) in establishing a legally defensible “reasonable belief” of customer identity. Work Item: <https://github.com/openid/eKYC-IDA-Registry-Profile/blob/main/Discussion-Papers/Format-Agnostic-Digital-Identity-Claims%2BValues.md>



## We're building a comparison tool for 3 groups



### Policy-Makers

- Build or assess their identity policy stacks
- Compare policies with other jurisdictions
- Design laws & policies that will interoperate with others



### GovTech

- Fill policy needs if a technical component is already in place
- Interoperate with other jurisdictions



### Private Sector

- Build components (e.g., a wallet) that can be implemented in different jurisdictions

