Trust Management for Interoperable Wallet & Login Ecosystems

David Kelts - Digital Identity Strategist;
Trust Architect, SIDI-Hub Technology & Policy

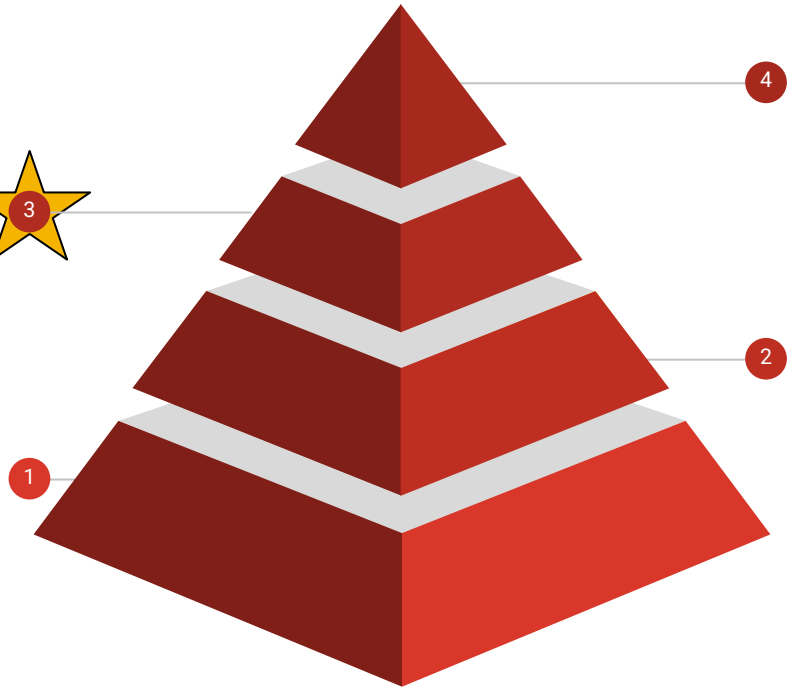
Interoperability

Trust Management: Conventions & Mechanisms

How do components & participants in your ecosystem trust each other in real-time? Is there component choice? Is the ecosystem open or controlled? Do you want reputation to rule? invite innovation?

Standards Cooperating

EUDI Wallet standards are being tested NOW at scale and across the globe with results proving that the standards mechanically work.



Global Acceptance

Credentials from multiple ecosystems exist; Wallet choice by Users is encouraged; People travel across borders and live outside of the ecosystem of their docs; Business crosses borders.

Imposing policy-level restrictions can thwart real-life interoperability of lvls 1-3

Usability & User Experience

Can all of your ecosystem participants effectively use the set of standards.

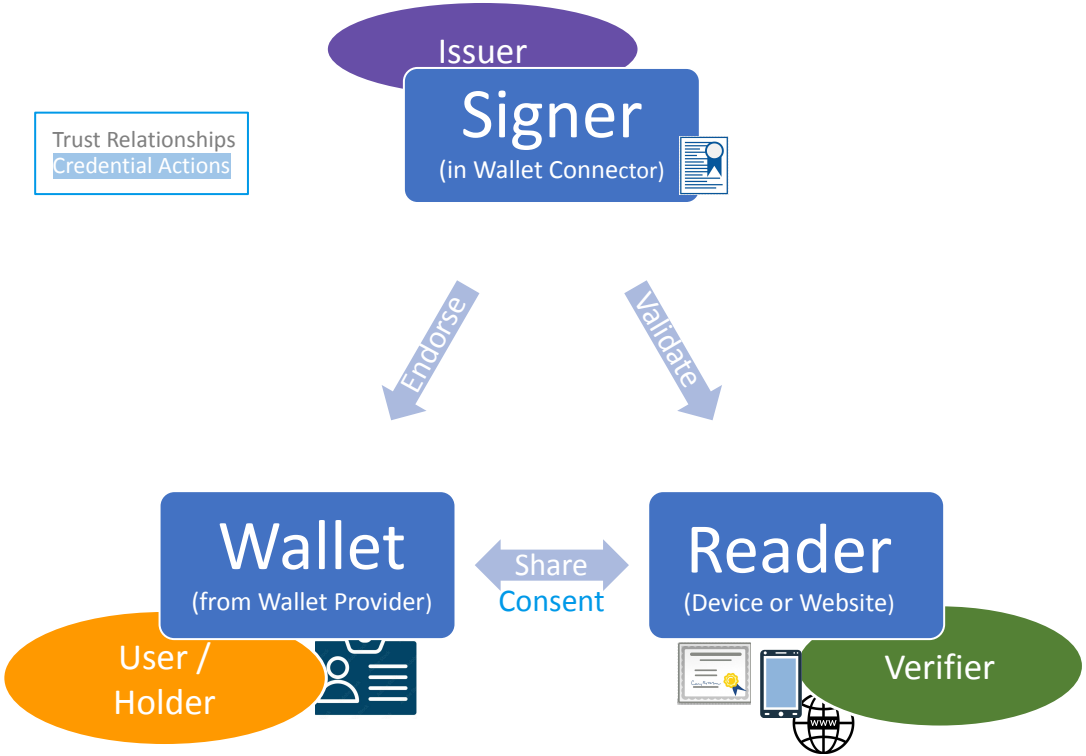
- Can Users QR Code Scan?
- Technology Match at Checkout?
- Overcome Resistance to Change?
- Do implementations encourage diverse workflows to support RPs?

Trust

Trust = Assurances that Mitigate Risk

Each participant in identity transactions carries risk. The **Ecosystem** works because each participant plays a role in providing assurances to the others that mitigate or meet that risk. Trust is the term used to express that ecosystem participants are meeting their obligations to provide assurances and fulfill their roles according to ecosystem expectations expressed in a **Trust Framework**.

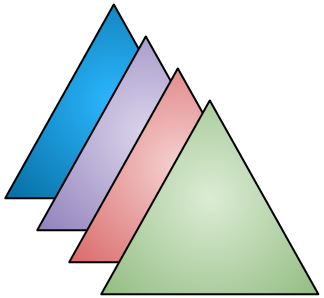
Wallet Credentials



SIDIHub

Some Truths About ID & Credentials

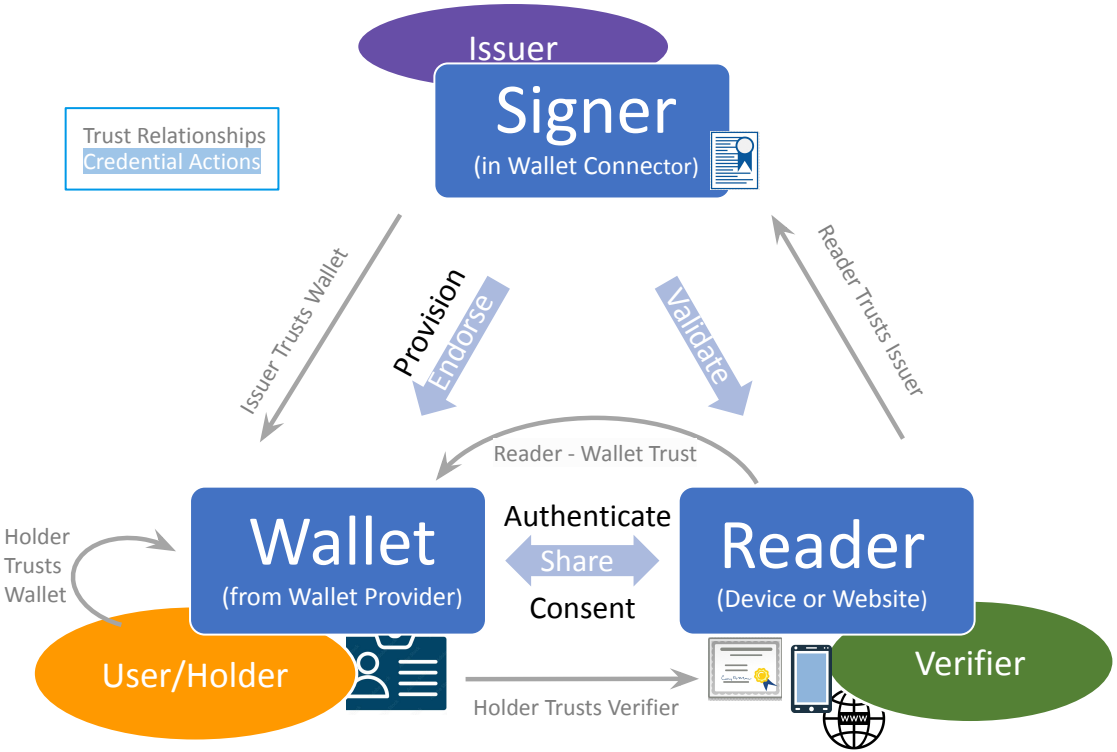
This adds complexity & dimensions to every “open” ecosystem



01	People Live & Work Elsewhere	• Moving from place of birth • Working or living in another city, state, or country • Global residency, migration, displacement
02	People have Credentials outside their origin ecosystem	• Going/went to school in another country • Achieving citizenship, marriage, profession • History of ID, Licenses, & Badges gets long
03	Verifiers have existing workflows	• Physical layouts for existing customer flows • Automated and Attended interactions with ID • Service delivery across in-person & online contexts
04	People have wallet preferences	• Choosing wallets for the best privacy & functionality • Global Wallets will hold credentials across Issuers • Free market competition for best functional value
05	Verifier acceptance rules differ	• Regulated Industries; Business policy, compliance • Qualifying age categories differ • Do you restrict Verifier access to all attributes?

SIDIHub

Wallet Ecosystem



Who has to Trust?

"Trust Vectors" that must be satisfied in an Identity Ecosystem* to accomplish:

- End-User **Choice of Wallet**
- RP **Choice of Reader** or Embedding
- **Interoperability****
- **Global Acceptance**
- **Risk Mitigation** for All Participants

* Wallet, Cloud Wallet, Login, Federated, Decentralized
** Defined on Slide 2 in 4 Layers

SIDIHub

Issuer Trusts Wallet to approve and provisioning credentials for Users into it.

Reader Trusts Wallet for Credential Protection and User Authentication.

User Trusts Verifier to consent to share ID.

Reader Trusts Issuer to validate the credential data as authoritative.

Ecosystem Trusts Reader to identify itself to Users to request ID Data (that it is authorized to request).

User Trusts Wallet to prevent user profiling, improper data sharing, consent violation.

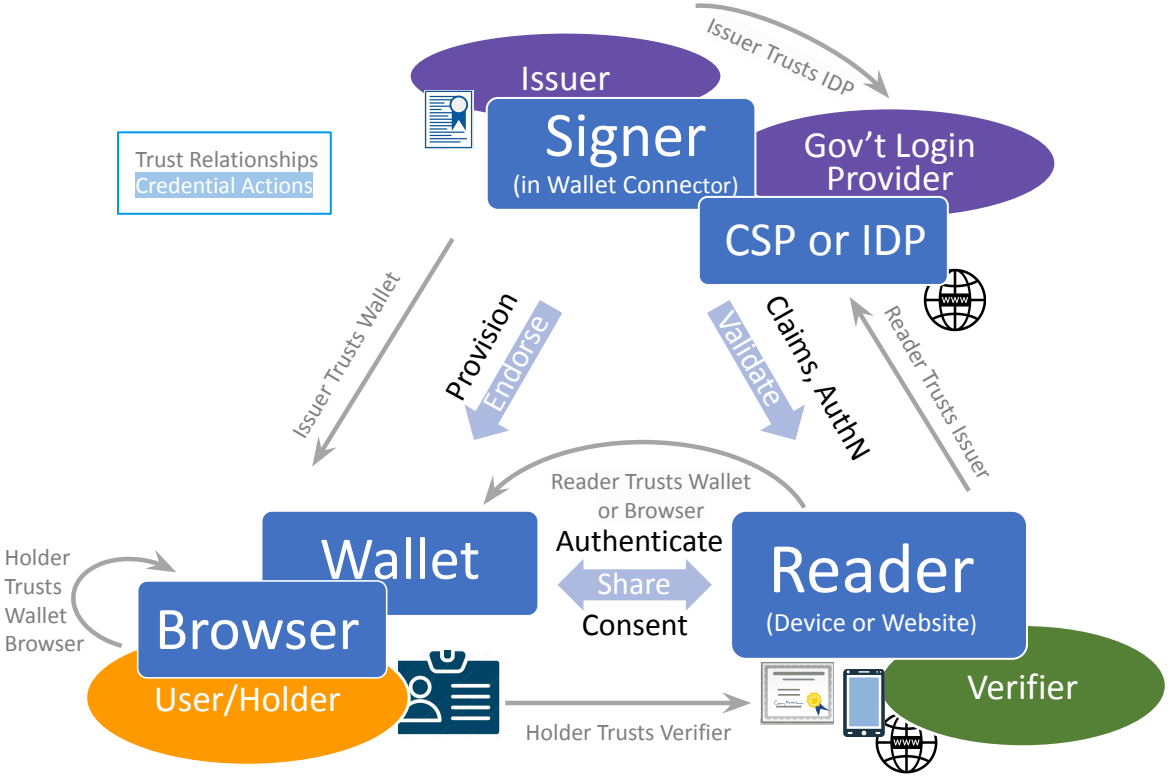
Mechanisms… With Conventions for Use

Mitigating risk of other Ecosystem Participants

- **Mechanisms** are methods, often standardized, for inspecting in real-time that a participant is a conforming member of the Ecosystem fulfilling their obligations
- **Conventions**, often policy, sit on top of mechanisms to configure that Mechanism for usage on a particular role, thereby allowing one role to be inspected differently than other roles. A Convention explains how to take part in the Mechanism and therefore expresses the meaning of the Mechanism

SIDIHub

Wallet & Login Ecosystem



Trust Elements & Validation Methods

Wallet Attestations

- Reputation
- Issuer, Registrar, Ecosystem Signatures
- Introspection
- Trust Registry

Issuer Public Keys

- VICAL
- PKDirectories
- Distributed Ledgers
- PKI Root Test

Reader Identification Certificates

- Introspection
- Association Member
- Registries
- Trust Registries

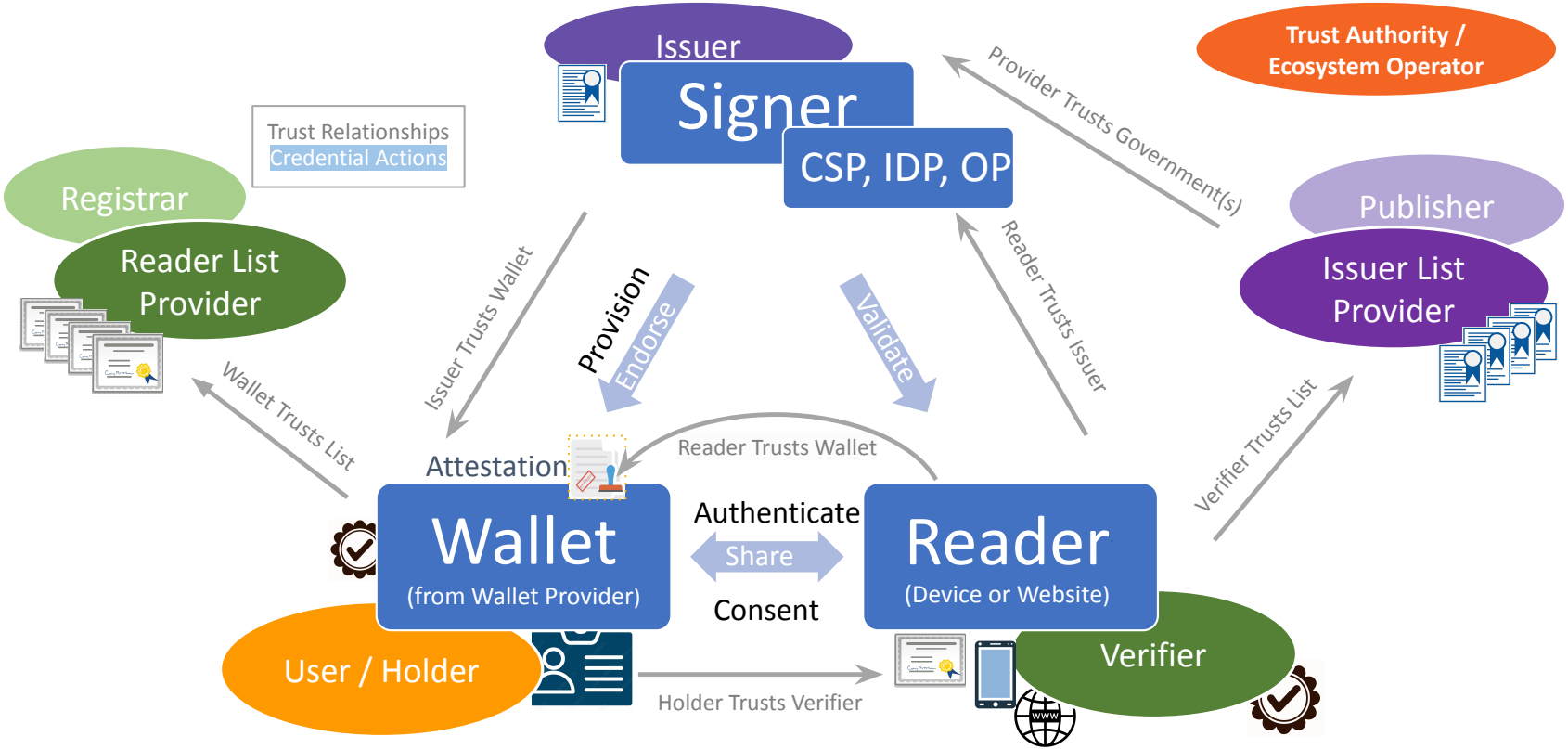
Trust Marks & Seals (Meets Requirements)

- Visual Seals
- Open Badges
- Brand Names
- Crowd-sourced Reputation

Smart Contracts

- Inspectable Requirements Conformance

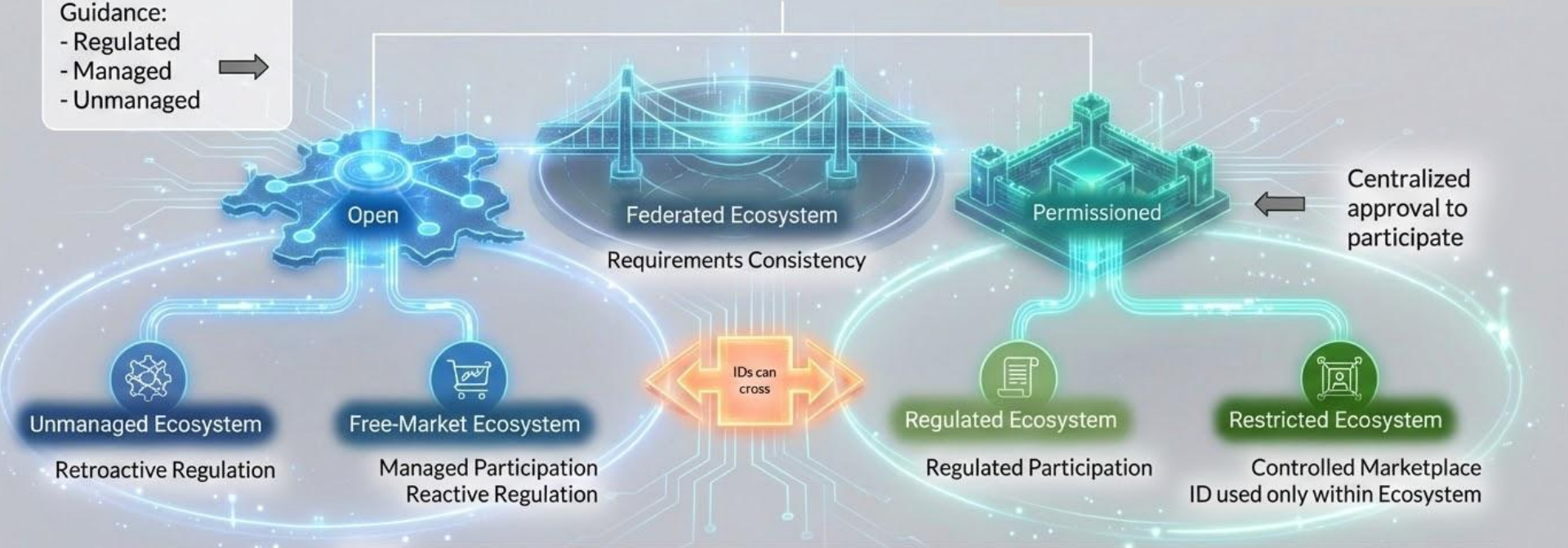
Wallet & Login Ecosystem with Trust Vectors



State or Proofing-Anchored

Foundational Digital ID Governance

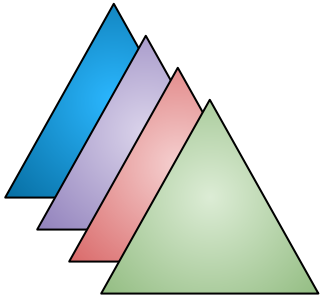
Guidance:
- Regulated
- Managed
- Unmanaged



Registrars can be deputized to operate Trust Mechanisms for a type of component (wallet, reader, issuer) and onboard participants according to regulation, managed requirements, or their own.

Ecosystem Operator Considerations

Let's revisit the complexity & dimensions to every "open" ecosystem



Reader Decisions

Can a **Verifier** identify itself the same across web and in-person?

Do Readers need to **multiple register**? within every Ecosystem they accept credentials from? With every Issuer they accept from?

Are there **Business Associations** that make sense to be Reader Registrars? Or that can be Trust Mark Purveyors?

Is it imperative to implement & enforce **Attribute Access Policies** that restrict Verifiers from ID data?

Wallet Decisions

Are you fostering competition in Wallets or holding 1:1 Issuer:Wallet?

Do you support multiple PID/mDL? If so, from the same PKI Hierarchy?

Do you require different credential protection or higher user authentication in **your** ecosystem?

Do you have public mechanisms for Trust Marks or live badges & seals?

SIDIHub