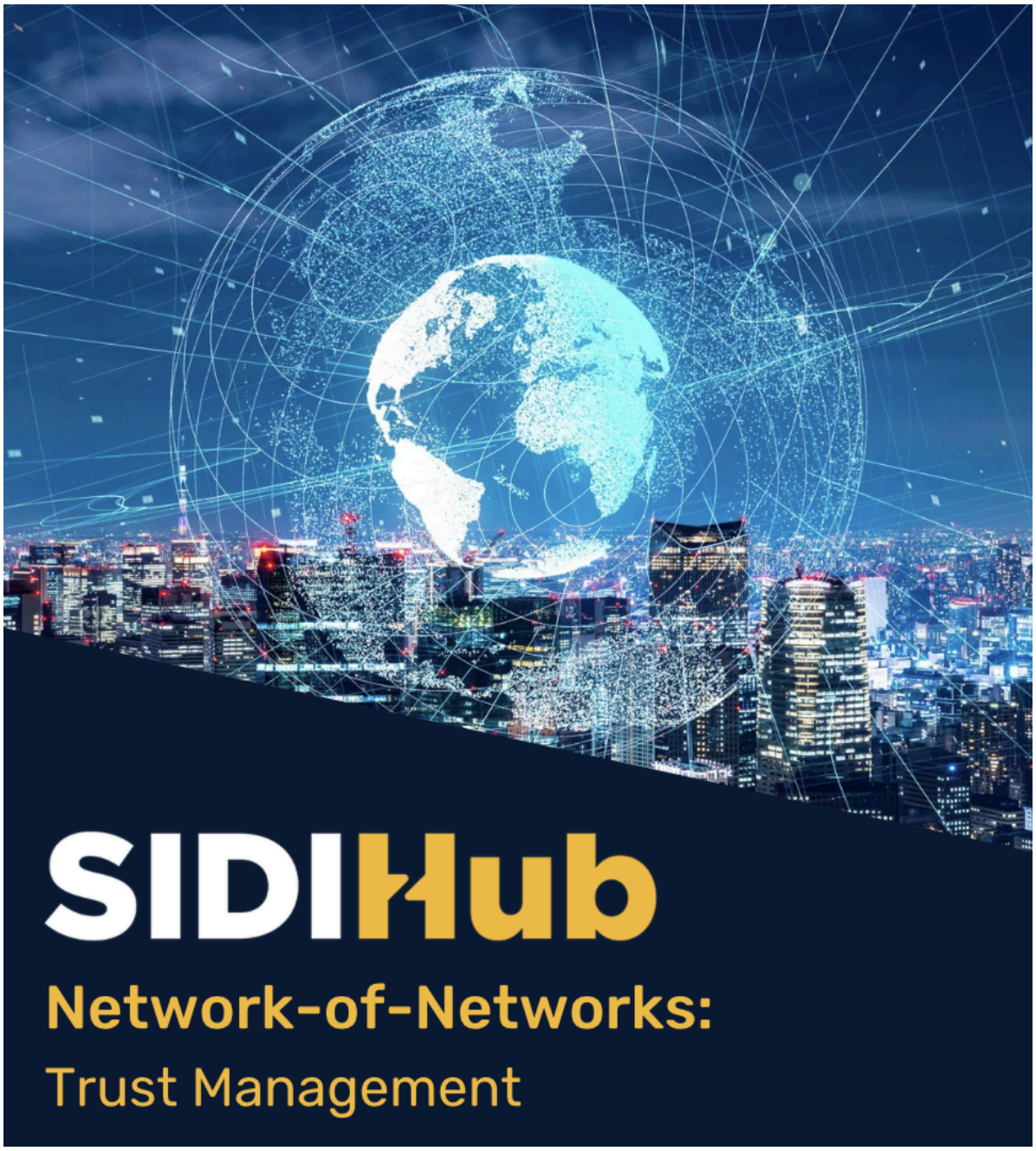
The document, "Trust Management: Defining the Challenge for Ecosystem Builders," is a conceptual analysis for ecosystem builders, policy-makers, and standards contributors focused on digital identity ecosystems, particularly those involving wallets and logins. It posits that trust is aligned across 6 Trust Vectors that must be analyzed to produce good ecosystem policy. Registrars operating Conventions that mediate membership in Trust Mechanisms give Ecosystem or Network Builders the ability to customize ecosystems, mitigate risk for trusted participation, and protect End-Users.



1: Defining the Challenge for Ecosystem Builders

Key Concepts: Managing Ecosystem Trust

- **Trust Management:** Defined as the rules, guidelines, conventions, and mechanisms that allow participants to determine if others have met their obligations and mitigated risk.
- **Trust:** Expressed as assurances that mitigate risk among participants in identity transactions.
- **Ecosystem Roles:** Defines key roles like **Issuers**, **Users**, **Verifiers** (using a **Reader**), **Wallet Providers** (publishing Apps), **Registrars** / Trust List Providers, and the **Ecosystem Builder**.
- **Structure:** It proposes understanding Trust Management through **Trust Vectors**, **Mechanisms**, and **Conventions** to inform ecosystem design and operation with or without governance.
  - **Trust Vectors:** The six critical trust relationships in wallet-based architectures that must be managed, such as **Issuer Trusts Wallet**, **User Trusts Verifier**, and **Reader Trusts Issuer**.
  - **Mechanisms:** Methods for inspecting participant conformity (e.g., ICAO Public Key Directory, Trust Lists, Wallet Attestations).
  - **Conventions:** Policies and guidelines that customize and govern the usage and meaning of the Mechanisms (e.g., how to join a Trust List) to Ecosystem participants.
- **Conclusion:** The document stresses the importance of an **Ecosystem Builder** establishing clear **Conventions** for utilizing mechanisms to reduce complexity, facilitate user choice, and operate transparently. Conventions overcome shortcomings like reliance on reputational trust, unclear system operations, and subversive actors.
- The document overlays Login and Wallet Ecosystems effectively, noting that while Trust Vectors and Conventions remain similar, Mechanisms may differ. Agentic systems likely also overlay.

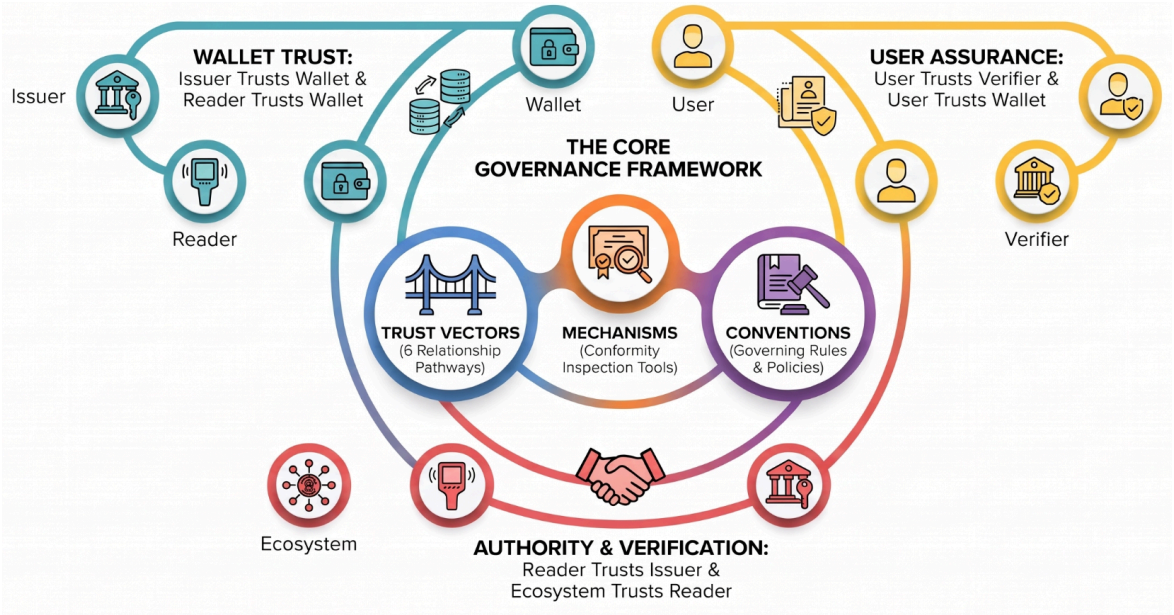


Fig 1: *Promoting transparent operation across 6 Trust Vectors mitigates risk and builds trust*

SIDIHub © 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Table of Contents

Trust = Assurances that Mitigate Risk **4**
Trust Management 4
Categories of the Mechanisms of Trust Management 5
Wallet Ecosystems **6**
Definitions 6
Adding User Authentication 7
Trust Vectors 7
Current Observed Patterns on Trust Vectors 9
Single-Provider Trust 9
Multiple Bi-lateral Contracts 9
Federation of Issuers or IDPs 9
Regulated Participation 10
Shortcomings in Observed Patterns 10
Lack of User Choice 10
Reputational or Implicit Trust Assumptions 10
Insecure Receipt Storage & Potential For User Profiling 11
Insufficient Risk Mitigation for Relying Parties 11
Trust Mechanisms **11**
Issuer List Provider 12
Reader List Provider 13
Wallet Attestation (List) Provider 13
Federation Login Ecosystems **14**
1:1 Pairing, RP Operates OpenID Provider 14
Two Additional Identity Provider Pairings 15
Overlaying Login & Wallet Ecosystems **16**
Issuer as Login Provider with Wallet(s) 16
Trust Vectors Don’t Change 18
Trust Mechanisms Still Apply 18
Conventions May Become More Complex 19
Applying Conventions Across Mechanisms **19**
Developing Conventions 19
Registrars Encourage Conventions 20
Document Map & Next Steps **20**
Credits **22**
Appendix: Trust Management Process **23**

SIDIHub © 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Trust Management: The Challenge

Defining the governance challenge for Ecosystem Builders. What **mechanisms** and **conventions** do policy makers need to shape an ecosystem, orchestrate trust between ecosystem participants, and convey that meaning globally?

*This document is a conceptual analysis intended for **Ecosystem Builders**, policy-makers, and standards contributors working on wallet or login **Digital ID Ecosystems**. It proposes a structured way to understand Trust Management through Trust Vectors, Mechanisms, and Conventions. Defining the Challenge with common terminology helps accomplish goals.*

This series of documents has the goal of informing ecosystem design, governance models, and future standardization efforts rather than prescribing any architecture or technology.

Trust = Assurances that Mitigate Risk

Each participant in identity transactions carries some risk. An **Ecosystem** helps because participants provide assurances that mitigate each other's transaction risk. **Trust** is the term used to express that ecosystem participants are sufficiently meeting their obligations to provide these assurances and fulfill their roles according to the Ecosystem Operator's expectations expressed in a **Trust Framework**[1]. Each transaction may carry variable risk for the participants and require more or further assurances at transaction time. This document helps the Ecosystem Builder assemble requirements that frame trusted participation.

Trust Management

Trust Management consists of the rules, guidelines, conventions, and mechanisms that allow any participant to discover in advance or determine in real time that another participant they interact with has met ecosystem obligations and, therefore, mitigates their risk. **Rules** are enforceable **Guidelines** that determine how each participant should fulfill their trust obligations for their role.

Trust Evaluation Mechanisms (called Mechanisms herein) are methods, often standardized, for inspecting that a participant is a verifiable member of the Ecosystem fulfilling their obligations - they are in conformity. The ICAO Public Key Directory (PKD) for passports is an example of a mechanism for obtaining materials to verify trust in a passport being read.

[1] https://sidi-hub.community/publication/governing-global-credential-ecosystems/

SIDIHub © 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Trust Evaluation Conventions (Conventions) may customize or configure the Trust Evaluation Mechanisms for usage within 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 for others in the Ecosystem. The policies for how to join the ICAO PKD and obtain approval as a country to upload certificates to the PKD are some of the Conventions surrounding the Mechanism and implementation.

Throughout this document, examples such as Trust Lists, Wallet Attestations, and federation discovery endpoints are discussed as Mechanisms, while the policies governing participation, approval, configuration, and usage of those Mechanisms are treated as Conventions.

Categories of the Mechanisms of Trust Management

- Centralized Authority (one trust anchor - a CA granting certificates)
- Hierarchical CA (common trust anchor, deputy authorities granting certificates)
- Federated (multiple trust anchors recognized by the Trust Model[2] or underlying framework; same or similar agreements amongst trust anchors)
    - Federation Trust List as mechanism for dispensing trust anchors for inspection
    - There may also be a mechanism for querying any participant about conformance
- Decentralized Trust Anchors
    - Utilizing technologies that allow multiple entities in cooperation to retain their sovereignty over trust anchors and specify their trust elements in a common place
    - Possibly Smart Contracts as discoverable, individual policy
    - Interoperability either mapped or coordinated by Trust Framework
- Organic or Free Market (lack of conventions or mechanisms which can create reliance on reputational trust only… until participants solve trust problems per their own motivation)
    - Reputational or sector-specific registries (of the above 4 types) are likely to emerge

The mechanisms in these categories are being defined in standardized ways within multiple communities and our next steps will gather information and evaluate available mechanisms. **Ecosystem Builders** must establish Conventions in their Ecosystem for inclusion in the chosen mechanisms in order to bring their values and operational model into being.

[2] https://openid.net/specs/openid-federation-wallet-1_0.html#section-3.1 as an example

SIDIHub © 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Wallet Ecosystems

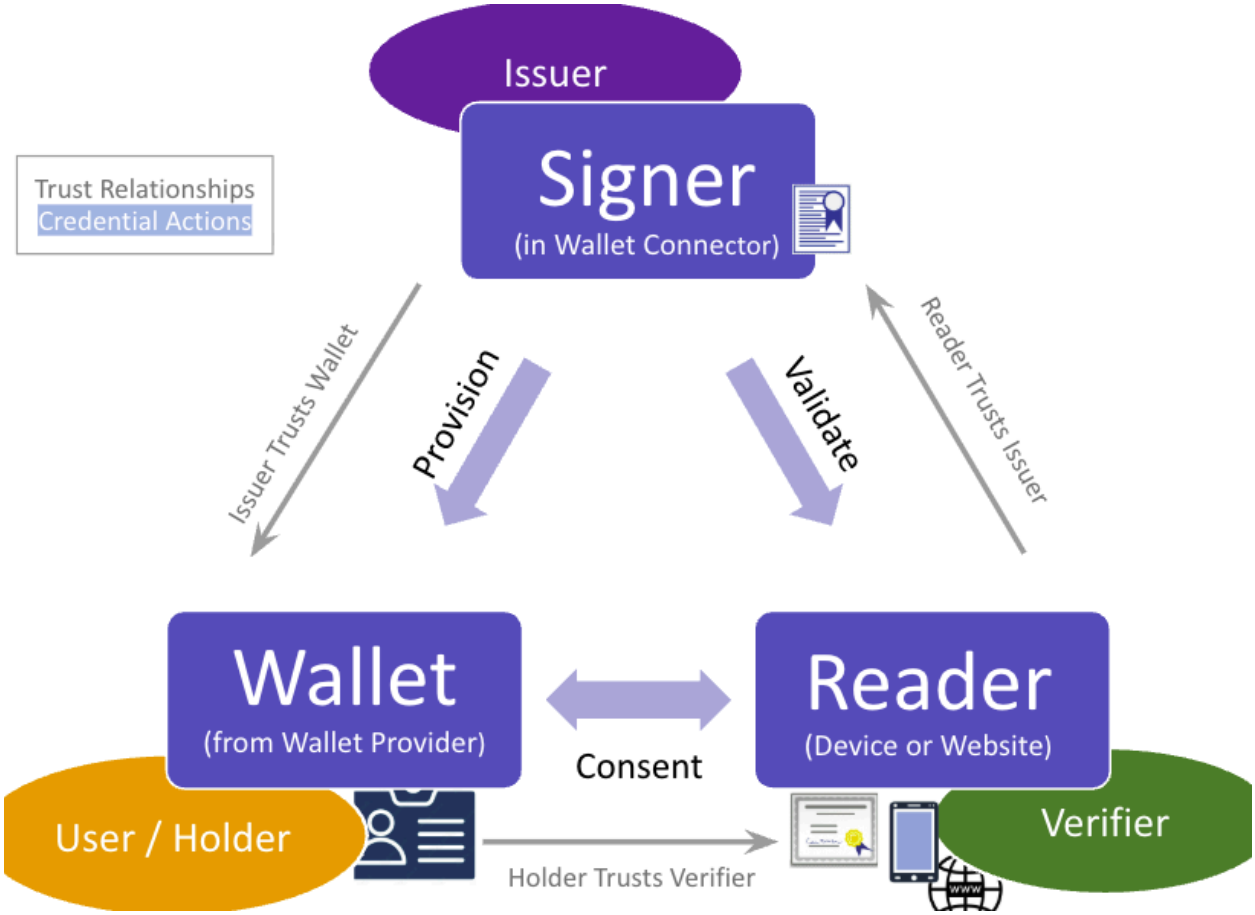


Fig 2: *Trust Relationships needed for Credential Actions in current 3-Party Wallet Ecosystems*

Definitions[3]

Issuers endorse Digital ID **Credentials** on behalf of **Users** (aka residents or citizens) as a verifiable representation of an accurate point-in-time collection of attributes about the User's identity. Endorsement is typically by cryptographic digital signature that indicates the accuracy and provenance of the attributes at the time of **Provisioning**. **Issuers** use a **Wallet Connector** to offer digitally signed (endorsed) **Credentials** to a **User** and they must trust the Wallet before Provisioning.

The **User** can store these **Credentials** in cloud or mobile **Wallets** operated by a **Wallet Provider**.

A **Verifier**[4] is an entity seeking to read and validate **Credentials** received from the **User**'s **Wallet** using a **Reader** during a transaction. Readers can be physical, an application, or a web service. The End User must trust the Verifier and be informed about the transaction to be comfortable giving

[3] Note that this paper uses a similar but simplified terminology from ISO/IEC mDL standards also used in https://openid.net/specs/openid-federation-wallet-1_0.html#section-3.1
[4] Also Credential Verifier https://openid.net/specs/openid-federation-wallet-1_0.html#section-3.1

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Consent. The Reader must trust a public key from the Issuer in order to validate the Credential data.

Issuers, **Verifiers** and **Wallet Providers** each operate within the rules of an **Ecosystem**. **Trust List Providers** help distribute certificates for good actors that conform to ecosystem rules. An **Ecosystem Builder** is a decision-making entity for policies and may authorize Trust List Providers.

Adding User Authentication

Users must authenticate to the Wallet app before sharing credentials, which gives the Verifier some confidence that the Credential presenter is the proper Holder. In many current transactions, the Holder shares a portrait to the Reader that the Verifier can then visually inspect.

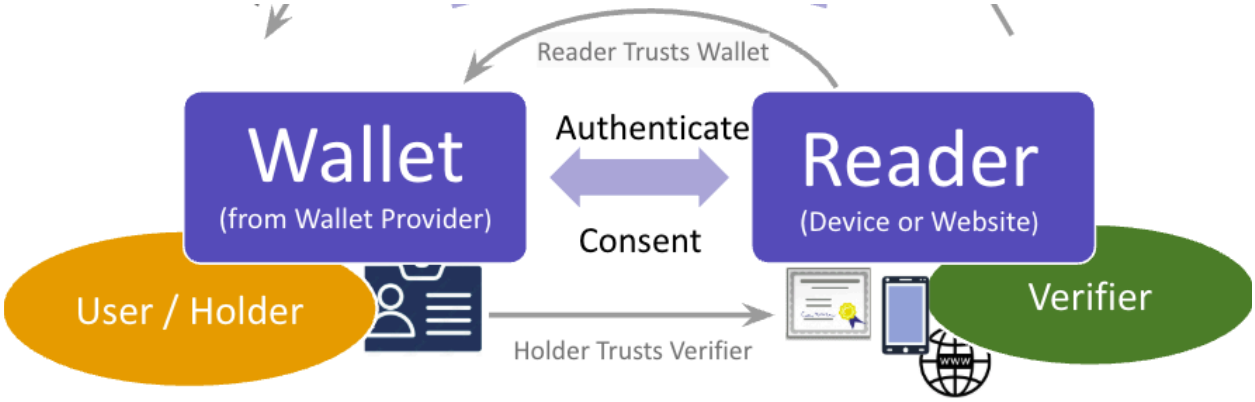


Fig 3: Adding the Trust Vector that will permit User Authentication by the Wallet app/service

When Users are provided the standardized ability to authenticate to their Wallet and provide the results of User Authentication to the Reader, a new trust relationship appears. The Reader must trust the Wallet software to trust the result of the User Authentication (sometimes called Holder binding).

For higher risk use cases, user authentication may need to be tied to an identity proofing level[5] that is represented by a particular Digital ID document in the Wallet. In this case, the result of the user authentication may need to bind the holder to a particular document in order to generate sufficient trust. For example, granting access to visit a Federal Building in the USA will require the REAL ID flag, which is a representation of a US NIST Identity Assurance Level **and** a verification of legal presence in the USA. The Relying Party granting access must confirm the user is bound to the proofing process which is inherent in only **one** Digital ID document in a Wallet full of documents.

This may require User Authentication trust to be bound directly to the document Issuer and merely performed by a Wallet that attests to conformity to the Issuer in advance so that the Issuer signs the Wallet/Device public key to include in their endorsed Digital ID document.

Trust Vectors

How can the verifier be assured that the Issuer is in fact the entity that officially endorses and is the authoritative entity to provision that credential? How can partners in a digital interaction be certain

[5] https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html Open ID Connect For Identity Assurance permits this connection of User Authentication to prior proofing as required by https://csrc.nist.gov/pubs/sp/1800/42/ipd for Financial Account Opening use cases. This may be resolved with https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0-05.html.

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

that a public key really belongs to the claimed entity? What protections are afforded the User as they present identity credentials across one or more ecosystems? How do Users establish some assurance about Verifiers and Readers they interact with? How do Verifiers and Issuers trust Wallets?

Below is the complete view of Trust Vectors associated with trust management for wallet-based architectures.

Assumptions:

- Issuer determines the lifecycle of credentials - endorsement, attached privileges,and revocation. These should be managed over time through standardized interfaces.
- The **Ecosystem Builder** sets policy across all of the Trust Vectors within their Ecosystem. Those policies, rules, conventions, and mechanisms may vary across different ecosystems.
- It is beneficial to have legislation behind policy and to have policy fit within local law. The set of policies in this context is often called a Trust Framework.
- It is beneficial to have an **Ecosystem Operator** who enforces the policy. This is done by managing conventions for participants to take part in Trust Mechanisms.

Vectors:

1. **Issuer Trusts Wallet**. The **Issuer** must trust the security and credential protection of a **Wallet** in order to approve provisioning credentials for its Users into that Wallet. The Issuer may also need to trust that the Wallet will appropriately authenticate the User during credential presentation. See also #6 User Trusts Wallet.
2. **Reader Trusts Wallet**. The **Reader** device used by the **Verifier** must trust assertions from the **Wallet** in order to establish that credential protection and **User** Authentication were adequately performed. This mitigates the Verifier's risk in the transaction.
3. **User Trusts Verifier**. To establish informed consent and approve the sharing of identity attributes, the **User** (of a **Wallet**) must trust the **Verifier** operating the **Reader**[6]. For instance, the **User** should know with some level of certainty that they are interacting with a known Reader in that context (e.g., the Reader at the automated checkout counter is operated by the **Verifier** store and is not a rogue **Reader**).
4. **Reader Trusts Issuer**. Upon receipt of a credential, the Verifier must ensure that the Reader validates the credential using the procedures established by the Issuer.
5. **Ecosystem Trusts Reader (Reader can Identify Itself).** The Reader can properly identify itself to Users as part of a request for attributes (extending Vector 3 to the Reader). In some instances, the Verifier has registered a Reader with a Registrar within an Ecosystem. In further instances an Ecosystem or Issuer **authorizes a Reader** to request scopes (data sets) and the Wallet could enforce those scopes on behalf of the User (these are called **Verifier Attribute Policies).**
6. **User Trusts Wallet.** The biggest hesitation of End Users to become Wallet Holders is whether the Wallet will profile them, share or leak their transaction receipts, report to government authorities, or monetize their ID and transaction data. Companies

[6] Some definitions refer to a Reader as a Verifier Instance or Relying Party Instance https://italia.github.io/eid-wallet-it-docs/versione-corrente/en/defined-terms.html#defined-terms-and-acronyms . Here we use Reader that is consistent with ISO/IEC 18013 terminology

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

involved in surveillance capitalism on the Internet will enter the Wallet space. Similarly, Wallets must not report transactions to the Issuer in order to keep User trust.

There are mechanisms in many standards for signing a request or providing an attestation during engagement of the standard communication so that two entities can trust each other. We're not talking about communication security here, although that also is established. This is how a component establishes and then trusts the identity and heritage of another component with which it communicates. The receiving component checks a cryptographic signature.

Current Observed Patterns on Trust Vectors

Single-Provider Trust

Many times in current ecosystems, such as Mobile Driver's Licenses in the United States, some of these Trust Vectors become trusted by default[7] because the same entity (often the Issuer) is publishing Wallet apps that connect to a Wallet Connector for provisioning and even publishing Readers that accept and verify credentials. While the reputation (commercial) or provenance (government) of the provider can engender trust, transitive trust isn't necessarily interoperable and can even lead to the appearance of, or fear of, collusion between components. This is resolved through mixed, user-chosen components necessitating the models below.

Multiple Bi-lateral Contracts

Some bilateral agreements are also made out-of-band for Wallet providers (often OS Platform Wallets) to accept credentials from Wallet Connectors when they meet Issuer requirements ahead of time and interactively to assure the Holder is the correct credential recipient. In the US mDL Ecosystem, as an example, for the Transportation Security Administration (TSA) to accept credentials from Wallets, they must establish a bilateral agreement with the Wallet-WalletConnector-Issuer combination.

Federation of Issuers or IDPs

Federations separate participants into roles and provide singular agreements, enforceable by the Federation, for each role. This reduces the complexity of relationships considerably and the preponderance of multiple, bi-lateral agreements between many Ecosystem players. You can see that Federations, typical in the login identity space, can extend to the wallet space by adding additional or modifying existing roles. The map of Trust Vectors does not change.

[7] You discover the other components manually and "trust" them because they are published by one Entity. When this happens on the Internet, "m1crosoft.com" becomes a method to trick users.

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Regulated Participation

Permissioned participation routes approval and compliance through a single entity or a set of deputized entities. This may be considered **Single Provider Trust**. Sometimes permission comes through government entities in Regulated Ecosystems (see Governance Models in Document #2 in our Document Map & Next Steps).

Shortcomings in Observed Patterns

Any of the possible shortcomings below could be addressed by Conventions and promotion or enforcement of Conventions by Registrars. This is covered below and in this series.

Lack of User Choice

User choice of components is *essential* for privacy, and allows for optimal technical flexibility and innovation because it promotes competition. Mechanisms and Conventions allow this . Mechanisms allow discoverability of the components and systems that are under agreement and in conformance with Ecosystem rules. Conventions for how a participant gets approved to be included in the Mechanisms set the levels of trustworthiness and risk mitigation.

From an adoption point of view, End Users typically do not enjoy having choices made for them by government providers and trust is lower without choice. Trust deters adoption.

Reputational or Implicit Trust Assumptions

Trust Marks come from cooperation between Ecosystem Builders and Relying Party Associations. Trust Marks indicate conformance to rules in a way that reputation and marketing do not. The lack of Trust Marks defaults people and businesses to reputational, implicit, or fear-based decisions on software and equipment they choose.

When there is no certification or trust marks to indicate conformance of commercial Readers (see Trust Marks and Registries discussed in our next paper) it is more difficult to get past assumptions that limit trust in the ecosystem. Ecosystem Builders overcome this.

While many End Users will choose based on the reputation of brand name Wallet apps, choice allows End Users to participate built on something more than reputation. This is also true when a State-published app is available. Some End Users will not trust State-issued Apps, some will want them. The same is true for Verifiers, actually. Some will choose State-issued or brand-name Readers and others will search for certifications. Trust is transparency. Transparency is not implicit. Certification schemes have meaning.

Implicit assumptions happen in closed ecosystems, such as Verifiers choosing Readers only from their Issuer or from Wallet Providers because of brand. This can function but it sacrifices diversity, and might inadvertently enable monopolistic or exclusionary behaviors. Ecosystem Builders have influence over the behavior in their ecosystem.

SIDIHub © 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Insecure Receipt Storage & Potential For User Profiling

Privacy-preserving, user-controlled secure receipt storage will be a selling point in the Wallet wars, but it has not become portable and standardized as a service even with the existence of Kantara/ISO standard consent receipts[8]. Users are not yet pointing apps to where they want to store receipts nor shielding apps from using AI and algorithms to profile their usage. Therefore, Ecosystem Builders should provide requirements against profiling users and for the security, portability, and unidirectionality of receipt storage as standards develop. Leaving it to the benevolence of cloud or device Wallet Providers may incite the protocol-level user profiling of the Internet and exacerbate user fears.

Insufficient Risk Mitigation for Relying Parties

Having certified Readers and knowing where to obtain Public Key Certificates for the Issuers whose Digital IDs are acceptable for a Verifier's policy or legal compliance are not enough to say that you trust Digital IDs and they meet your transaction risk levels.

Stated another way, establishing technical trust that Digital ID systems will work is not the same as staking the livelihood and legal compliance of a business on the decision to accept Digital IDs, even when workflow improvements are obvious. What will bring Verifiers over the hump and ensure that their risk is sufficiently mitigated in both the old physical-world and new Digital ID at the same time? Insurance, certifications, group approvals through the associations in which they are members, and explicit policy or legal instructions help. Clear guidance and Conventions from Trust Management is necessary.

Trust Mechanisms

Given the complexity of Ecosystems, border-crossing, and global business operation, there must be mechanisms to distribute public keys and certificates to participants who approve transactions. **Trust Mechanisms** should have controls placed on them as to how public keys can be included in the mechanism or how identifying certificates are obtained from it. This gives *meaning* to the mechanism. The Mechanism attests to the behavior of its members.

Issuer Lists also indicate the types of credentials that the Issuers in the Trust List are authorized to provision. Issuers in the Trust List have met the requirements set forth by the Trust List Provider (or the Ecosystem / Federation). List Providers may collaborate with other list providers to form a Federation that encompasses similar credentials.

As mentioned above, a List Provider can establish Conventions by policy or law that define these controls and determine how participants become members of their Trust List. The Trust List also expresses what it means to be a member of the list so that all participants

[8] https://www.iso.org/standard/80392.html, https://kantarainitiative.org/work-groups/ancr/, and https://kantarainitiative.org/download/consent-receipt-specification/

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

can trust it. Consuming a Trust List reduces independent individual trust relationships because the conventions were formed for the group of member-participants.

The Trust List itself becomes a form of trust anchor. The Verifier needs to have only one relationship that it trusts - with the Reader List Provider. Knowing that the Provider operates in a manner consistent to mitigate their risk is a partial solution. On top of that, the Provider may institute policy about what IDs are acceptable, how to behave, how to handle and treat Holder attributes, etc. These policies may fit with their role as a Network Operator[9].

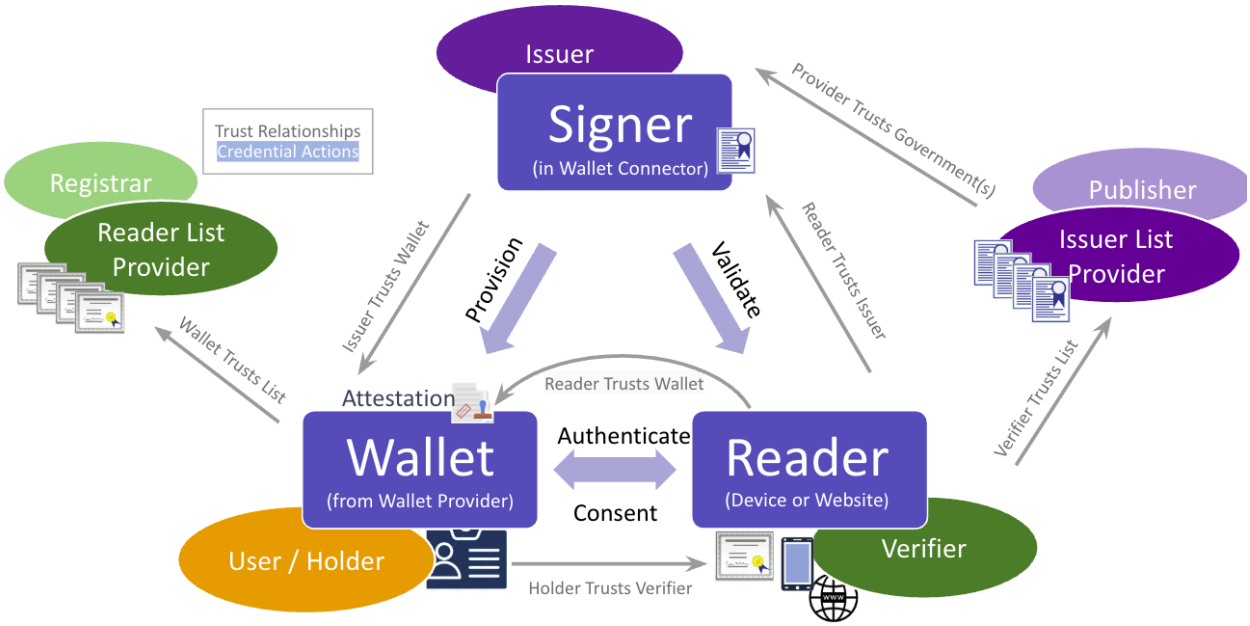


Fig 4: Wallet Ecosystem with Trust Vectors and Mechanisms for conveying trust

Issuer List Provider

This is perhaps the most well-known “list” mechanism currently. The Reader must check the cryptographic signature on credential data in order to verify it. Many Readers pull public keys from an Issuer List Provider to perform that verification.

Some Readers have an embedded list or pull an updated list in real time from their services software, In this case the Trust List Publisher is the same entity as the Reader publisher. However, Issuer List Providers are cropping up around the world to publish lists of public keys for Verifiers (a/k/a Relying Parties) to approve and load into their Reader devices.

Multiple Issuer List Providers are expected. For instance, AAMVA in the US, AustRoads in Australia, and eReg in Europe are expected to publish a list of public keys for their Issuers. For businesses with global reach, they may need to set conventions to harmonize lists from

[9] Document #2 in Document Map & Next Steps, “Trust Governance”

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

multiple Issuer List Providers according to their policy and trust requirements. Similarly, Ecosystem Builders may approve Issuer Trust Lists from multiple other Ecosystems.

Many other Mechanisms are applicable to groups of public keys: PKD Directories, Distributed Ledger, DID-Key Mechanisms, etc.

Reader List Provider

For the Wallet to provide confirmation and information to the User that shows the Reader belongs to the Verifier (is not a rogue) and is operated according to Verifier and Ecosystem policy, it must introspect certificates or cryptographic signatures received from the Reader before or during credential requests. Preformulated, bilateral agreements can apply here when the Wallet is expected to reply only to one or more known readers. But in open ecosystems such as our Digital ID ecosystems today where visual user authentication is performed by a Verifier who receives the document, more flexibility is required.

Ecosystem Builders can decide to become, or can appoint, **Registrars** who inspect the characteristics of the Verifier (business, agency, individual) in order to include them in a **Reader List**. Doing so turns the role into that of an **Ecosystem Operator** because it adds enforcement and operational duties. In Organic Governance, Registrars may enforce.

Wallet Attestation (List) Provider

A Wallet[10] should be able to provide a **Wallet Attestation**[11] to a Reader that identifies its specific instance (without identifying information) and information about how it was functions, who built it, who authorized it, and what operations it can perform. This can be essential for the Reader to trust any dynamic, transaction time information from the Wallet such as User Authentication. For user authentication after the Wallet Attestation is presented, the Wallet would match the live holder to the credential and express the result to the Reader for it to evaluate.

Note: Implementations in the EU and USA *as of 2025* do *not* send Wallet Attestations to Readers - they make an assumption about how User Authentication[12] is performed.

---

[10] The European Wallet implementing acts define this as a Wallet Unit running for one end user https://eudi.dev/latest/annexes/annex-1/annex-1-definitions/ to distinguish it from the app in the stores.
[11] Defined, therefore, in EUDIWallet implementing acts as a Wallet Unit Attestation (see link above).
[12] Unfortunately, those assumptions may not be interoperable - Europe assumes" eIDAS Substantial before release of credential information, USA includes the portrait image for the Verifier to visually match

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Similarly, the Wallet can[13] provide a **Wallet Attestation** to the Wallet Connector of an Issuer to allow it to verify that the Wallet meets its requirements to provision a credential. This is separate from the process that confirms the identity of the Holder to be the rightful owner of the credential. That process often follows the inspection of the Wallet Attestation. Conceptually this is very similar to above. In order for the Wallet Connector to trust dynamic, registration time information from the Wallet, it must trust the attestation that the software process meets its requirements and that of the ecosystem.

Wallet Attestations are currently being defined[14] [15] [16], and Lists mechanisms could be utilized similarly to Reader and Issuer Lists in order to allow groupings of Wallets

Federation Login Ecosystems

Utilizing similar terminology to above, Verifiers will often allow online login for access to services on their Website through an external Identity Provider (IDP). In this document, we'll discuss only OpenID Provider (OP) functioning in this IDP capacity. **The Trust Vectors are similar to that of a Wallet Ecosystem.**

The Verifier typically chooses the OP ahead of time, either through a 1:1 tight coupling or by selecting a well-known, reputable identity provider that matches their requirements. The Verifier's Website obtains certificate and trust information from the OP by querying Well-Known endpoints of the OP defined in the OpenID Connect standards. These endpoint mechanisms are called **OpenID Provider Discovery Endpoints** when they are used by groups of Websites across the same OP within an Ecosystem. The Ecosystem Builder or Operator sets the rules, conventions, and policy that overlay meaning onto the certificates and information that Verifiers can gather from the mechanisms. There are also **OpenID Federation**[17] endpoints with list-like mechanisms.

1:1 Pairing, RP Operates OpenID Provider

The User's Browser and a Website perform a certificate exchange to establish a trust relationship that the website being visited is that of the registered Verifier, and a lock icon is displayed in the browser bar when the User can trust secure communications to the website. TLS lock icons are an important mechanism to remember for their potential

---

[13] In the EUDIWallet context, the Wallet *must* provide the Wallet Attestation to the Wallet Connector https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/discussion-topics/c-wallet-unit-attestation.md

[14] https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/blob/main/docs/technical-specifications/ts1-eudi-wallet-trust-mark.md

[15] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/discussion-topics/c-wallet-unit-attestation.md

[16] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74932

[17] https://openid.net/specs/openid-federation-1_0.html

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

application in Wallet Ecosystems. However, the UX must display similar trust marks in more meaningful and obvious ways in our Digital ID ecosystems if not enforce safety.

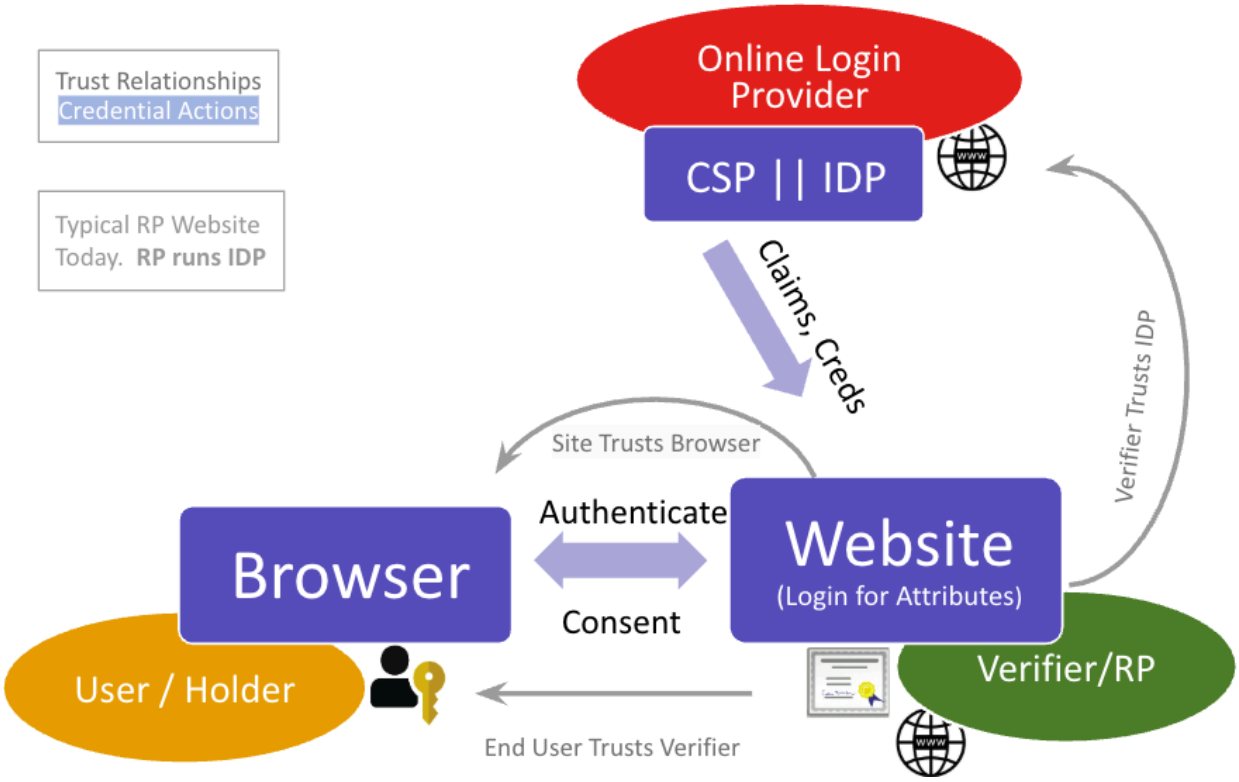


Fig 5: *Relying Party / Verifier operated or trusted Identity Provider*

At transaction time, the Website trusts the Browser to act as the User's agent and collect Passkeys (credentials) that will unlock the User's account at the Website. When attribute information is required about the User, the Website can query token and user information endpoints of the OP that trigger user consent gathering, and then validate the information received using channel authentication or cryptographic validation if the data is signed.

You'll see that conceptually these are very similar to Wallet Ecosystems but operate in different contexts. Information about the User comes from the OP in credential form instead of directly from the User in credential form so the cryptographic signature validation has a different path.

Two Additional Identity Provider Pairings

As ecosystems evolve, Issuers (sometimes Governmental Issuers) are deploying Open ID Identity Providers (OPs, that may or may not also be a SAML IDP[18]). These OPs can have the advantage of being an implementation of the Rules and Guidelines for a National Ecosystem with simpler legal agreements because all member identities and all registered

[18] Often in IETF, these may be called AS Authorization Servers and may not represent identities.

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Verifiers follow guidelines. They also can be authoritative sources for attributes given regional Identity Proofing.

Wallet Providers are also deploying OPs.These could be deployed as login across related online services based on the reputation of the Wallet Provider, or they may be deployed for the purposes of issuing credentials using Open ID for Verifiable Credential Issuance. These can have the advantage of being a one-stop shop for Verifier / Relying Parties.

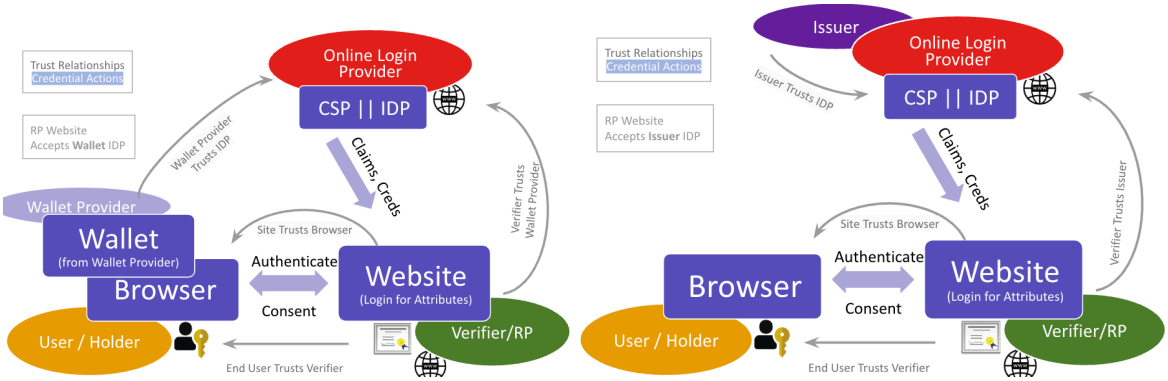


Fig 6 & 7: *Consider the meaning of Trust behind two OP deployments: Wallet or Issuer*

These three OP deployment pairings: Verifier/RP, Wallet, and Issuer (including Governmental Issuers) will co-exist. The meaning behind accepting identity credential actions or data from any one of them is different. The policy and guidelines they follow during operation also differ as does their ability to make enforceable rules out of them in conformance with law and the expectation of their users. When you query the Federation endpoint mechanism, what conventions were followed that are providing you your result?

Overlaying Login & Wallet Ecosystems

Issuer as Login Provider with Wallet(s)

When you overlay a Government login provider (in OpenID Connect terminology this is often called an “OP” - OpenID Provider) with a Government Digital ID document Issuer, you gain additional synergies. If coordinated, it can open service delivery across channels WHILE improving the User’s privacy in their personal business interactions. The login credentials and wallet credentials can operate across different mechanisms to provide strong user authentication as well as proven and accurate attributes. Those different mechanisms fit different use cases. The person is the same across contexts. This is what businesses and service provider agencies want. Combined ecosystems are positive.

Using the OP to login to the Wallet application(s) is possible and a preferred first step toward authenticating a new user of a wallet application or before obtaining a new

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

credential. The login and KYC/onboarding services can operate in synchronization with each other to serve Users and different issuers. Then at transaction time, these mechanisms also serve to lower the risk level of Verifiers when communicated.

This combination of a Federation Login Ecosystem **with** a Wallet Ecosystem is just being deployed and is a promising setup for consistent and equivalent distribution of attribute claims to Verifiers across web and in-person reader contexts. Claims provided to website Relying Parties are provided by the OP in the form of signed JWTs after a login and consent event or directly from the user wallet in mdoc form after consented ISO/IEC 18013-7 device engagement. After an initial in-person token exchange using ISO/IEC 18013-5, claims to in-person Verifiers can be delivered through the same mechanisms.

The Trust Vectors are identical in this “Federation+Wallet Hybrid” but the ability for the Ecosystem Builder to flexibly handle all potential use cases improves.

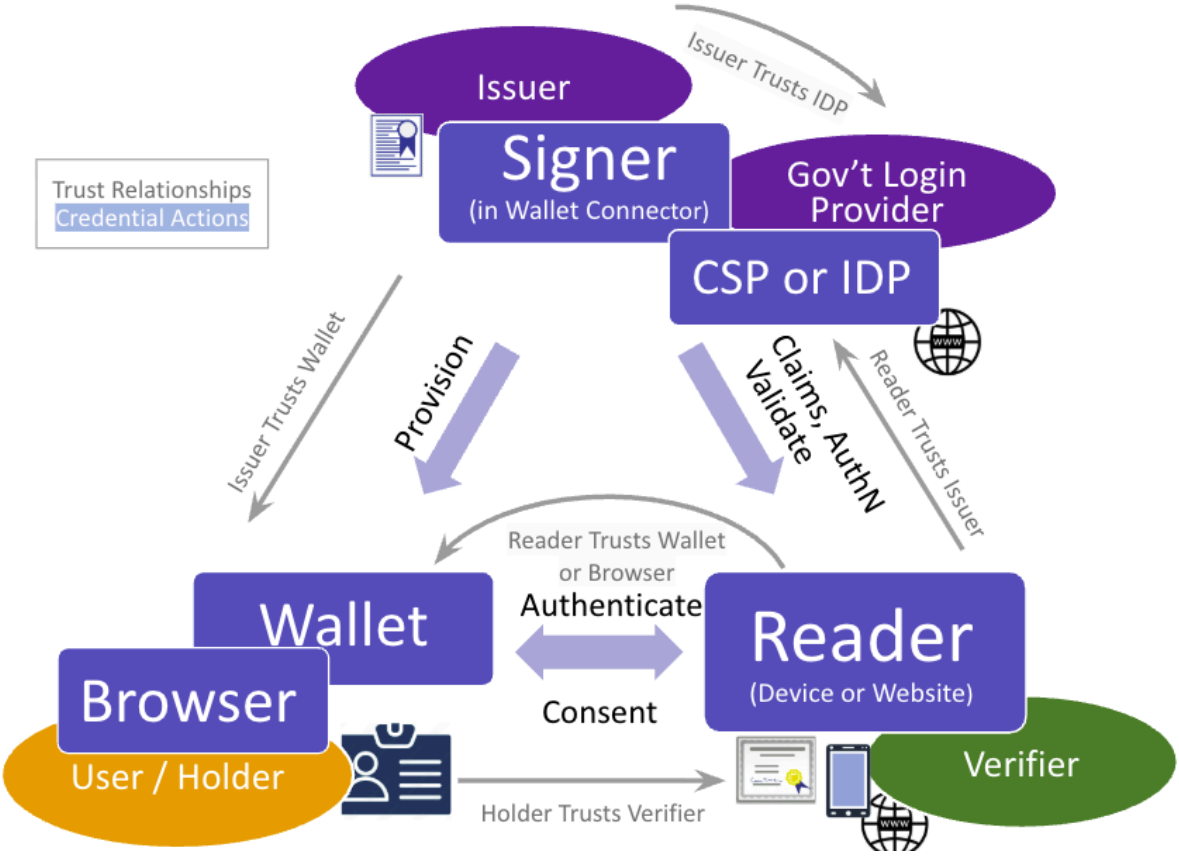


Fig 8: *Overlaying a Wallet Ecosystem with a Login Ecosystem doesn’t change the Vectors or Mechanisms but it does increase the number of components to support interactions.*

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Trust Vectors Don’t Change

You can see that the Trust Vectors do not change when you overlay Digital ID documents and Login. The parties and components still interact and the participants' trust considerations vary only by the context of the interaction (e.g., in-person versus unattended over-the-internet) and perhaps by the provider of components (government or private).

In the Verifier to Issuer channel, the claims delivery, data authentication, and credential validation actions perform the same even if implemented via login or wallet sharing. Therefore, it is interesting to note that the 18013–5:OIDC flow takes a token from the Wallet and allows the Reader to spend the token calling Authorize at the OP to authenticate the user and release signed claims—this is the standard OIDC Core[19] flow. Combined wallet and login systems can combine signed-data delivery mechanisms for different interactions.

The types of Verifiers may change, however, in overlaid login and wallet ecosystems. Acceptance of a login credential is most likely when the Verifier is a government agency or associated entity (the Verifier could be purple in Fig 8). Logically, one might expect a commercial Verifier not to accept a Government Login OP but to prefer their own or a commercial login service. In those situations, expect the Verifier to request a government-signed wallet credential to support regulated or high assurance use cases after their customer is already logged in using their chosen OP.

Conversely, despite the assurance of complete data anonymity when no claims are requested or only AgeOver is requested, one may not expect an End User to use their Government OP to log in to a business. The user perception of privacy, even amidst exquisite technical controls, is the subject of our #2 in Document Map & Next Steps.

The exceptions are well-known regulated transactions that require Government ID like alcohol purchase, online age verification, etc. From a consumer comfort level, most of these are better left to commercial OP implementations… or authorized aggregators such as deputized in the UK as DVS - Digital Verification Services[20].

Another Trust Vector to analyze is the parallel between the Wallet Attestation and the Mechanism in use for TLS certificate introspection when creating secure connections from browsers to RP web sites. The parallel to the security of the connection and to the operational trust of the wallet/app/browser on behalf of the Reader/Website are similar. Further, the Convention for obtaining identifying certificates for websites to present to Users makes operational business sense

Trust Mechanisms Still Apply

[19] https://openid.net/specs/openid-connect-core-1_0.html
[20] https://www.gov.uk/government/collections/uk-digital-verification-services-trust-framework

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

It is logical, since Verifiers want to service the same customer across all service delivery channels, that Wallet and Login Ecosystems can share Trust Mechanisms.

Logistically, even as the reasons become less and the liability becomes more, many Verifiers still may want to operate their own login service (OP or IDP). They have invested in maintenance and operation, and retiring it despite advantages may take time. Similarly, social logins, professional logins, and financial logins each represent different facets of the end user, who may want to keep these facets logistically separate from each other. The End User may not use their social login to obtain government services nor their government provided login for commerce. That choice does not change the Trust Vectors or the effectiveness of Trust Mechanisms, however. It increases the componentry subject to trust.

Each List Provider that operates a Trust Mechanism must take into account that their dependents may come from a larger and different pool than suspected. That is fine.

Conventions May Become More Complex

Now, however, there are similar Mechanisms for distributing trust and public key material that must be implemented in parallel so that each ecosystem—wallet and login—can function independently. Could they be utilized across the ecosystems? Could a Reader of a wallet credential obtain the Issuer List from the Login OP well-known endpoints? Or that endpoint redirects the Reader to the Ecosystem service, directory, ledger?

Key here is to establish conventions that make it simple for Verifiers to obtain what they need for omni-channel service delivery without onerous effort, and to make sure that real-time delivery of trust vector materials is efficient and accurate while providing for revocation.

Applying Conventions Across Mechanisms

Developing Conventions

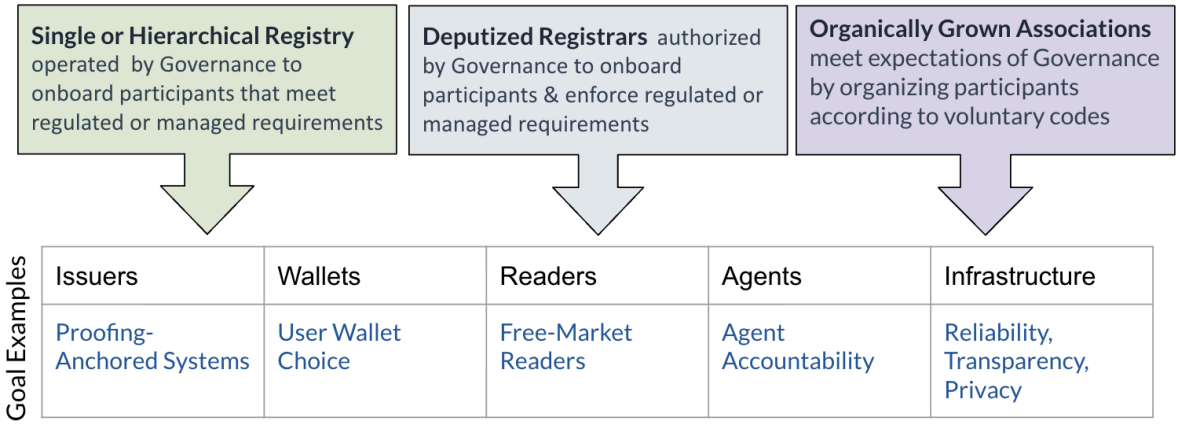
In either of these types of Ecosystems, it is important for the Ecosystem Builder to establish **Conventions** for how Trust Mechanisms are utilized and given meaning. The Conventions - the collection of rules, policies, and guidelines for inclusion in a mechanism - become the reason components can trust each other and the way that participants can verify assurances of trust in real time. The meaning mitigates risk in real time.

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

As an example in a Wallet Ecosystem, AAMVA in the US has publicly posted their Mobile Driver's License Implementation Guidelines[21] that express the rules, policies, and guidelines that AAMVA will enforce before allowing an mDL Credential Issuer to place their public key in AAMVA's Digital Trust Service[22]. Verifiers can choose to load AAMVA's Trust List (in VICAL[23] format) into their Readers to verify cryptographic signatures on mDL. In addition, Users have assurances[24] of the behavior of Issuers that provision their mDL.

Registrars Encourage Conventions

Registrars operate a Trust Mechanism to accomplish a goal or policy. They may gain their authority to do so by legislative, authoritative, or influential means. This allows them conceptually to fit within any Ecosystem Governance structure and across structures. It allows the Ecosystem Builder to deploy policy across the domains they influence or control.



Document Map & Next Steps

This document is the first in a series that provides a pathway to solve Trust Management.

1) Trust Management_ Defining the Challenge for Ecosystem Builders.docx (this document) defines the trust challenge and solutions for an Ecosystem Builder to deploy managed trust in a Digital ID ecosystem.
2) Trust Management_ Developing Conventions Using Trust Vectors explains how Ecosystem Builders develop Conventions (requirements) that will mitigate participants' risk and foster interoperability for assured acceptance of credentials.

---

21 https://www.aamva.org/assets/best-practices,-guides,-standards,-manuals,-whitepapers/mobile-driver-s-license-implementation-guidelines-1-2

22 https://www.aamva.org/identity/mobile-driver-license-digital-trust-service is the Trust List

23 https://www.raidiam.com/developers/docs/concepts/trusted-lists/vical/

24 https://medium.com/@dkelts.id/what-does-meets-aamva-guidelines-do-for-mdl-users-4d0c137ca8be

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 Attribution 4.0 International.
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

3) Trust Management: Mechanisms to Promote & Enforce Conventions explains how an Ecosystem Operator can deploy mechanisms that generate inter-component and participant trust in a functional slice of the ecosystem.

Please provide feedback through https://sidi-hub.community/ and https://tida.community/

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

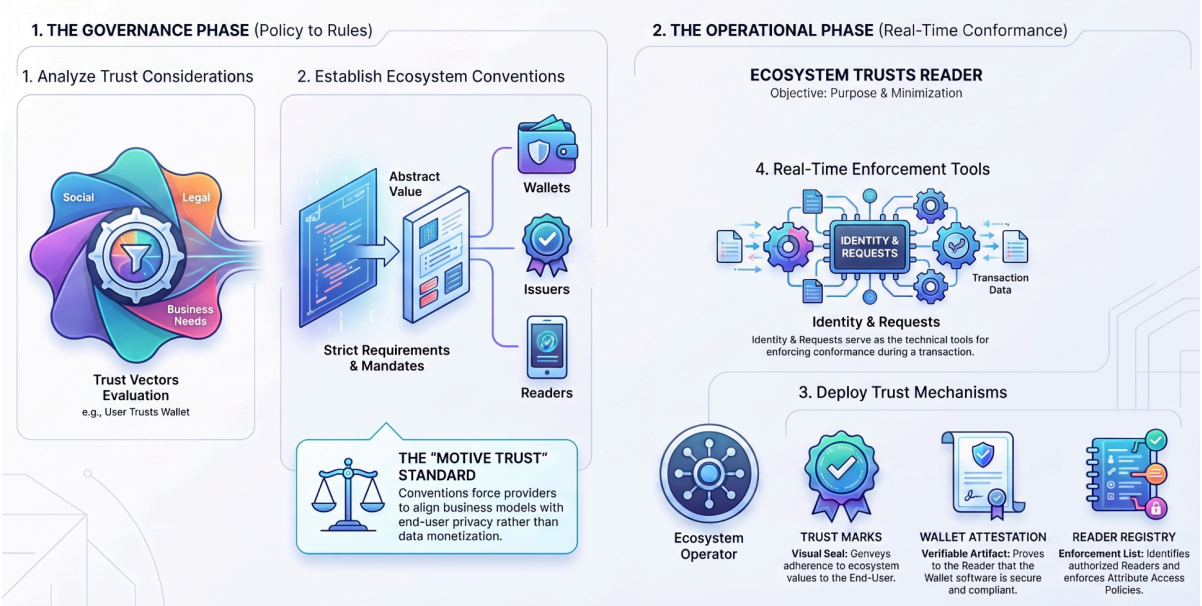
Credits

Contributors	Organization
David Kelts (Editor)	Decipher Identity, LLC. 0009-0004-3917-4419
Debora Comparin	Thales Group and Secure Identity Alliance
Paul Templeman	Independent Consultant & OpenID Foundation 0000-0002-0443-7176
Rachelle Sellung	Fraunhofer IAO 0000-0003-1235-030X
Isaac JJK Henderson	Fraunhofer IAO
Lucy Yang	Tech Serves a Purpose
Reviewers	
SIDI-Hub.community	Safe, Interoperable Digital ID Infrastructure
Andreas Aabye	
Edgar Whitley	London School of Economics
Shigeyo Suzuki, PhD	Keio University
Giuseppe De Marco	Innovation Dept, Government of Italy
Takehisa Shibata	Price Waterhouse Coopers
Arvid van der Bruggen	Kiwa Nederland
Leonardo Contreras	Gestión de Seguridad Electrónica, S.A. &,
Supporters	Three organizations formed, funded, staffed, and promoted https://sidi-hub.community/ and the events which coalesced a global view of managing trust for Digital ID. SIDI Hub has become part of the ITU's https://tida.community/ open for new contributors.
Stephanie Delabriolle	Secure Identity Alliance
Gail Hodges	Open ID Foundation
Jeff Reich	Identity Defined Security Association

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Appendix: Trust Management Process

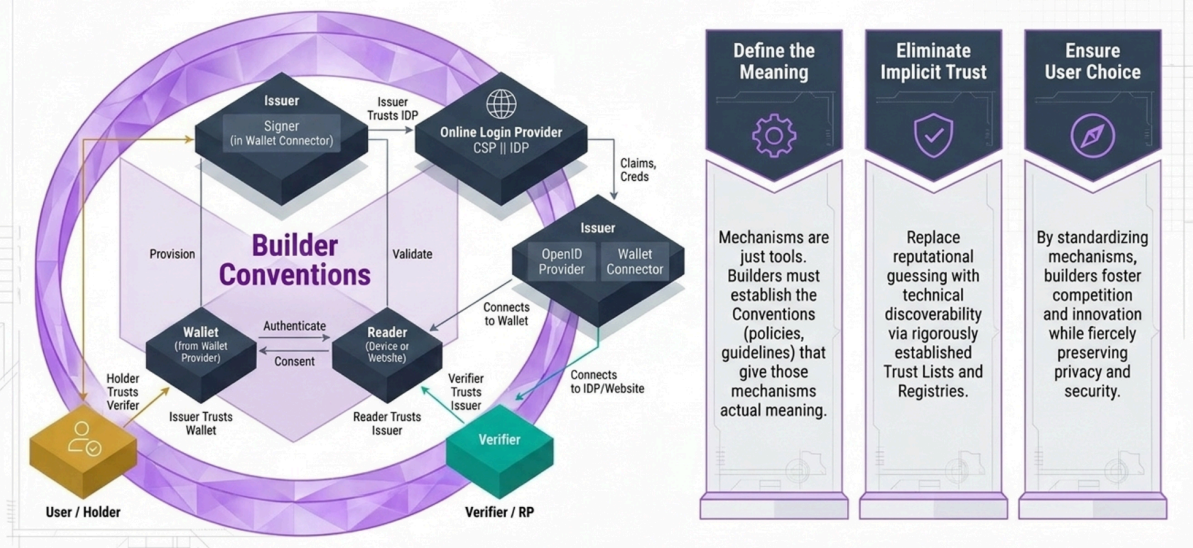
1. Ecosystem/Network Operator's System View



1. Establish and Understand Your Ecosystem (or Network) **Governance**
2. Analyze Trust Vectors to Establish Conventions
   a. Use Document #2 in Document Map & Next Steps
   b. Put Governance into Trust Elements and Mechanisms
3. **Operationalize** Trust Mechanisms for real-time access by participants & components
4. Establish real-time enforcement tools, certifications, and Ecosystem policy

SIDIHub © 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

2. Ecosystem Builder’s Mandate



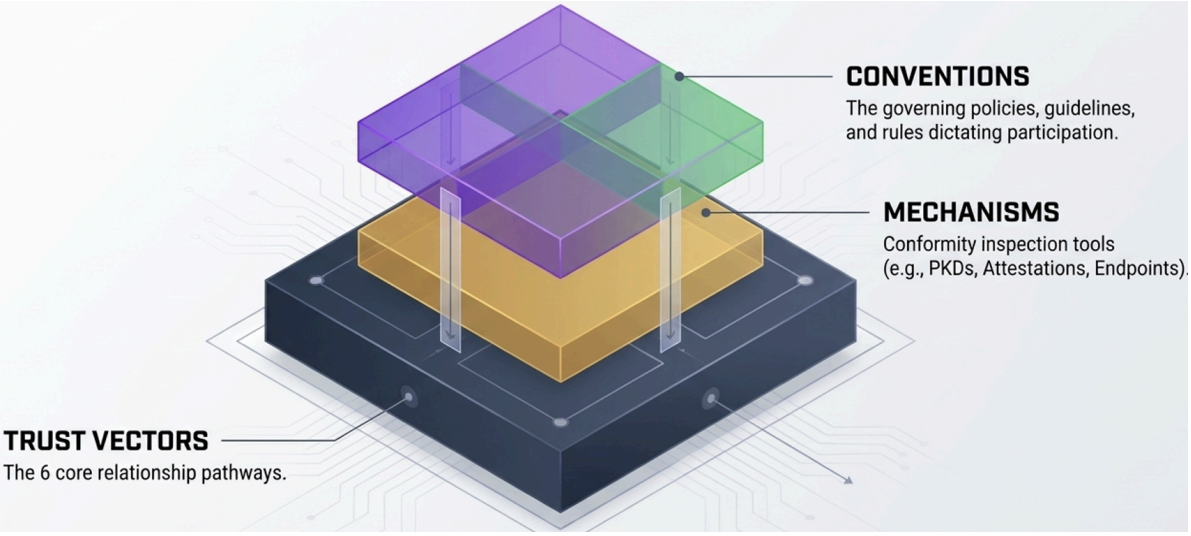
The Ecosystem/Network Builder can overcome existing shortcomings of a functioning ecosystem by applying intelligent control mechanisms that shape participant behavior. Several important considerations of Ecosystem Trust may not be automatically included in the technical design or policy management of an Ecosystem or Network (subset within a larger ecosystem).

For this reason, the Builder should always pursue;

- ☐ Consumer Protection
- ☐ Data Processing Standards
- ☐ Transition to Interactive Data Processing given the value of authoritative data
- ☐ Explicit Trust over reputational or single-provider trust (that bolsters interoperability)
- ☐ User Choice in components, communication, and participation
- ☐ Verifier Choice in equipment and workflows
- ☐ Anti-surveillance by technology and policy on all sides - Issuer, Wallet, Verifier

SIDIHub © 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

3. Stabilizing Trust Across All Six Trust Vectors



Conventions are policies that can be parceled into responsibilities of each component in an Ecosystem and therefore enforced through membership in well-known Trust Mechanisms.

All participants look to their chosen Trust Mechanisms for guidance to participate in the ecosystem, reduction of complexity, and common policy. In particular, Verifiers want to solidify and improve their business processes instead of sorting out identity policy.

The Ecosystem Builder bolts these concepts together across an entire ecosystem. A Network Builder may select a slice of a larger ecosystem or across ecosystems to provide guidance and policy to a subset of Ecosystem participants that share common needs. For instance, Payment Networks can consider adding Digital ID trust Conventions for their merchant and retailer populations. It extends their scope without impacting the core.

© 2025-26 SIDI Hub Community is licensed under CC BY 4.0 **Attribution 4.0 International.**
Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org