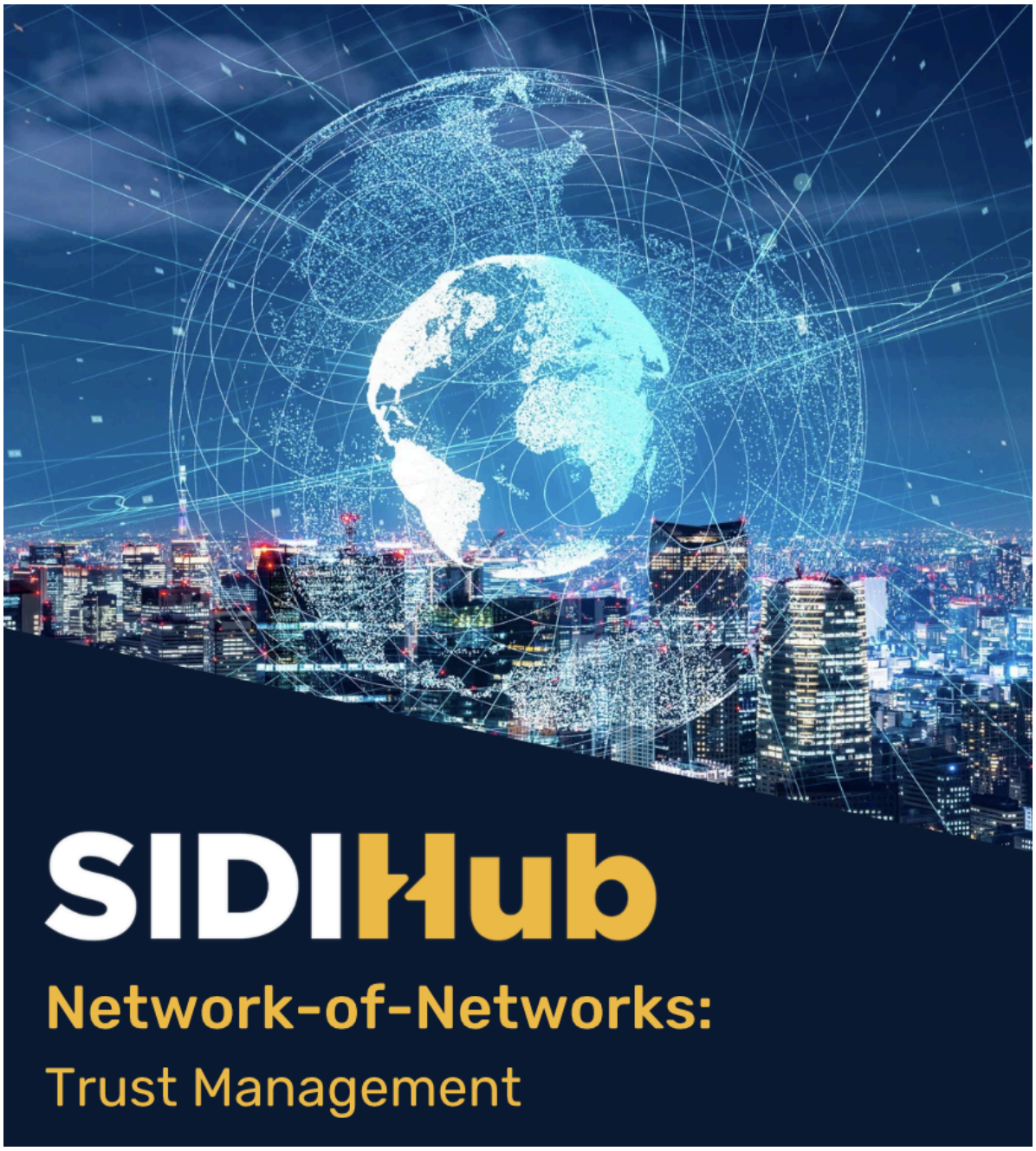
The document, "Trust Management: Defining the Challenge for Ecosystem Builders," is a conceptual analysis for ecosystem builders, policy-makers, and standards contributors focused on digital identity ecosystems, particularly those involving wallets and logins. It posits that trust is aligned across 6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



Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Key Concepts

- **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** (with a **Reader**), **Wallet Providers**, **Trust List Providers**, and the **Ecosystem Builder**.
- **Structure:** It proposes understanding Trust Management through **Trust Vectors**, **Mechanisms**, and **Conventions** to inform ecosystem design and 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).
- **Conclusion:** The document stresses the importance of an **Ecosystem Builder** establishing clear **Conventions** for utilizing mechanisms to reduce complexity, facilitate user choice, and overcome shortcomings like reliance on reputational trust, unclear system operations, and subversive actors. It overlays Login (OpenID) and Wallet Ecosystems, noting that while Trust Vectors remain similar, the Mechanisms and Conventions may differ.

Table of Contents

to be added

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. The **Ecosystem** works because other participants provide assurances that mitigate or meet that risk. Trust is the term used to express that ecosystem participants are meeting their obligations to provide these assurances and fulfill their roles according to ecosystem expectations expressed in a **Trust Framework**[1]. This document helps the Ecosystem Builder assemble requirements that frame trusted participation.

Trust Management

Trust Management is 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 their obligations and, therefore, mitigates 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.

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

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

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

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 this document 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

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Wallet Ecosystems

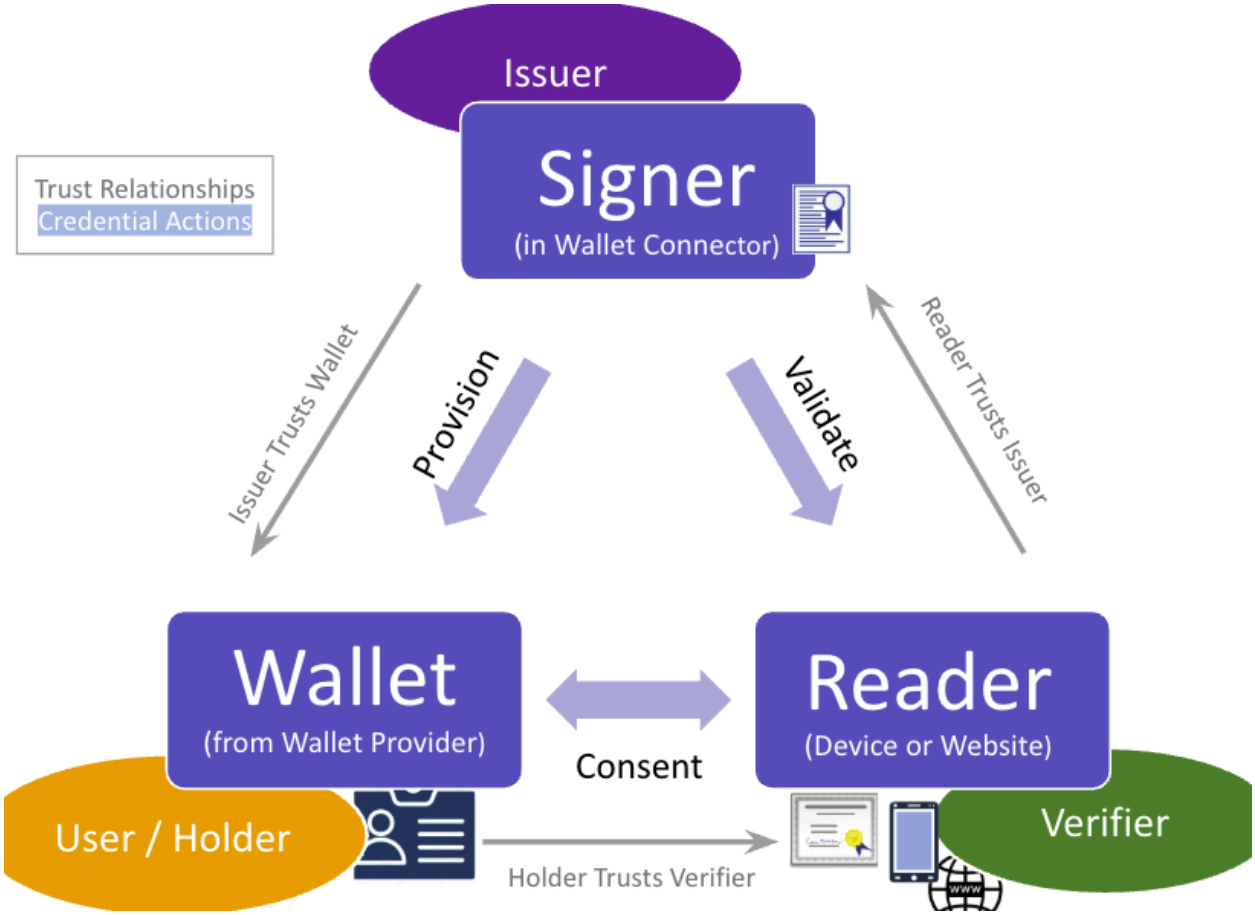


Fig 1: Trust Relationships needed for Credential Actions in current 3-Party Wallet Ecosystems

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**.

[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

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

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 to give **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.

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.

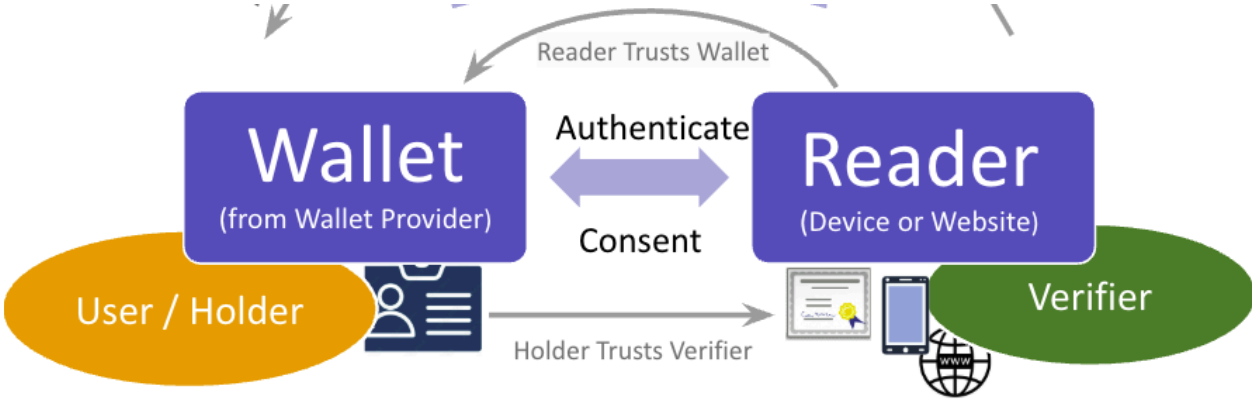


Fig 2: Adding the Trust Vector that will permit User Authentication by the Wallet app/service

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).

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 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:

[4] Also Credential Verifier https://openid.net/specs/openid-federation-wallet-1_0.html#section-3.1

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

- 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. Conversely, the Wallet should not report transactions to the Issuer.
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**[5]. 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 involved in surveillance capitalism on the Internet will enter the wallet space.

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

[5] 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

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

component with which it communicates. The receiving component checks a cryptographic signature.

Current Observed Patterns of Trust Vectors

Single-Provider (Homogeneous) 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[6] 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.

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.

Regulated Participation

Shortcomings in Observed Patterns

Lack of User Choice

Furthermore, to facilitate User choice in their components, which is critical for privacy, and allow for optimal technical flexibility and innovation, Mechanisms and Conventions are required. Mechanisms allow discoverability of the components and systems that are under

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

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

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.

Reputational or Implicit Trust Assumptions

RP's choosing Readers only from their Issuer; nothing to indicate trust of Commerial Readers.
Choosing brand name wallet apps; Not trusting State-issued Wallet apps. The lack of definition defaults people and businesses to reputational, implicit, or fear-of-non-compliance decisions on software and equipment they choose.

Shortcomings in Security of Receipt Storage & Usage 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[7]. 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 about internet privacy.

Trust (List) Providers

Since there are multiple Issuers and multiple Verifiers in ecosystems, and Verifiers may operate multiple independent Readers, there must be mechanisms to distribute public keys and certificates to participants in the ecosystem. These Mechanisms may have controls placed on them as to how public keys can be included in the mechanism. 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).

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, then, also expresses what it means to be a member of that list so that other participants can trust. Consuming a Trust List reduces independent individual trust relationships because list creation was performed for participants according to known convention.

The Trust List itself becomes a form of trust anchor. The Verifier needs to have only one relationship that it trusts - knowing that the List Provider operates in a manner consistent to mitigate

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

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

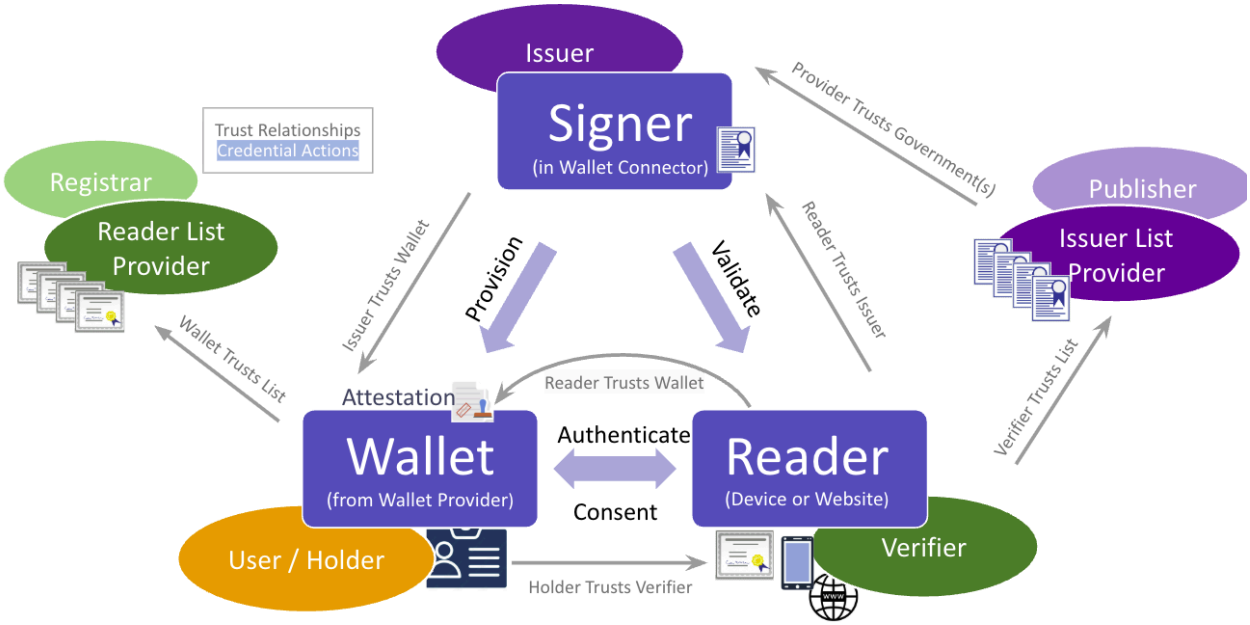


Fig 3: Wallet Ecosystem with Trust Vectors and Mechanisms for conveying trust on these vectors

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 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.

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

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 Attestations

A Wallet[8] should be able to provide a **Wallet Attestation**[9] to a Reader that identifies its specific instance and information about how it was built, 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 because there is an assumption about how User Authentication[10] is performed.

Similarly, the Wallet can[11] 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

---

[8] 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.
[9] Defined, therefore, in EUDIWallet implementing acts as a Wallet Unit Attestation (see link above).
[10] 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
[11] 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

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

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[12] [13] [14], 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**[15] endpoints with list-like mechanisms.

1:1 Pairing, RP Operates OpenID Provider

The User's Browser and the Website perform a certificate exchange to establish a trust relationship that the website being visited is that of the 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 application in Wallet Ecosystems.

---

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

13 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://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74932

15 https://openid.net/specs/openid-federation-1_0.html

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

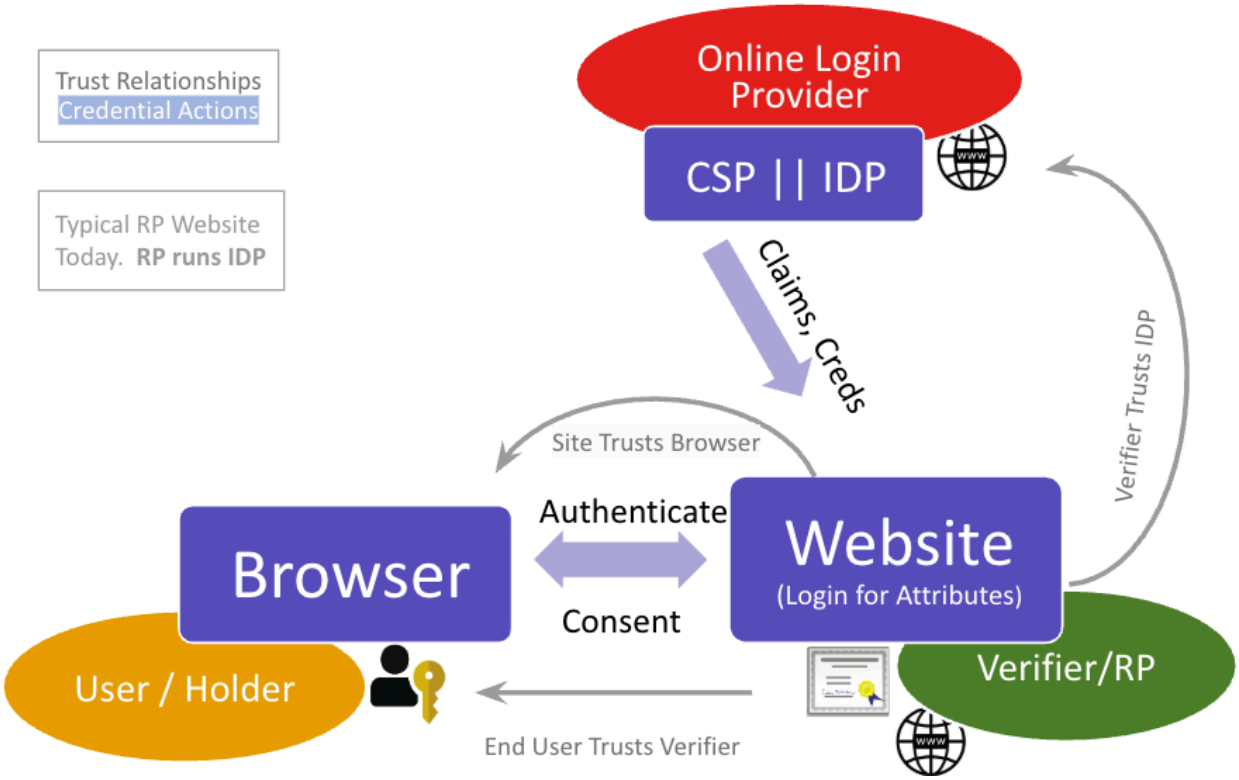


Fig 4: Relying Party / Verifier operated or trusted Identity Provider

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 be a SAML IDP[16]). 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 Verifiers follow guidelines. They also can be authoritative sources for attributes given regional Identity Proofing.

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

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

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.

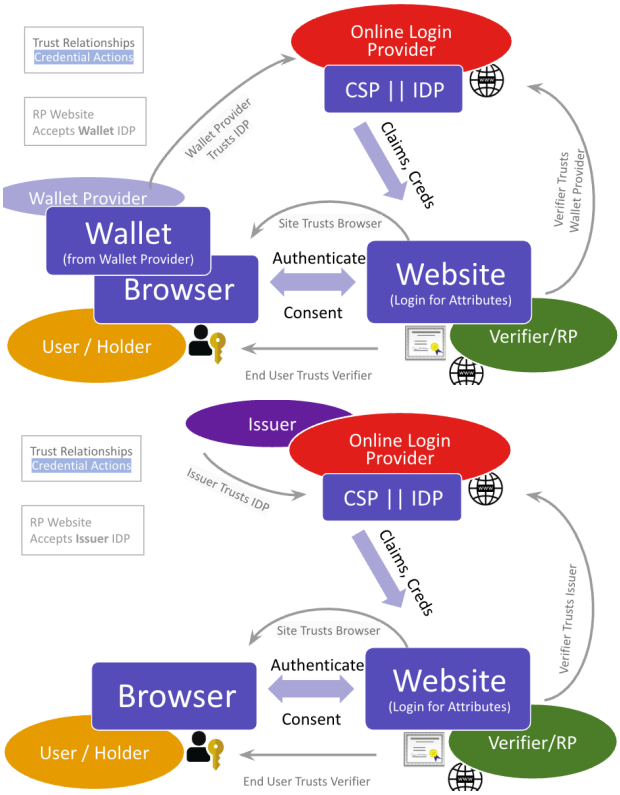


Fig 5 & 6: Consider the meaning of Trust behind two possible OP deployments: Wallet or Issuer

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?

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

Overlaying Login & Wallet Ecosystems

Issuer OP Paired with Wallet

When you overlay a Government login 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 across contexts.

This combination of a Federation Login Ecosystem **with** a Wallet Ecosystem has not yet been deployed but 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, either after a login event or ISO/IEC 18013-7 device engagement that authorizes release after obtaining consent. After an initial in-person token exchange using ISO/IEC 18013-5, claims to in-person Verifiers are delivered through the exact same mechanisms in the form of OpenID4VP.

The Trust Vectors are identical in this "Federation+Wallet Hybrid" but the ability for the Ecosystem Builder (or the Issuer) to flexibly handle all potential use cases improves.

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

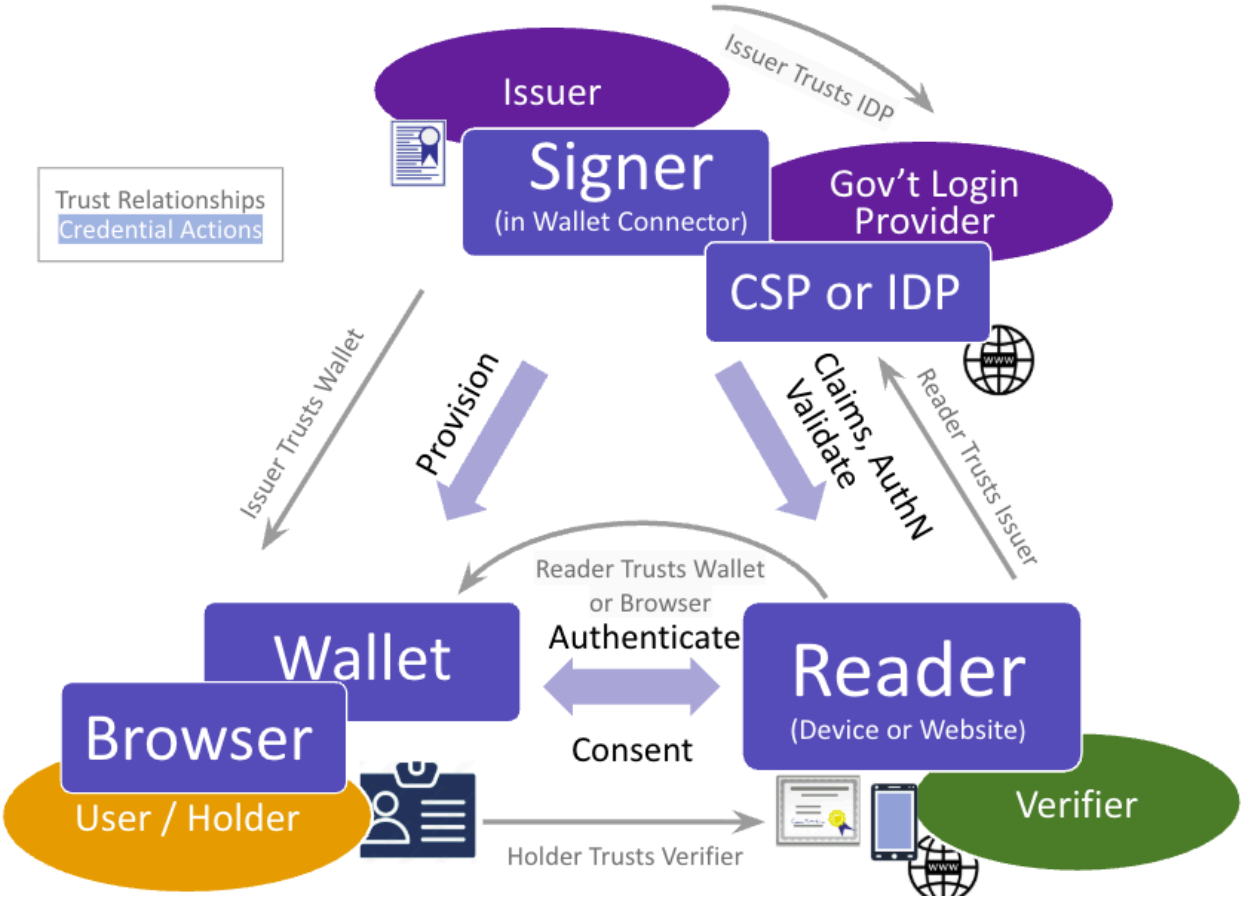


Fig 7: Overlaying a Wallet Ecosystem with a Login Ecosystem does not change the Trust Vectors but it does increase the potential number of Mechanisms.

Trust Vectors Don't Change Much

You can see that the Trust Vectors do not change much when you overlay Government Digital ID documents and Government Login. The types of Verifiers change, however. In the Verifier <-> Issuer channel, the Claims delivery, AuthN, and Validate credential actions are complementary to each other. Also 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 per the mdoc data model—this is the standard OIDC Core flow.

This configuration is most likely when the Verifier is a government agency or associated entity (they should be purple in Fig 7). I would not expect a commercial Verifier to accept a Government OP and, conversely, despite the assurance of complete data anonymity when no claims are requested, for an End User to expect to use their Government OP to log in to a business. The exceptions are well-known regulated transactions that require Government ID like alcohol purchase, online age verification, etc. From a consumer comfort level, most

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

of these are better left to commercial OP implementations… or authorized aggregators such as specified in UK.

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/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

Mechanisms and Conventions 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

In either of these types of Ecosystems, I want to point out how important it is for the Ecosystem Builder to establish **Conventions** for how wallet and federation mechanisms are utilized. The Conventions - the collection of rules, policies, and guidelines for inclusion in a mechanism - become the reason components can trust each other and verify assurances of that trust in real time.

As an example in a Wallet Ecosystem, AAMVA in the US has publicly posted their Mobile Driver's License Implementation Guidelines[17] 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 Trust List that they call Digital Trust Service[18]. Verifiers can choose to load AAMVA's Trust List (in VICAL[19] format) into their Readers to verify cryptographic

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

[18] https://www.aamva.org/identity/mobile-driver-license-digital-trust-service

[19] https://www.raidiam.com/developers/docs/concepts/trusted-lists/vical/

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org

signatures on mDL. In addition, Users have assurances[20] of the behavior of Issuers that provision their mDL.

Next Steps

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

1) Trust Management: Defining the Challenge defines the trust challenge and creates a process for an Ecosystem Builder to deploy managed trust in a Digital ID ecosystem.
2)
3)

Provide feedback on this document through https://sidi-hub.community/

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

Editors: David Kelts david@decipher.id and Debora Comparin debora.comparin@secureidentityalliance.org