ayra

trusted relationship network

Ayra Technical Whitepaper

https://ayra.forum/

Public Review Version 0.0.11

16 January 2025

Andor Kesselman

Dave Poltorak

Drummond Reed

Darrell o' Donnell

Nicky Hickman

Maxwell Baylin

Nayan Banerjee

Plus contributions from many Ayra Association Members

NOTE: The Global Acceptance Network (GAN) has been rebranded to Ayra.

Executive Summary

The Ayra (eye-rah) Association (formerly the Global Acceptance Network—GAN) governs the Ayra Trust Network, a network of networks designed to enable secure exchange of verifiable data across digital trust ecosystems. This document focuses on the three primary technical challenges that hinder cross-ecosystem value creation. It describes the technical solutions that Ayra Association members are collaborating to design and implement.

Key technical challenges for trusted value exchange

- **Inconsistent terms across ecosystems:** Aligning rules and practices for data sharing and trust between ecosystems is costly and difficult to scale. Each ecosystem operates with its own standards, making seamless collaboration challenging.
- **Credential definitions are not known:** Credential types and definitions vary widely, lacking semantic agreement across ecosystems. This inconsistency hinders verifiers in creating accurate presentation requests and exchanging verifiable data.
- **Technical variability:** Ecosystems often have unique technical requirements, standards, and change management processes. These differences create barriers to:
    - Seamless verifiable data exchange.
    - Efficient querying of trust registries.

Why Ayra is well positioned to solve these challenges

The Ayra Association is chartered as a neutral Swiss nonprofit organization specifically to provide open neutral multi-stakeholder governance for the global infrastructure required to tackle these challenges. Central to its strategy is a network of metaregistries that facilitate interoperable cross-ecosystem trust relationships.

Due to the emphasis on cross-ecosystem value exchange rather than the interests of any single ecosystem, the Association can help members focus on the specific pain points hindering interoperability. This collaborative approach can address gaps that individual ecosystems lack the incentive to resolve, driving real progress in trusted data exchange.

Ayra's solution

- **Cross-ecosystem acceptance via a trust network of metaregistries**
  The Ayra Association governs a global **Ayra Trust Network** supported by a set of ecosystem metaregistries. These metaregistries convey the state of recognized ecosystems and interoperate seamlessly with other registry-of-registry systems to facilitate trusted interactions across ecosystems.
- **Enhanced data discoverability with the Ayra Type Catalog**
  To address the very real pain of semantic interoperability, the Ayra Type Catalog simplifies registration and discovery of credential types and definitions..

- **Technical alignment via a Conformance Test Suite and Ayra Interoperability Profiles**: Without tools to verify interaction patterns and measure real interoperability, technical convergence would not be possible.

Immediate next steps

- Launch a **sandbox environment** to pilot the Ayra Trust Network and initial **Ayra Interoperability Profiles**.
- Refine and expand the **Conformance Test Suite** to support broader use cases and vendor requirements.
- Collaborate with stakeholders to align **technical and governance frameworks** for global adoption, acknowledging that governance challenges remain an essential focus for future work beyond the technical scope of this paper.
- Initiate the first wave of **operational pilots and proof-of-concepts (PoCs)** to demonstrate the real business value of cross-ecosystem trusted data exchange.

Recommended Pre-Reading

If you are new to Ayra, the Introduction To Ayra Whitepaper is the best place to start.

We also recommend two additional white papers as pre-reads: The Ecosystem of Ecosystems Model for Decentralized Digital Trust Infrastructure and The Special Network Effects of Ayra Network Credentials. They describe the overall problem and solution space, the design principles for the Ayra Trust Network, and the special credentials being designed for cross-ecosystem interoperability. These papers also define key terms utilized here.

Intended Audience

This paper is intended for CTOs, technical architects, IAM experts, implementers, and others who want an overall technical understanding of the design goals, architecture, and roadmap for the Ayra Trust Network. Please see the Recommended Pre-Reading for other topics if this document is not the right fit for you.

Scope

This whitepaper outlines the foundational technical vision and immediate challenges that the Ayra Trust Network must address to enable trusted data exchange across ecosystems.

While the primary focus is on technical aspects, including interoperability and infrastructure, it acknowledges that business cases and governance procedures are critical for long-term success. However, these areas are outside the scope of this paper.

Where relevant, references to other Ayra white papers will provide additional context. The aim of this paper is to define a clear path forward for the technical evolution of the Ayra Trust Network through structured processes, including Architectural Decision Records (ADRs) and Requests for Comments (RFCs), which will incorporate feedback from the community.

Table Of Contents

Introduction: The Challenges to Cross-Ecosystem Exchange of Trusted Data....6
Introducing the Ayra Trust Network....10
- How metaregistries enable cross-ecosystem trust relationships....11
  - Operational architecture of the Ayra Metaregistry Network....13
  - Cluster recognition via metaregistries....13
- How the Ayra Type Catalog assists with semantic interoperability....15
- The role of Ayra Interoperability Profiles and the Conformance Test Suite....17
  - Verifiable Credential Exchange Profile....18
  - Authority Verification Profile....19
  - Using the Ayra Conformance Test Suite....20

Ayra Metaregistry Network roadmap....21
Ayra Network Credentials....22
Multi-Network flows....23
Additional scenarios for the Ayra Trust Network....25
Next steps....26
Future considerations....26
Conclusion....26
Appendices....28
- Appendix A: Credential Exchange Technical Interoperability Profile details....28
- Appendix B: Authority Verification Profile details....30
- Appendix C: Ecosystem Recognition procedure....32
- Appendix D: Conformance Test Suite - high level architecture....33
- Appendix E: Example CTS roadmap....35
- Appendix F: The Ayra Operated Metaregistry....37
- Appendix G: Technical Challenges for the Ayra Metaregistry Network....38
- Appendix H: Technical Challenges Of Ayra Network Credentials....40
- Appendix I: Trust Registry Query Protocol....41
- Appendix J: Challenges With Interoperability Profiles....43

Member and Contributor Acknowledgements

We would like to acknowledge the valuable contributions from Ayra Association members and community contributors, specifically (by last name): *Sankarshan Mukhopadhyay, Kai Otsuki, Markus Sabadello, Jo Spencer, Alex Tweedale,* and *Takashi Yamamoto*.

Without their support and guidance, this document would not have been possible. For a list of Ayra Association members, please see https://ayra.forum/.

Terminology

- **authority statement:** A machine-readable expression of authorizations granted to an entity governed by a governance framework. Authority statements are typically written to and queried from a trust registry.
- **Ayra Association:** A Switzerland-based nonprofit organization that serves as the governing body for the Ayra Trust Network. https://ayra.forum
- **Ayra Governance Framework:** The governance framework maintained by the Ayra Association to manage the Ayra Trust Network.
- **Ayra Interoperability Profile:** Ayra-developed binding specifications to standardize frictionless cross-ecosystem interactions.
- **Ayra Operated Metaregistry**: A metaregistry operated directly by the Ayra Association (vs. metaregistries operated by other Ayra Trust Network members).
- **Ayra Trust Network**: A trust network of registries and metaregistries that serves as the backbone of the Ayra ecosystem of ecosystems. Managed by the Ayra Association and governed by the Ayra Governance Framework.
- **Ayra Metaregistry Network:** The set of metaregistries recognized by the Ayra Trust Network. All registries in the Ayra Trust Network use the Trust Registry Query Protocol (TRQP) for interoperability. This component is at the heart of the Ayra Trust Network.
- **cluster:** short for **trust cluster**.
- **credential family:** A set of digital credentials that are intentionally designed to work together to accomplish a shared set of data exchange and/or trust objectives.
- **digital trust ecosystem:** A digital ecosystem in which the participants are one or more interoperating trust communities. See the Trust Over IP Glossary for more information.
- **ecosystem:** short for **digital trust ecosystem**.
- **ecosystem recognition :** The process of a metaregistry adding an authority statement referring to the trust registry for an ecosystem.
- **entity authorization:** A set of authority statements recorded in a trust registry describing the authorization granted to an entity governed in that ecosystem.
- **metaregistry:** A trust registry whose primary function is to recognize or authorize other trust registries within a particular ecosystem or group of ecosystems (cluster).
- **trust cluster:** A group of ecosystems sharing a credential family, governance policies, and one or more metaregistries in order to achieve a shared set of trust objectives.
- **trust registry :** A registry that serves as an authoritative source for trust graphs or other governed information describing one or more trust communities. A trust registry is typically authorized by a governance framework.
- **trust network:** A logical network of parties who are connected via trust relationships (such as via a membership agreement) conforming to requirements defined in a legal regulation, trust framework or governance framework. A trust network is more formal than a digital trust ecosystem..

Introduction: The Challenges to Cross-Ecosystem Exchange of Trusted Data

When data exchange moves from intra-ecosystem to inter-ecosystem, it runs into technical obstacles including data authenticity, authorization, and non-interoperable formats and protocols. Add to this the challenges of alignment on business and governance policies.

Without a cohesive solution, exchange of verifiable data across ecosystems is stymied.

To demonstrate how this problem manifests, consider a single digital trust ecosystem comprising issuer, holder, and verifier systems.

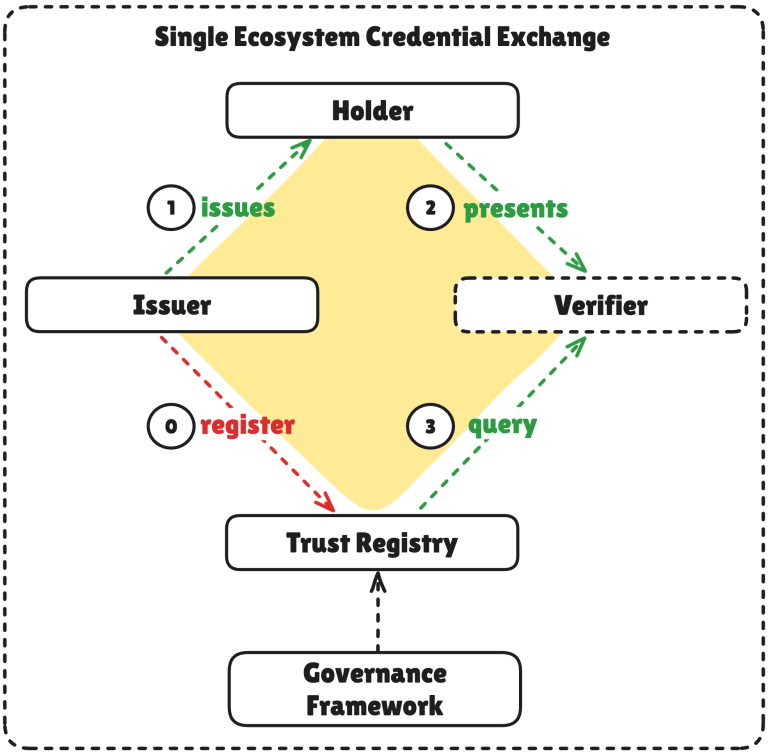

Figure 1: A single ecosystem comprising issuers, holders, verifiers, and a trust registry

This example is illustrative

While credential exchange use cases are discussed in this paper, the Ayra Trust Network is **not limited** to credential exchange. It can be used for any type of cryptographically verifiable data exchange. In theory, all actors may be registered into an ecosystem trust registry, not just a credential issuer as demonstrated in figure 1. For extensions to the simple cases described, see Additional Scenarios for the Ayra Trust Network.

In the example in Figure 1, the following steps occur:

1. **Issuer Registration**: The governing body of an ecosystem registers an issuer in their system of record. The registration process is governed by the ecosystem's governance framework. The list of issuers is then exposed as a trust registry, which signals the issuer's compliance with the ecosystem's policies.
2. **Credential Issuance**: Once registered, the issuer issues a credential to a holder. The holder stores this credential securely in a digital wallet. The specific process for credential issuance may vary across ecosystems, depending on their governance and technical frameworks.
3. **Presentation Exchange**: The verifier requests proof from the holder as part of an interaction. The holder responds by presenting a proof of the credential to the verifier, allowing the verifier to establish trust in the credential presented. The method for exchanging credentials can vary widely and is again specified by the ecosystem's governance and technical infrastructure.
4. **Verification**: The following tasks are discussed in detail in the Ecosystems of Ecosystems white paper:

#	Task	Description	Required Support
1	**Verify digital signature**	Verify that the credential presentation has a valid digital signature produced by the private key bound to the public key.	None (can be verified using cryptography alone)
2	**Verify public key**	Verify that the public key is controlled by the credential issuer.	Verifiable identifiers (e.g., DIDs)
3	**Verify issuer (or verifier) authorization**	Verify that the issuer (or verifier) is authorised within an ecosystem to issue (or verify) this specific type of digital credential.	Trust registry
4	**Verify credential status**	Verify that the credential is not suspended, expired, or revoked.	Revocation registry

Table 1: The four core steps in verification of digital credentials

When applied to digital credentials (widely referred to as "verifiable credentials" due to the W3C standard of that name), this general process of verifiable data exchange has been successfully implemented in many ecosystems, resulting in billions of credentials issued[1].

Figure 1 shows a single governance framework with one governing body and one trust registry. This ensures consistent terms and automatic acceptance of credentials within the ecosystem. The trust registry is well-known, and the ecosystem uses a single tech stack,

[1] As one example, as of this writing over 2 billion COVID vaccination credentials based on W3C Verifiable Credentials have been issued.. https://covid19dashboard.mohfw.gov.in/.

making it easy for verifiers to know how to query the registry (or trusted actors can even be hard-coded). Credentials are well-defined, enabling the verifier to construct presentation requests aligned with the verifiable data they need.

In short, credential exchange and verification is seamless.

Now let's look at what happens when a verifier **outside** the ecosystem tries to leverage that same verifiable data as shown in figure 2:

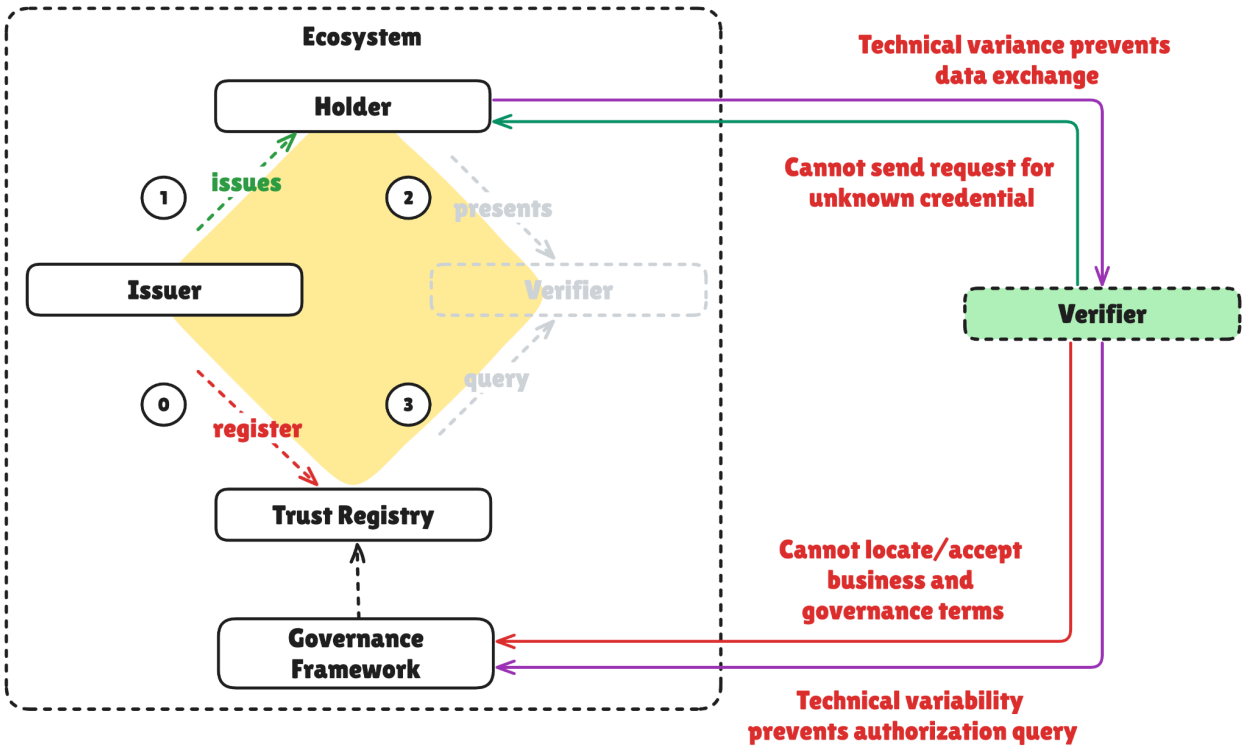

Figure 2: The barriers to a verifier outside of the ecosystem trust boundary.

Table 1 compares the intra-ecosystem case to the inter-ecosystem case:

Category	Intra-ecosystem	Inter-ecosystem
Ecosystem governance framework	Pre-established, well-known, consistent terms, and already accepted.	Unknown, not centralized, lacking a pre-accepted governance framework.
Trust registry	Well-known, uses the same tech stack, easy to query, or has pre-established or hard-coded trust mechanics.	Unknown trust registry, potentially using a different technology stack, no uniform way to establish trust.
Credential types and definitions	Well-defined, with semantic agreement and known requirements up-front.	No semantic agreement on data meaning, and credential types unknown at implementation.
Technical Interoperability	Minimal technical variety, reducing friction in interoperability. .	Diverse technical standards can result in non-interoperable systems.

Table 2: Comparing intra-ecosystem and inter-ecosystem verifiable data exchange.

These challenges to inter-ecosystem verifiable data exchange can be summarized as:

1. **Inconsistent terms across ecosystems**
   Governance frameworks (aka trust frameworks) are typically focused on their respective ecosystems. They lack standardized mechanisms, consistent terms, or pre-established agreements to extend trust across ecosystem boundaries.
2. **Credential types and definitions not known or shared**
   Without semantic agreement on the meaning of data or the mapping between ecosystems, verifiers won't know how to request the data they need.
3. **Technical variability**
   Different tech stacks using different credential formats, different exchange protocols, different trust registry protocols, and different cryptographic algorithms are a major barrier to interoperability. Couple this with differ change management processes and timescales, and it is no surprise that cross-ecosystem exchange of verifiable data is so rare.

These challenges are exactly why the Ayra Association and the Ayra Trust Network were created.

Introducing the Ayra Trust Network

The Ayra Trust Network is comprised of the components in table 2:

Component	Description	Challenge Addressed
Ayra Metaregistry Network	A set of metaregistries serving the Ayra Trust Network's state of recognized ecosystems	Cross-ecosystem authority verification
Ayra Type Catalogue	A registry of credential data types and definitions	Semantic interoperability
Ayra Interoperability Profiles	Technical requirements for compatibility with the Ayra Trust Network. Categories: • *Verifiable Data Exchange* for credential exchange (currently Messaging and API based proposals) • *Authority Verification Protocol* for trust registries (anchored on the Trust Registry Query Protocol)	Technical variability
Ayra Conform-ance Test Suite	Tests conformance of systems with the interoperability profiles	Technical variability

Table 3: The major components of the Ayra Trust Network

Experienced Internet and IAM architects will immediately understand the rationale for the Ayra Type Catalogue, Interoperability Profiles, and Conformance Test Suite (CTS). The most distinguishing feature of the Ayra Trust Network—and the driving reason for founding the Ayra Association as a global multi-stakeholder governance organization—is the metaregistry architecture at the heart of globally-scalable digital trust infrastructure.

The overall rationale for this architecture—and what it does and does not have in common with DNS as another global-scale digital public utility—is explored in depth in our companion white paper The Ecosystem of Ecosystems Model for Decentralized Digital Trust Infrastructure. **That paper is the recommended background for the rest of this section.**

The key design goals of this metaregistry architecture are:

- **Sovereignty**: The Ayra metaregistry layer only interconnects ecosystems—each ecosystem is sovereign for everything inside its "borders".
- **Scalability**: The metaregistry layer needs the same scalability as DNS.
- **Security**: Metaregistries must operate in a tamper-proof and incorruptible manner.
- **Sustainability**: Just as with the Internet and DNS, the metaregistry layer must be strong enough not to break but also resilient enough to evolve.

Additional details on the technical challenges for the set of metaregistries are described in Appendix F: Technical Challenges for the Ayra Metaregistry Network

How metaregistries enable cross-ecosystem trust relationships

In the scenario in figure 2, the verifier needs to decide if they can accept verifiable data produced in a different ecosystem. To help reach this decision, the verifier needs to answer the two questions shown in figure 3. (For purposes of this example, we assume Ecosystem A and Ecosystem B are technically interoperable). These questions are:

1. Do I recognize the governance framework of Ecosystem A?
2. Is the issuer authorized to issue this type of data within Ecosystem A's governance framework?

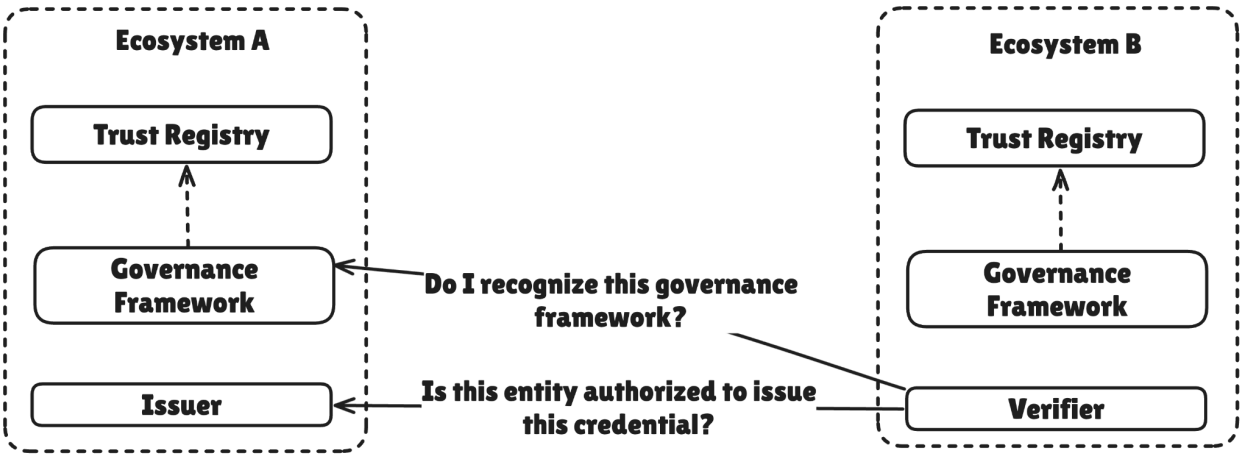

Figure 3: The two fundamental queries required cross-ecosystem authority verification.

The first question is called **ecosystem recognition**. It is a complex question that is not easily automated (and in the end always ultimately depends on human policy decisions). But the Ayra Trust Network and the Ayra Governance Framework offer two tools to make ecosystem recognition easier:

1. **Verifiable governance frameworks**. All Ayra-recognized ecosystems are required to have a Web-accessible ecosystem governance framework that has a persistent, cryptographically verifiable identifier (such as a DID).
2. **Trust registry interoperability**. An Ayra-recognized ecosystem must have at least one trust registry endpoint that has passed the Ayra Conformance Test Suite. This ensures the coherence and performance of the Ayra Trust Network as a whole (in a manner similar to how ICANN safeguards the interoperability of DNS).

The second question is called entity authorization. This is exactly what the Trust Registry Query Protocol (TRQP) is designed to do. It takes machine-readable queries in the following form:

"Does Entity X have Authorization Y in the context of Ecosystem Governance Framework Z?"

TRQP queries can ask this question for any authorization of any entity in any ecosystem. Furthermore, because an ecosystem is itself an entity (with its own verifiable identifier), TRQP can be used to query any metaregistry for the recognition and authorization information about that ecosystem.

For the Ayra Metaregistry Network, the Ayra Association defines an Authority Verification Profile, to standardize inter-ecosystem authority queries.[2]

Figure 4 illustrates TRQP queries for both entity recognition and issuer authorization.

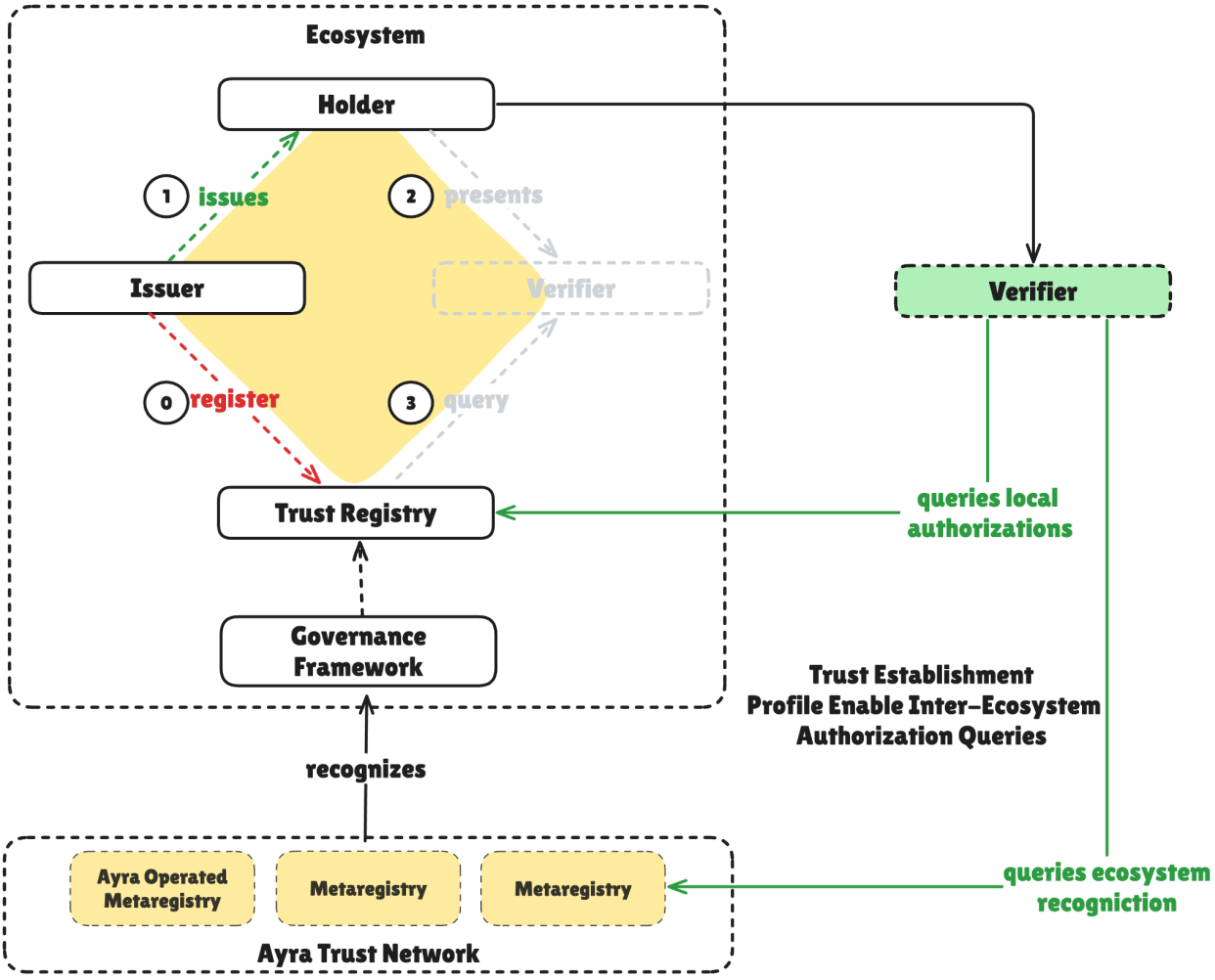

Figure 4 : Examples of queries to perform both ecosystem recognition and entity authorization.

[2] The metaregistry operated by the Ayra Association is called the Ayra Operated Metaregistry.

Operational architecture of the Ayra Metaregistry Network

The metaregistries that serve the Ayra Metaregistry Network are equipped with an interface to access and read the current network state. These interfaces need to expose two sets of capabilities:

1. **Network administrator capabilities** to manage the set of recognized ecosystems. Operations include create, update, and delete operations.
2. **Network resolution capabilities** to read the current state and return a TRQP query result to a consumer.

Details for the exact data models, interfaces, storage choices, and requirements for network operators will be described over various RFC's to enable operators to serve the network. Additional technical and governance policies for operation of these metaregistries will be defined in the Ayra Governance Framework. See Appendix F for a discussion of the technical considerations involved.

Cluster recognition via metaregistries

New or existing ecosystems may converge into a **trust cluster**: a group of ecosystems who align to achieve a shared set of trust objectives. The business case for trust clusters is introduced in the Introduction to Ayra paper. Typically the participants in a cluster will agree on a shared credential family, governance policies, and one or more metaregistries.

Further details on the business and governance purposes of clusters can also be found in the Special Effects of Network Credentials and Ecosystems of Ecosystems Whitepaper.

Technically, cluster recognition is similar to ecosystem recognition but requires the cluster to establish its own metaregistry (or set of metaregistries). These metaregistries must be formally recognized by the Ayra Metaregistry Network. They act as the authoritative recognition bodies for their respective clusters, and each cluster manages the ecosystems within their scope.

Figure 5 is an example of how a cluster would form and then be recognized by the Ayra Metaregistry Network.

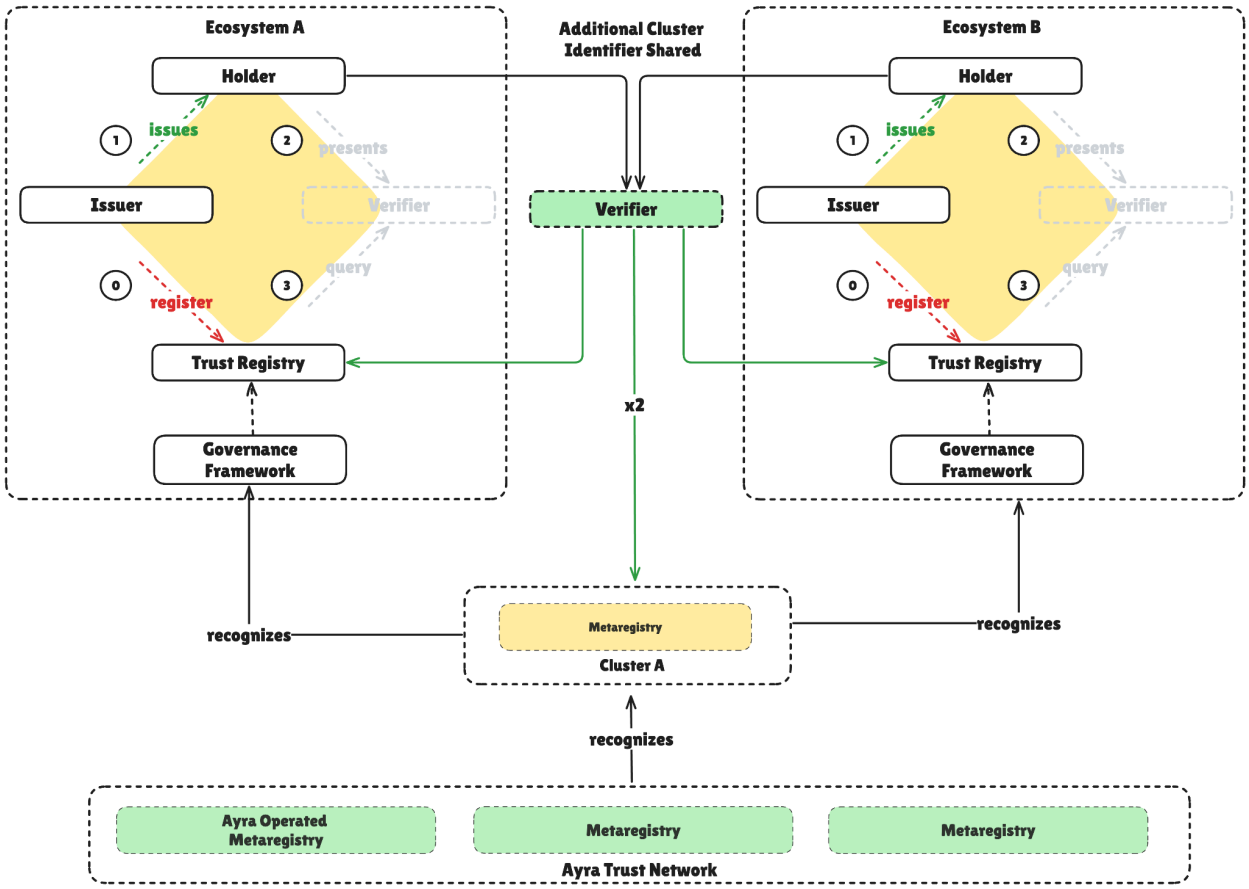

Figure 5: A new cluster being recognized by the Ayra Trust Network

The Ayra Trust Network recognizes clusters as metaregistries of ecosystems, similar in structure to the Ayra Metaregistry Network. Cluster recognition follows the same principles described in Multi-Network Flows. In this diagram, Ayra recognizes Cluster A and Cluster A recognizes ecosystem A and B.

Note that, while Cluster A contains its own metaregistry serving the ecosystems in the cluster, it is not (yet) a metaregistry in the Ayra Metaregistry Network. If that was desirable, Cluster A would first need to meet the requirements in the Ayra Governance Framework and then be provisioned to join the Ayra Metaregistry Network.

How the Ayra Type Catalog assists with semantic interoperability

Inter-ecosystem exchange of verifiable data—including verifiable credentials—presents the same classic semantic interoperability challenges that data integrators have struggled with for years. For example:

1. Verifiers need to know precisely what claims—from what credentials—from what issuers—in what ecosystems can be requested from a holder with a reasonable degree of confidence the holder will be able to respond.
2. Holders need to have a sense of what claims—from what credentials—from what issuers—in what ecosystems are worth obtaining to maximize the value of their digital wallet to the holder's digital life.
3. Issuers need to know what claims—in what credentials—in what ecosystems—will actually produce the most business value to issue.

There is no silver bullet for overcoming these challenges. However, for cross-ecosystem verifiable data exchange, there is general agreement that type catalogues can be a key facilitator. The goal of the Ayra Type Catalogue is to complement other open community efforts, such the Credential Schemas work at the Decentralized Identity Foundation (DIF) and the Credential Catalog built by Fides to provide the Ayra community with:

1. A machine-readable and human-readable repository for registration and discovery of data type definitions, credential schemas, Overlays Capture Architecture (OCA) definitions, and other credential metadata.
2. Usage guidelines and statistics that can help guide technical interoperability and governance choice.
3. Applicable business rules, whether at the ecosystem, cluster, or network-wide levels.
4. Version management of all of the above.

The roadmap for the Ayra Type Catalogue will be primarily guided by business requirements from Ayra Association members, particularly those building trust clusters. Figure 8 illustrates how the Ayra Type Catalogue might assist a verifier with discovery of a credential schema.

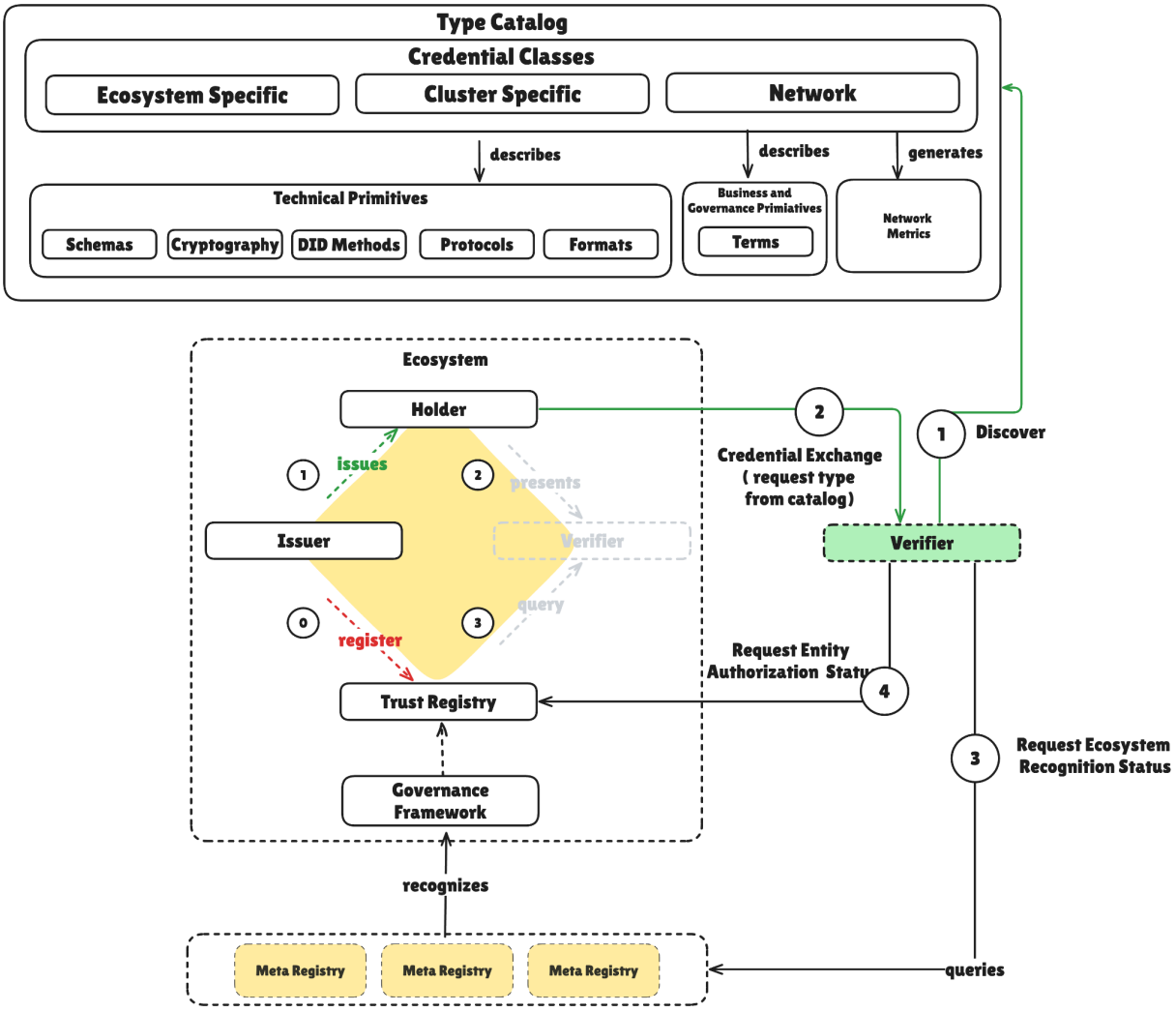

Figure 6: How the Ayra Type Catalog could facilitate credential schema discovery.

At the outset, the primary utility of the Ayra Type Catalogue will be in documenting the Ayra Network Credentials together with credential families designed by the first trust clusters.

The role of Ayra Interoperability Profiles and the Conformance Test Suite

Interoperability profiles are a proven approach to aligning technology stacks across ecosystems. They address divergences in protocol interpretations, feature implementations, and supported data formats, which often create rigid boundaries between ecosystems.

Interoperability profiles are not a new concept. Examples include the OpenID4VC High Assurance Interoperability Profile, the JWT Presentation Profile from Decentralized Identity, and the eIDAS Interoperability Profile, among others. However, a persistent challenge with interoperability profiles is the friction associated with their adoption and integration into existing ecosystems.

The Ayra Interoperability Profiles aim to overcome these challenges by leveraging the inherent value of the trust network. By making deliberate technical choices that align with large-scale adoption patterns and the cluster strategy Ayra Association believes will bring immense value across ecosystems, we believe these profiles will achieve the necessary traction and success for widespread implementation.

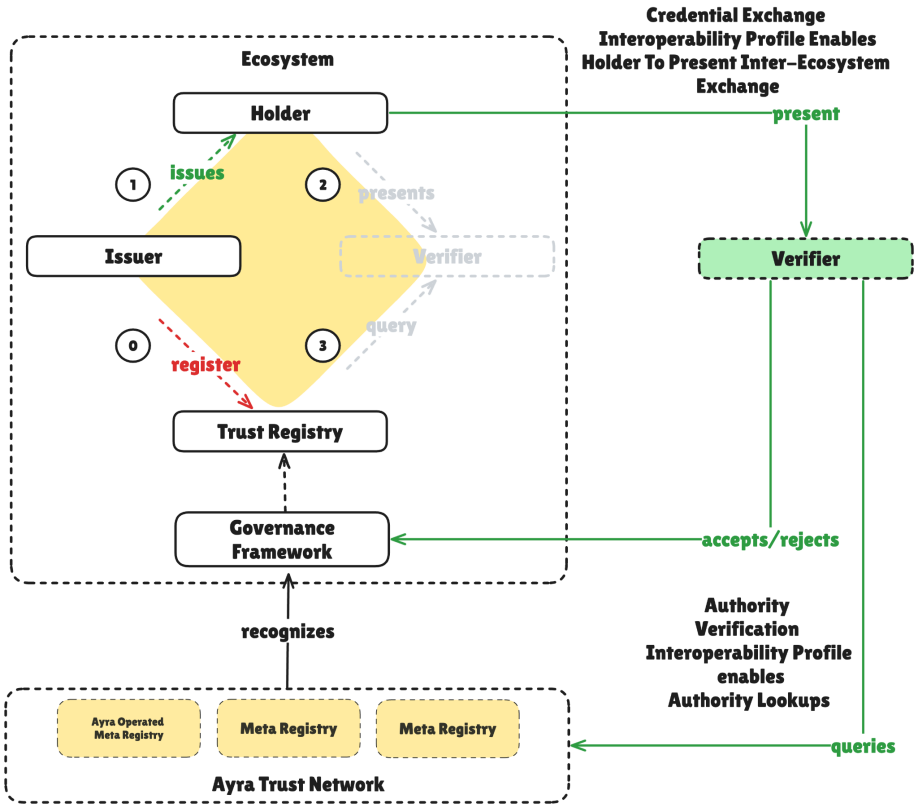

Figure 7 : Three interoperability challenges addressed by Ayra Interoperability Profiles

The two primary Ayra Interoperability Profiles on which the Ayra Association is initially focused are:

1. **Verifiable Credential Exchange Profile** : aligns technical ecosystems against credential exchange.
2. **Authority Verification Interoperability Profile** : align technical requirements for establishing authentication and recognition queries.

While we describe them in detail below, please note that they will continue to mature over an RFC process in collaboration with Ayra Association members.

Verifiable Credential Exchange Profile

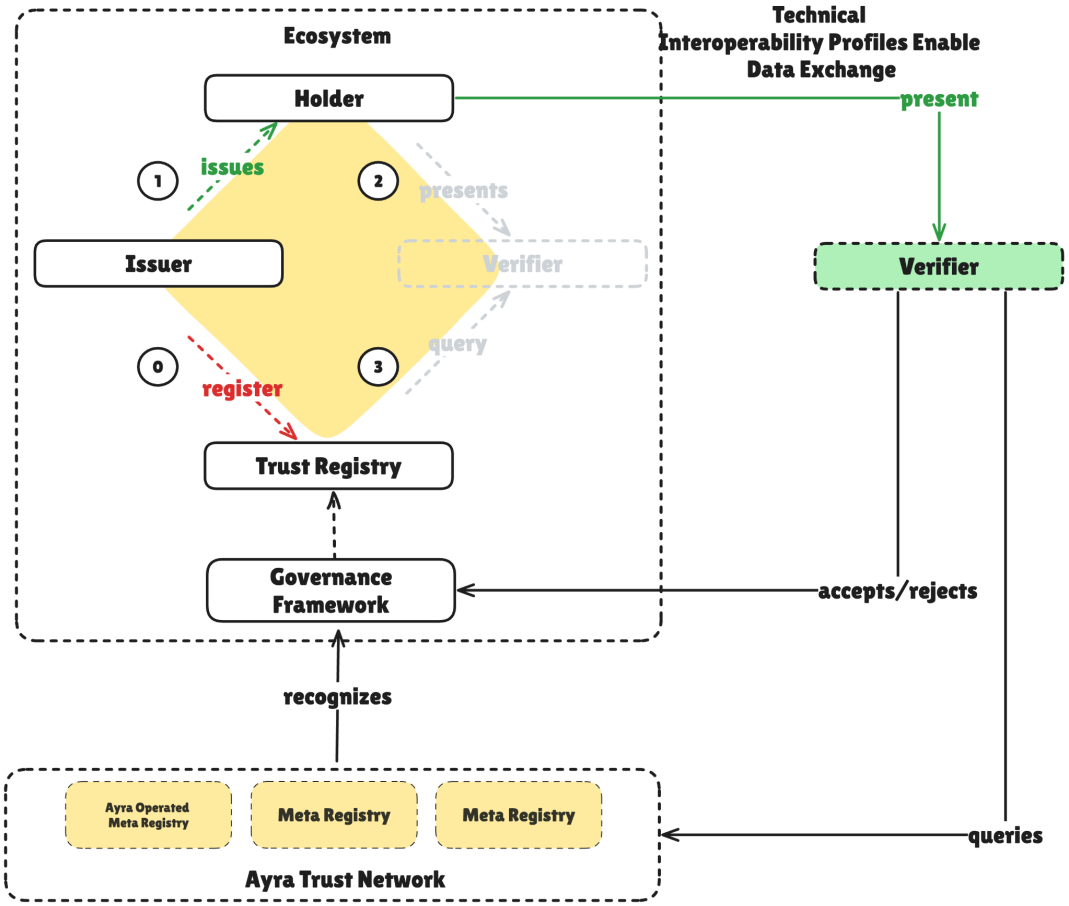

Fig 8 : By aligning against an interoperability profile, the holder and verifier can interact across ecosystem boundaries.

These profiles define the protocols, credential formats, cryptographic mechanisms, and related technical requirements necessary for ensuring interoperability across varying implementations.

Ayra Trust Network will support primarily two profile patterns at the beginning:

- API Communication Pattern : currently focused on an OID based credential exchange pattern.
- Messaging Communication Pattern : currently focused on a DIDComm secure, long lived connection.

For more information about the initial interoperability profiles, please see Credential Exchange Technical Interoperability Profile Details.

Authority Verification Profile

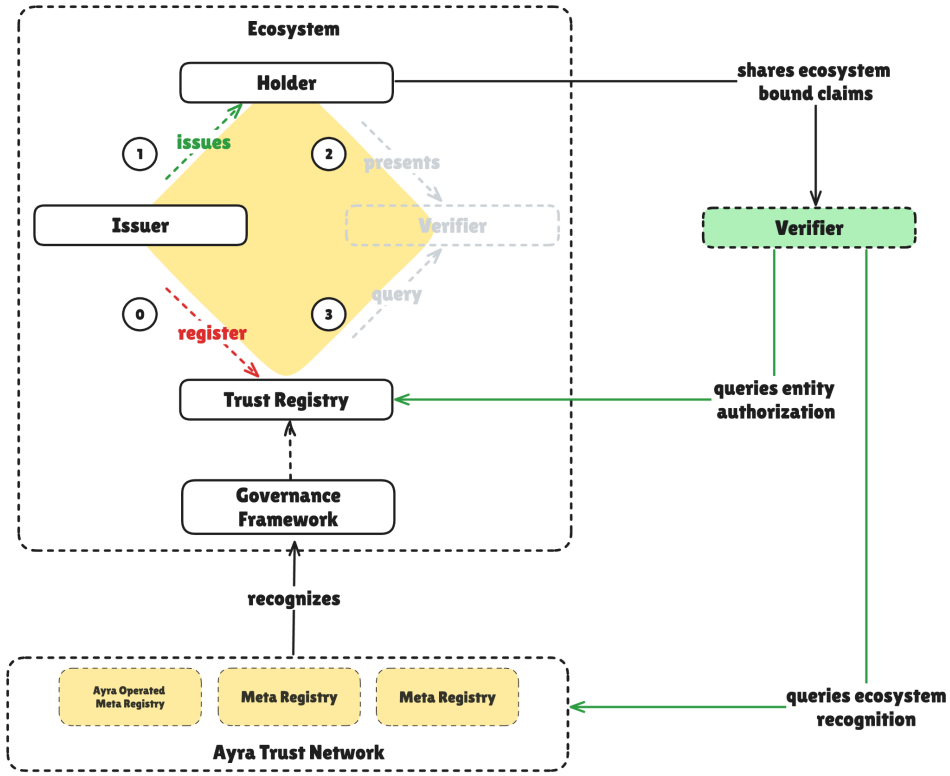

Fig 9 : Authority Verification Profile enables the query of entity authorization and ecosystem recognition.

The Authority Verification Profile focuses on aligned technical requirements for establishing authentication and recognition queries. For a *verifier*, it defines the query procedure to the metaregistry network, to solve the challenge around **ecosystem recognition**. It also enables the query against an ecosystem for **authorization.** For *ecosystem participants*, it defines compatibility requirements for the ecosystem trust registry. For metaregistry operators, it defines the operational protocols to be compliant with the network.

The profile currently leverages the Trust Registry Query Protocol (TRQP) and will mature over time as additional requirements come in.

See the current Appendix B: Authority Verification Profile for more information about the current state of the profile.

Using the Ayra Conformance Test Suite

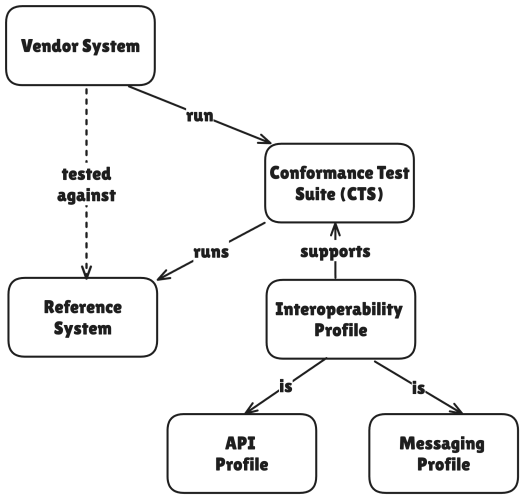

Fig 10 : Systems involved in the CTS

The Conformance Test Suite is a tool designed to validate that systems adhere to the defined interoperability standards.

It serves multiple purposes:

1. **Validation**: Ensures that implementations comply with Ayra's technical specifications.
2. **Consistency**: Reduces discrepancies in how standards are implemented.
3. **Trust**: Provides confidence to stakeholders that certified systems will work together as intended.

The test suite helps to identify and resolve interoperability issues early in the development lifecycle. This proactive approach minimizes the risk of technical misalignment and promotes a more cohesive network ecosystem.

The CTS can be run offline, is developed as open-source software, and is intended to be used by certification bodies. Importantly, the CTS is not a test suite itself. Instead, it acts as a wrapper, utilizing existing open-source test suites that align closely with the specifications they evaluate.

The CTS must accommodate the evolution of profiles over time while minimizing friction and overhead for vendors and system upgrades.

For more information, please see the Appendix D: Conformance Test Suite - High Level Architecture and Appendix E: Sample CTS Roadmap to learn more.

Ayra Metaregistry Network roadmap

The Ayra Association must carefully balance its short-term operational goals with its long-term vision for the Ayra Metaregistry Network. In the near term, the focus is on operationalizing and managing the Ayra Operated Metaregistry to demonstrate tangible value and establish trust among stakeholders. This is represented by the first two phases of the development roadmap in table 4:

Phase	Description
Sandbox	The initial phase where experimental features and technologies are tested in a controlled, isolated environment. The sandbox allows for iterative development, feedback integration, and validation of core functionalities without impacting live operations.
Single Ayra Operated Metaregistry (Staging)	At this stage, the Ayra Association operates a single Metaregistry within a staging environment. This phase focuses on testing the registry's scalability, security, and operational workflows under near-production conditions. It serves as a critical step to refine processes before live deployment.
Single Ayra Operated Metaregistry (Production)	At this stage, the staging environment comprising the Ayra Association operated metaregistry is promoted to production. The focus is on delivering value by enabling trusted data exchange, ensuring robust performance, and meeting the immediate needs of the Arya ecosystems.
Multiple Ayra Operated Metaregistries (Staging)	At this stage, The Ayra Association distributes responsibilities for managing the Ayra Metaregistry Network state to meta registries not operated solely by itself. Interoperability mechanisms are validated under distributed governance frameworks. This requires Ayra Association to have a robust auditing process and set of procedures for accredited organizations to serve the Ayra Metaregistry Network.
Multiple Ayra Operated Metaregistries (Production)	The final stage of maturity where the distributed operation of meta registries is promoted to a production environment. This state emphasizes a shift control, ecosystem collaboration, and scalability while maintaining low operational costs and high trust.

Table 4 : A high level roadmap for the Ayra Metaregistry Network

The overall intent is to evolve the Ayra Operated Metaregistry to deliver enhanced security, greater scalability, and distributed control. This progression will reduce centralized control points, distribute responsibilities across participating ecosystems, and maintain low operational costs as the trust network grows. This phased development strategy aligns with commitment to delivering robust, efficient, and scalable solutions while fostering collaboration and trust across ecosystems.

Ayra Network Credentials

Ayra Network Credentials are defined in detail in the The Special Network Effects of Ayra Network Credentials paper. They serve a different purpose than ecosystem-specific or cluster-specific credentials which are tailored for use within a single ecosystem or across a specific industry, jurisdiction, or other cluster.,

By contrast, Ayra Network Credentials are designed to fulfill nearly universal requirements for establishing digital trust relationships and thus are designed to be issued and accepted across nearly all Ayra-recognized ecosystems. For that reason they are governed at the Ayra Trust Network level by the Ayra Governance Framework.[3]

The technical challenges of network credentials are discussed in the Appendix G: Technical Challenges Of Ayra Network Credentials. They include considerations such as cluster and ecosystem authorization, flexible cryptographic security with post-quantum readiness, and projection mapping to support multi-languages and formats.

[3] Ayra will likely need to support additional metaregistry functionality to authorize clusters and ecosystems to issue and/or verify Ayra Network Credentials.

Multi-Network flows

The Ayra Trust Network is envisioned as one of many potential trust networks, each varying in scale and not mutually exclusive within an ecosystem. It recognizes the need for interoperability with other trust networks.

In the diagram below, another cross-ecosystem trust network spans ecosystems B and C, while the Ayra Trust Network spans ecosystems A and B. This illustrates the ability of multiple trust networks to interoperate, supporting a diverse array of ecosystems simultaneously.

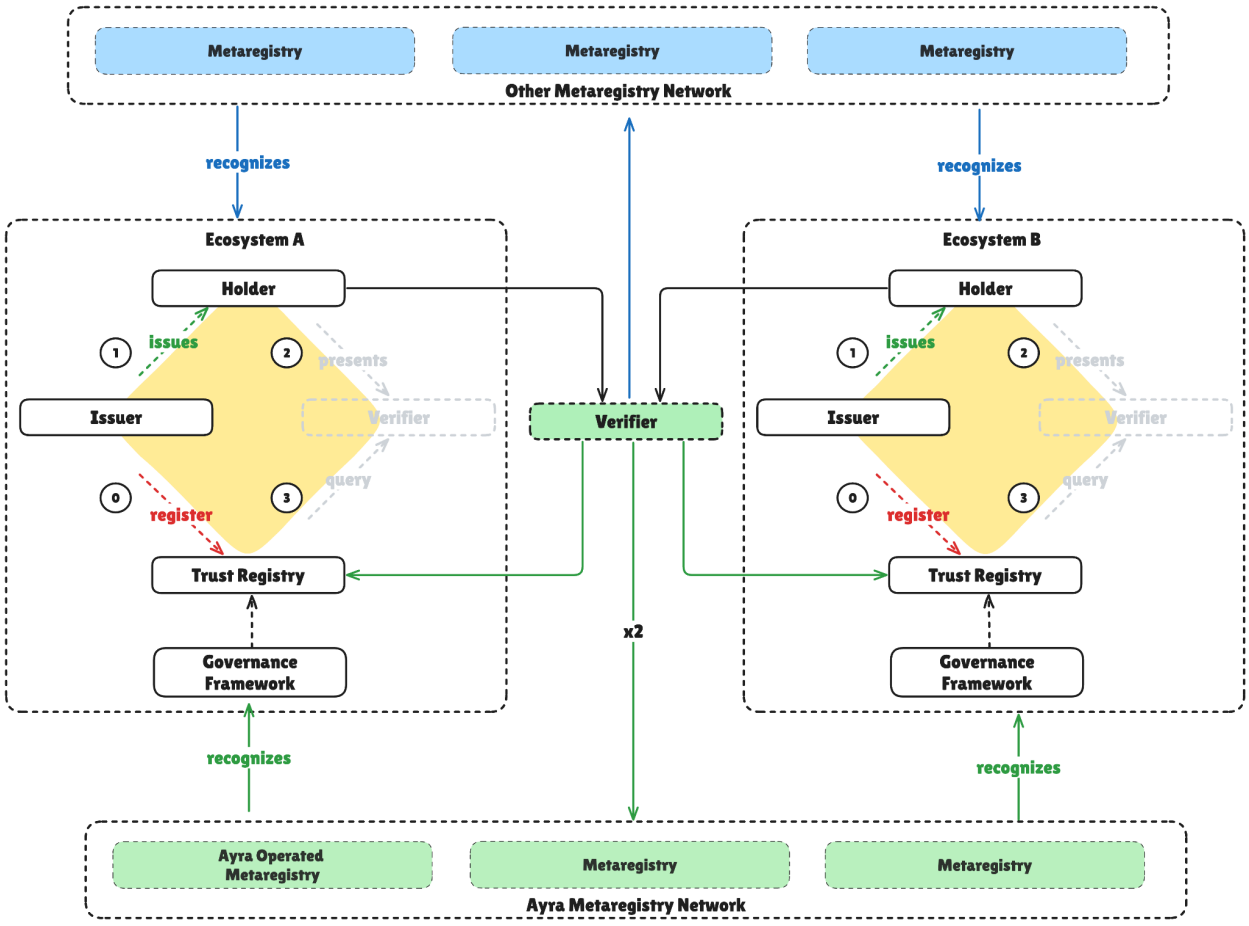

Figure 11: The diagram above illustrates two ecosystems and two trust networks, with Ayra as one of the trust networks. Other trust networks may also exist outside of Ayra Metaregistry Network.

Trust networks evolve into heterarchical model

Acceptance and recognition of another trust network functionally means supporting recognition of another set of metaregistries. This is an interface provided by the TRQP.

The Ayra Network forms a heterarchical relationship with other trust networks. This model emphasizes the interconnected nature of diverse trust networks, where the Ayra Network collaborates and interoperates with others while maintaining its unique governance and operational framework.

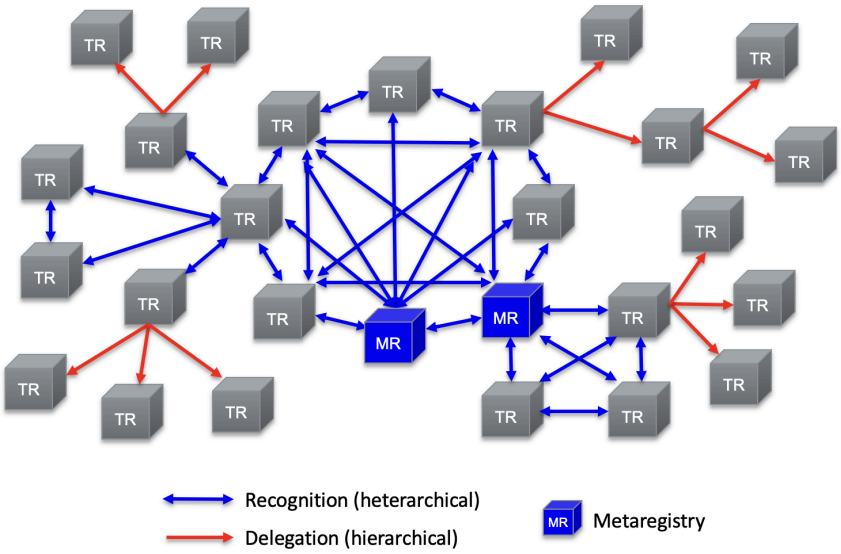

Figure 12: The heterarchical design pattern of the Ayra Trust Network

For more details, refer to the [Ecosystems of Ecosystems paper].

Additional scenarios for the Ayra Trust Network

The Ayra Trust Network is not limited to credential exchange; it supports diverse verification models across ecosystems, enabling trust and secure data interactions. These scenarios highlight the network's ability to manage complex interactions involving verifiers, ecosystems, and signers, demonstrating its utility in cases where simple credential exchange is insufficient. Below are two examples that showcase its capabilities:

1. **Document Signing and Verification**:
    - A verifier ensures the authenticity and integrity of signed documents by validating the signature and confirming the signer's status within the issuing ecosystem. The Ayra Trust Network simplifies this process by enabling checks on the signer's registration and the ecosystem's recognition, ensuring secure cross-ecosystem verification.
2. **Verifier Authenticity Check**:
    - During an interaction, a holder may need to confirm the authenticity and trustworthiness of a verifier. Using the Ayra Trust Network, the holder can verify whether the verifier is registered and recognized within the appropriate ecosystem, ensuring the interaction is secure and compliant with governance standards.

Further exploration of these use cases may be explored in future papers.

Next steps

The Ayra Association is now poised to deliver the foundational elements of the first trusted data economy within the Trust Network. Our immediate focus is on creating a sandbox environment equipped with technologies designed to enable trusted cross-ecosystem data exchange.

The initial set of technologies outlined above represents the critical tools necessary to establish the foundational network effects required at a limited scale. These technologies provide the essential infrastructure to facilitate secure, interoperable interactions between ecosystems.

As we gather insights from sandboxed experiments and real-world implementations, we aim to iteratively refine and expand these capabilities. Our vision is to evolve from this initial stage into a robust, globally scaled network, facilitating billions of high-value transactions across interconnected ecosystems. This iterative approach ensures that the Ayra Trust Network grows sustainably while remaining aligned with the principles of trust, scalability, and value creation.

Future considerations

While this paper focuses on trusted data interactions, it is important to recognize that this alone may not be sufficient to drive long-term value creation. Market dynamics will ultimately determine whether the Trust Network creates enough value to sustain its growth and adoption.

To enhance the **Trust Network**, various ideas have been proposed, such as integrating payment rails or other features to add value to the ecosystem. While these concepts are intriguing, their requirements are not yet fully understood. As such, Ayra Association's focus must remain on the immediate next steps of trusted data exchange.

Future considerations must balance ambition with practicality, ensuring that the Trust Network remains focused on its core mission while leaving room for strategic evolution.

Conclusion

This paper centers primarily on the pressing challenge of trusted data exchange within and across ecosystems. However, the scope of the Ayra Trust Network may be broader if required by its members to achieve value. While this focus may appear limited, the scale and complexity of the challenges Ayra Association seeks to address are monumental.

We are confident, however, that with the collective input from our members and the expertise of the dedicated team we have assembled we can effectively tackle these challenges. Our solutions will not only meet the high standards set by our core principles but will also deliver robust outcomes aligned with the evolving needs of the trust network. Potential areas of future value creation include, but are not limited to, credential exchange payment rails and mechanisms for ecosystem and credential discovery.

Finally, we extend our deepest gratitude to our members for their significant contributions, which have been instrumental in advancing our mission. Your collaboration and insights are foundational to the progress we continue to make together.

Appendices

Appendix A: Credential Exchange Technical Interoperability Profile details

The table below outlines the initial credential exchange interoperability profiles for the Ayra Trust Network. These profiles may evolve as the system matures. However, DIDComm and OID4VC are expected to remain the core pathways for the next few years, with potential upgrades.

Component	**Messaging Based Profile v0.0.1**	**API Based Profile v0.0.1**
Abstract Data Model	VCDM 1.1	SD-JWT VC
Credential Format	LDP-VC	SD-JWT VC
Data Representation or Encoding	JSON-LD	JSON
Credential Exchange and Lifecycle Standards	• DIF Presentation Exchange Aries RFC 0453 (Issue Credential v2) • RFC 0454 (Present Proof v2)	• OID4VCI (OpenID for Verifiable Credential Issuance) • OID4VP (OpenID for Verifiable Presentations)
Transport and Credential Exchange Protocols	DIDComm v1 with Aries RFC 0023 (DIDExchange)	• OID & OID4VCI/VP HTTPS-based REST endpoints • Data Integrity and Cryptographic Assurance
Proof Standard	LD-Proofs	SD-JWT Proofs
Cryptographic Signature	Ed25519 Signature 2018	ES256 (P-256 curve)
Key Management and Identifiers (for Issuers)	Decentralized Identifiers (did:key, didwebvh, did:web)	Decentralized Identifiers (did:webvh)

Key Management and Identifiers (for Holders)	Decentralized Identifiers (did:key)	Decentralized Identifiers (did:key)
Revocation Mechanism	Bitstring Status List	Token Status List

Future profile enhancements may include, depending on market and technology readiness:

- **Abstract Data Model:** Verifiable Credential Data Model 2.x
- **Credential Format:** SD-JWT or SD-JWT VC (For Message Based)
- **Transport and Credential Exchange Protocols:** DIDComm v2 (For Message Based)
- **Key Management and Identifiers:** did:webvh, selection of DID Traits

Appendix B: Authority Verification Profile details

The authority verification profile describes the required procedures and process to technically answer the following questions:

- **Ecosystem Governance Framework Acceptance :**
  - Is your ecosystem governance framework compatible with mine?
  - Are our business and governance terms aligned and acceptable to me (as an individual or organization)?
- **Entity Authorization within the Ecosystem Governance Framework**:
  - Is the issuer of the data authorized within your governance framework?

The following describes a TRQP profile leveraging DIDs and HTTP. This profile is being refined in collaboration with Trust Over IP and may evolve over time.

Component	**Authority Verification Profile API Based**
Trust Establishment Protocol	Trust Registry Query Protocol (TRQP)
Ecosystem Identifiers	Decentralized Identifiers (DIDs)
Trust Registry Identifiers	DIDs
Trust Registry Metadata Model	JSON
Signing Envelope	JSON Web Signatures (JWS)
Transport	HTTP(s)
Encoding	JSON
API Pattern	RESTful
Ecosystem Governance Framework Resolution Mechanism	HTTP(s) Human Readable
Authorization Data Model	HTTP(s) resolvable URI
DateTime Format	ISO8601.
Protocol Specification	Described here
Reference Propagation Method	A-priori verifiers will configure their system to check a pre-aligned set of authority registries.
Ecosystem Governance Framework	DIDs with Service Profiles

Model	
Authorized MetaRegistries Lookup	TBD

Appendix C: Ecosystem Recognition procedure

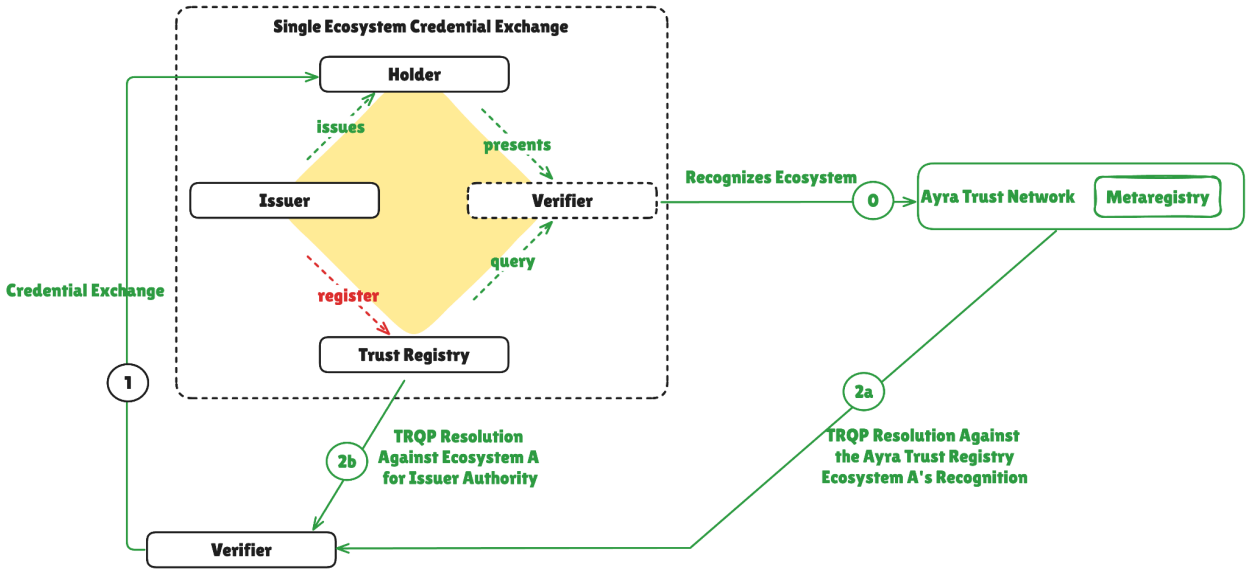

Figure 7: This example demonstrates a verifier undergoing the Trust Establishment process using the TRQP Registry Query Protocol following credential exchange.

The figure above describes the process for ecosystem recognition. The sequence is as follows:

1. **Ecosystem Recognition:** Ecosystem registers with Ayra Association and is recognized by the Ayra Trust Network.
2. **Credential Exchange**: As a pre-trust establishment operation, Credential Exchange takes place, during which the verifier performs cryptographic verification on the payload. In this credential exchange, propagation of the data around ecosystem governance framework and network to query may be exchanged. Due to the high degree of optionality to achieve this propagation of information (such as a priori or in the credential), the exact mechanics of this will be described in future RFC's.
3. **Step 2a – Inter-Ecosystem Recognition Check:** Verifier queries one of the metaregistries in the valid set authorized by the Ayra Trust Network via TRQP to understand the recognition status of Ecosystem A. For optimization purposes, these results may be cached.
4. **Step 2b – Intra-Ecosystem Authorization Verification:** Issuer Authorization Status is resolved via the Trust Registry Query Protocol against Ecosystem A.

Appendix D: Conformance Test Suite - high level architecture

The first version of the CTS is a full-stack application with a separate frontend and backend, designed for local use by technical end users. Both components are written in TypeScript. The frontend uses the Next.js framework (v15), while the backend uses the Express framework. Communication between the two occurs via RESTful HTTP APIs and WebSockets, with the latter providing real-time logging and status updates for test runs.

The backend persists data to a Postgres SQL instance using the Prisma library.

The application adopts a contract-first development approach using ts-rest, enabling a shared, type-safe API contract. This ensures that compilation fails if the API is not correctly implemented.

Integration with the Aries Agent Test Harness is achieved by running it as a local batch job through its `manage` script. The OpenID Conformance Suite integrates directly via API calls and requires it to be running in the background.

> Planned enhancements aim to eliminate the need for manual actions by end users placing a system under test. These improvements include automating the download and execution of required test suites in the background as needed.

The alpha version supports creating system objects, selecting profiles for testing, and running multiple test runs with basic conformance reporting. The Aries Agent Test Harness integration currently supports service verification only, with further development needed to support wallet testing. Conversely, the OpenID Conformance Suite supports wallet testing but requires additional work to enable service testing on the verifier side.

The general principle for integrating test suites is to use a canonical model managed by the CTS to capture the system-under-test configuration. For each system, a profile configuration is created, containing the specific data required to run tests for that profile. For instance, testing OID4VCI/VP requires different parameters than testing DIDComm, which are defined at the profile configuration level (as illustrated in the entity relationship diagram). With a profile configuration in place, the tool can initiate test runs against the system under test. It tracks progress, provides a summary of results, manages test run failures, and reports errors to the end user. Upon successful completion, the system's conformance status is reported for the corresponding profile.

For the AATH, results are processed from disk by parsing an output JSON BDD log file generated by the Behave Framework and converting it into a canonical results model. For the OID Conformance Suite, the log APIs are queried for the specific module or test run, and the retrieved data is processed into a canonical model.

Appendix E: Example CTS roadmap

The following table outlines capabilities required for the initial release and those envisioned for the long-term roadmap. Not all features will be supported in the initial version of the CTS. Over time, additional capabilities will be introduced, including support for certification processes conducted by authorized third parties in controlled, lab-like environments.

The table provides a capability matrix with classifications indicating the expected availability of each feature. It uses the terms initial, next/following, and future to suggest priority and sequencing without committing to specific dates, as resource allocation has yet to be finalized.

Capability	Initial	Next	Future
Deployment Topology and Execution Model			
Local and Offline Testing (on standard developer hardware)	✅		
Manual Execution (through a GUI, by a developer)	✅		
Automated Execution (CI/CD)		✅	
Cloud Hosted (Self-Service)			✅
Authorised Certification Service in Lab Environment			✅
Conformance Focus			
Verifiable Data Exchange Interoperability	✅		
Network Credential Support		✅	
Trust and authorisation attestation		✅	
Test Suite Integration			
Aries Agent Test Harness	✅		
OpenID Conformance Suite	✅		
Trust Registry Query Protocol*		✅	
Profile Support			
Initial API-Centric (OID4VCI/VP, SD-JWT VC)	✅		
Target API-Centric (As per initial with BBS+ and TRQP)			✅

Capability	Initial	Next	Future
Initial Message-Centric (DIDComm v1, LDP-VC)	✅		
Target Message-Centric (DIDComm v2, SD-JWT, VCDM2)			✅
Versioning and upgradeability	✅		
User Experience and Interface			
System configuration	✅		
Test run management, multiple profiles	✅		
In-app Conformance reporting	✅		
Exportable reporting		✅	
Interoperability Validation Dashboard		✅	
Historical Conformance Visualisation			✅
Conformance Attestation			
Text based report	✅		
Verifiable credential		✅	
Role/Service Type Support			
Holder & Mobile Wallet - Presentation	✅		
Relying Party & Service/Agent - Verification	✅		
Issuer & Service - Issuance			✅
Holder & Mobile Wallet - Credential Acceptance			✅

Appendix F: The Ayra Operated Metaregistry

In the alpha version of the Ayra Operated Metaregistry, the backend was written in Golang, selected for its ability to handle the high concurrency needs anticipated for the registry, as well as its efficiency in writing concurrent code.

The frontend, developed in TypeScript using Next.js, was chosen due to the team's familiarity with the framework and its rapid prototyping capabilities. It features a gRPC-based set of APIs and supports the TRQP Swagger API for HTTP resolution.

A pre-storage operation ensures signed objects meet non-tamperability requirements; this functionality is currently a custom implementation. Key management for signing is kept simple, utilizing an Ed25519 key generated at startup. The backend interface supports multiple storage types. Initially, a BoltDB (key-value) store was implemented, with a Postgres implementation underway at the time of writing. Authentication is handled via an API key layer.

Client runs both the GRPC and HTTP services. A frontend was built using NextJS and Typescript. It uses zustand for state management. The UI shows only a few core pages:

1. A page that lists ecosystems of ecosystems
2. A page that describes a set of ecosystems bound to the ecosystem of ecosystem

The service also runs the Ayra Operated Trust Registry, which supports the Ayra Association member management system.

Appendix G: Technical Challenges for the Ayra Metaregistry Network

Executing the vision of a neutral, global, and scalable trust network of metaregistries will require the Ayra Association to address several challenges. While we outline some of these challenges below, this list is not exhaustive.

- **Network Metaregistries** must be able to support the technical requirements of the Ayra Associations governance system.
    - **Process Management:** The registries must be able to support process level management and enforcement determined by the governance teams. Since the governance process will evolve, so will the registry requirements.
    - **Control Points:** The Ayra Trust Network must maintain a level of control in managing its state. We envision stages of control as the trust network scales and anticipate that operational control will become more distributed as the trust network matures.
    - **Transparency:** It will have to define the boundary conditions of what should be public and what should be private. It is likely that the Arya trust metaregistries will have auditability requirements, in which case appropriate mechanisms must be developed to allow for auditing among the permitted parties.
- **Near Term Execution vs. Long Term Vision:** The Ayra Trust Network metaregistries may need to make pragmatic, temporary technical choices in the short term, which could conflict with long-term requirements. Therefore, the Ayra Trust Network must carefully balance delivering near-term value with maintaining the flexibility needed to achieve its long-term goals.
- **Globally Equal Access:** The infrastructure must operate on an international scale with minimal infrastructural bias. For example, ICANN facilitates 13 root identities (12 of them independent) distributed globally, supported by over 1,500 servers. This setup enhances the likelihood of equitable DNS resolution across geographical regions. Similarly, the Ayra Trust Registry may, in time, need to adopt a distributed delivery model to achieve comparable scalability and fairness.
- **Security:** The security of the Trust Registry is paramount. Over time, SOC 2 and SOC 3 audits may become necessary to ensure compliance and reliability. A key ceremony will likely be conducted to support key generation, and both the ceremonies and cryptographic methods are expected to mature as the Trust Registry evolves.
    - To remain resilient, the Trust Registry may need to adopt advanced signing algorithms, such as Post-Quantum Cryptography Schemes, which are increasingly becoming regulatory requirements in some regions. Furthermore, a sophisticated understanding of attack vectors and threat models will be essential as the Trust Registry transitions into full operation.
- **Scalability:** The Ayra Trust Registry must account for scalability requirements as the organization, its members, and the trust network grow. These requirements extend

beyond infrastructure to include managing and administering the overhead associated with entries in the registry. Without careful attention to operational scalability, the costs of creating and updating the registry could become prohibitively expensive.
    - For example, 95% of ICANN's operating budget comes from registrar operating fees.[4] A similar challenge could arise for the Trust Registry if operational overhead is not effectively managed.
- **Change Capabilities**: The Ayra Metaregistry Network must have robust change capabilities, allowing it to support the coexistence of old and new service versions until the former are deprecated. This ensures seamless transitions, avoids disruptive migrations, and provides clear policies and support for managing upgrades across the trust network.
- **Privacy :** The Ayra Trust Network Metaregistries must uphold the privacy requirements of network participants while maintaining a balanced approach to meet the overall needs of the network.

4 https://www.icann.org/en/system/files/files/registry-registrar-level-fees-adjustment-30oct24-en.pdf

Appendix H: Technical Challenges Of Ayra Network Credentials

Network credentials play a pivotal role in establishing trusted interactions across the Ayra Trust Network. To ensure their efficacy and alignment with the broader ecosystem, the following requirements and considerations have been identified:

1. **Governance by the Ayra Association:** Network credentials must be governed by the Ayra Association, which will define and maintain the authoritative list of issuers.
2. **Support for Multilingual and Multidomain Projection:** As the Ayra ecosystem expands, network credentials will likely need the capability to project across multiple languages and domains. The **Overlay Capture Architecture (OCA)** is a strong candidate to facilitate this adaptability, offering a framework for multilingual and multidomain representation.
3. **Adoption of Widely Available Credential Formats:** To maximize accessibility and interoperability, network credentials should prefer widely adopted credential formats. This approach will simplify implementation and ensure compatibility across diverse systems and platforms.
4. **Alignment with Ayra Trust Network's Technical Interoperability Profile:** Network credentials must be technically interoperable with the Ayra Trust Network's interoperability profile. This requirement ensures seamless data exchange, enabling ecosystems and clusters to interact with confidence.
5. **Support for Advanced Privacy Features:** In the future, network credentials may need to incorporate advanced privacy-preserving techniques, such as **Selective Disclosure** and **Zero-Knowledge Proofs (ZKPs)**. These methods would enhance data minimization and protect sensitive information during credential exchange.
6. **Inclusion of Trust-Establishing Information:** Network credentials must include the required metadata and information to facilitate the trust establishment process effectively. This could include issuer details, credential versioning, and cryptographic proofs to verify authenticity and validity.
7. **Flexible Cryptographic Security with Post-Quantum Readiness:** Network credentials must be designed with flexible cryptographic security to accommodate evolving threats. This includes the ability to eventually transition to **post-quantum cryptographic algorithms**, ensuring long-term resilience against quantum computing threats while maintaining current security standards.

Appendix I: Trust Registry Query Protocol

The Trust Registry Query Protocol (TRQP) is a specification currently in implementers draft at Trust Over IP. The protocol serves to provide a simple interface to enable querying of systems of record that provide the information that drives a trust registry.

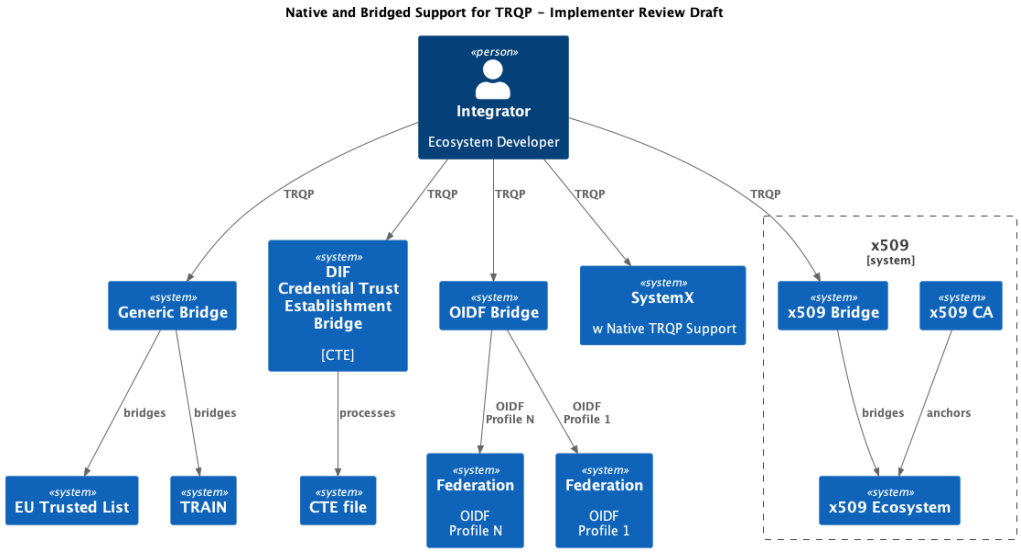

Figure 14: The TRQP is an inter-ecosystem trust protocol that bridges into various intra-trust ecosystems.

The Trust Registry Query Protocol (TRQP) addresses two fundamental questions that enable the goals of the Trust Establishment Interoperability Profiles to be possible:

- "Does Entity X have Authorization Y within the context of Ecosystem Governance Framework Z?"
- "Is Ecosystem X recognized for Y for Ecosystem Governance Framework Z"

For instance, in the credential exchange scenario described in the first section, the Trust Registry Query Protocol (TRQP) enables the resolution across ecosystems for the authorization question:

"Is Issuer X authorized to issue Credential Y under Ecosystem Z?"

Trust Registry vendors within the Ayra Trust Network will need to implement a bridge between their intra-ecosystem framework and the TRQP. The TRQP is NOT meant to replace an existing intra-trust framework, such as Open ID Federation, X509 Chains, EBSI Trust Chains, TRAIN, or others. The TRQP is meant to be a bridge across frameworks and is an *inter-trust framework*.

As of today, the TRQP specification is moving toward an abstraction layer, which is instantiated via profiles. The Ayra Trust Network will need to support a TRQP profile, which is described in more detail Appendix B: Authority Verification Profile.

Metaregistries in the Trust Network must be able to support the TRQP to be technically compliant with the network.

- All Ayra registries on the trust network will support the TRQP.
- The TRQP does NOT replace an intra-ecosystem trust framework. It is a complement.
- The TRQP is a bridge across various trust frameworks and is agnostic to a particular intra-trust method.
- The TRQP does NOT specify how to develop an inter-trust bridge for a particular ecosystem.
- The TRQP is meant to answer one question: "Does Entity X have Authorization Y, in the context of Ecosystem Governance Framework Z?"

Appendix J: Challenges With Interoperability Profiles

Developing a strategy for interoperability profiles is complex and involves overcoming numerous challenges. Below is a list of considerations currently under discussion, to be addressed through future Request for Comments (RFCs) with members.

- **Versioning**: Interoperability profiles will evolve over time due to a range of factors. Advances in technology, such as the adoption of new cryptographic algorithms like post-quantum standards, and the development of credential formats with enhanced capabilities, such as selective disclosure or unlinkable revocation using zero-knowledge proofs, will drive updates to these profiles. Regulatory and compliance changes, including updates to privacy laws like GDPR or the introduction of new jurisdictional standards, will also necessitate modifications. Additionally, performance and security considerations, such as addressing vulnerabilities in older profiles or implementing optimizations for improved efficiency, will play a crucial role in the ongoing maturation of interoperability profiles.
- **Machine Readability** : Machine readability is a critical aspect of ensuring seamless data exchange and interaction across ecosystems in the Ayra Trust Network. By enabling systems to interpret, process, and act on data without human intervention, machine-readable formats enhance efficiency, accuracy, and scalability in trusted data interactions. A well-designed machine-readable framework ensures that credentials, policies, and metadata can be uniformly understood and processed by diverse systems. This involves adopting standardized data formats, such as JSON-LD or CBOR, which are both lightweight and compatible with modern data exchange protocols. Machine-readable formats must also support extensibility, allowing for the integration of new features, such as selective disclosure, revocation statuses, or additional metadata, without disrupting existing functionality.
- **Selection Is Challenging** : To ensure adoption and long-term relevance, Ayra Association and its members must carefully select profiles that are aligned with the strategic roadmaps of existing vendors while addressing pressing needs such as privacy and data sovereignty requirements for regions like the European Union. This alignment is critical for fostering trust among stakeholders and maintaining the trust network's longevity.