ayra

trusted relationship network

The Special Network Effects of Ayra Network Credentials

A White Paper from the Ayra Association

https://ayra.forum/

Version 3.02
20 February 2025

Drummond Reed
Darrell O'Donnell
Andor Kesselman
Dave Poltorak
Jo Spencer
John Phillips

Audience and Purpose

This white paper is written for Internet professionals of all kinds—CIOs and CISOs; security, privacy, and trust architects; policy experts; product managers; developers—who want to understand why a small set of carefully designed digital credentials designed for the Ayra Trust Network have extraordinary adoption potential due to their unique network effects.

Abstract

The mission of the Ayra (eye-rah) Trust Network is to enable global interoperability of verifiable data—especially *verifiable digital credentials*—across digital trust ecosystems of any size, type, or location. Those credentials will fall into three categories: 1) **ecosystem-specific credentials** that are designed only for use within a single ecosystem, 2) **cluster-specific credentials** that are designed to work across the group of ecosystems participating in a trust cluster; and 3) **Ayra Network Credentials** that are explicitly designed to be issued and accepted across any Ayra-recognized ecosystem that needs them.

Ayra Network Credentials follow seven design principles that uniquely apply to digital credentials intended for nearly universal adoption: global interoperability, global governance, simplicity, extensibility, privacy preservation and progressive disclosure, "minimum viable friction" for acceptance, and—most importantly—they must be carefully designed as a family.

The four foundational credentials in the Ayra Network Credential family are: 1) **Organization ID** ("Org ID"—for legal entities), 2) **Community ID** (for any other type of group that is not a legal entity but still needs verifiable trust relationships), 3) **First Person Credentials** (privacy-preserving proof of personhood for individuals), and 4) **Verifiable Relationship Credentials** (proofs of verifiable trust relationships that underpin First Person Credentials).

If these four credentials are very carefully designed together—in Ayra Network Credential Projects and Working Groups hosted by the Ayra Association—they can produce not just one but *four* compounding network effects. These network effects have the potential to catapult adoption of open standard digital wallets and digital credentials into the mainstream.

Recommended Pre-Reading

These two papers are recommended background for this paper:

Introduction to Ayra (7 pages): ➤ Why has digital trust eroded so badly? ➤ Why is this such a threat to AI? ➤ How the "friend-of-a-friend" pattern works; ➤ How credit card networks solved the acceptance problem; ➤ How Ayra is and is not like a credit card network ➤ What is a trust cluster? ➤ What are the first trust clusters that are forming? ➤ How do I get started building the trust cluster I need?

The Ecosystem of Ecosystems Model for Decentralized Digital Trust Infrastructure (19 pages): ➤ Interoperability challenges of digital trust ecosystems; ➤ Why the Ayra Trust Network follows a heterarchical "ecosystem of ecosystems" model; ➤ How this differs from the hierarchical model of DNS; ➤ The special role of Ayra trust clusters.

Recommended follow-up reading:

Ayra Technical White Paper (50 pages): ➤ Core technical architecture of the Ayra Trust Network; ➤ The ToIP Trust Registry Query Protocol (TRQP); ➤ Ayra Interoperability Profiles ➤ The Ayra Conformance Test Suite (CTS); ➤ The Ayra Type Catalogue; ➤ The Ayra Technical Working Group.

Table of Contents

Introduction **5**
The 7 Design Principles of Ayra Network Credentials **7**
#1: Global Interoperability 7
#2: Global Governance 7
#3: Simplicity 8
#4: Extensibility 8
#5: Privacy Preservation and Progressive Disclosure 8
#6: “Minimum Viable Friction” for Acceptance 9
#7: Designed as a Family 10
The Ayra Network Credential Family **10**
Organization ID (“Org ID”) Credentials 11
Community ID Credentials 12
First Person Credentials 12
Verifiable Relationship Credentials (VRCs) 14
Business VRCs 15
Community VRCs 16
Personal VRCs 16
The Special Network Effects of Ayra Network Credentials **18**
#1: The Trust Network Effect 18
#2: The “Zero-to-Hero” Network Effect 19
#3: The First Person Network Effect 20
#4: The Trusted Channel Network Effect 20
Ayra Network Credential Projects **21**

Acknowledgements

The authors would like to thank the many members of the Ayra Association who contributed to this paper, and in particular representatives of the Member Advisory Council and the Ayra Ambassadors. This represents a collective effort by the entire community.

Introduction

The mission of the Ayra Trust Network is to enable global interoperability of verifiable data—especially *verifiable digital credentials*—across digital trust ecosystems of any size, type, or location. By interoperability, we specifically mean both of the following:

- A relying party (a.k.a. verifier) in one ecosystem can verify that the issuer of a credential in a different ecosystem was authorized to issue that credential.
- A holder of a credential issued in one ecosystem can verify that a relying party in a different ecosystem is authorized to request that credential.

Over time, these basic patterns will apply to thousands of different digital credentials that relying parties will need to verify for countless use cases in business, government, and social interactions. Figure 1 illustrates how these credentials fall into three functional categories:[1]

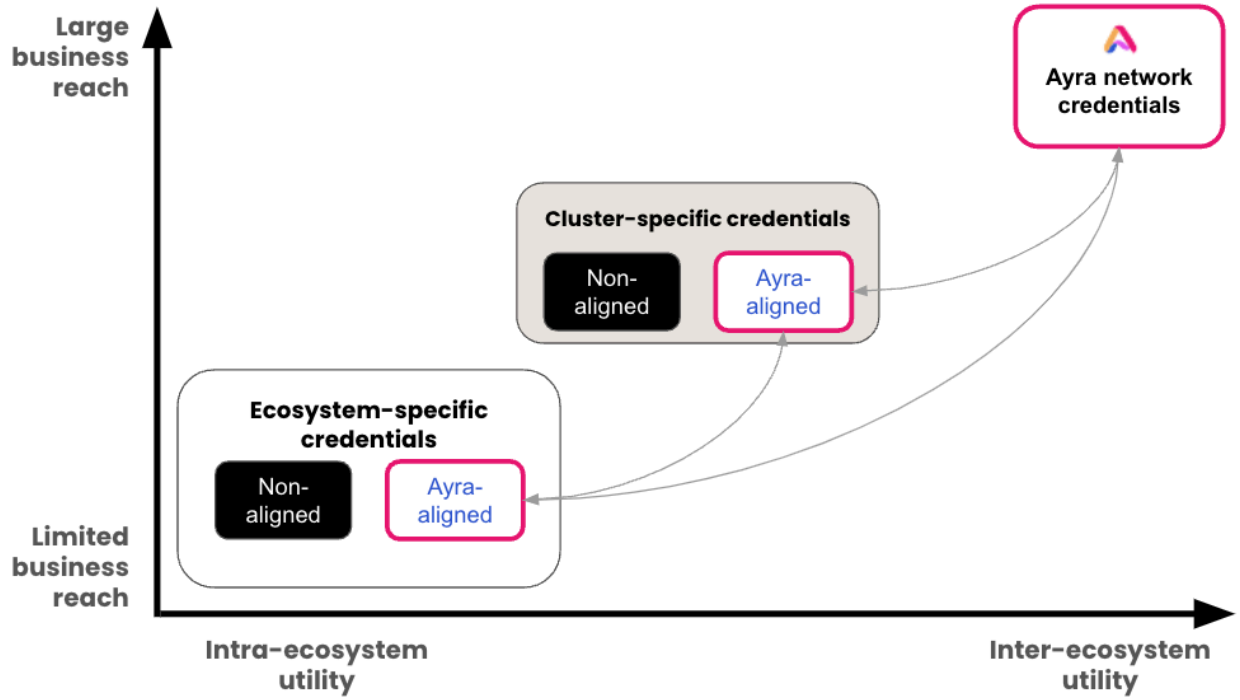

Figure 1: The three functional categories of credentials supported by the Ayra Trust Network

Moving from the narrowest to the broadest scope in figure 1:

1. **Ecosystem-specific credentials** (ESCs) are designed and governed for use primarily within a single digital trust ecosystem. This does *not* mean ESCs only have value in that ecosystem—they may still be accepted by relying parties in other ecosystems. However, that extra value is accidental *unless* ESCs are intentionally designed to work

[1] Credit for this diagram: Jo Spencer and John Phillips of Sezoo Digital

with other credentials in the Ayra network. This is what it means to be "Ayra-aligned".[2] *Examples*: *city parking pass credentials, coffee loyalty credentials, university alumni credentials.*

2. **Cluster-specific credentials** (CSCs) are designed for usage across a cluster of cooperating ecosystems—but not globally. CSCs are governed by the ecosystems within that cluster. Although clusters can design their own CSCs from scratch, clusters who are part of the Ayra Trust Network can greatly benefit from being Ayra-aligned. *Examples*: *academic research library credentials, professional certification credentials, smart city resident credentials, vaccination credentials.*
3. **Ayra Network Credentials** have the broadest scope and are "Ayra-aligned" by definition. They are explicitly designed to interoperate across any cluster or ecosystem in the Ayra Trust Network who wants to issue and/or accept these credentials.

The purpose of this paper is to explain the special potential of this third category of credentials as they are only possible with a digital public utility like the Ayra Trust Network.

[2] "Ayra-aligned" specifically means: a) the credential definitions use data types registered in the Ayra Type Catalogue for semantic interoperability, b) the governance framework specifies use of one or more Ayra Interoperability Profiles, and c) issuance and verification policies take advantage of other Ayra credentials. See the https://ayra.forum/ayra-technical-whitepaper/ for more details on these topics.

The 7 Design Principles of Ayra Network Credentials

These design principles apply uniquely to Ayra Network Credentials.

#1: Global Interoperability

As figure 1 illustrates, the #1 design goal for Ayra Network Credentials is to provide the broadest possible utility across ecosystems recognized in the Ayra Trust Network—utility for their issuers, holders, and verifiers (aka relying parties).

This design goal has one inescapable consequence: Ayra Network Credentials must use an open standard credential format and exchange protocol that has the potential to be supported by any ecosystem within the Ayra Trust Network.

This is the purpose of Ayra Interoperability Profiles (AIPs) and the Ayra Conformance Test Suite (CTS): to make it easier to implement compatible technologies that can be tested and proven to work between ecosystems with the Ayra Trust Network.[3]

#2: Global Governance

Global interoperability also requires that Ayra Network Credentials be governed at the Ayra Governance Framework level. This is in contrast to cluster-specific credentials or ecosystem-specific credentials which are governed at the cluster or ecosystem level.

Governance at the Ayra Governance Framework level means:

- Each Ayra Network Credential will have its own *credential governance framework* that specifies both the technical requirements as well as the policies governing issuers and verifiers.
- The governing body of a cluster or ecosystem that wishes to issue or accept Ayra Network Credentials must be certified to meet the requirements of those credential governance frameworks.
- Those governing bodies must in turn certify the issuers and verifiers within their ecosystems against those requirements.

See the Introduction to Ayra paper for a list of the Ayra Projects that will be focused on producing credential governance frameworks for specific Ayra Network Credentials.

[3] See the Ayra Technical White Paper for more details about AIPs and the CTS.

#3: Simplicity

As the most generic of digital credentials, the dominant design principle for Ayra Network Credentials is *simplicity*. In other words, they should have as few required claims (a.k.a. attributes or properties) as possible, and those claims should be for data that is universally required to achieve the credential's purpose.

For example, a verifiable relationship credential (VRC) issued by an employer to an employee as proof of employment could have as little as two required claims:[4]

1. A unique cryptographically-verifiable identifier, such as a decentralized identifier (DID), pseudonymously identifying the employee in the context of the employer.
2. A type claim with a value of "employee".

All other claims could be optional.

#4: Extensibility

Precisely because each Ayra Network Credential should be as simple as possible, the Ayra Governance Framework should define a standard extension mechanism that applies to all of them (such as an array of name/value pairs). This design principle not only helps protect the core simplicity, but makes Ayra Network Credentials an ideal way to "start the conversation" between parties when they are forming a digital trust relationship for the first time.

Either party can request the appropriate Ayra Network Credential from the other. Then their respective software agents can inspect the extension to determine how best to proceed with progressive disclosure (described below).

This design pattern can be applied to credential definitions at any level of the Ayra Trust Network—network, cluster, or ecosystem. Furthermore, interoperability of extensions can be greatly enhanced using *type catalogues* into which members can register the extensions they need for semantic interoperability. This is a core purpose of the Ayra Type Catalogue.[5]

#5: Privacy Preservation and Progressive Disclosure

One benefit of constraining Ayra Network Credentials to be as simple and lightweight as possible is that it can also maximize personal privacy preservation. By defaulting to *disclosing the minimum personal data possible* in order to start a trust relationship, Ayra Network Credentials encourage data minimization. For example, the verifiable relationship credential for an employee (described above) has only two claims.

---

[4] In addition to version, status, and expiry claims which should be standard across all Ayra Network Credentials.

[5] See the Ayra Technical White Paper for more details about the Ayra Type Catalogue.

Although the initial level of assurance provided by such a credential may be low, the fact that either party can prove they hold at least one Ayra Network Credential—and thus are a member of the Ayra Trust Network—can help establish at least a "toehold level of trust". Even such a toehold exceeds the current state of the Internet—where, to quote the famous New Yorker cartoon, "No one knows you're a dog."

Once this first toehold is achieved, it becomes easier to proceed with progressive disclosure, i.e., for either party to request other cluster-specific or ecosystem-specific credentials as required to achieve the level of assurance needed in a specific context.

This could give a major lift to privacy on the Internet, especially compared to the vast amounts of personal data that relying parties must collect today to fight fraud and bad actors. It could also head off the potential threat that digital wallets could lead to a "papers please" Internet where every website asks for a copy of your mobile drivers license simply because it can.

#6: "Minimum Viable Friction" for Acceptance

Another design objective of Ayra Network Credentials is to make them as easy and fast as possible for relying parties to accept. This goes directly to the cold start problem (aka chicken-and-egg problem) that all digital credentials face: issuers won't decide to issue until there is enough relying party demand, and relying parties won't demand until there is enough issuer supply.

Ayra Network Credentials are specifically designed to break this bottleneck by providing a set of very simple credentials that: a) have at least some immediate value to relying parties, and b) require the minimum friction to accept (including support for peer-to-peer issuance and verification of verifiable relationship credentials). As a general rule, this means there will be no charge for accepting an Ayra Network Credential.

This principle also avoids the gnarly question of how relying parties can compensate issuers for credential verification without "phoning home" to the issuer (a privacy anti-pattern the decentralized digital identity community desperately wants to avoid).

This does not mean verification of higher assurance Ayra Network Credentials (or other cluster-specific or ecosystem-specific credentials) will be free. Successful business models for digital credentials are still evolving. One important longer-term goal of the Ayra Association is to develop and implement a privacy-preserving credential payment protocol that can be used across any ecosystem or cluster in the Ayra Trust Network.

#7: Designed as a Family

To paraphrase John Donne, at the Ayra Network Credential level, “no credential is an island”. This is especially true of Ayra Network Credentials because they need to be explicitly designed to work together as explained in the next section.

The Ayra Network Credential Family

Given these seven design principles, the first four proposed members of the Ayra Network Credential family represent foundational building blocks of almost all digital trust relationships as shown in figure 2:

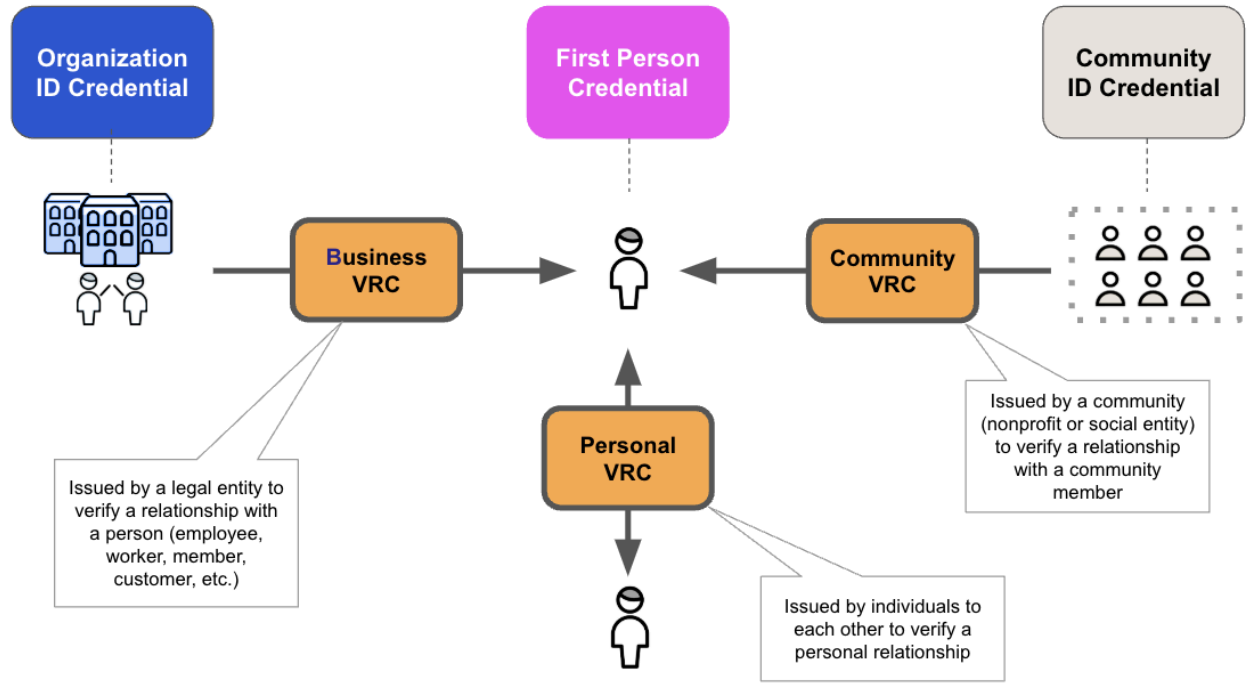

Figure 2: The first four proposed credentials in the Ayra network credential family

Note that the credentials in purple in figure 2 all represent instances of a verifiable relationship credential (VRC)—a credential the holder can use to prove they have a trust relationship (at some level of assurance) with the issuer. For reasons explained below, VRCs are a fundamental component of the trust relationships facilitated by the Ayra Network Credentials family.

The following sections describe each of these four foundational Ayra Network Credentials in more detail.

Organization ID ("Org ID") Credentials

The need for a standard identifier for legal organizations of any kind is widely acknowledged in the world of verifiable digital credentials. In dealing with a business, you cannot achieve any significant level of trust unless you can verify the authenticity of the organization you are dealing with—whether a corporation, partnership, sole proprietorship, nonprofit, NGO, government agency, or any other kind of legal entity.

However, verifying the authenticity of an organization is not an easy problem. While every legal jurisdiction has some prescribed way to register a legal entity, neither the identifiers nor the process is coordinated across jurisdictions. This caused havoc within the financial industry after the 2007-2008 global financial crisis as described in the Michael Lewis book The Big Short.

One outcome of that crisis was the establishment of the Legal Entity Identifier (LEI) as a new global standard (ISO 17442). LEI infrastructure is a textbook example of establishing a globally federated system to verify the identity of legal organisations. Administered by the international nonprofit Global Legal Entity Identifier Foundation (GLEIF), the LEI system uses a global network of Local Operating Units (LOUs) around the world that assign LEIs to individual legal entities. Each LOU collects and validates a set of reference data for the legal entity, including official business registrations in one or more jurisdictions. GLEIF and the LOUs also ensure uniqueness, i.e., that a legal entity has only one LEI.

Recognizing the need for the LEI to transition into the digital world, in 2020 GLEIF began working with Trust Over IP (ToIP) to develop a digital credential that binds an LEI to a cryptographically verifiable identifier called a vLEI. The GLEIF website has extensive documentation explaining how vLEIs leverage their contained LEIs for organisational identity verification, including the entire GLEIF vLEI Ecosystem Governance Framework.[6]

With the vLEI, the organizational ID asserted by a legal entity can be verified in seconds—essentially eliminating the potential for fraud based on unauthorized use of that vLEI.

The purpose of the Org ID credential is to bring this same functionality to the Ayra Trust Network. The root claim in this credential is a decentralized identifier (DID) that meets the assurance requirements of the Ayra Governance Framework.

- If the organization has a vLEI to use as their DID, this requirement is already met.
- If the organization does not yet have a vLEI, it can request one through a Qualified vLEI issuer or obtain an Org ID credential from any qualified Ayra ecosystem using a DID that meets the security requirements of the Ayra Governance Framework. The extensibility payload can then include any other identifiers of the legal entity that meet the requirements of the Ayra Governance Framework. The more identifiers are included, the more trust signals that the Org ID credential offers to a verifier.

[6] Based on the ToIP governance framework specifications.

- If the organization subsequently obtains a vLEI, it can be added to the extensibility payload to bring it up to a higher level of assurance.

The link between the Org ID credential and the Business VRC shown in figure 2 is created by using the DID in the Org ID credential as the Issuer DID for the Business VRC. See the Verifiable Relationship Credentials section for more.

Community ID Credentials

In contrast with formal legal entities, there are many other types of groups and communities that are not legal entities, yet have a very real existence online and/or offline. Examples include online communities and forums, open source software projects, advocacy groups, fan communities, gaming clans and guilds, support groups, church groups, and chat groups.

For many people, relationships within these communities can be every bit as important as their business relationships. So the Ayra Trust Network should provide a mechanism for these communities to have their own cryptographically verifiable ID, so they too can issue and receive the benefits of community VRCs.

Since community VRCs are a key component of First Person credentials, developing the requirements for Community ID credentials will be a key part of the work of the First Person Project. The goal is to provide a path for any legitimate online community and its members to take full advantage of the Ayra Trust Network.

First Person Credentials

In the two-sided network of organizations and individuals represented by the left half of figure 2, both sides need to be able to verify the other. Org ID is discussed above. But any form of "personal ID" on the Internet is an order of magnitude harder for a host of reasons:

1. **Privacy.** Privacy-preserving digital credentials is an incredibly deep and complex topic that has been debated across the decentralized identity industry since its birth in 2015. Even an effort as massive as the European Digital Identity Wallets initiative still has not been able to determine how best to protect the privacy of EUDI wallet users.
2. **Scale.** There are at least an order of magnitude more people in the world than legal entities. This greatly compounds the challenge of achieving any widely acceptable baseline digital identity verification solution for individuals.
3. **National and cultural norms.** Regulations and social attitudes about personal identity, privacy, and agency vary widely around the world. Finding common ground for people to be comfortable with personal digital identity credentials is hard.
4. **Technical capabilities**. Most businesses have the technical personnel, equipment, and training to manage organizational identity and customer relationships. The opposite is true for individuals. In fact, many longtime experts in cryptography and public key infrastructure (PKI) have been very skeptical that individuals will be able to

safely manage cryptographic keys. Thankfully, the combination of cryptocurrency wallet innovations and intense UI/UX development by wallet vendors is steadily overcoming this challenge. However, there are still major usability challenges for the digital wallets and vaults required for First Person credentials to be successful.

For all these reasons, the decentralized identity community has struggled to develop a widely acceptable personal identity credential. However, in August 2024 there was a breakthrough in the form of a new paper called Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online. The abstract begins:

> *Anonymity is an important principle online. However, malicious actors have long used misleading identities to conduct fraud, spread disinformation, and carry out other deceptive schemes. With the advent of increasingly capable AI, bad actors can amplify the potential scale and effectiveness of their operations, intensifying the challenge of balancing anonymity and trustworthiness online. In this paper, we analyze the value of a new tool to address this challenge: "personhood credentials" (PHCs), digital credentials that empower users to demonstrate that they are real people—not AIs—to online services, without disclosing any personal information. Such credentials can be issued by a range of trusted institutions—governments or otherwise. A PHC system, according to our definition, could be local or global, and does not need to be biometrics-based.*

While this 63-page paper (with 33 contributing authors) does not propose a specific design for personhood credentials (PHCs), it does present an exhaustive list of requirements for this powerful new trust tool. The two most important are listed on page 2:

1. *Credential limits: The issuer of a PHC gives at most one credential to an eligible person.*
2. *Unlinkable pseudonymity: PHCs let a user interact with services anonymously through a service-specific pseudonym; the user's digital activity is untraceable by the issuer and unlinkable across service providers, even if service providers and issuers collude.*

The paper also takes a strong stance that the only effective mechanism to achieve unlinkable pseudonymity is zero-knowledge proof cryptography (ZKP). From page 2:

> *[A PHC] empowers its holder to demonstrate to providers of digital services that they are a person without revealing anything further. Building on related concepts like proof-of-personhood and anonymous credentials, these credentials can be stored digitally on holders' devices and verified through zero-knowledge proofs. Importantly, such proofs do not reveal the individual's specific credential (nor any aspects of their identity).*

With this background, we can define a First Person credential as a PHC that leverages the Ayra Trust Network to provide proof of personhood based on verifiable first-person relationships between Ayra Trust Network members. This is often called a "social-graph-based" approach to proof of personhood. See Vitalik Buterin's 6500-word essay on proof of personhood for a detailed explanation of this approach.

The Achilles heel of most social graph-based approaches is *privacy*: they require aggregating a centralized social graph that can be analyzed to detect bad actors. The secret to First Person credentials is that this "social graph" is not centralized. Instead it is captured entirely in VRCs that live only in the digital wallets of the Ayra Trust Network members that engage in First Person relationships (personal wallets for individuals and enterprise wallets for businesses and communities).[7]

First Person credentials are further privacy-preserving because they do not reveal any of these relationships (or any other personal data of the holder). They only reflect the aggregate count of a person's VRCs as illustrated in figure 3:

Figure 3: Example of what a First Person credential might look like in a person's digital wallet

[7] The name "First Person" was chosen to reinforce that all of the VRCs in this "decentralized social graph" represent direct first-person relationships with the holder. See Doc Searls: Why We Need First Person Technologies on the Net.

Verifiable Relationship Credentials (VRCs)

As shown in figure 2, the verifiable relationships proposed to be counted in First Person credentials fall into the three categories in table 1:

VRC Category	Description
Business	Verify the relationship between a legal entity (with an Org ID) and a person, such as: • Employee • Worker/Contractor • Officer • Director • Shareholder • Customer • Member • Donor
Community	Verify the relationship between an informal social entity (with a Community ID) and a person in its community, such as: • Member • Volunteer • Contributor • Maintainer
Personal	Verify the personal relationship between two people, both of whom issue VRCs to the other.

Table 1: Three categories of VRCs

Business VRCs

Business VRCs represent a powerful new way businesses of all kinds can build stronger, richer, more productive trust relationships with their stakeholders. They can be issued using the verifiable identifier (e.g., DID) bound to the business by its Org ID credential.

The first obvious use of business VRCs is for employee, worker, or contractor credentials.

GLEIF's vLEI framework features two similar business relationship credentials: an *Official Organizational Role Credential* (OOR—for official positions within an organization) and the *Engagement Context Role Credential* (ECR—for any other type of relationship with a person). Just as an Org ID credential can be linked to a vLEI for higher assurance, a Business VRC can be a vLEI OOR or ECR credential.

Business VRCs also open up major new opportunities in CRM (Customer Relationship Management)—specifically in the new field of VRM (Vendor Relationship Management). Because maximizing the value of customer relationships is the entire purpose of CRM systems, issuing a business VRC to customers can have all of the following benefits to the issuing business:

1. It is an immediate signal of appreciation to your customer.
2. It adds to your customer's count of verifiable relationships in the First Person credential.
3. If your company offers a communications account (phone, fax, email, social network, secure chat, etc.)—or verified access to a specific account—this credential can give your customer a verifiable proof-of-address.
4. It can be used across your partner companies for affiliate marketing.
5. Its extensibility payload can include product and/or customer profile data that is both richer and more expressive *and* more privacy-preserving than cookies.
6. Lastly, a Customer Relationship credential can automatically provision a secure, private, unphishable communications channel—one that can begin working immediately and grow into a full personal AI agent-to-business AI agent channel. See The Trusted Channel Network Effect.

Community VRCs

Member relationships are the lifeblood of many organizations such as NGOs, civil society organizations, buying clubs, social networks, and informal online communities.The exact meaning of membership and the level of assurance it represents varies with the organization and its membership types. Nonetheless, organizations whose membership criteria are clear enough to comply with the requirements of the Ayra Governance Framework can issue Community Relationship credentials that will be included in the count of verifiable relationships in the First Person credential.

Community VRCs have all the same advantages to a community as business VRCs with the additional benefit that members who are comfortable sharing a portion of their personal relationship graph (the set of VRCs they have in their digital wallet) with the community can benefit from easily discovering new relationships within that community.

Personal VRCs

As important as businesses and communities can be in our lives, our deepest trust relationships are with other people. Personal VRCs are designed to empower individual Ayra Trust Network members to create their own connections and verify their own person-to-person relationships in a highly privacy-preserving way.

Due to the infrastructure that the Ayra Trust Network provides, the process of exchanging Personal VRCs is surprisingly easy. Let's say Alice decides to create a First Person relationship

with Bob. She displays a First Person QR code on her smartphone for Bob to scan. This works the same way QR codes can be used to create new connections on LinkedIn, WhatsApp, Signal, WeChat, Line, etc.) as illustrated in Figure 4:

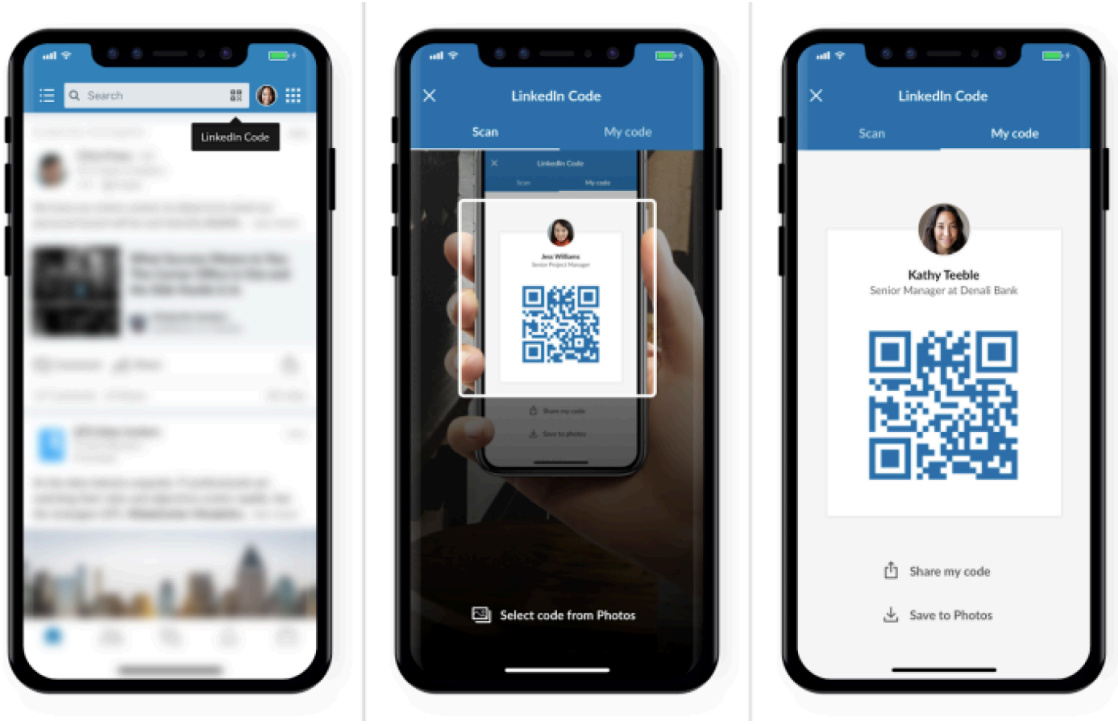

Figure 4: The process of forming a new LinkedIn connection with a LinkedIn QR code

Here is what happens when Bob scans Alice's First Person QR code:

1. It triggers Bob's First Person-enabled digital wallet to generate a pairwise peer DID for Alice and send it to Alice's wallet.
2. When Alice's wallet receives the message, it generates Alice's pairwise peer DID for Bob, and sends it back to Bob's wallet.
3. Now both Alice's and Bob's wallets issue a personal VRC to the other. In both cases, the credential is signed by the private key for the issuer's pairwise peer DID. The only two required claims in the credential are the two pairwise peer DIDs.

Once both Alice and Bob receive the signed credential from the other, each can now provide cryptographic proof of the relationship by presenting a proof of the credential signed with their own private key for their own pairwise peer DID. A verifier only needs to verify the issuer's signature against the issuer's DID and the holder's signature against the holder's DID.

Of course, it is trivial for an attacker to mount a Sybil attack by creating an army of bots issuing fake Personal Relationship credentials to each other. This is why a personal VRC credential does not count towards the holder's VRC count in their First Person credential unless it chains up to an Ayra trust anchor. Details about the First Person credential trust model will be published in an upcoming Ayra white paper on the **First Person Project**.

The Special Network Effects of Ayra Network Credentials

Numerous business books have been written about how network effects are the primary growth driver for the massive digital platforms that dominate the Internet today. As Eric Chan notes in *The Cold Start Problem* (his book devoted entirely to jumpstarting network effects):

> *Just look at the companies that have made it into the "Billion Users Club". Apple has 1.6B iOS devices, while Google has 3B. Facebook has 2.85B users across their social network and messaging apps. Microsoft has over 1.5B devices running Windows, and another 1B running office. In the Chinese technology ecosystem, the companies behind WeChat, TikTok, and AliPay all enjoy ecosystems numbering a billion users each. These are the tiny number of technology products that have reached incredible scale, and perhaps unsurprisingly, all of them leverage a network effect.*

What makes Ayra Network Credentials special is that they have *multiple cross-reinforcing network effects* as explained in this section.

#1: The Trust Network Effect

Network effects are typically achieved either at the *device* level (e.g., the more telephones on a telephone network, the more valuable the phone to each user) or the *member* level (e.g., the more members on a social network, the more valuable the network to each member).

But because Ayra Network Credentials are designed to work together as a family, they achieve network effects at the *credential* level. In other words, the more Ayra Network Credentials on the Ayra Trust Network, the more valuable the Ayra Trust Network becomes for every member. For example:

- The more Org ID and Community ID credentials issued, the more business and community VRCs can be issued.
- The more business and community VRCs issued, the more First Person credentials can be issued.
- The more First Person credentials issued, the more personal VRCs can be issued.
- The more personal VRCs issued, the more it drives demand for Org ID and Community ID credentials.

And so the flywheel turns.

This is the *trust network effect*. Achieving the trust network effect was the fundamental reason the Ayra Trust Network was established as a "trust network of trust networks" that can interconnect any number of digital trust ecosystems just like the Internet can interconnect any number of local area networks.

#2: The "Zero-to-Hero" Network Effect

Back in 1900, the only way to achieve the network effect with the original device that started it all—the telephone—was for every new user to buy, install, and learn how to use a completely new gadget. In AT&T's annual report in 1900, company president Theodore Vail put it this way:

> *A telephone without a connection at the other end of the line is not even a toy or a scientific instrument. It is one of the most useless things in the world. Its value depends on the connection with the other telephone and increases with the number of connections.*[8]

No wonder it took many decades for telephones to become ubiquitous. Today, with the Internet and the Web, joining a new network can be almost frictionless. For example, in a brilliant design move, webmail pioneer Hotmail automatically added a footer to every Hotmail message with a link offering the recipient a free Hotmail account. One click and a new user could sign up and start sending their own Hotmail in minutes—becoming yet another carrier of the Hotmail "virus".

Many social networks have followed the same playbook—in fact so many that eventually it led to a backlash against "invitation spam".

So far, digital credentials have not been able to tap into this dynamic. One reason is that they require digital wallets to work. Unfortunately, interoperable digital wallets—wallets that use open standard credential formats and exchange protocols that make it easy for developers to build new applications—are still in short supply.

With the Ayra Trust Network, Ayra Network Credentials, and the Ayra Conformance Test Suite, we can change that. This is how an existing user can invite a new user "zero to hero":

1. A First Person credential holder generates an Ayra QR code to invite a new First Person relationship as illustrated in figure 4.
2. If the person scanning the QR code does not yet have an Ayra-compatible digital wallet, the QR code can direct the user to a Ayra Association microsite where they can download one.
3. Once installation is finished, the user's new Ayra-compatible digital wallet will automatically connect to the microsite, which will then privately connect them to the party that generated the original QR code.
4. Now the two parties can complete the First Person connection dance and issue mutual personal VRCs.

And now the cycle can repeat. Because each new person in the Ayra Trust Network adds to the overall network effect.

---

[8] American Telephone & Telegraph Company, "Annual Report for the Year Ending December 31, 1900", filed March 26, 1901, Google Books. As quoted in The Cold Start Problem, page 20.

#3: The First Person Network Effect

First Person credentials were so-named because they represent relationships that people form directly, one-on-one. While some of these relationships are with businesses and communities, far more are with other individuals.

Because these real-world person-to-person relationships can go from "zero-to-hero" so quickly, the First Person QR code is the Ayra equivalent of the Hotmail invitation link. Add to this the reputational incentive to forming new First Person relationships because each one (up to a limit) helps you increase the strength of your First Person credential.

This is the "First Person network effect". It is a same-side network effect because it gives individuals the power to create and control their own personal relationship graphs and to use them with apps and services as they see fit—unconstrained by third-party business models or terms of service.

But it is also a cross-side network effect because the more First Person credentials, the more incentives businesses have to form First Person relationships with their customers. So the Ayra Trust Network can grow from both sides of the two-sided market in the left half of figure 2.

#4: The Trusted Channel Network Effect

The final network effect harkens back to the telephone as the origin of the very term "network effect". To repeat AT&T president Theodore Vail's quote, as a breakthrough new communications device, the value of the telephone "*depends on the connection with the other telephone and increases with the number of connections*".

This is true of any breakthrough new communications channel, from the fax machine to social networks. So how do Ayra Network Credentials represent a new type of channel?

The secret is in the cryptographically verifiable identifiers (pairwise peer DIDs) exchanged in every VRC. These can serve as the endpoints for a secure, private communications channel between the two parties. This new **trusted channel** is extraordinarily powerful:

1. *It can provide bidirectional authentication and encryption* equal or better to HTTPS web connections without either party needing X.509 certificates.
2. *It is fully private to the two parties*, so the channel can be used for confidential messaging and data exchange that meets regulatory requirements in industries such as financial services and healthcare.
3. *It uses cryptographically verifiable identifiers* (e.g., DIDs) pre-exchanged between the parties, so they are essentially unphishable.
4. *It can last as long as either party wants to keep the relationship*, since the pairwise peer DIDs have no dependency on any external registry or service provider.

5. *It can be used for automated workflows between digital agents of any kind*, including personal and business AI agents.

Trusted channels are in fact such an important new dimension of Internet communications that they will be the subject of a separate white paper forthcoming from the Ayra Association.

Ayra Network Credential Projects

A core theme of this paper is that Ayra Network Credentials must be carefully designed as a family to maximize the utility and synergy of each family member. This is the reason the Ayra Association is launching specific Ayra Network Credential Projects to serve as high-value collaboration forums for Ayra Association members.

See the Introduction to Ayra paper for descriptions of the first two Ayra Network Credential Projects—the **Org ID Project** and the **First Person Project**.

To join an Ayra Network Credential Project—or get started on forming your own Ayra trust cluster—please connect with us via the Ayra Trust Network website: https://ayra.forum/