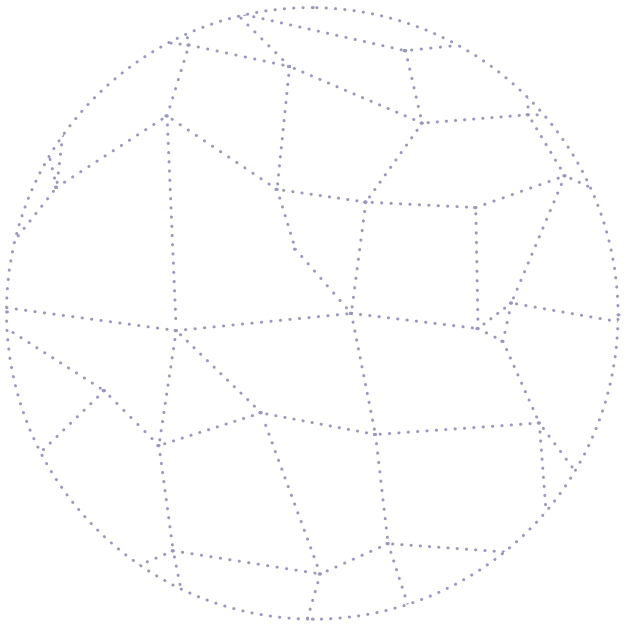
Making Sense of Identity Networks

There are several ongoing global initiatives seeking to create robust digital identity networks. These identity networks will give people greater control over their personal data and allow digital identities to be portable. They will help to detect and reduce fraud, and they will provide mechanisms to ensure identity data is up to date. This paper considers the different types of identity networks that already exist or are being developed, presents a high-level framework to understand and assess them, and provides guidance to decision-makers, policymakers, CIOs, government officials, journalists or any organization considering participating in such a network.

The content of this paper has been submitted by DIACC member Consult Hyperion

Table of Contents



The content of this paper has been submitted by DIACC member Consult Hyperion

About the Authors

Consult Hyperion

Steve Pannifer, Justin Gage

Consult Hyperion[1] is an independent strategic and technical consultancy, based in the UK and US, specialising in secure electronic transactions. With over 30 years' experience, we help organisations around the world exploit new technologies to secure electronic payments and identity transaction services. From mobile payments and chip & PIN, to contactless ticketing and smart identity cards, we deliver value to our clients by supporting them in delivering their strategy. We offer advisory services and technical consultancy using a practical approach and expert knowledge of relevant technologies. Hyperlab, our inhouse software development and testing team, further supports our globally recognised expertise at every step in the electronic transaction value chain, from authentication, access and networks, to databases and applications.

For more information contact pressoffice@chyp.com.

Whitepaper Development Methodology

The goal of the paper is to provide an objective and impartial comparison of identity networks. To achieve this goal, we adopted a consistent language and described abstract examples for identity networks using that language. We then used this as a basis for the analysis.

This paper was developed in consultation with DIACC through a community review process. Consult Hyperion received input and feedback from several DIACC members that helped us refine the terminology, examples and key characteristics that are important to consider when comparing identity networks.

Inevitably, there will be specific examples of identity networks that do not map precisely onto one of the abstract examples presented. We believe that the examples, as they are, provide a good enough representation of the many specific identity networks that exist today. The methodology presented for analyzing and comparing identity networks can easily be applied to any specific alternative identity network that may exist.

[1] http://www.chyp.com

Executive Summary

Digital identity is an area of strategic importance to a growing number of organizations. Digital is a key channel for service delivery. High-value services, such as banking and health care, are being transformed by digital technology. Even when a service is physical, such as transportation, it is often being enabled digitally. All aspects of business including marketing, sales, supply, delivery, and support are experiencing a massive shift towards digital. Digital identity is the key to ensuring, security, privacy, and convenience for people and businesses as they participate in the digital economy.

The lack of widescale digital identity is not due to a lack of effort. There are numerous government and industry initiatives actively seeking to build and promote digital identity networks. These will give individuals, organizations and potentially devices digital identities that enable all types of digital service.

Today identity is often siloed, with customers needing to have separate relationships with each organization they deal with and each organization keeping a separate (and likely different) digital version of the customer. This creates massive friction and risk. Without reliable and portable digital identity, consumers, governments, and businesses will have a significant lack of trust in online interactions, which in turn will prevent everyone from fully realizing the full potential of digital services.

The concept of digital identity is undergoing change too, from something narrow (basic identification use cases) to broader information about the subject and developing an ongoing ecosystem of trust between parties interacting digitally.

Identity networks can be a way to address these issues, provided that they:

1. Allow digital identities to be portable, help to detect and reduce fraud, and provide mechanisms to ensure identity data is up to date;

2. Create a collaborative environment where the needs of all stakeholders (not just a few) are met; and

3. Establish appropriate governance to ensure a standardized, interoperable and auditable approach.

Comparing identity networks can be difficult, however. While in general, all identity networks are trying to solve similar problems, they can go about it in quite different ways. This paper considers the different types of identity networks that already exist or are being developed and presents a high-level framework to understand and assess them.

The paper concludes with 4 key questions to be considered when contemplating participating in an identity network:

- Are you comparing like with like?
- Are you building for now or the future?
- Does the implementation meet your specific needs?
- What are the network user needs?

This paper is intended for decision-makers, policymakers, Chief Information Officers, government officials, journalists or any organization considering participating in an identity network.

1 Why Identity Networks Matter

In the physical world, we make do with approximations to identity

For most of us, identity is not something we need to (or want to) think about with any regularity. In our day to day lives in the physical world, identity is often an afterthought.

For example:

- If you need to buy something that requires you to be of a certain age, you show a driver's license as proof you are eligible
- If you want to open a new account with a cable, internet or utility provider, you need to show proof that you live at the address being serviced
- If you need to travel internationally, a passport can provide proof of your citizenship while abroad and your right to travel outside of your home country
- If you want to open a business bank account, you need to provide paper documents demonstrating the incorporation of the business

We use these documents in the physical world because they are the lowest common denominator and have been the best tool available at scale to act as proof of identity. They are (usually) easy to carry so they have also become convenient for other purposes for which they were never originally intended. A driver's license was only intended to prove someone was eligible to drive, not to be used to show proof of age. Over time however, this has become the de facto document for everyday identity.

These documents are, however, easy to forge, manipulate, steal, or copy to use for fraudulent purposes. This is not helped by the fact that service providers make copies and distribute these copies whenever needed.

In the digital world, we need to do better

Today we often make do with the same approximations to identity when designing digital services. We repeatedly ask customers to enter information about those documents which only serves to proliferate customer data, increasing the chances that the customer's identity will be compromised. Because the security practices of service providers will vary considerably, whilst one organization may protect its customer data well, that data may be at risk in other organizations the customer deals with.

The proliferation of data is not just a security issue. Each organization the customer deals with, will hold its own (and likely different) digital version of the customer. Some of what a mobile operator knows about their customer is the same as what the electric company knows for the same customer, but there will inevitably be differences in data about the way the customer uses the service, their preferences, their habits, and anything else the customer discloses, knowingly or not. This creates massive friction and duplication of effort for the customer, who needs to manage their "identity" with each service provider. Any time changes need to be made (e.g. address change, new phone number, updated payment information, etc.), the customer must contact each one individually. It also locks customers into relationships with an organization because they don't want to lose all the data associated with their account. That might seem good to the service provider, but it is not in the interest of the customer.

Establishing the identity of the customer is only one half of the problem. Customers also need to know and be assured of the identity of the businesses and governments they deal with. Today this is often accomplished through brand recognition, however as businesses' ability to have a digital presence and never have a physical interaction with a customer grows, customers will need greater assurance that they can trust an online business is being accurately represented and is trustworthy. Without this, customers will have no reliable way of determining a legitimate business from one that was set up purely to perpetrate fraud. This aspect continues to be overlooked by the digital identity industry.

Current federated identity solutions are only a partial solution

The most prevalent solution to these problems to date is federated logon, where users can log onto one site using an account from another site. This is commonly used in social media platforms. These solutions can remove a lot of the friction that exists with digital identity today. Users no longer need to remember dozens of passwords for each of the sites they use. Instead, social logon allows them to access those sites in the same simple way. And the use of strong authentication by those providers helps to prevent account takeover too.

These services, however, often come at a cost: privacy. The advertising-driven business models of social media platforms rely on collecting excessive amounts of personal data in order to profile users for advertising purposes, which ultimately serves the purpose of the providers and not the user.

Furthermore, the digital identity offered by social media platforms is generally considered low assurance since it is based on self-asserted data. Identity federation itself may be a valid approach if provided by a regulated industry such as financial services.

There are examples of federated authentication services that protect user privacy, such as authenticating to government services using an online banking account, but this distinction is not typically obvious to the average user.

Digital identity networks are a way to address these issues

Some countries, such as the Nordics, have a history of collaborative approaches to digital identity that is suitable for regulated services. In the case of the Nordics, the banks have over several years provided "BankID" services for use in financial services, government services, and the wider economy. Several other initiatives – some national, some international – are seeking to create similarly robust and ubiquitous digital identity networks in other regions.

These identity networks will allow digital identities to be portable, they will help to detect and reduce fraud, and they will provide mechanisms to ensure identity data is up to date. They will create collaborative environments where the needs of all stakeholders (not just a few) are met. The work of the DIACC, and in particular the Pan-Canadian Trust Framework, is helping to ensure that this is accomplished in identity networks in Canada and internationally.

> This paper considers the different types of identity networks that already exist or are being developed, presents a high-level framework to understand and assess them and provides guidance to decision-makers, policymakers, CIOs, government officials, journalists or any organization considering participating in such a network.

Mary – Before

Without an identity network

Mary is a small business owner who is not currently a participant in a digital identity network. She is digitally savvy and has many online accounts with service providers. She often needs to take information from one service provider to another (either as a private customer or a business owner) but she has no way to do this digitally. Instead, she still relies heavily on paper-based processes, making phone calls, or even going to a physical location to get things done.

Consumer

Mary needs access to the results of her recent lab tests from her health care provider. To gain access, she needs to go into the office of the provider after the results come in to pick up a paper copy of the results. To share the results with another provider, she also must sign a paper records release authorization. These results are usually shared by either fax or post, and when by post she has to wait until the provider receives the results before she can discuss them with that provider.

Business

As a small business owner, Mary has many potential suppliers available to deliver the products she needs to operate her business, however since she doesn't have an easy way to vet which suppliers are legitimate, provide the best pricing or offer better services, she chooses to work with one based on a recommendation from a former colleague. She knows she could likely get better service if she shopped around a bit, but she doesn't have the time available it would take to review all the options either by calling other suppliers or requesting information from them.

Government

In order to operate her business, Mary needs to obtain and keep current numerous business licenses and permits. Whenever she needs to apply for a new license or renew an existing one, she either has to go to her nearest government service location in person, or she might be able to print out forms to fill out and post. Once she submits her forms, it usually takes weeks or months for her application to be processed. If there were any problems with the application, she may have to go back to the service center or call in to provide new information. Once the application is complete, the permit or license approval is posted back to her business address.

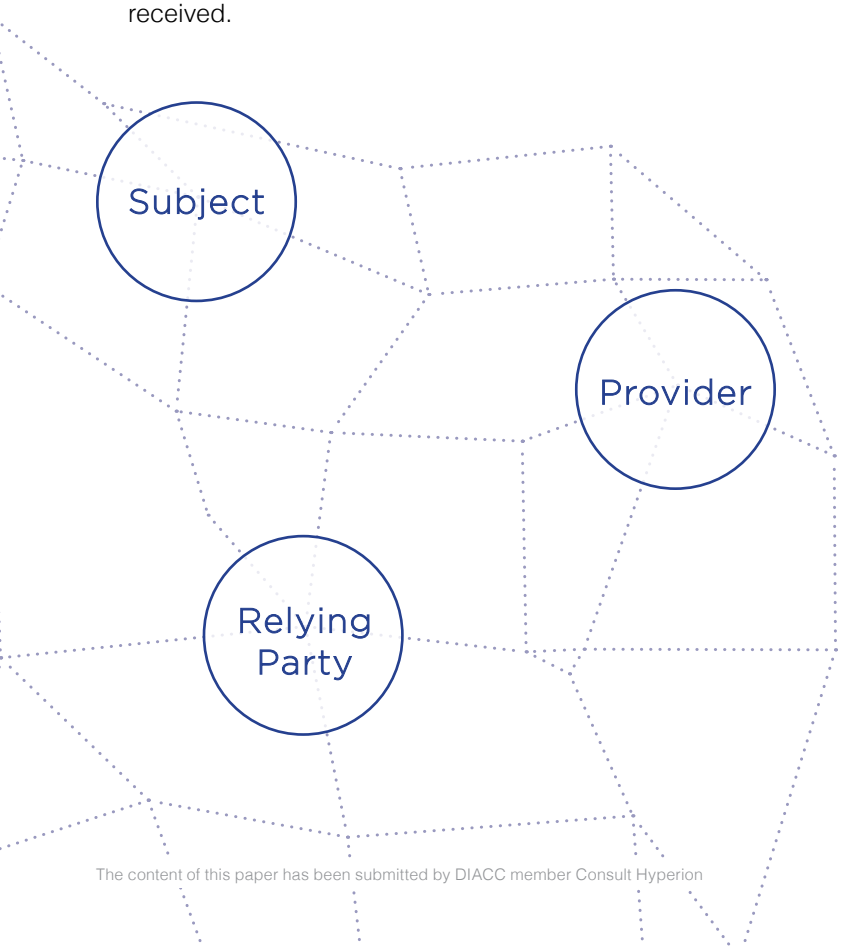
2 Identity Network Elements

The digital identity network landscape is fragmented, with several established and new identity networks. While there are many differences between the various networks, they also have a lot in common. This section describes the common aspects of these networks – namely who they serve, the functions they provide and how they are structured.

Network Users

A digital identity network exists to serve three main types of network user:

- Subject: A unique individual, organization or device distinguishable from others.
- Provider: An individual, organization or device that has information about the subject, that the subject may wish to share with relying parties.
- Relying party: An individual, organization or device that wants to determine the identity or some information about the subject, in order to transact with that subject digitally and be able to trust (or rely on) the information received.



In any network there will, by definition, be a multiplicity of these network users. In many cases, a network user may take on a different role, depending on the context. For example, an online business could be a relying party seeking to identify a new customer, a provider asserting something about an existing customer to a third party, or a subject wishing to show that the online business is reputable to a potential new customer.

These network user types are common across all identity networks. In some, they are more narrowly defined or used than others, but the basic concepts are the same.

Network Functions

Identity networks exist to support the following functions:

- Identification: The process of establishing a real, unique and identifiable subject.
- Authentication: The means by which a subject can assert their identity including showing it is the same subject as one seen before.
- Authorization: Giving the subject the means to control (to authorize) the sharing of their information from providers to relying parties. Information is disclosed in the form of a **credential** – containing the information (or **"attributes"**) being shared together with the associated metadata that links it to the subject and describes its provenance.

The scope of identity networks can vary. At one extreme, there are examples of identity networks that just provide authentication, allowing subjects to establish a digital relationship with a relying party. The relying party will be able to recognize the subject each time they interact based on the authentication information but no further information about the subject is provided via the network. At the other extreme, there are examples of identity networks that provide subjects with the facility to share information (in the form of credentials) with a high degree of flexibility and confidence. Many identity networks sit between these extremes supporting all the above functions but where the information available to be shared is limited by the providers involved and the intended scope of the identity network.

Network Layers

It is helpful to think of identity networks in layers. For the purposes of this paper we describe four layers:

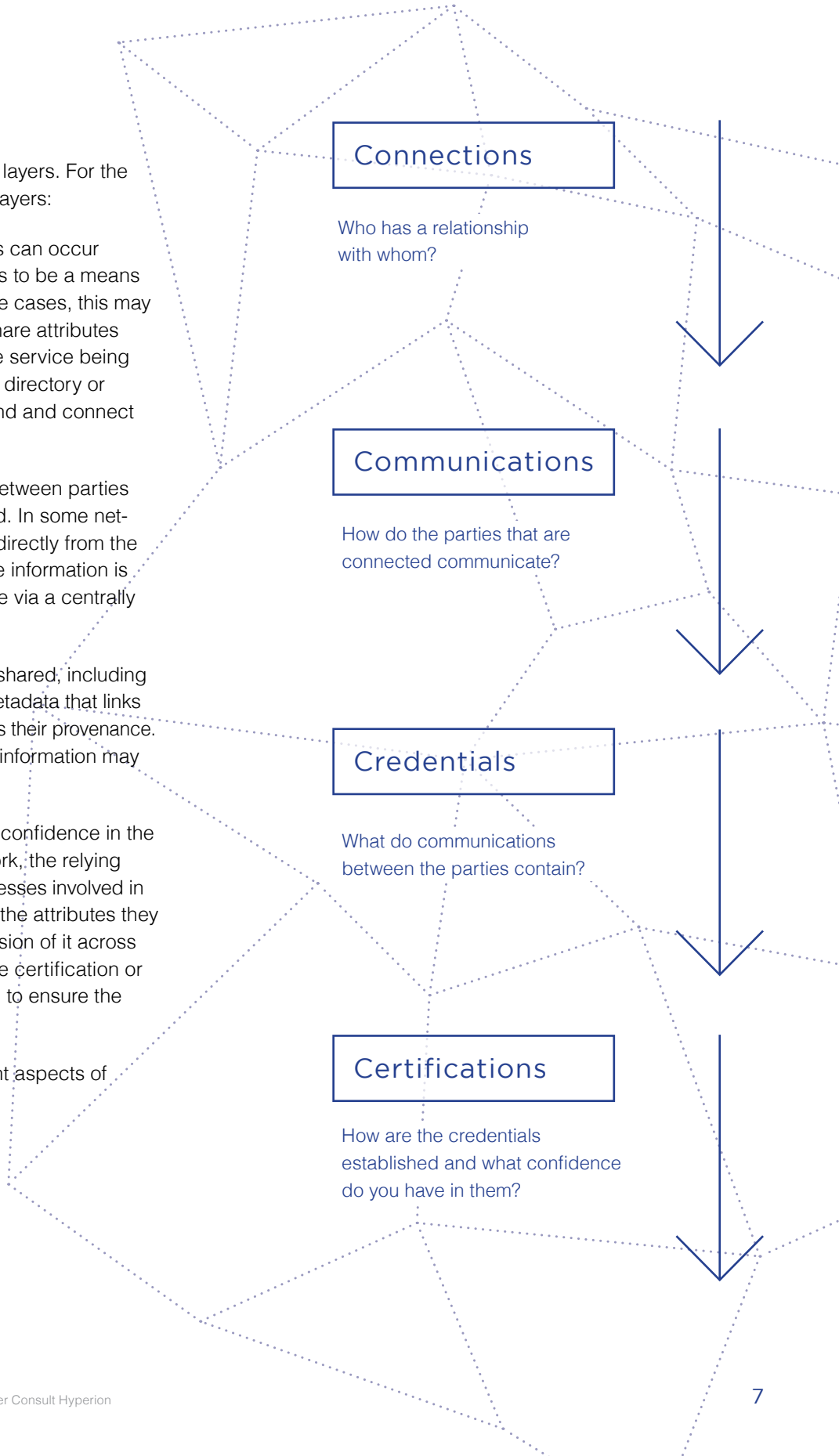
Connections: Before any communications can occur between parties in a network, there needs to be a means for parties to discover each other. In some cases, this may be automatic, as the parties wishing to share attributes may already be communicating about the service being requested, for example. In other cases, a directory or something equivalent, allows parties to find and connect with each other.

Communications**:** The communications between parties carry the credentials that are to be shared. In some networks, this information is communicated directly from the provider to the relying party. In others, the information is only communicated indirectly, for example via a centrally operated hub or via the subject.

Credentials**:** The information that is to be shared, including attributes, together with the associated metadata that links those attributes to the subject and describes their provenance. The structure, content, and format of this information may vary between network types.

Certifications**:** For a relying party to have confidence in the credentials received via an identity network, the relying party will need to be confident in the processes involved in the establishment of the credentials, and the attributes they contain, as well as in the secure transmission of it across the identity network. Often this will involve certification or audit of parties that are being relied upon to ensure the credentials and attributes are robust.

These layers help to compare the different aspects of networks in a consistent way.



3 Identity Network Architectures

To illustrate the layers presented in section 2, we provide four examples of identity network architectures. These are not exhaustive. They are simply meant to illustrate at a high level some of the approaches taken.

The intention is that the framework (in sections 2, 4, 5 and 6) can be applied to specific network solutions or implementations as required, by the reader.

The four examples described below show how the network users interoperate. Two types of interaction are shown:

- Identity Network Interactions: Interactions between parties that are part of the process of sharing the requested information (e.g. credentials) with a relying party over the identity network.
- Service Interactions: Other relevant interactions that are not directly part of the identity network. These include the establishment of digital relationships or the delivery of services, before or after the identity network interaction.

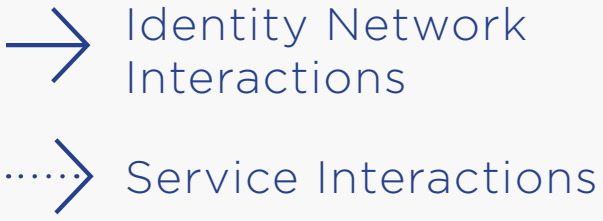


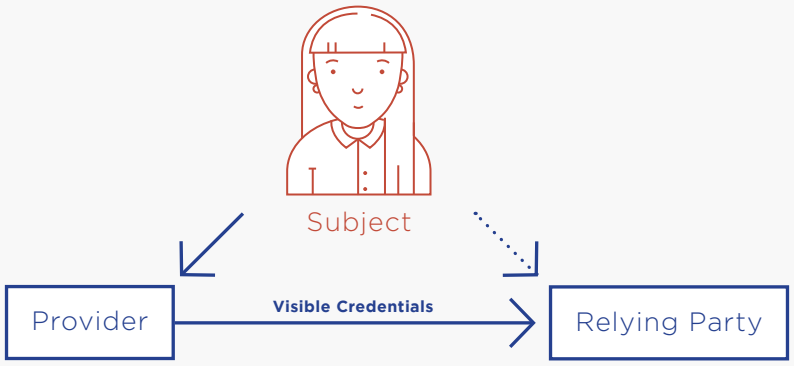
Figure 1, Key for example architecture diagrams

The diagrams focus on the transmission of credentials from the provider to the relying party. We classify credentials into two types:

- Visible Credentials, meaning that both the sending and receiving parties can see the content of the credentials. Credentials will likely be transmitted through a secure communication method but the parties at each end of the communication will be able to see the content.
- Invisible Credentials, meaning that at least one party cannot see the content of the credentials.

Example 1 – Federation

Figure 2
Federation



Federation allows a subject to use a digital identity managed by one organization to access services from another organization. The most prevalent example of this is social logon, where the subject logs onto a website using their social media account. This involves the social media site authenticating the customer (to their own standards) and a confirmation of the authentication and identity data being sent to the website being accessed (i.e. the relying party).

In this model, the subject has a single provider relationship. That provider is usually referred to as the subject's "identity provider". The subject may have a relationship with the identity provider for some other purpose (e.g. to access social media, to obtain a mobile subscription account, to access financial services). In this case, the role of the organization as an identity provider is a by-product of the primary service provided to the subject.

The subject can, of course, use multiple identity providers. This will result in the subject having multiple discrete digital identities.

The identity provider will collect (and in some cases verify) information about the subject. Some of this information will be collected for the primary service offered to the subject. Other information will be collected specifically for the purposes of digital identity. This information will be used to formulate the credentials to be shared via the identity network.

Connections

When a subject tries to access the services of a relying party, the relying party needs to establish which identity provider the subject uses. This could be done by providing the subject with a list to choose from, but this quickly becomes unwieldy as the number of identity providers grows. An alternative is to use a directory, allowing the relying party to look up which identity provider the subject uses.

Communications

The relying party and identity provider communicate directly. The relying party will request credentials from the identity provider. The identity provider will then authenticate the subject and obtain consent to share the requested credentials. The credentials are then transmitted directly from the identity provider to the relying party.

Credentials

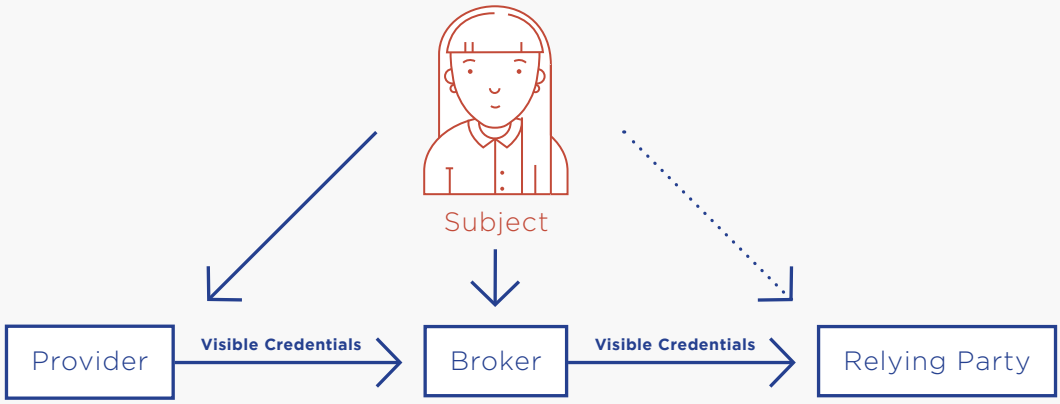
The range of credentials that can be supported in this example may be limited, as it depends on the level of support and capabilities of the identity provider. The credentials themselves may not be digitally signed and hence not cryptographically verifiable. The amount of metadata provided will also vary between networks.

Certifications

The reliability of the credentials will depend on the processes employed by the identity provider, and consequently, they will be the focus of any certification process performed in the network.

Example 2 – Broker

Figure 3
Broker



An identity broker shares many characteristics of the federation example:

- The subject has a single provider relationship, also commonly referred to as an "identity provider". The subject could, of course, have relationships with more than one identity provider. This would result in multiple digital identities for the same subject.
- The identity provider may provide other services to the subject with digital identity being a by-product.
- The scope may be limited to identification and authentication, with only a very limited set of credentials being supported by identity providers.

The key difference, as illustrated in the diagram above, is the presence of a broker that sits between identity providers and relying parties. Examples of this include some of the government and bank-led identity schemes in Europe.

Connections

The broker is used to facilitate connecting the subject with the correct identity provider as well as the transmission of identity information from the identity provider to the relying party. Typically, when a subject tries to access the services of a relying party, the relying party calls the broker. The broker then asks the subject to select an identity provider from a list or may employ more sophisticated means to determine the correct identity provider.

Communications

The relying party and identity provider do not communicate directly. All communication is via the broker. The relying party will request credentials from the broker. The broker will pass this request onto the relevant identity provider. The identity provider will then authenticate the subject and obtain consent to share the requested credentials. Then the credentials are transmitted from the identity provider to the relying party, via the broker. The credentials will be visible to the broker as they pass through but typically will not store or otherwise process them.

Credentials

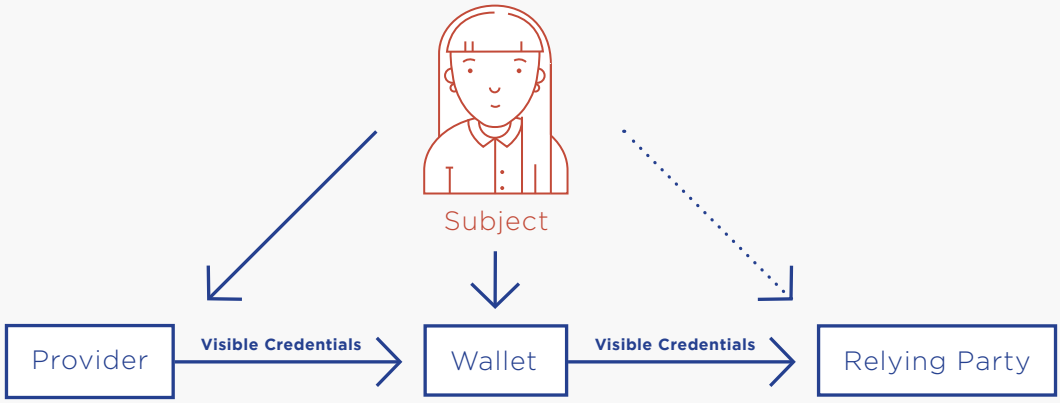
As with the federation example, the range of credentials that can be supported in this example may be limited, depending on the level of support and capabilities of the identity provider.

Certifications

Similarly, the reliability of the credentials will depend on the processes employed by the identity provider and consequently, they will be the focus of any certification process performed in the network.

Example 3 – Wallet

Figure 4
Wallet



The wallet example takes a different approach.

- The subject has a secure wallet in which they can store credentials received from providers. The wallet will use cryptography to ensure that only the subject is able to see and control the contents.
- The subject may have multiple wallets. Depending on the network the subject may need to obtain their wallet from specifically approved providers, or the subject may be able to choose one that suits their needs.
- A directory or ledger may also be used to enable relying parties to verify the provider of a credential.

Wallet approaches tend to focus on credential sharing (sometimes referred to as attribute exchange) rather than identity per se. Examples include networks commonly referred to as “self sovereign identity”.

Connections

The wallet is the means through which parties connect in this example. The wallet may be a service, app or device. It provides the subject with the functions required to collect, manage and share credentials.

The wallet will establish connections or relationships with providers and relying parties (with the subject’s consent). Depending on the network these connections or relationships may persist.

Communications

Credentials are always transmitted from provider to relying party via the wallet. Any credentials that the wallet processes will be visible to the wallet but cryptographically protected by one or more keys that are under the control of the subject. In other words, the wallet will provide secure storage but will itself be able to see the credentials it processes.

The wallet will play a role in helping the subject determine which providers and credentials will satisfy the requirements of the relying party. The aim however is that subjects will connect their wallet to many providers (who in other transactions will be relying parties).

Credentials

Wallets are usually designed to enable a flexible exchange of credentials. Identification can be achieved through the sharing of credentials that identify the subject. Authentication is also achieved by the sharing of credentials – a credential will only be valid if it has been signed by a cryptographic key under the control of the subject.

A “provider directory” may also be present allowing relying parties to lookup and locate providers, allowing them to check the source of credentials.

Certifications

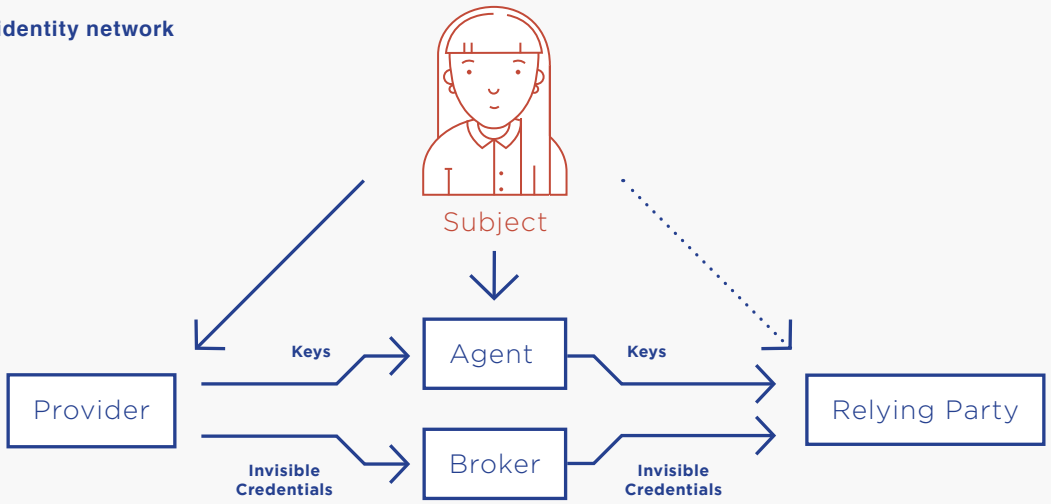
The reliability of the credentials (and the attributes contained within them) in the wallet example will depend on

the nature of the credential and provider in question. When a provider is authoritative (e.g. the driver's license authority stating whether someone has a current driver's license or not) the relying party will need to be sure that the credential was issued by that provider, pertains to the subject and has not been altered. When the provider has derived the attributes contained in a credential (e.g. a bank stating it has verified the subject's age) the relying party will need some assurance of the processes employed.

The wallet example envisages a wide range of providers, each issuing one or more credentials about the subject. Consequently, any certification process may need to be wide-ranging and extensible. An alternative approach, to limit the scope of certification, may be to define "domains" of usage where specific providers can be certified to issue specific credentials for defined purposes.

Example 4 – Blinded Broker

Figure 5
Blinded broker identity network



The blinded broker shares many characteristics of the wallet example, but also contains some key differences.

- The subject has a secure user agent which they use to control the transmission of credentials from provider to relying party. The credentials do not flow through, nor are they stored, in the agent. Instead encrypted credentials are transmitted via a broker with the encryption keys (only) being shared via the agent. This results in the content of the credentials being invisible to the broker. It can also allow the provider and relying party to be blinded (i.e. not to know who the other party is).
- The subject may have the ability to enable multiple agents, though typically will have only one. While many organizations can be providers in this example, an agent is often obtained from specifically approved providers.
- This example uses an approach where credentials are exchanged in a way that is "invisible", one that the participant cannot see. The credential is encrypted as it travels through the broker, with the keys used to recover the data being transmitted through a different channel (the agent).

A blinded broker is typically operated by a trusted organization or consortium, who determine what providers and relying parties can participate in the network. This participation is often based on a contractual agreement between the various parties and the network operator(s). The Verified.Me service in Canada is an example of this approach.

Connections

The agent and the broker are the means through which parties connect in this example. The agent may be a service, app or device. It provides the subject with the functions required to collect, manage and share credentials.

The broker will establish connections or relationships with providers and relying parties (with the subject's consent). Depending on the network these connections or relationships may persist.

Communications

Credentials are always transmitted from provider to relying party via the broker, but only once it is confirmed that the credentials are to be exchanged, under the control of the subject. The credentials will be invisible to the broker. They will be cryptographically protected by keys that are under the control of the subject and to which the broker does not have access.

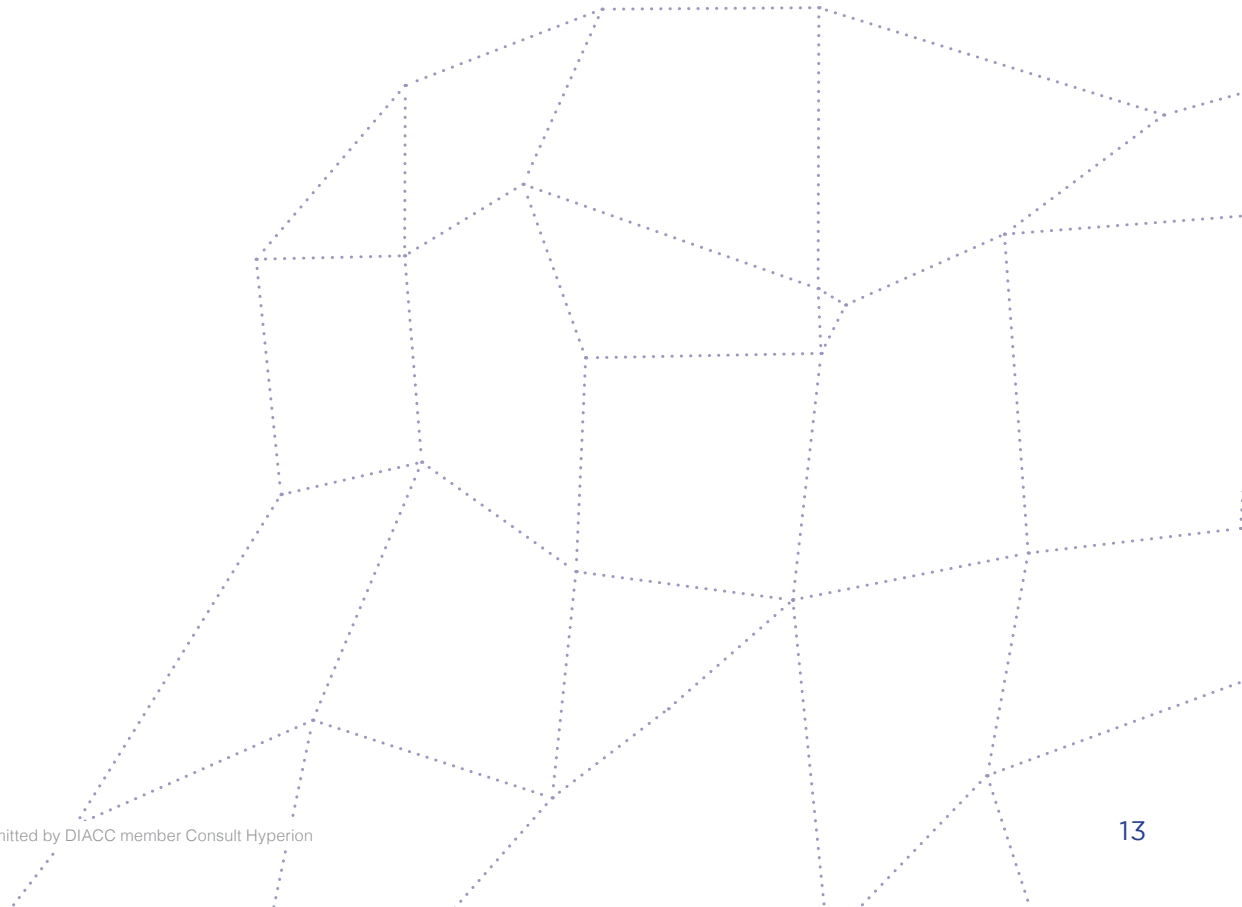
The wallet will play a role in helping the subject determine which providers and credentials will satisfy the requirements of the relying party. The aim however is that subjects will connect their agent to many providers (who in other transactions will be relying parties).

Credentials

A blinded broker approach is usually designed to enable a flexible exchange of credentials. Identification can be achieved through the sharing of credentials that identify the subject.

Certifications

The reliability of the credentials (and the attributes contained within them) in this example will be based on the governance and rules the network operator(s) implement to determine what credentials and attributes can be provided by approved providers. Specific providers can be certified to issue specific credentials for defined purposes. Since the network operator does the vetting of the providers on behalf of the rest of the network participants, and the network participants agree to the terms of being part of the network, there is inherent reliability of these credentials. If any providers or relying parties are determined to be introducing false or fraudulent credentials, they can be either suspended until the problem is resolved or removed from the network.



Mary – After

With an identity network

Mary is a small business owner who has decided to participate in a digital identity network. She is digitally savvy and has many online accounts with service providers. She realizes that one of these providers, who she trusts, now offers an ability to take advantage of a digital identity wallet service. She sets up two wallets – one for her and one for her business. In each context of her life, she can now carry out everyday tasks more efficiently, waste less time on manual processes, and have more trust in who she is dealing with online.

Consumer

Mary needs access to the results of her recent lab tests from her health care provider. To gain access, she proves who she is to her health care provider's eHealth system using credentials from her digital identity wallet. The lab test results are then disclosed to Mary's wallet, which only she can see. She can then share those results with another health care provider if she gives consent to that provider to have access to the lab results. She can also revoke access to the results at any time.

Business

As a small business owner, Mary has many potential suppliers available to deliver the products she needs to operate her business. Through her identity network, she's able to verify legitimate supplier businesses and interact with them virtually to get offers. She's also able to utilize a bidding system to request prices for an inventory of goods and easily compare prices across suppliers.

Government

In order to operate her business, Mary needs to obtain and keep current numerous business licenses and permits. Whenever she needs to apply for a new license or renew an existing one, now she's able to do this online without having to either walk into a government service center or mail in paper forms. She also gets a decision faster, usually within a few days, and is issued a digital license that can be used in other contexts to prove her business is licensed.

4 Requirements of an Identity Network

Identity networks are more than technology. For multiple parties to collaborate in a safe, secure and predictable way there need to be clearly defined legal, business, and technical rules that determine how participants behave.

The purpose of this document is not to give an exhaustive set of requirements for identity networks. However, to allow a comparison of the four network examples described above, this section provides an outline of the requirements of an identity network. These are high level and cover the key things that users of identity networks will need.

The requirements are generic and should apply in one way or another to every identity network.

The requirements are grouped into two areas:

- Governance: setting and enforcing the rules of the identity network
- Operation: implementing and operating the rules of the identity network

To work, identity networks need to serve and meet the needs of all network users. So, for each requirement, the key need(s) of the three network user types (subject, provider, relying party) is listed.

Governance

Requirement 1 - Participation

Most identity networks define rules that govern who can use the network. These rules may restrict who can be a provider or relying party, or place requirements on those network users to be vetted in some manner. Rules will define how subjects participate in the network too. This could include defining how a subject initially joins the network but also how their access to the network is maintained over time. The rules of participation could include the commercial terms and other legal or regulatory restrictions.

We are only considering the rules for network users (subjects, providers and relying parties) to participate in the network as opposed to the delivery of the network itself. Of course, in a distributed or decentralized network, the rules for participation in the delivery of the network are intertwined with the architecture and need to be defined. In section 5, we consider how different network architectures (and hence delivery models) impact these generic requirements.

The basic requirement of each network user is as follows:

Network user	Requirement
Subject	Be able to participate (inclusion)
Provider	Clear rules for participation and confidence in other participants
Relying party	Clear rules for participation and confidence in other participants

Requirement 2 - Transparency

Identity network users gain confidence in the network when the functioning of the network is transparent and understandable. There will be several areas of interest to network users.

All network users will want to have confidence that sensitive data is protected. In particular, network users will need to know that personal data is processed in line with data protection laws, including obtaining explicit consent from the subject to whom that data pertains, when necessary.

Network users will also need to understand, to some level, the processes used to establish, maintain and secure digital identities. This will be of particular interest to relying parties who may make business decisions based on the digital identity information they receive.

The basic requirement of each network user is as follows:

Network user	Requirement
Subject	Transparency over how credentials, and the attributes they contain, are used and clear straightforward means to manage credentials
Provider	Assurance that consent is correctly obtained, from the subject, to release credentials (when the consent is not obtained directly by provider)
	Transparency over downstream use of credentials
Relying party	Transparency over production and provenance of credentials that are relied upon

Requirement 3 - Accountability

Accountability is concerned with ensuring all parties act responsibly while upholding their obligations. Of course, no system or organization is perfect so when things go wrong, parties that incur a loss may be entitled to recourse. This could include, for example:

- If a subject's digital identity is stolen or taken over, the subject (who may be an individual, organization or device) may want assistance recovering their digital identity and to be compensated for any financial loss.
- If a relying party provides a service in error based on incorrect information from a provider, then the relying party may want protection against any reputational or financial loss.

The basic requirement of each network user is as follows:

Network user	Requirement
Subject	Have recourse in the event something goes wrong, including being able to repair erroneous personal data and seek redress for harm caused
Provider	Relying parties of credentials are responsible and will be held accountable in the event of a breach
Relying party	Clear liability arrangements
	Verifiable or audited evidence of provider processes

Operation

As with any secure system, the operational requirements of a digital identity network can be distilled down to three fundamentals: confidentiality, integrity, and availability.

Requirement 4 - Confidentiality

Confidentiality is concerned with ensuring credentials are protected from unauthorized or inappropriate disclosure. This includes ensuring that credentials are only shared with consent and that once consent has been given, the system ensures that only legitimate parties see the data.

Identity networks should include features to minimize the credential information disclosed. For example, disclosing that a subject "is over 18" as opposed to disclosing the subject's date of birth.

Identity networks should prevent the use of credentials, and associated information, for the tracking and surveillance of subjects.

The basic requirement of each network user is as follows:

Network user	Requirement
Subject	Credentials are only shared with consent
	Data is only used for purposes that the subject agrees to
	Network does not enable tracking or surveillance of a subject
	Network does not include honeypots that if breached would impact many subjects
Provider	Legal basis to share data
	Being confident no data protection issues arise from downstream use of credentials
Relying party	Credentials received are minimized to mitigate data protection risks
	Data is only used for purposes that the subject agrees to

Requirement 5 - Integrity

Ensuring that an identity network protects the integrity of credentials is vital to maintaining confidence in the network. All network users need to be sure that credentials are transmitted reliably and cannot be altered maliciously or otherwise. Some identity networks may allow new credentials to be derived from others (e.g. "is over 18" to be derived from date of birth). In these cases, the integrity of data end-to-end must still be maintained.

Relying parties, in particular, need to be sure that the credentials they receive (and act on) are correct, unaltered and pertain to the subject in question. Without this, they would be unlikely to use the network.

Identity networks should include non-repudiation, meaning network users cannot deny sharing credentials after the fact. They should also include measures to detect and prevent fraudulent activity.

The basic requirement of each network user is as follows:

Network user	Requirement
Subject	System protects against identity theft and other abuse
Provider	Credentials cannot be altered downstream, resulting in fraud, disputes and/or inconvenience to subject
Relying party	Credentials are issued to the subject, have not been revoked and are received unaltered from the provider
	Network detects and mitigates against fraud

Requirement 6 - Availability

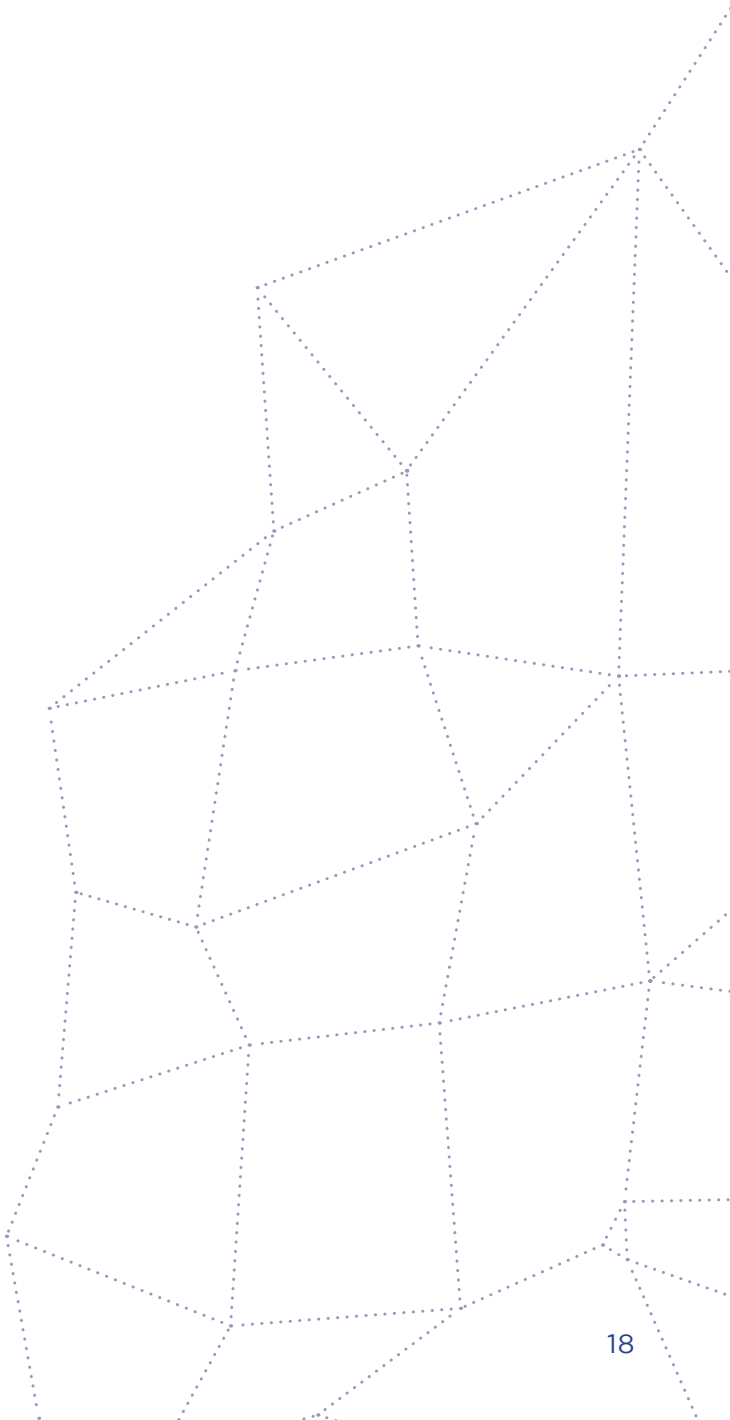
Identity networks need to be sufficiently available for the services that they enable. This includes ensuring that the network and the inputs to the network (e.g. providers) are available when they need to be. Without this, digital services will not function.

The architecture of an identity network and the way it is used will determine the service levels required from each of the participants in order to maintain sufficient availability. The architecture will also determine where denial of service may occur. Of course, the aim should be to avoid single points of failure.

As well as technical availability, there is a more fundamental inclusion issue. Access to identity networks has often been more difficult for certain groups, e.g. people who do not have access to the right documentation. Identity networks should be designed so that all rightful network users can get access. This should include ensuring that a network user cannot be denied access without a legitimate reason.

The basic requirement of each network user is as follows:

Network user	Requirement
Subject	Digital identity can be used when required
	Digital identity cannot be inappropriately taken away
Provider	System does not place onerous service level requirements on provider
Relying party	System is available when needed, depending on whether it supports offline or online transactions



5 Comparing Identity Networks

Two models for delivery – Trust and Agency

Identity networks meet the requirements of the network users described above through a combination of:

- Trust: The network user needs to trust the network to ensure that their requirements are met, and
- Agency: The network user can act independently and make their own free choice over how their requirements are met

Some identity networks place a greater emphasis on trust and the need to ensure that the participants in the network are trustworthy. Other identity networks place a greater emphasis on agency, seeking to give greater control to network users – which of course also brings with it, greater responsibility. In the end, all identity networks rely on a combination of trust and agency.

To provide a high-level comparison of the four identity network types (federation, broker, wallet and blinded broker) we consider for each of the major requirements, whether they are met more through trust or more through agency. The aim is not to judge whether trust or agency should be preferred, only to make a comparison. It will then be down to the potential participant to assess which approach aligns more with their needs.

In all cases, we assume the best about the network types in question in order to provide a fair comparison. The aim is to show objectively the differences arising from the architectural approaches. We assume that the networks:

- Are implemented in a secure and privacy-respecting way (as far as the architectures allow)
- Include all legal/contractual measures as may be necessary to operate the network correctly

At a high level, the network examples can be generally summarized as follows:

Federation

Provides more agency to providers

Broker

Requires the most trust overall

Wallet

Provides more agency to subjects and relying parties

Blinded Broker

Requires trust, but also provides agency to the subject

Of course, the reality may be different when considering an actual network. Understanding the characteristics of an architecture is a starting point in choosing a network. As discussed in sections 6 and 7, the details of the specific network in question should be also understood.

Comparing approaches

The following table illustrates how the four example network architectures, described above, compare in terms of their reliance on trust or agency.

	Federation			Broker		
	Provider	Subject	Relying Party	Provider	Subject	Relying Party
Governance						
Participation	Agency	Trust	Agency	Trust	Trust	Trust
Transparency	Agency	Agency	Trust	Agency	Agency	Trust
Accountability	Agency	Agency	Agency	Trust	Agency	Trust
Operation						
Confidentiality	Agency	Trust	Trust	Trust	Trust	Trust
Integrity	Agency	Trust	Agency	Trust	Trust	Trust
Availability	Trust	Trust	Trust	Trust	Trust	Trust

	Wallet			Blinded Broker		
	Provider	Subject	Relying Party	Provider	Subject	Relying Party
Governance						
Participation	Trust	Agency	Agency	Trust	Trust	Trust
Transparency	Trust	Agency	Trust	Trust	Agency	Trust
Accountability	Trust	Trust	Trust	Trust	Agency	Trust
Operation						
Confidentiality	Trust	Agency	Agency	Trust	Agency	Agency
Integrity	Agency	Trust	Agency	Agency	Trust	Agency
Availability	Agency	Agency	Agency	Trust	Trust	Trust

Appendix A provides a more detailed assessment including the rationale for each categorization of either “Trust” or “Agency”. The table shows some clear differences between the network architectures which are discussed below. As with all such assessments, there will inevitably be differences when comparing against an actual identity network implementation.

Trust and Agency in Federation Networks

Federation networks are often considered to be trust-based. Subjects typically rely on a single provider to manage their identity. However, subjects do have a level of agency. They can choose which provider to use, or even to have multiple digital identities by using multiple providers. Because the subject has a specific relationship within the network (with the provider), it should be relatively clear who they would complain to in the event that their digital identity was compromised. Of course, the level of recourse they would have with the provider would be dependent on the specific terms of the service offered by the provider (which may be mandated by the network itself in order to participate in the network).

Providers have agency in that they have much greater visibility over where digital identities are being used compared to the other network architectures. While this may be good for providers, it is less privacy-respecting for subjects and creates the risk that a provider could prevent a subject from accessing services from certain relying parties. Appropriate governance is required to ensure that the interests of the subject are protected.

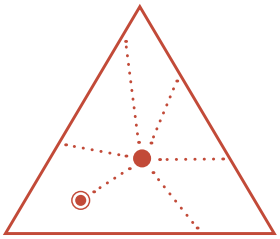
While not commonly done, federated identity networks could apply cryptographic integrity controls to the transmission of credentials. This would provide non-repudiation in provider-to-relying party communications.

Trust and Agency in Broker Networks

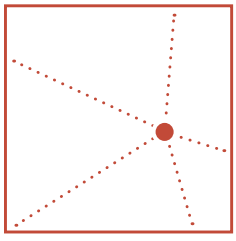
In many respects, broker and federation networks are similar. In both the subject has a single provider relationship, who they need to trust to manage their identity.

The key difference in the broker example is the presence of a broker between providers and relying parties. The broker provides a means to integrate the parties but more importantly provides a privacy "air gap" between providers and relying parties. As a result, providers should not be able to see where credentials are being sent – this reduces the agency afforded to providers but also reduces the trust that subjects need to have in providers. On the other hand, the broker itself is a potential point of surveillance requiring subjects to trust that inappropriate monitoring or analysis of network usage does not occur. The network governance must ensure this does not happen.

Typically, the broker can see all credentials flowing across the network. Normally this will be transient and the expectation on the broker will be that it will not record the credentials, however the subject needs to trust that this is the case.



Federation Network



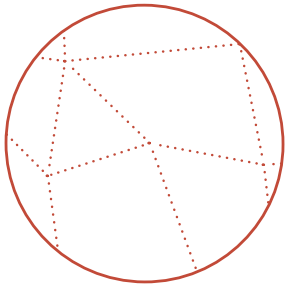
Broker Network

Trust and Agency in Wallet Networks

Wallet networks are designed to provide agency to subjects. They do this by placing the wallet, which is controlled by the subject, between providers and relying parties. As each subject has their own wallet, the network is in effect decentralized with the control sitting with the subjects, at the edges.

The user must trust the wallet but, when implemented well, it will give them complete control of the flow of credentials (or proofs derived from them). Emerging standards, such as those for decentralized identifiers and verifiable credentials, will allow wallets to be interoperable at the "connections", "communications" and "credentials" layers. This will provide the subject with greater agency, allowing the subject to connect to any number of providers and relying parties (who support the standards), enabling the sharing of credentials between them (always via the subject).

From a governance perspective, there is still a need for trust. Relying parties will need to determine which providers are suitable for them and to be able to tell the subject (or their wallet) which providers are acceptable. This will require a governance framework that allows a relying party to assess the level of trust they put in credentials received from one provider (or provider type) over another.

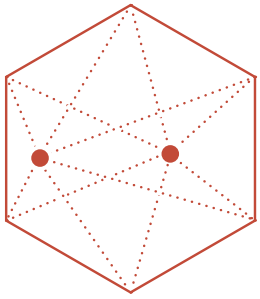


Wallet Network

Trust and Agency in Blinded Broker Networks

A blinded broker network is similar to a "broker network" except that the broker is not able to see any of the credentials as they are transmitted. The broker still provides a privacy "air gap" between providers and relying parties, meaning that both need to trust the network as it is responsible for vetting which providers and relying parties can participate. It also sets standards for providers, or groups them according to type (e.g. regulated entity, non-regulated entity) in order that the relying party can specify the type of provider that will meet their needs without necessarily knowing exactly which provider is to be used.

The blinded broker network, by providing the subject with an agent, gives greater agency to the subject. The agent, in combination with the blinded broker, allows the subject to control the sharing of their credentials and minimize the risk of exposure during transmission.



Blinded Broker Network

6 Choosing an Identity Network

There are many factors in determining whether to participate in an identity network or not. This section discusses some of the key considerations.

Utility

The range of services offered by identity networks varies. Understanding whether a particular identity network will serve your needs requires considering the following:

Identity transactions supported

As highlighted in section 2 above, identity networks can provide identification, authentication or authorization services.

Many established identity networks have focused on identity verification and logon services. Often the newer identity networks are looking to extend the scope to support the exchange of credentials, under the subject's control.

Sector

Some identity networks are built for or within specific sectors, e.g. government sector or financial services. Where this is the case, the ability of those networks to be used in other sectors will depend on:

- Legal, regulatory or commercial restrictions limiting their use
- Flexibility to support the requirements of another sector
- Privacy concerns arising from opening up the network

Other identity networks are designed to be usable in a range of sectors. The question then is whether the needs of your sector can be supported by the identity network.

Scope

Most identity networks to date have focused on providing portable digital identities to individuals and often just to enable them to access services. But digital identity applies to far more than consumer-to-organization interactions.

Organizations have identities. Today these identities may be manifested through registers of companies and the like. These identities along with any associated credentials, need to be available in digital form for organizations to be able to function effectively in the digital economy.

Connected devices have identities too. While devices usually act on behalf of individuals or organizations, there will be credentials (e.g. serial number) that stay with the device regardless of who it is acting for. It is therefore useful to consider devices as having identities in their own right.

Across the digital economy, transactions will be performed between every conceivable permutation of individual, organization, and device. Which of those apply to you will determine whether a specific identity network meets your needs.

Mode

Credentials will be transmitted from providers to relying parties in one of two modes:

- Real-time: the credential is obtained from the provider real-time, at the point it is requested by the relying party. The mode is supported by all network architectures.
- Store and forward: the credential is obtained from the provider ahead of when it is requested by a relying party. This mode typically only applies to wallet network architectures, where credentials can be stored in a wallet until the subject chooses to share them with a relying party.

There are advantages and disadvantages to each approach. Real-time credentials will be more current (up to date) but depend on the provider being online. Store and forward credentials are simpler to orchestrate (you know if you have the necessary credentials) and do not require the provider to be online. Revoking credentials is more challenging (but possible) and ensuring credentials are up to date may be an issue.

Identity migration

In an ideal world, it should be possible for subjects to migrate their digital identities, i.e. choose a different organization to help them manage it. In federation and broker examples, where usage may be limited to identification and authentication, this often involves starting from scratch with a new provider. In other words, migration is not built into the network design.

Wallet identity networks sometimes give the subject significant choice over their wallet. This suggests that if a subject is unhappy with one wallet, they could move to another wallet – including transferring all stored credentials. Whether or not this is actually supported by wallets is another matter as the process is likely to involve subtle cryptographic key management processes that if implemented badly could leave a wallet open to takeover or theft – although depending on implementation may not enable a scalable attack.

For identity networks that support the broad exchange of credentials, the need to support migration will be more pressing, as the task of re-establishing all credentials (or all connections) could be onerous for the subject.

Interoperability

Identity networks clearly need to be able to interoperate with the systems employed by network users. It is often highly desirable for identity networks to conform to industry standards. This may allow identity networks to interoperate with each other or allow network users to choose to employ an alternative identity network, avoiding being locked into proprietary solutions.

Adoption

To be successful an identity network will need to be adopted by subjects, providers and relying parties. Some potential network users may only wish to participate in a network with sufficient rates of adoption or growth rates indicating future adoption levels. For others, this may be less of an issue.

Trust

As discussed in section 4, all identity networks rely on trust to some level to meet their requirements. When evaluating a particular network, the following may need to be considered in this area.

Governance

In every identity network, the governance arrangements are key to determining how the network is implemented and what controls are put in place to ensure the network remains safe and secure. Ultimately, however, you will need to rely on regulation or legal contract to gain a level of certainty on how well you or your customers' interests are protected.

Where regulation of identity systems exists today, it tends to relate to specific government-controlled identity systems. For most identity networks, the rules are set by a commercial organization or a consortium, so you will need to rely on your contract with that body, whether direct or indirect.

Some wallet networks are seeking to create open, transparent and sustainable governance structures. Only time will tell how these structures are held legally accountable in any particular jurisdiction. You should consider carefully what recourse you or your customers would have – either from the network itself or from the organization through which you obtain access to the network.

Transparency

Transparency is a key enabler for trust. The more open a system is to public scrutiny, the more likely it is to be robust. The same principle sits behind open-source software.

All identity networks leverage open protocols for interoperability reasons. These provide an element of transparency. The specific components within a network – providers, wallets, etc. may not be open source, however.

Assurance

Alongside transparency, there will also be a need for assurance processes, that ensure that services are robust and auditable. This could include assessing the processes employed in the sourcing of attributes and the issuance of credentials. It could also include ensuring that appropriate security standards and other best practices are followed.

You should consider the protections built into the network including the ability to monitor and detect fraud, how compromised credentials are revoked and how the network ensures that network users behave appropriately, e.g. relying parties only answer for credentials that they need.

Funding

Understanding how a network is funded will help you determine what the incentives are for the various players in an identity network. In particular, if the funding of the

identity network (or some component of it) is in conflict with the protections the network is supposed to provide, that could raise serious trust concerns.

This has been a constant issue for social networks that depend on targeted advertising for revenue, which is in direct conflict with delivering a privacy-respecting service. There are also questions over content providers who employ subscription models. It is often far from clear how personal data is used.

Maturity

The digital identity landscape is rapidly changing with much innovation occurring. While this is producing potentially compelling new models for how digital identity is done, it will take time for these new initiatives to mature and be tested at scale. You need to be aware of the maturity of any digital identity network to ensure you can mitigate any risk arising from the lack of maturity.

Privacy

Privacy is fundamental to identity networks, especially those serving individuals. It is paramount that privacy principles (such as the PIPEDA Fair Information Processing Principles) are upheld and that systems are built with privacy-by-design. Nonetheless, you should assess whether the approach to privacy taken by any identity network under consideration meets your specific needs.

Choice

Choice allows subjects to have some say over who processes their personal information, allowing them to decide, to some extent, who they wish to trust.

In the federation and broker examples, subjects will choose a provider to manage their digital identity. They will not be able to choose the partners that the provider collaborates with, however. Often these partners will provide background data sources that are used to establish the subject's identity.

In the wallet example, the subject will choose which wallet to use to manage their digital identity. The subject may also be able to choose which providers to connect to, in order to obtain credentials – so long as they have relationships with enough providers to facilitate a choice.

The blinded broker example allows the subject to choose providers that the network has vetted and brought into the network.

Data protection

You should take care to ensure that your data protection obligations are met, bearing in mind that data protection law varies between jurisdictions and different laws may apply to government and private sector organizations.

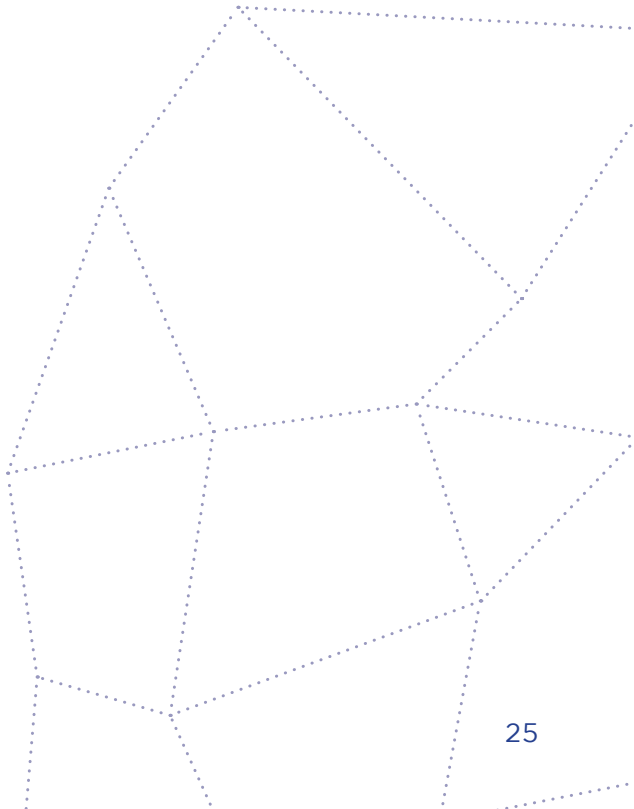
Transparency

Transparency is important in protecting privacy as well as in governance. The way that personal data is held and used must be understandable and clear to subjects for them to be able to use the identity network confidently.

Accountability

Accountability complements transparency providing network users, but subjects in particular, confidence that the providers of the network will be held to account in the event that personal data is compromised.

Wallet networks attempt to give the subject agency with respect to their digital identity. This could place additional responsibility on the subject and reduce the accountability of the identity network itself. Getting the balance right here will be important to ensure subjects have both control and recourse.



7 Final Considerations

Comparing identity networks may not be a straightforward exercise. The different architectures do not map directly onto each other and networks of the same type may vary in implementation. The following general points should be considered when evaluating any identity network.

Are you comparing like with like?

Some identity networks provide all four layers described in section 2 above (connections, communications, credentials, certifications). Others focus on the first three layers only (connections, communications, credentials).

If two networks do not provide the same layers, it may not be possible to make a direct comparison between them. When comparing two or more identity networks it is important that you ensure you are comparing like with like, otherwise any conclusions drawn will likely be incorrect.

When an identity network does not cover the certifications layer, it will be necessary to plug that gap, for example by defining a trust framework and associated governance. Typically trust frameworks are not defined in isolation. Rather they contain the agreed rules that govern how a network is used within a specific sector or context.

Are you building for now or the future?

The examples presented in section 3 reflect developments occurring in the market, with the general direction of travel being towards architectures that are more decentralized and more centered around the subject. The maturity of individual identity networks will vary considerably.

For some organizations, digital transformation will take years to achieve. While digital identity is central to any such transformation, what that means will depend on where the organization is in its transformation journey. For example, an organization may first seek to replace existing manual identification processes with a digital equivalent. That may provide some immediate benefits to the organization and its customers. In the long run, full digital transformation could fundamentally change the way that customer data is managed, enabling new digital services and user experiences not previously possible. When selecting an identity network, it is important to consider both short term requirements and longer-term goals – as the identity network required to address these needs could differ, requiring a roadmap to ensure that the approach taken in the short term does not prevent achieving those longer-term goals.

Does the implementation meet your specific needs?

The examples presented in this paper provide a guide but are not a substitute for ensuring the specific identity network in question, and its implementation, meet your needs.

The wallet and blinded broker examples given use strong cryptographic mechanisms that, if implemented well, provide high levels of authentication and integrity. Federation and broker networks on the other hand, are often based on less advanced logon-based controls, which can be susceptible to account takeover. The examples are however only illustrative. It is essential you understand the strengths and weaknesses of any network you consider.

You should use the requirements, listed in section 4 above, as a guide to defining your own detailed requirements. These can then be used to ensure that a specific identity network under consideration meets your needs.

What are the network user needs?

In section 5, we considered whether identity networks are more trust or more agency based. We have not however argued which of trust or agency is better – if indeed there is a simple answer to that question. In reality, some combination of both is needed.

Network users need to be sure that identity networks are safe, secure, reliable and proportionate. Inevitably, network users will need to trust the suppliers of identity network services on some level. On the other hand, solutions should be open to scrutiny and architected to minimize (as far as possible) the trust that must be placed on suppliers.

7 Final Considerations

The need for trust is likely to be greatest for individuals, who typically will have the least capability to determine whether something is fit for purpose or not. They also typically have the least ability to manage their identity information well. So, while a network may provide agency in its design, it is likely that individuals will still need to rely on an organization they trust to participate safely in any identity network.

Getting the right balance of trust and agency will be key to ensuring that the needs of network users are met and that they have confidence in the network.

As the world becomes increasingly connected, it is vital that services are built that better protect the data of individuals and businesses. But this must be done in a way that reduces friction, supports inclusion and provides choice. Otherwise services will not be used, or certain segments of the population could be excluded. Identity networks put individuals and businesses back in control of their data, supporting seamless but secure access to the rapidly developing digital economy. Choosing the right identity network requires careful consideration, but it is an important step in digital transformation.

Appendix A – Assessing Networks

Federation

Requirement	Primary Basis	Rationale
Governance		
Participation		
Provider	Agency	Can see who the relying party is
Subject	Trust	Relies on provider to be inclusive
Relying party	Agency	Can see who the provider is
Transparency		
Provider	Agency	Usually provider will control the consent process
Subject	Agency	Consent process will be provided by provider to subject
Relying party	Trust	Processes followed by provider to produce credentials not auditable by relying party. Relying party either has to trust provider directly or third-party audit process
Accountability		
Provider	Agency	Knows where credentials are being used so could seek recourse
Subject	Agency	Single relationship (with provider), so clear place to seek recourse
Relying party	Agency	Knows where credentials come from so could seek recourse
Operation		
Confidentiality		
Provider	Agency	Knows where credentials are being used so can, to some extent, hold relying parties to account
Subject	Trust	Subject has no visibility or part in provider-to-relying party communications
Relying party	Trust	Relies on provider to only share minimal credentials
Integrity		
Provider	Agency	Provider communicates directly with relying party so could put non-repudiation measures in place
Subject	Trust	Relies on provider to implement identity theft protection
Relying party	Agency	Relying party receives credentials directly from provider so could put non-repudiation measures in place
Availability		
Provider	Trust	Provider needs to be able to meet requirements of network
Subject	Trust	Relies on provider being available and continuing to provide service
Relying party	Trust	Relies on provider being available

Broker

Requirement	Primary Basis	Rationale
Governance		
Participation		
Provider	Trust	May not see who the relying party is
Subject	Trust	Depends on availability of suitable provider
Relying party	Trust	May not see who the provider is
Transparency		
Provider	Agency	Usually provider will control the consent process
Subject	Agency	Consent process will be provided by provider to subject
Relying party	Trust	Processes followed by provider to produce credentials not auditable by relying party. Relying party either has to trust provider directly or third-party audit process
Accountability		
Provider	Trust	May not know where credentials are being used so will rely on network to hold relying parties to account
Subject	Agency	Single relationship (with provider), so clear place to seek recourse
Relying party	Trust	May not know where credentials originate from so will rely on network to hold provider to account
Operation		
Confidentiality		
Provider	Trust	May not know where credentials are being used so will rely on network to hold relying parties to account
Subject	Trust	Subject has no visibility or part in provider-to-relying party communications Potential point of surveillance at the broker
Relying party	Trust	Relies on provider to only share minimal credentials
Integrity		
Provider	Trust	Has to trust broker not to alter data
Subject	Trust	Relies on provider to implement identity theft protection
Relying party	Trust	Has to trust broker not to alter data
Availability		
Provider	Trust	Provider needs to be able to meet requirements of network
Subject	Trust	Relies on provider being available and continuing to provide service
Relying party	Trust	Relies on provider (and broker) being available

Wallet

Requirement	Primary Basis	Rationale
Governance		
Participation		
Provider	Trust	Cannot see who the relying party is
Subject	Agency	Anyone should be able to get a wallet
Relying party	Agency	Can see who the provider is
Transparency		
Provider	Trust	Provider may have to trust wallet to collect consent
Subject	Agency	Consent process will be provided by wallet to subject
Relying party	Trust	Processes followed by provider to produce credentials not auditable by relying party. Relying party has to trust either provider directly or third-party audit process
Accountability		
Provider	Trust	May not know where credentials are being used so will rely on the network to hold relying parties to account
Subject	Trust	While subject can see a full history of credential sharing, the process of obtaining recourse may be complex with multiple providers. No single place to go for recourse
Relying party	Trust	May not know where credentials originate from so will rely on the network to hold provider to account
Operation		
Confidentiality		
Provider	Trust	Does not know where credentials are being used so will rely on the network to hold relying parties to account
Subject	Agency	Subject controls the end-to-end transmission of credentials
Relying party	Agency	Protocols designed to support minimal disclosure
Integrity		
Provider	Agency	Integrity of data cryptographically protected
Subject	Trust	Will rely on wallet to protect against identity theft
Relying party	Agency	Integrity of data cryptographically protected
Availability		
Provider	Agency	Depending on implementation provider may not need to be “always on”
Subject	Agency	Subject is not reliant on provider as credentials are stored in wallet, controlled by subject
Relying party	Agency	Not reliant on provider being available

Blinded Broker

Requirement	Primary Basis	Rationale
Governance		
Participation		
Provider	Trust	Cannot see who the relying party is
Subject	Trust	Relies on network to be inclusive
Relying party	Trust	Cannot see who the provider is
Transparency		
Provider	Trust	Provider may have to trust agent to collect consent
Subject	Agency	Consent process will be provided by agent to subject
Relying party	Trust	Processes followed by provider to produce credentials not auditable by relying party. Relying party has to trust either provider or governance provided by network
Accountability		
Provider	Trust	Does not know where credentials are being used so will rely on the network to hold relying parties to account
Subject	Agency	Single relationship (with network), so clear place to seek recourse
Relying party	Trust	Does not know where credentials originate from so will rely on network to hold provider to account
Operation		
Confidentiality		
Provider	Trust	Does not know where credentials are being used so will rely on the network to hold relying parties to account
Subject	Agency	Subject controls the end-to-end transmission of credentials
Relying party	Agency	Protocols designed to support minimal disclosure
Integrity		
Provider	Agency	Integrity of data cryptographically protected
Subject	Trust	Relies upon strength of authentication to the agent
Relying party	Agency	Integrity of data cryptographically protected
Availability		
Provider	Trust	Provider needs to be able to meet requirements of network
Subject	Trust	Relies on provider being available and continuing to provide service
Relying party	Trust	Relies on provider (and broker) being available

Appendix B – Terminology

Term	Definition
Agency	The network user can act independently and make their own free choice over how their requirements are met
Agent	A service provided to a subject, allowing the subject to control the sharing of credentials (but not store credentials – see wallet below)
Attribute	A quality or characteristic of a subject
Broker	An identity network architecture based on a centralized service connecting providers and relying parties
Blinded Broker	An identity network architecture based on a centralized service connecting providers and relying parties, but where that service is unable to see the content of credentials it processes
Credential	One or more attributes together with associated metadata that links them to the subject and describes their provenance Credentials are issued by providers
Decentralized	An identity network architecture where providers and relying parties do not connect directly. Instead, they connect to a wallet, under the subject's control
Federation	An identity network architecture using a subject directory to connect provider and relying parties
Hub	A network component connecting providers and relying parties
Identity	A reference for a real, unique and identifiable subject
Identity Network	The governance, operations and technical infrastructure allowing credentials to be conveyed from providers to relying parties, directly or indirectly, with the consent of the subject
Identity Provider	A provider in a federation or broker identity network
Network User	A digital identity network exists to serve three main types of net-work user, including subject, provider, and relying party
Provider	An individual, organization or device that has information about the subject, that the subject may wish to share with relying parties. Information is shared in the form of credentials
Provider Directory	A service allowing relying parties to discover and locate the provider of an issued credential

Appendix B –
Terminology

Term	Definition
Relying Party	An individual, organization or device that wants to determine the identity or some information about the subject, in order to transact with that subject digitally and be able to trust (or rely on) the information received
Subject	A unique individual, organization or device distinguishable from others
Subject Directory	A service allowing relying parties to discover and locate the identity provider of a subject
Trust	The network user needs to trust the network to ensure that their requirements are met
Wallet	A service provided to a subject, allowing the subject to store and control the sharing of credentials