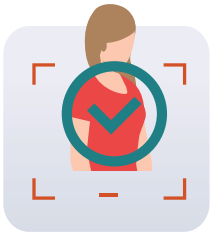
DIACC

Making Sense of Identity Networks Summary

Why do identity networks matter?

Identity plays a big part in our everyday lives, from opening a new account to proving your age, to travelling internationally.



Today identity is often fragmented, 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 realizing the full potential of digital services.

Digital identity networks are a way to address these issues, as they will give people greater control over their personal data, allow digital identities to be portable, help to detect and reduce fraud, and 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.

Who do identity networks serve?

Network users:

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.

What functions do identity networks support?

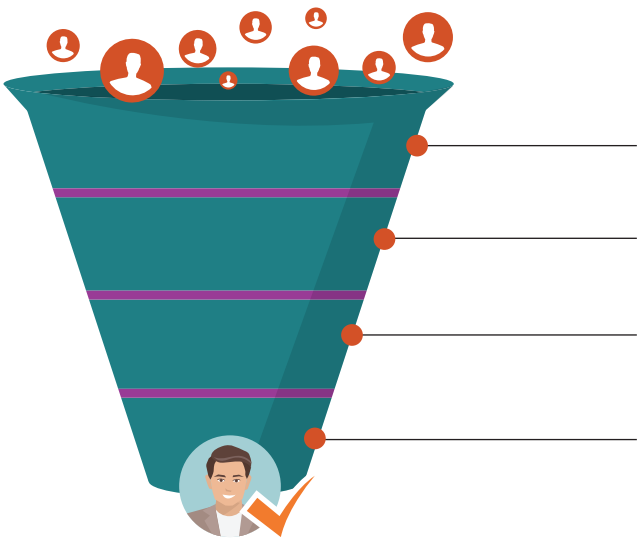
Identification
The process of establishing a real, unique and identifiable subject.

Authentication
The means by which a subject can assert their identity including showing it is the same subject as the one seen before.

Authorization
Giving the subject the means to control the sharing of their information from providers to relying parties. Information is disclosed in the form of a credential – containing the information (or "attributes") shared along with metadata that links to the subject and describes its provenance.

How to visualize identity networks?

It is helpful to use layers to describe identity networks. Here are four layers help to compare the different aspects of networks in a consistent way.



Connections
Who has a relationship with whom?

Communications
How do the parties that are connected communicate?

Credentials
What do communications between the parties contain?

Certifications
How are the credentials established and what confidence do you have in them?

Identity Network Architectures - Four Examples

These are not exhaustive. They are simply meant to illustrate at a high level some of the approaches taken. The intention is that the overall framework can be applied to specific network solutions or implementations as required.

Two types of interactions:

Identity network interactions

Interactions between parties sharing credentials over the network.

Service interactions

Other relevant but indirect interactions (e.g. delivery of services)

Two types of credentials:

Visible Credentials

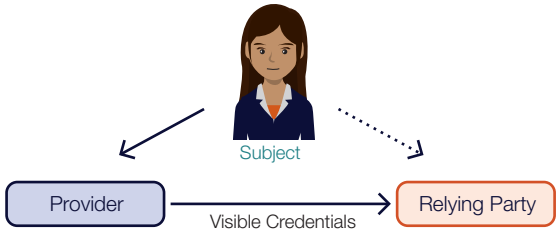
Both the sending and receiving parties can see the content of the credentials. Credentials likely transmitted through a secure communication but the parties at each end will be able to see the content.

Invisible Credentials

At least one party cannot see the content of the credentials

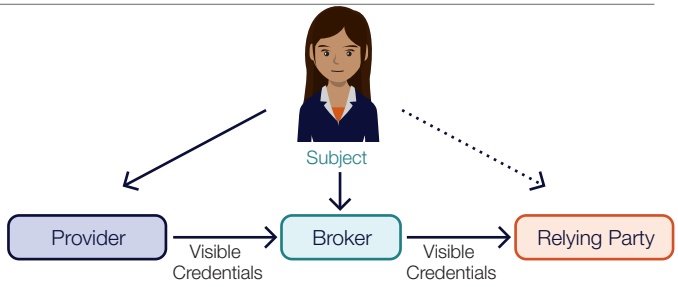
Federation

Allows a subject to use a digital ID managed by one organization ("identity provider") to access services from another organization (i.e. social logon). Subject has a single provider relationship, but can use multiple identity providers which results in multiple discrete digital identities.



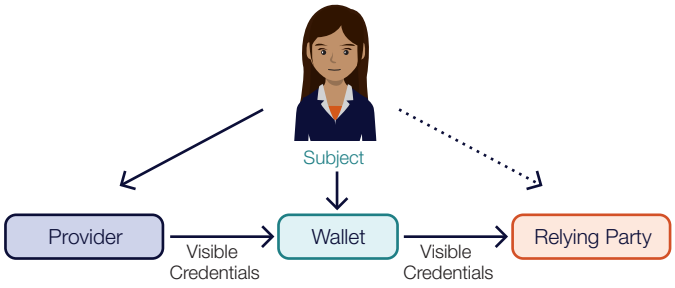
Broker

Similar to federation but with a 'broker' facilitating transmission between the provider and relying party/ies. Broker is used to connect the subject with the correct identity provider. Subject has a single provider relationship. Scope may be limited to identification and authentication.



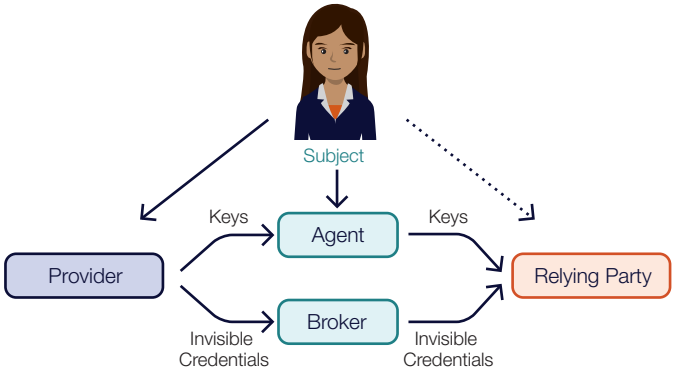
Wallet

Subject has a secure wallet in which they can store credentials received from providers. Only the subject is able to see and control the contents of the wallet. A directory or ledger may also be used to enable relying parties to verify the provider of a credential. Tends to focus on credential sharing (sometimes referred to as attribute exchange).



Blinded Broker

Similar to a wallet, but the subject uses a secure user agent to control the transmission of credentials, and the broker is not able to see any of the credentials as they are transmitted. It can also allow the provider and relying party to be blinded (i.e. not to know who the other party is).



What are the requirements of an identity network?

Governance

Requirements refer to setting and enforcing the rules of the network.

Participation:
Clear rules for who can be a provider or relying party, how network users are vetted, how subjects can join and participate, and how access for all network users is maintained over time.

Transparency:
Confidence that personal data is processed in line with data protection laws, including obtaining explicit consent from the subject. Understanding the processes used to establish, maintain and secure digital identities.

Accountability:
All parties act responsibly while upholding obligations. What recourse does subject have in the event something goes wrong? Provider and relying party have clear accountability and liability arrangements.

Operational

Requirements refer to implementing and operating the rules of the identity network.

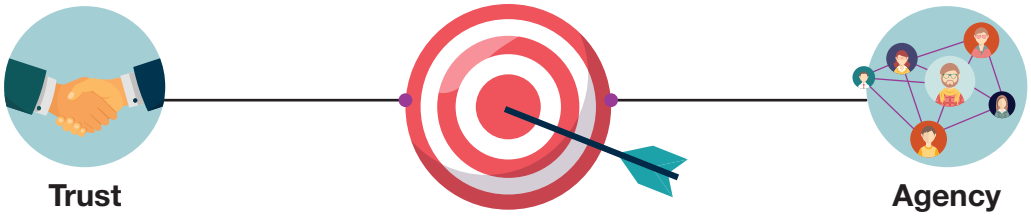
Confidentiality:
Ensuring credentials are protected from unauthorized/inappropriate disclosure (i.e. data minimization) and only shared with consent. Prevent the use of credentials for tracking and surveillance.

Integrity:
All credentials are transmitted reliably, and cannot be altered maliciously. Must ensure integrity of data end-to-end if/ when credentials are derived. Clear measures to detect and prevent fraudulent activity.

Availability:
Networks should be designed so that all network users can get access, are available when required and are inclusive for all.

What are the models for delivery?

Identity networks meet the requirements of the network users described above through a combination of Trust and Agency.



Trust
The network user needs to trust the network to ensure that their requirements are met.

Agency
The network user can act independently and make their own free choice over how their requirements are met.

All identity networks rely on a combination of both.

What are the factors to consider when determining whether or not to participate in an identity network?

Sector

Some identity networks are built for or within specific sectors (e.g. government or financial services). Consider whether the needs of your sector can be supported by the identity network.

Governance

Governance arrangements are key to determining how the network is implemented, what controls are put in place to ensure that it remains safe and secure.

Scope

The type of transactions that can be performed between every conceivable permutation of individual, organization, and device (e.g. connected devices also have identities).

Transparency

The more open a system is to public scrutiny, the more likely it is to be robust.

Mode

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

- **Real-time**
  Current; dependent on the provider being online. No concerns with ensuring credentials are up to date.
- **Store and forward**
  Easier to orchestrate, does not require the provider to be online. The credential is obtained from the provider ahead of time.

Assurance

Need to ensure that services are robust and auditable, including processes to source attributes, issue credentials, adhere to security standards, monitor and detect fraud, and revoke credentials.

Funding

If the funding of the network conflicts with the protections it is supposed to provide, trust concerns can be raised.

Identity migration

Ability to choose a different organization to manage digital identity (including credentials).

Maturity

Ensuring the network is mature, can be tested at scale, and can mitigate any risk arising from a lack of maturity.

Interoperability

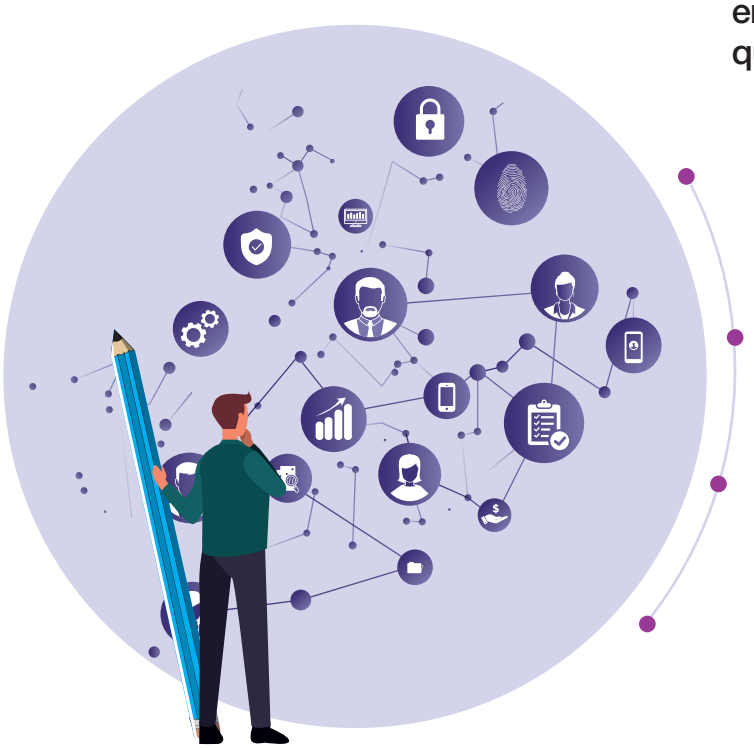
Identity networks need to be able to interoperate with the systems employed by network users and preferably conform to industry standards.

Privacy

Crucial that privacy principles are upheld, systems are built with privacy-by-design. Other important principles: choice, data protection, transparency, accountability.

Adoption

Importance of an identity network being adopted by subjects, providers and relying parties.



As a decision-maker within your organization, ensure that you are asking yourself these key questions when evaluating 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 users' needs?

Join the DIACC

Be part of the world-leading community unlocking economic and social opportunities for all by building a robust, secure, interoperable, and privacy-enhancing digital identification and authentication ecosystem.

Contact

The Digital ID and Authentication Council of Canada

diacc.ca @mydiacc /company/mydiacc /mydiacc