Canadian Credential Trust Alliance

A trust network for Canadian credentials

An introduction for Canada’s credentialing organizations

Operated by Oliu™ Partnership Corp.
June 22, 2026

Credentials are going digital across Canada

Across healthcare, skilled trades, safety, and education, the way Canadians prove what they are qualified to do is moving from paper and PDFs to verifiable digital credentials. Three things have lined up at once.

The standard is ready.

The W3C Verifiable Credentials standard is production-mature and in use today.

The policy environment has aligned.

Canada has committed to reducing the friction Canadians face when their credentials cross provincial lines.

Issuers are ready to move.

A generation of credentialing authorities is ready to go beyond paper.

Proving a credential is real is slow, manual, and easy to fake

These are not future problems. They are the daily friction in the credentialing business today.

Verification is manual.

When an employer needs to confirm a certificate is real, someone has to check it by hand, or call the school that issued it.

Fraud is hard to catch.

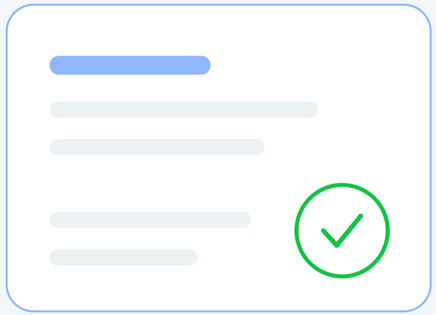
A paper certificate or a PDF can be altered. There is often no fast, reliable way to tell a real one from a forged one.

Credentials do not travel.

Proof earned with one provider, in one province, often cannot be trusted somewhere else without re-proving it.

A verifiable credential is proof that can be trusted instantly

It is the digital version of a certificate or a ticket, with one important difference. It is signed so it cannot be faked, and anyone with a legitimate reason can confirm it is real in seconds.



Issued

by the organization that grants it, such as a training or certification body.

Held

by the person it belongs to, on their own phone.

Verified

by anyone who needs to trust it, without calling the issuer.

Three roles, one trusted connection

The network connects three parties. Each keeps control of their own part.

The issuer

grants the credential and decides what to issue, to whom, and on what terms. For a safety certificate, that is the certifying body.

The holder

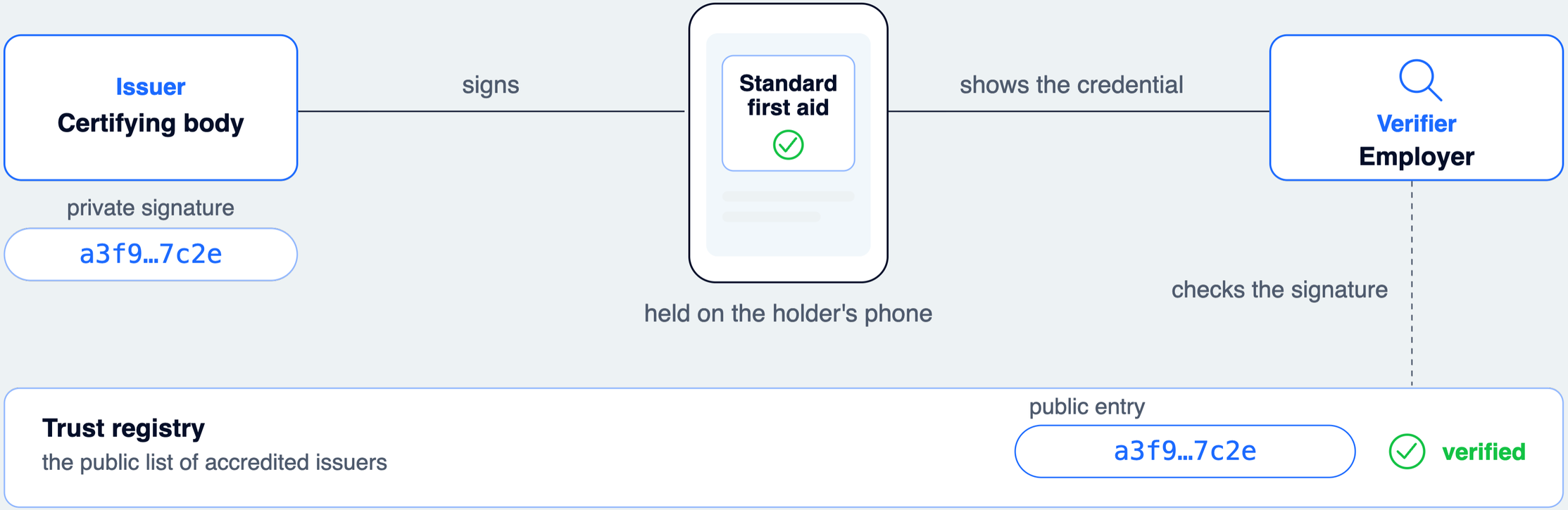
earns the credential and keeps it in a free wallet on their phone. They control when it is shared, and with whom.

The verifier

is anyone with a legitimate need to confirm a credential is real. An employer, a site supervisor, a regulator.

Like a passport, but you decide what the officer sees

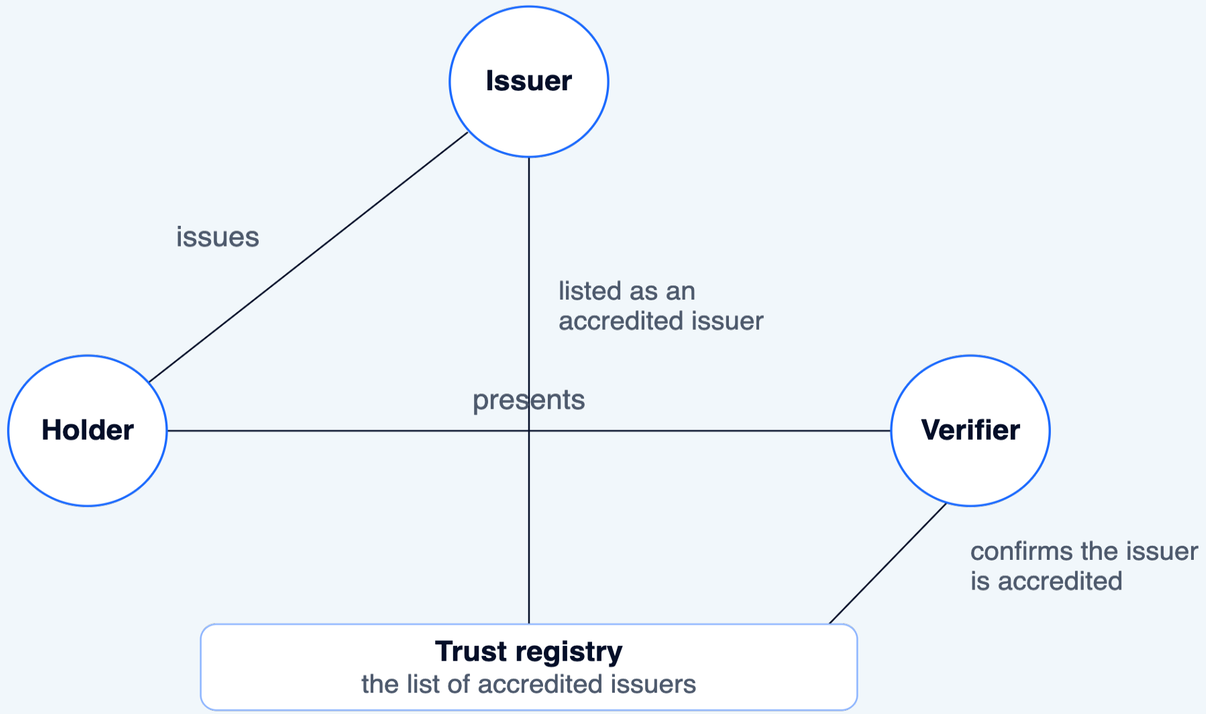
A border officer can confirm your passport is genuine without calling the country that issued it. A verifiable credential works the same way, with one upgrade: you choose which credential to show, and you can prove one thing without revealing everything else.



No personal data crosses the network. The verifier gets a yes or no, not your file.

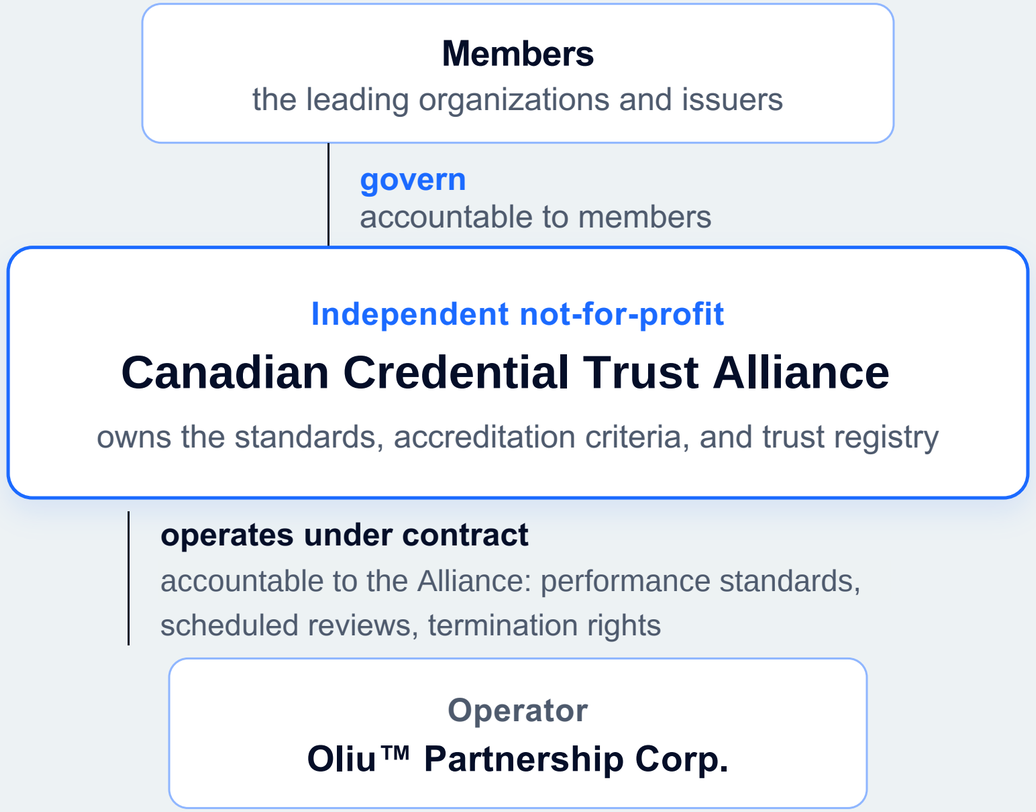
The triangle of trust

The same relationship, drawn simply. This is the shape every verifiable credential follows.



Trust is the product, so trust is governed independently

The network is run by an operator, but it is owned and governed by an independent, not-for-profit alliance answerable to its members. That separation is the whole point.

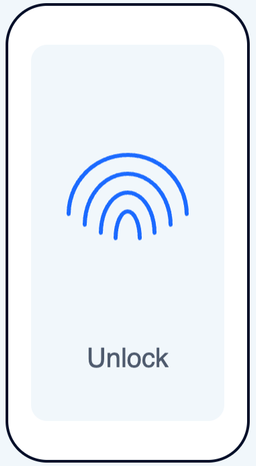


The network survives the operator, by design.

The wallet is free, and it stays in the holder's control

Credentials live in a free wallet on the holder's phone. The holder decides what to share and when.

To open the wallet, the holder uses the same Face ID or fingerprint they already use to unlock their phone and their banking app. That is what **biometric** means here. The biometric never leaves the phone, and the network never sees it. It is a familiar, everyday layer of protection, not a central database of faces or fingerprints.



The network is built so it cannot watch you

Privacy is not a policy promise here. It is built into how the system works.

No central file.

The network does not hold a database of people's credentials. Credentials live with the holder.

The operator cannot see who is checking what.

The architecture is designed so the operator cannot scrape personal credential data or track which verifiers are checking which credentials.

The verifier gets proof, not data.

A verifier receives a cryptographic confirmation, not access to the holder's personal information.

What the network will accomplish

A pan-Canadian trust network for verifiable digital credentials will play a foundational role in shaping Canada’s economy.

Credentials that travel.

A certificate becomes instantly verifiable anywhere in Canada, without re-proving it.

Protection against fraud.

Credentials become tamper-evident. An altered certificate fails verification.

Less administrative drag.

Verification becomes automatic, which means fewer "can you confirm this certificate" requests to chase.

The opportunity: the first movers set the standard

A major issuer in its sector is a natural anchor for trusted credentials nationally. Joining early means helping write the rules, not inheriting them.

Shaping the network’s promise.

Early movers help author the vision for the pan-Canadian trust network, and shape key founding decisions.

Influence over the standard.

Participate in decisions about the charter and accreditation standards that every issuer in the network will follow.

Build a trust network that works.

Directly contribute to a solution that will work, informed by the expertise and experience in the founding cohort.

Lead the solution.

Lead a national conversation about how to ensure digital credentials are verified, trustworthy, and mobile.

Leading organizations are exploring this together

A group of respected credentialing authorities has convened to explore shaping the Alliance and its standards. Nothing is settled yet. These are the kinds of organizations that would form the foundation of an independent governance body, and they are choosing to be part of the conversation early.

St. John Ambulance

Alberta Construction Safety Association

Alberta Hunter Education Instructors Association

BCRSP

BASES

CannAmm

Danatec

What to weigh honestly

A network like this is worth doing, and it is worth going in with eyes open. Three things are worth naming.

A standard only works when it is shared.

Early movers see the most value once others join. That is why a shared, sector-wide standard for proof of credentials matters. We are advocating, with government and with stakeholders such as WSIB, that proof of prior credentials become a common standard, so that the convenience of carrying a credential between providers does not depend on each provider going it alone.

This is infrastructure, not a revenue line.

Joining is about solving a sector problem and shaping the standard, not a near-term commercial return.

Governance is the safeguard against lock-in.

Because the not-for-profit alliance owns the standards and can replace the operator, no single vendor can capture the network. That is the structural answer to "what if this goes wrong."

The serious people already know this work

This is not starting from nothing. The conversation is already underway at the levels that matter.

01 Invited to speak in the Senate during the Canada and European Union discussion on interoperable credentials, alongside Credivera.

02 Engaged with the Digital ID and Authentication Council of Canada and the Digital Governance Standards Institute.

03 In conversation with ministers of labour across the country, federally and provincially.

04 Designed so the wallet works alongside the foundational identity wallets that provinces are developing, not in competition with them.

A short look at how this works

Captions on • 1.5 minute cut • 3.5 minute cut

An invitation to help build it

This is the early, shaping phase of a national network. The most useful thing a leading issuer can do now is take part in the conversation that defines how it works.

Take part in the conversation that is exploring how the Alliance and its standards should work.

Participate in the early conversations that will set the network's governance and structure

Becoming a member of the network follows naturally from there.

The question is not whether credentials go digital in Canada. It is who helps make sure it is done right.