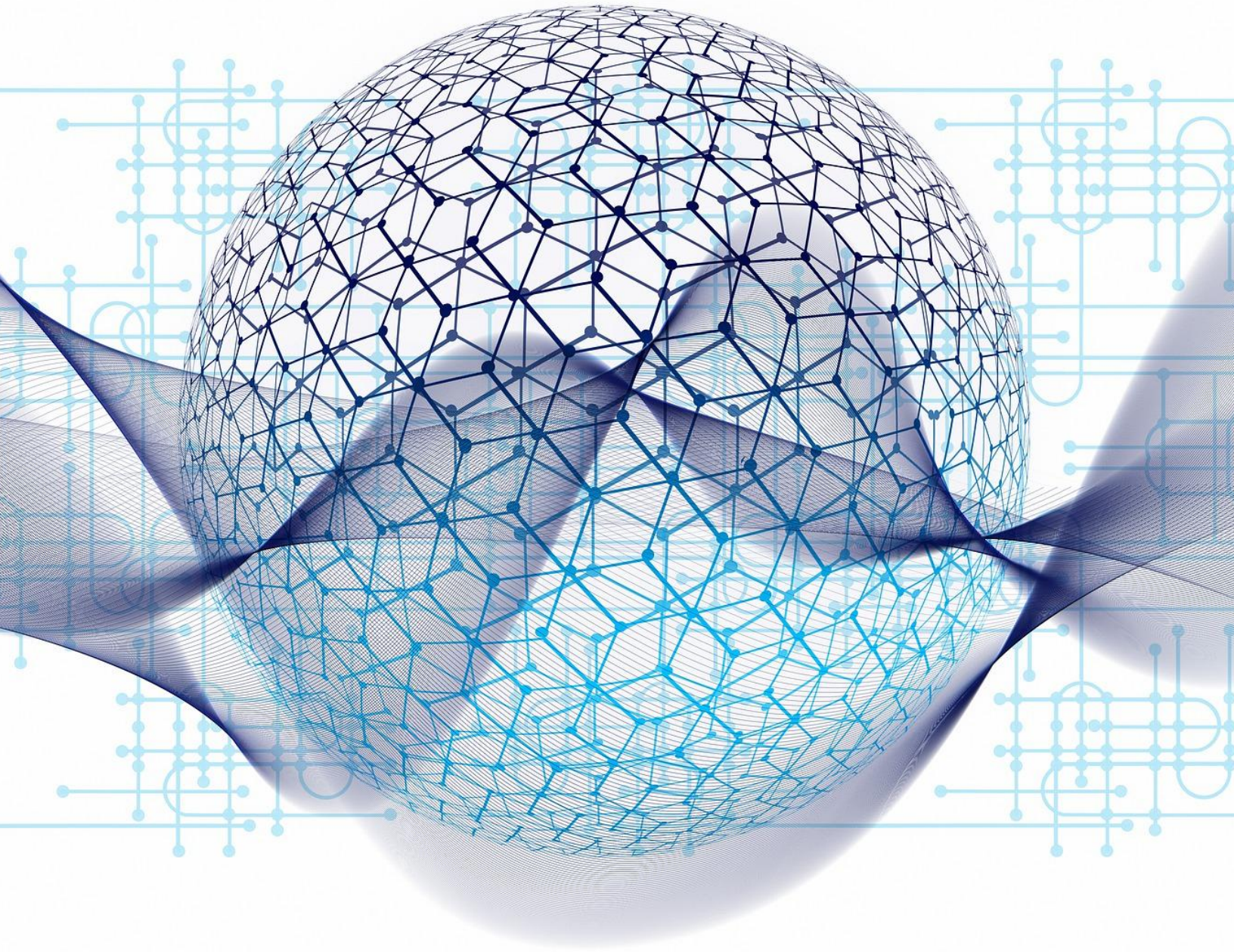


Perspectives on the Adoption of Verifiable Credentials

DIACC CCIAN

Table of Contents

About the DIACC

Created as a result of the federal government's Task Force for the Payments System Review, the Digital ID & Authentication Council of Canada (DIACC) is a non-profit coalition of public and private sector leaders who are committed to developing research and tools to enable secure, robust, and scalable Canadian digital ID solutions and services. With privacy, security, and choice at the forefront of all DIACC initiatives, the DIACC aims to enable all Canadians to participate safely and confidently in the global digital economy.

About This Report

The comments and findings presented herein reflect interviews conducted with representative organizations concerning the level of interest in using verifiable credentials in their respective organizations and industry sectors.

Most interviewee responses reflect an organization acting as a relying party. When working in this role, the organization relies on some or all of the data that comprises a verifiable credential. This role is generally synonymous with that of a "verifier" as defined in the World Wide Web Consortium (W3C) [Verifiable Credentials Data Model v1.1].

However, the contents of this report are of interest to entities acting in the other roles the W3C defines in the Verifiable Credentials Data Model ecosystem:

1. Issuer - A function an entity performs by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder.
2. Holder - A role an entity might perform by possessing one or more verifiable credentials.
3. Subject - An entity claims are made about (part of a verifiable credential).

Introduction

As The Digital Identification and Authentication Council of Canada (DIACC) notes in the paper "Making Sense of Identity Networks Summary", the physical and digital identities that represent us and by which we are known to others online are fragmented; we maintain discrete and separate relationships with each organization (and many individuals) with which we transact and they, in turn, must create and retain different identity records for us. Data fragmentation creates friction and risk, ultimately preventing the Canadian economy from realizing the full potential of digital services."

Large segments of the identity management community consider viable solutions to these long-standing and pervasive issues to be those that:

1. Support and improve the portability of identity information.
2. Provide mechanisms that preserve the integrity of identity information while minimizing opportunities for fraudulent use.
3. Increase the control individuals exercise over their identity information (ideally by providing people with direct management of information assets).

Solutions that provide or enable these objectives often adopt a "decentralized" or "self-sovereign" approach to identity management.

As with any solution intended to support a function as complex as identity management, multiple technologies figure prominently in decentralized identity systems (with distributed ledger technology among the most prominent at present). Verifiable credentials are also broadly considered an essential enabling technology of decentralized identity.

This report examines relative interest levels among industries using verifiable credentials as part of their identity management offerings. This report also provides a brief discussion of critical issues and challenges associated with representative verifiable credentials with the intent of informing and delimiting additional work the committees of DIACC may undertake concerning the general use of verifiable credentials in Canada's digital identity ecosystem.

This report does not examine or consider enabling technologies related to the generation, use, and management of verifiable credentials (e.g., blockchain, digital wallet, and public key cryptography components) except in broad terms. The Pan-Canadian Trust Framework (PCTF) components discuss these technologies to some extent although the framework itself strives to be technology agnostic.

Key Concepts

This section describes critical verifiable credential concepts that define the primary subject of this report - to establish a consistent interpretation among readers. A complete treatment of the conceptual architecture of verifiable credentials and related technologies is beyond the scope of this report.

Note: This document largely conforms to conceptual definitions and terminology adopted by the W3C in the [Verifiable Credentials Data Model v1.1] specification.

Credentials

The W3C defines a credential as “a set of one or more claims made by an issuer”. In more practical terms, a credential in its most basic form is information an organization or individual asserts to be true about someone or something. The driver's license is a frequently-cited example of a shared physical credential many of us keep on our persons regularly. This credential, issued by a government agency, asserts that someone (i.e., the subject) is entitled to operate a motor vehicle on public roadways. Beyond this, most driver's license credentials also provide information attesting to the following:

- The identity of the subject (e.g., the driver's name, address, and photo);
- Restrictions on the subject's ability to drive (e.g., the driver must wear corrective lenses); and
- Status of a credential (e.g., the license expires on a given date).

For this report, passports, university degrees, and proof of COVID-19 vaccination status are also examples of credentials that organizations can issue to individuals. Examples of credentials also include:

- Certificates of origin (attesting to the fact a shipment of coffee is from Costa Rica);
- Articles of incorporation (attesting to the fact that a legal entity does exist); and
- Safety certificates for commercial vehicles (attesting to the roadworthiness of a car).

Digital Credentials

Digital credentials are data objects composed of the same or substantially similar data as their physical counterparts. In this respect, they are considerably more flexible and able to support a broader range of use cases than the username and password pair used for authentication purposes that have traditionally defined a credential in the information technology industry.

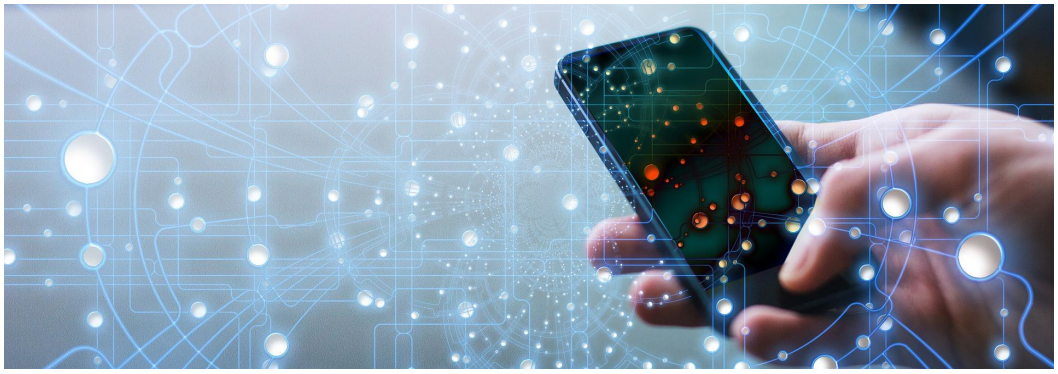
Verifiable Credentials

The W3C defines a verifiable credential as a tamper-evident credential with authorship that another party can cryptographically verify. A verifiable credential is a digital credential with integrity (i.e., no alteration of data). Authenticity (i.e., the credential originated with the designated issuer) is verified online using the credential with digital signatures and other enabling technologies.

Interest in Verifiable Credential Technology

The concept of portable identity information that can be verified online dates back several years: The W3C released a public draft of a [Verifiable Claims Data Model] in 2017 and the Sovrin Identity Network, which also included the concept of claims, had its beginnings several years earlier. Since these initial efforts to establish what is now widely considered a foundational component of decentralized identity, the identity management and broader IT communities have refined the concept of verifiable credentials, developed technical specifications for related enabling technologies (with considerable interest in the architecture and data model of decentralized identifiers and produced a sizeable body of literature and discussion about the technology. With the stabilization (if not a universal endorsement of low-level details) of technical specifications and broad-based knowledge of the potential benefits and implementation requirements for verifiable credentials, the range and availability of commercial and open-source solutions for their deployment continue to increase.

The interest of the broader identity management community in verifiable credentials continues to drive these developments and is also evident in the DIACC member community. In short, there is appreciable interest in incorporating verifiable credentials into digital identity processes and systems.

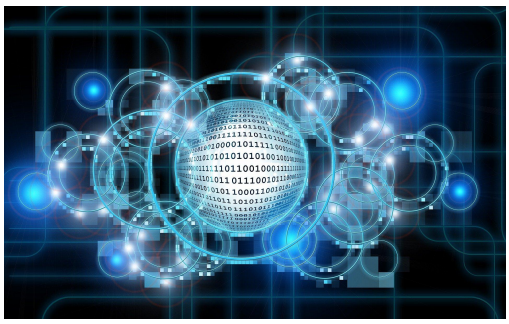


Use Cases and Applications

The flexibility of verifiable credentials concerning the data they can express and the things to which they can be issued to or that they can describe (i.e., human, organizational, and goods as subjects) make it challenging to itemize each use case and application that has prompted more than a passing interest in the technology. The ability for verifiable credentials to provide high-assurance identity attributes about persons engaged in online transactions is the typical application prompting interest in the technology. The attractiveness of this ability is unsurprising, given that it is also a core use case underlying the development of the technology. Interest in verifiable credentials regarding identity ecosystems or networks lies in the value to organizations or systems when acting as a "verifier" (to use W3C terminology). Extending the use of verifiable credentials beyond the use of identity information to support routine business processes is also a matter of interest. For example, within the DIACC member community, there is awareness of and interest in the potential for verifiable credentials to replace the username-password pairs that are a foundation of and are arguably the weakest component in current authentication systems.

Factors Driving Interest

The value-proposition of verifiable credentials to verifiers, and consequently the high level of interest in them, is attributable to the considerable potential of the technology to dramatically reduce the effort, time, and cost required to assess the trustworthiness of identity attributes. This potential, most commenters believe, can be realized by using electronic data with verifiable credentials to support the automation of processes designed for verification and validation purposes.



Current processes are often cumbersome, slow, expensive, and dependent in whole or in part on offline service channels and manual validation. The slow and cumbersome experience is because many identity attributes are only available as physical credentials (e.g., driver's licenses, health cards, and other paper documents). There is currently a high level of trust in these physical credentials, given the ability of service agents to inspect them to assess the authenticity and the issuer's identity and (in many cases) ensure that they are not fraudulent. Of course, the physical nature of the credentials severely limits the extent to which they can be automated processes - without compromising security and privacy (e.g., a person can send photocopies of their driver's license electronically, but the recipient will have reduced confidence in the integrity, privacy, and authenticity of the credential). A consequence of this is that personal information is routinely transcribed or scanned into enterprise information systems.

Given the digital format of verifiable credentials, organizations can incorporate them into automated validation and verification processes with relative ease compared to their physical counterparts. More important is that the technical design of verifiable credentials inherently supports encryption based on public key cryptography. Public key cryptography support allows real-time verification using the public key of the credential issuer rather than physical inspection of a credential or post-transaction audit of business rule compliance and self-asserted (by the subject) data. The privacy of the individual and the verifier's business operations is enhanced because the verifier usually completes verification without the credential issuer's participation (or even knowledge of the event).

In this respect, DIACC member interest in verifiable credential technology mirrors most organizations in the broader digital identity and IT communities. It reflects a broad appreciation of a core use case of verifiable credentials. However, interest in the technology extends beyond automated identity attribute validation and verification. Organizations acting as verifiers, particularly those in the financial services and public sectors, are interested in verifiable credentials to reduce the volume of personal information stored and managed in enterprise IT systems.
Many organizations collect and retain enormous volumes of personal information. Some of these records determine the identity of people online and secure access to their service accounts. Collected information is typically required to assess eligibility for document enrollment in various programs and services. Entities also use collected information to customize and optimize business processes and operations. Regardless of the purpose for personal information collection and retention, especially in large volumes, collections of personal information represent acute, multi-faceted security threats to the collecting organization:

- Large repositories of client data are the perfect (almost exemplary) target for skilled malicious actors motivated by the benefits of a successful attack;
- Malicious actors can exploit data discrepancies between systems to circumvent knowledge-based security mechanisms and to compromise multiple systems through the linkages established between federated data stores;
- A single data breach can result in large volumes of compromised information because data is in a single repository or multiple linked systems; and
- The collecting organization may need help to regain control over data and systems as large volumes of data are quickly and efficiently compromised.

Verifiable credentials, when implemented with other enabling technologies (chiefly personal digital wallets), can reduce the need to collect and retain personal information. This reduction in the need to collect and retain personal information is partly a function of incorporating verifiable credentials into automated data validation and verification processes which is faster than manual and paper-based processes. It is also partly a function of the fact that verifiable

credentials are by design not only issued to a particular subject (e.g., a person) but the credential data object provided to the subject; in most implementations, an issuer not only generates and cryptographically signs a credential for the subject but also deposits that verifiable credential into a digital wallet or similar receptacle. The resulting return of control over personal digital information is central to the decentralized approach to identity and its utility as a privacy-protecting technology through the continued collection and retention of personal information in enterprise systems: the subject can disclose personal information as quickly and efficiently as retrieving a card carried in a physical wallet, making on-demand requests from verifiers easier to implement and accommodate.

Challenges and Issues

DIACC members identify several challenges and associated issues related to the widespread adoption and use of verifiable credential technology. Despite challenges, authorities and other parties can implement verifiable credentials into existing digital identity processes and systems. Instead, they are notable factors that may dampen short-term interest in and adoption of the technology pending satisfactory resolution - potentially through multi-sector frameworks like the PCTF.

Trust Relationships Between Participants

The ability to cryptographically verify the integrity (i.e., no alteration of data) and authenticity (i.e., that the credential originated with the purported issuer) of a verifiable credential significantly increases the security of verifier trust in the personal information contained in the credential. However, technical verification of the credential as a data object does little to increase assurances in other trust factors relevant to a verifier. These include the accuracy of personal information (e.g., a driver's license contains correct and current address information), the authority of the issuer to make specific claims about the subject (e.g., the authority of a logistics firm to issue licenses to operate large commercial vehicles to its employees may be considered questionable by certain verifiers), or that a revoked or otherwise invalid credential was rendered unusable by an appropriate authority for just cause (e.g., rather than the result of a compromised system).

These concerns can undermine the trust relationship between verifiers and issuers regardless of the technical integrity of the verifiable credentials underpinning that relationship.

Note: The PCTF Credentials (Relationships & Attributes component provides a list of critical requirements for establishing trust between issuer and verifier that does not affect the trustworthiness of a verifiable credential. Ensuring implementation of specific relationship requirements will help resolve noted concerns in whole or part.

Lack of Regulatory and Commercial Precedent

Organizations, particularly those in highly regulated industries, look to regulatory and commercial precedents to reduce or eliminate some of the issues that may undermine the trust relationship between verifier and issuer. Regulations, commercial conventions, and widely implemented standard provisions in business agreements frame the relationship and set out shared expectations concerning liability, redress, and corrective action if there is a process or technical failure. Regardless of specific application, there are a few precedents that verifiers can easily and readily adopt into their business arrangements concerning using verifiable credentials.

Technical Standards Paralysis

An overarching goal of digital identity ecosystems built around verifiable credentials is to provide portable, interoperable data objects to network participants that can replace the paper-based physical certificates, currently the primary means of presenting and verifying personal information. DIACC members recognize that a high degree of standardization collaboration, based on available specifications, is necessary to achieve the goal of high assurance data portability.

The W3C Verifiable Credentials Data Model is gradually gaining adoption. The W3C data model, however, essentially keeps to this tight scope. This data model leaves questions and requirements concerning standards for related and enabling technologies (e.g., data encoding formats, cryptographic modules, and digital wallet standards - including an assurance based

Pan-Canadian Trust Framework Digital Wallet component published by DIACC with multi stakeholder input) to implementers.

In this unsettled technical standards environment, verifiers are wary of implementing specifications and technologies without guaranteeing broader digital identity and IT community adoption.

First Mover Commitment

Verifiers envision digital identity ecosystems in which verifiable credentials are workable and ubiquitous. The general level of interest (and hype) in the broader digital identity and IT communities and the concerted efforts of standards bodies and vendors to deliver practical solutions for online services to support such a vision. However, the absence of a "first mover" whose influence (due to size, economic position, regulatory authority) and actions can bring together ecosystem participants around verifiable credential implementations is a risk to broad-based technology adoption. Verifiers need issuers to generate and sign verifiable credentials. Issuers need assurance that sufficient verifiers will justify investments in verifiable credential technology as worthwhile. A clear first mover is necessary to catalyze and break the cycle of "no issuers, no verifiers, no verifiers, no issuers," moving industries and communities of interest to a digital identity framework based on verifiable credentials.

Conclusion

Verifiable credentials can revolutionize how we store and share personal information. This technology promises greater privacy, security, and convenience in many contexts by enabling individuals to control their data. However, as with any new technology, there are significant challenges to be addressed by developers, implementers, and adopters if society is to realize its potential fully.

Despite the challenges identified in this paper, the adoption of verifiable credentials is gaining momentum, and there is increasing interest in their potential applications across various industries. As technology evolves, we will likely see further innovation and refinement. Verifiable credentials represent a significant opportunity for individuals, organizations, and society. By addressing the challenges and working collaboratively to build a robust and secure

ecosystem, we can ensure that this technology delivers on its promise and enables us to create a more trustworthy, decentralized, and secure digital future.