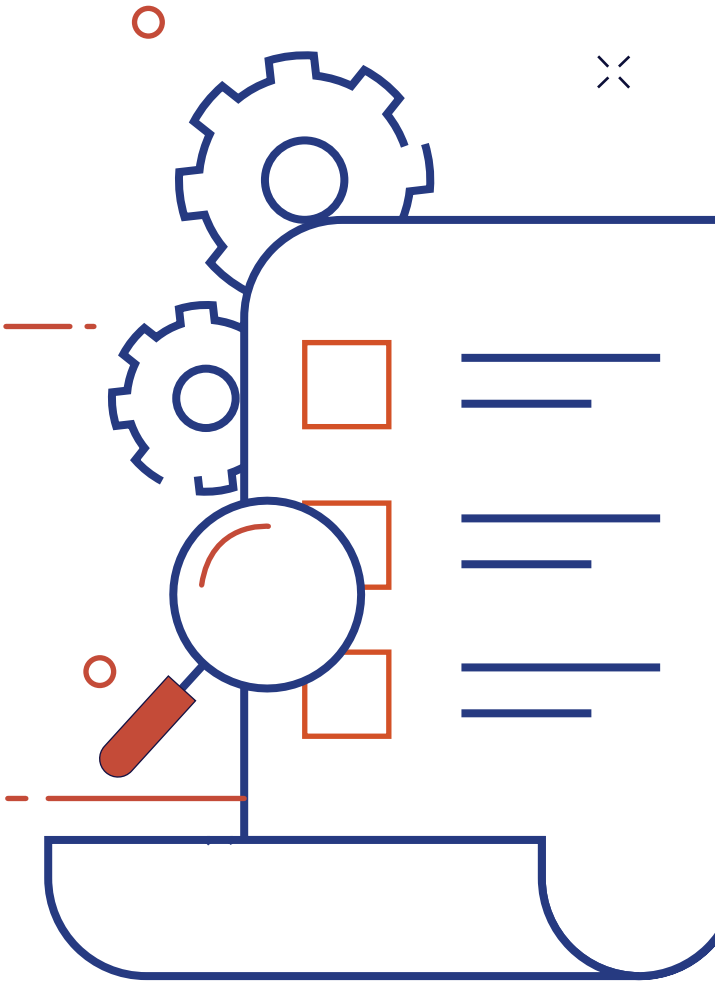
DIACC

Making Sense of Digital Wallets

Guidelines for Design

Table of Contents



Introduction

Recent advances in the state of the art of digital identity systems are putting the user back in control of their information and their privacy. An important building block of this advancement is the digital wallet for users. This document proposes what a trusted digital wallet should aim to do. Without it, software developers are left to guess, the marketplace offering will be fragmented, and ultimately will result in delaying the adoption of user-centric digital identity solution.

Background

For the past 15 years governments, enterprises, social media giants, and software companies have been developing user identification and authentication mechanisms to provide secure access for their users to electronic or digital services. Over this time, we have experienced technology advances in moving from simple and low strength username/password mechanisms to strong cryptographic and biometric authentication techniques, most recently facilitated by the almost universal adoption of smartphones.

At the same time, we have seen the evolution of identity solutions from single service authentication systems (modelled on solutions designed for enterprise internal systems) to shared (or federated) authentication solutions using internet standard protocols such as SAML, Oauth 2.0, and OpenID Connect. Many Canadians are familiar with using their Google and Facebook accounts to access other provider's services, thereby reducing the number of username/passwords they need to manage. In Canada, notable shared solutions in use by governments include Government Sign-in by Verified.Me (formerly SecureKey Concierge) adopted by the Government of Canada, the BC Services Card in British Columbia, and the MyAlberta Digital ID solution.

Most recently there has been a significant development of blockchain based identity solutions that build upon the preceding technologies and promise to provide enhanced user experience, security, privacy, and utility for both service providers and their users.

What is a digital wallet?

A key aspect of these new blockchain based solutions is the presence of a digital software application (sometimes referred to as a user agent) held by the user, often on their smartphone, that acts as a secure container for the user's identity information, delivering both a strong authentication solution and a provider of verifiable identity information (or credentials) to services that need to know something about a user. It is this software application that many are referring to as the Digital Wallet. A wallet gives user access to and control over their identity information so they can share when registering for a new service, or when accessing a service they have already.

In addition to these developments with digital identity systems, there has been steady progress with the payments industry in developing mobile phone applications that perform secure contactless and web payment transactions. While we can imagine that payment and identity functions will be combined into a single digital wallet product in the future, the focus of these guidelines is with respect to the identity component.

Why do we need guidelines?

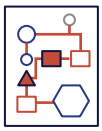
Digital Identity and Authentication Council of Canada (DIACC) has made excellent progress in developing industry standards and practices with the Pan-Canadian Trust Framework™ (PCTF)." The PCTF describes the roles, services, and requirements to ensure alignment, interoperability, and confidence of digital identity solutions, that are intended to work across organizational, industry, and jurisdictional boundaries. However, the PCTF does not directly address implementation specific requirements for various solution architecture or implementation, including for a trustworthy Digital Wallet component when applicable. In this new architecture, it is critical that the digital wallet is indeed trusted and that Canadians are protected and know which digital wallets they can safely use. Service providers and Relying Parties in turn need to know that the information they hold, send, and receive is protected by digital wallet solutions.

Of urgent concern is the development of a set of guidelines to underscore the need for security, privacy, and interoperability of these digital wallets. Without these guidelines, there is great risk that wallet providers will deem it acceptable to sacrifice the areas of concern addressed by the principles for expediency or for business models that are detrimental to the wallet holders. The lack of these guidelines may result in fragmentation and slower adoption of the networks that the wallets are supporting.

At the June 2020 DIACC Innovation Expert Committee meeting, the Digital Identity Laboratory and others proposed, and the IEC accepted, that a working group develop a draft Digital Identity Wallet Principles for review. This is a set of durable and high-level principles for security, privacy, interoperability, agency and other aspects. These principles will need to be sufficiently high level that they will stand the test of time in supporting innovation and various business models but will also ensure that the needs of Canadians, Canadian businesses, and the public sector are met. The working group has developed a draft principles document that is intended to be complementary to these guidelines.

Approach in developing the guidelines

The guidelines are intended to be high level aspirational goals for software development teams designing and building digital wallet technology solutions for the Canadian marketplace.

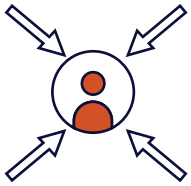


The guidelines will not be technology or business model specific. The digital marketplace includes several different approaches and these guidelines should not be intentionally prejudicial towards a particular approach, noting that some approaches may be stronger in alignment with the guidelines than others.

The guidelines are intended to address the interests of Canadian users, Identity Providers (issuers), Relying Parties (verifiers), and Network providers.

The guidelines should be built upon the PCTF principles of User-centric, Trust, Privacy by Design, and Integrity and leverage previous works such as the 7 Laws of Identity, the Ten Principles of Self Sovereign Identity, Canada's Digital Charter, DIACC Digital Identity Ecosystem Principles, and especially using the work of the DIACC IEC working group.

5 Key Guidelines



1

Wallets should be User Centric in design

- Work in the interest of Users
- Support Users if things go wrong
- Support the Identity Providers, Relying Parties, and Networks that Canadians want and need.
- Provide Users with evidence of the alignment of the digital wallet to these principles and supporting standards, such as a recognized trust mark.

2

Wallets should protect User's privacy

- Provide Users with visibility and control over the Disclosure and storage of identity information
- Support minimal disclosure techniques for identity information.
- Prevent possible Collusion across Network operators, Identity Providers, Relying Parties.
- Provide Direct Disclosure to a party and prevent Surveillance by any 3rd party.

5

Wallets should be accessible to all Canadians

- Support modern industry standards for accessibility.
- Be available for all Canadians regardless of their financial ability.
- Provide familiar, intuitive, simple, and informative user experience so that Users can make good choices.

4

Wallets should be Interoperable

- Use modern industry standards for identity information exchange.
- Support Network business models by enabling their policies.

3

Wallets should be secure

- Provide Users with information and tools to help to securely manage, store and Disclose identity information.
- Identify and authenticate all parties to a transaction so that Users make informed choices.
- Authenticate Users using methods consistent with industry assurance standards (Level of Assurance).
- Use proven and modern industry security standards.
- Use modern software development industry best practices.

Next Steps

These guidelines are intentionally high level so that they will support various business models and technologies and will hopefully also be durable as these models and technologies evolve, as they are sure to do. However, since they are high level, software developers and those organizations testing and assessing products will need objective implementation guidance in the form of technology standards. For this next step, the Digital Identity Laboratory of Canada proposes to work with DIACC members and others, to develop the technology standards that can be used to align with these guidelines.

During the discussions of these guidelines a common theme arose, namely that further work is needed assessing, updating and augmenting the PCTF with similar/supporting guidelines for development of Networks, Identity Providers and Relying Parties in this new architecture.

Definitions

1.	User	A person that holds a digital wallet, typically on their smart phone.
2.	User-Centric	A system designed with the User's interests as a guiding principle.
3.	Identity Provider (or Identity Issuer)	A service that sends identity information to a digital wallet to be stored for use by the User.
4.	Relying Party (or Identity Verifier)	A service that receives identity information from a digital wallet.
5.	Network	A group of Identity Providers and Relying Parties and associated infrastructure that enable a digital wallet to securely receive and send identity information. Networks have standards, policies, and governance over how they operate.
6.	Disclosure	The passing of identity information from a digital wallet to a Relying Party.
7.	Direct Disclosure	Disclosure that ensures that identity information is passed directly from a wallet to a Relying Party and no other party.
8.	Collusion	The process of linking identity information from two or more Relying Parties.
9.	Surveillance	The process of recording transactions occurring across multiple Relying Parties, Identity Providers, or a Network, excluding a digital wallet itself.

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