PCTF Digital Wallet Component Overview

Document Status: Final Recommendation V1.0

In accordance with the DIACC Operating Procedures, Final Recommendations are a deliverable that represents the findings of a DIACC Expert Committee that have been approved by an Expert Committee and have been ratified by a DIACC Sustaining Member Ballot.

This document was developed by DIACC's Trust Framework Expert Committee with input from the public gathered and processed through an open peer review process. It is anticipated that the contents of this document will be reviewed and updated on a regular basis to address feedback related to operational implementation, advancements in technology, and changing legislation, regulations, and policy. Notification regarding changes to this document will be shared through electronic communications including email and social media. Notification will also be recorded on the Pan-Canadian Trust Framework Work Programme.

Table of Contents

1. Introduction 3
1.1 Purpose and Anticipated Benefits 3
1.2 Context 3
1.3 Scope 5
1.3.1 Digital Wallet Types and Implementations 6
1.3.2 In-Scope Topics 7
1.3.3 Out-of-Scope Topics 8
1.4 Relationship to the Pan-Canadian Trust Framework 8
2. Conventions 9
2.1 Terms and Definitions 9
2.2 Abbreviations 13
2.3 Roles 14
3. Trust Relationships 15
4. Trusted Processes 17
4.1 Conceptual Overview 18
4.2 Process Descriptions 19
4.2.1 Wallet Instantiation and Security Processes 19
4.2.2 Credential Management and Use Processes 21
4.2.3 Consent Processes 23
5. References 23
6. Revision History 24

1. Introduction

This document provides an overview of the PCTF Digital Wallet Component, a component of the Pan-Canadian Trust Framework (PCTF). For a general introduction to the PCTF, please see the PCTF Model Overview. The PCTF Model Overview describes the PCTF's goals and objectives and provides a high-level overview of the PCTF.

Each PCTF component is described in two documents:

1. **Overview**: Introduces the subject matter of the component. The overview provides information essential to understanding the Conformance Criteria of the component. This includes definitions of key terms, concepts, and the Trusted Processes that are part of the component.
2. **Conformance Profile**: Specifies the Conformance Criteria used to standardize and assess trust elements that are part of this component.

This overview provides information related to and necessary for consistent interpretation of the PCTF Credentials (Relationships & Attributes) Conformance Profile.

1.1 Purpose and Anticipated Benefits

The purpose of this component is to provide a framework that Digital Identity Ecosystem Participants can use to assess the degree to which the Digital Wallets that are part of their respective ecosystems accomplish the following:

1. Provide Citizens and Consumers with a Digital Wallet that complies with the human rights principles of preserving people’s privacy and control over their information.
2. Introduces a consistent identity metaphor and consent-driven automated experience across all Ecosystem Participants to reduce impact on users caused by Digital Transformation.
3. Contribute to a stable infrastructure with longevity and world-wide interoperability by adopting and supporting relevant standards as appropriate (e.g., W3C Standards for Verifiable Credentials and DIDs).
4. Counter cyber vulnerability and extortion by enabling Service Providers to incrementally replace existing login mechanisms, some of which may be exploitable, without suffering negative impact to business.
5. Establish an environment of trust within which the Wallet’s Holder can interact with other Ecosystem Participants such as Issuers, Verifiers, and other Relying Parties.

1.2 Context

The physical Wallet is a private container for the Holder's cash, payment cards, proof of identity, and other documents. Digital Wallets are analogous to physical Wallets in that they contain digital versions of the Wallet Holder's identity proofs and related assets. These assets typically include digital versions of familiar physical cards and documents (e.g., driver's license, proof of insurance, health cards, etc.). Digital assets are often stored as a form of credential (often a Verifiable Credential) – and this term is used throughout this document to refer to Wallet contents. A digital identity Wallet may also store cryptographic keys used by the Wallet's Holder. Digital Wallets are typically small software applications residing on personal computing devices.

A well-designed Digital Wallet ensures the security of its sensitive and confidential contents while making it easy for the Wallet Holder to use digital identities proofs and credentials in online and face to face interactions. A well-designed digital identity Wallet can enhance privacy by providing the Wallet Holder with control over and visibility into when, where, how, and what Wallet contents are disclosed to third parties.

Digital Wallets may be used to provide their users with responsibility and control of the use of their data and credentials, so particular attention was given during the development and review of this component to issues of usability, accessibility, affordability, diversity, equity, inclusion and intersectionality. It is highly recommended that providers of Digital Wallets should consider how to limit their potential for restricting or excluding segments of society from access to digital services.

The concept of Digital Wallets as a way for Holders to store, manage, and use digital identities and related assets emerged as identity systems evolved from application specific user authentication mechanisms to sophisticated systems that share and verify identity assets among multiple entities (applications, service providers, other individuals, etc.) in various federation and trust arrangements.

Among the specific factors that have encouraged the emergence of Digital Wallets are:

1. **Increasing concerns about privacy invasion** – Surveillance of users by commercial and state actors has become visible and is now a political factor driving public policy. Browser makers and software vendors have made efforts to reduce opportunities to track users online. However, the use of e-mail addresses and phone numbers (which are personally identifiable information) as universal identifiers remains common practice.
2. **Limitations of legacy identity solutions –** A major business consideration, if not a considerable challenge, for organizations attempting to digitalize an important and valuable service is minimizing the redundancy, duplication, and overlap that can result as identity solutions proliferate within and between service providers. As this happens, users are faced with managing multiple digital identities and related assets. This is evident in the widespread use of password managers to ease the burden of keeping each service relationship secure. Digital Wallets can help Wallet Holders manage a growing number of identity assets and

control the sharing and use of these assets in their digital relationships and interactions.

3. **Fragmented user experience –** Service providers understandably provide users digital experiences that are optimized for their own processes. Digital user experiences seldom consider the full extent of an individual's digital relationships and interactions. The result is that many individuals are left to navigate widely dissimilar and often confusing digital services. Digital Wallets can provide a trusted, consistent, and familiar user experience for key aspects of interactions involving digital identities (i.e., storing, retrieving, and presenting identity information).
4. **Professionalization and militarization of cyber-attacks** – Fragmented user experiences, the existence of numerous single purpose digital identities, and proliferation of personal information across internet-connected systems make it easy for skilled and motivated malicious actors to compromise personal information and privacy. Digital Wallets can help mitigate many attack vectors (primarily phishing and other attacks based on obtaining personal information). Moreover, Digital Wallet Holders can help improve overall cybersecurity by selectively sharing only the identity information needed for a specific purpose or interaction (e.g., via a Zero-Knowledge proof or Derived Predicate).
5. **Industry standards for verifiable credentials and personal information** – A significant barrier to near real-time digital interaction is the need to revert to time-consuming, labour-intensive processes for validating identities and personal information. These validations are necessary to maintain process integrity for high-value services but erode efficiency and user experience. Where opportunities exist to automate data verification (e.g., a connection between the service provider and the CRA to confirm taxable income), information security and privacy mechanisms may be difficult to implement without compromising user experience or contravening existing legislation. Portable, cryptographically Verifiable Credentials, used in conjunction with Digital Wallets, are now gaining acceptance as a way for service providers to obtain high assurance data while ensuring security and transparency for the Wallet Holder. The World Wide Web Consortium (W3C) Verifiable Credentials Data Model 1.0 has attracted wide interest and support as the core data standard to facilitate interoperable verifiable credentials.

1.3 Scope

Topics that are considered in and out of scope define the scope of this PCTF component. Digital Wallet types and their typical contents are also a key determinant of component scope.

Note: Other components of the PCTF should be considered as part of any assessment. Requirements that are directly addressed by other components are not duplicated here. It is recommended in particular that the Authentication, Privacy, Notice & Consent,

Verified Person, and Verified Organization components should be included in any assessment of a Digital Wallet.

1.3.1 Digital Wallet Types and Implementations

The term “Digital Wallet” appears throughout this document and is an indicator of this PCTF component’s scope. The focus of this component are Digital Wallets that contain digital identities and related assets. The design of these Digital Wallets is such that they are optimized to help the Wallet Holder manage and use:

1. Personal identity documents and Attributes (e.g., foundational evidence of identity, social insurance numbers, passports, driver’s licenses, public health cards, proof of citizenship, proof of residency, proof of age, etc.).
2. Personal information about and relationships with significant others (e.g., proof of marital status to another individual, proof of custodianship over minors, proof of employment status at an organization).
3. Encryption and signing keys to support Attribute verification and digital document signing.

Digital Wallets may also contain and facilitate use of:

1. Digital payment information (e.g., credit cards) for various services and websites.
2. Authentication details (e.g., usernames/passwords) for various services and websites.

Because of this overlap with Digital Wallets and applications designed exclusively for digital payments and financial transactions (e.g., a Bitcoin cryptocurrency Wallet) certain conformance criteria specified for this PCTF component may be applicable to Wallets and applications used exclusively for digital payments. However, this profile will not explicitly address those types of Wallets. Similarly, applications that function strictly as password managers or form-filling utilities are not considered in scope for this PCTF component.

The scope of this PCTF component is not limited to a particular implementation approach for Digital Wallets and specifies conformance criteria generally applicable to all Digital Wallets, whether they are implemented as:

1. Native apps on smartphones and other mobile devices.
2. Progressive web apps that execute on other devices.
3. Traditional web hosted applications that execute on servers.

The scope of this PCTF component is not limited to Digital Wallets used by a single individual. The scope of this component includes:

1. Digital Wallets designed for use by individuals operating on their own behalf, their family members, or for individuals that are representing a business or another type of organization.
2. Organizations that require control of a corporate Digital Wallet that their employees and representatives can use for authorized purposes.

1.3.2 In-Scope Topics

In scope for this PCTF component are the following topics:

1. Product and Service Quality: from a trust perspective, the software development, distribution, and Holder support processes used to implement and support a Digital Wallet are critical aspects. Third party testing and validation of Digital Wallets and the provision of trust marks can improve a Digital Wallet's trustworthiness. For progressive web apps and web hosted Wallets the Infrastructure (Technology & Operations) Component of the PCTF should apply to these hosting services.
2. The following functional capabilities of Digital Wallets and standards are in scope:
    1. Authentication of a Holder to open, use, and provide consent to a Digital Wallet, such as use of mobile phone biometric and pin code authentication, multi-factor authentication mechanisms, and username/password mechanisms.
    2. Ability for Digital Wallets to authenticate Credential Issuers, Verifiers, and associated Verifiable Data Registries.
    3. Key Management technology standards for securely managing and storing public/private keys, including optional ability to export, import, and backup/recovery of keys.
    4. Credential Management technology standards for securely managing and storing credentials held by Digital Wallets, including optional ability to export, import, and backup/recovery of credentials, and support issuer branding and policies.
    5. Ability for Digital Wallets to store and present attestation tokens from established/existing issuers.
    6. Technology standards for request and provision with issuers, including digital signatures.
    7. Technology standards for credential presentation with verifiers, including digital signatures.
    8. Support for minimal disclosure.
    9. Holder dialog to support informed decisions to disclose or not, including consent dialog.
3. Accessibility and inclusivity standards applicable to Digital Wallets.
4. Plain language and standard display format (i.e., Wallet and cards representation).
5. Multi-Language Capability.
6. Informed, traceable Consent and activity/history logging and reporting.

Note: PCTF Overview and Conformance Criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy, and regulations in their jurisdiction.

1.3.3 Out-of-Scope Topics

The following topics are considered not in scope for this component:

1. Technology standards, processes, and policies applicable to Credential Issuers and Credential Verifiers, except as directly related to Wallet functionality.
2. Technology standards, processes, and policies applicable to Verifiable Data Registries, except as directly related to Wallet functionality.
3. Technology standards, processes, and policies applicable to third party testing and validation of Digital Wallets for the purposes of issuing trust marks.

1.4 Relationship to the Pan-Canadian Trust Framework

The Pan-Canadian Trust Framework consists of a set of modular or functional components that can be independently assessed and certified for consideration as trusted components. Building on a Pan-Canadian approach, the PCTF enables the public and private sector to work collaboratively to safeguard digital identities by standardizing processes and practices across the Canadian digital ecosystem.

Note: The Digital Wallet component partially overlaps with the Authentication, Notice & Consent, and Credentials (Relationships & Attributes) components. As such, this PCTF component represents an intersection point between several other components and expands conformance criteria to include a specific tool available to participants in Digital Identity Ecosystems.

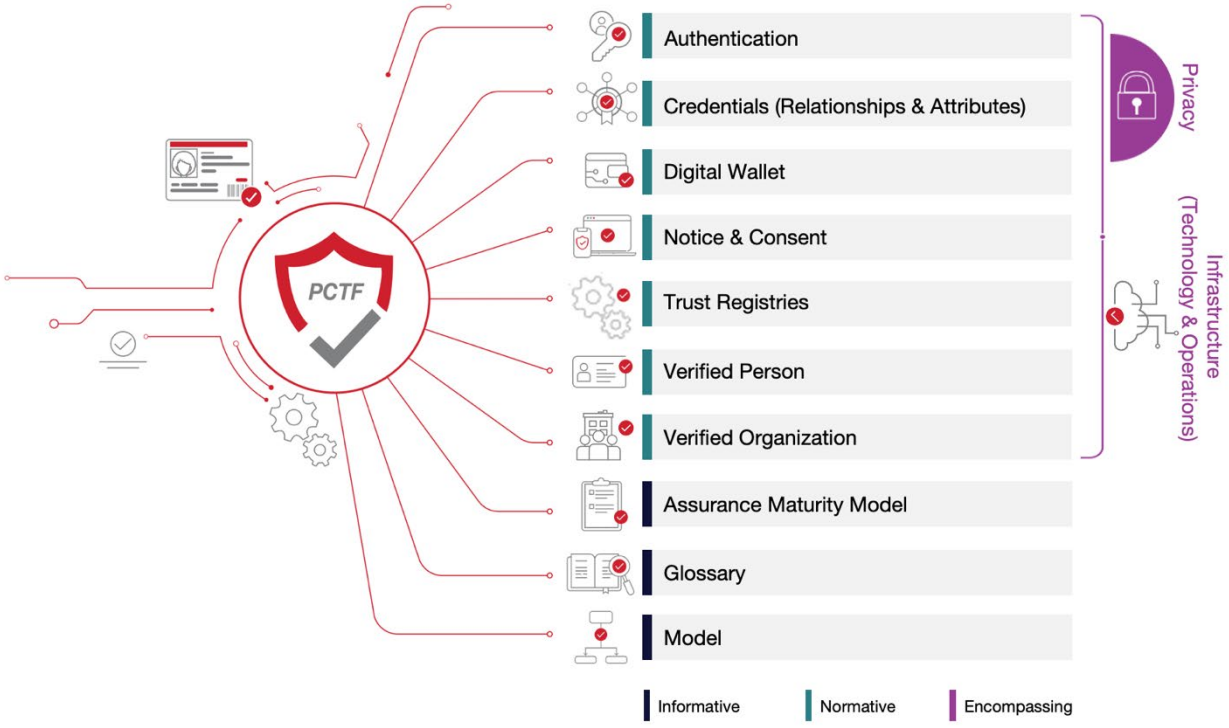

Figure 1. Components of the Pan-Canadian Trust Framework

2. Conventions

This section describes and defines key terms and concepts used in the PCTF Digital Wallet Component. This information is provided to ensure consistent use and interpretation of terms appearing in this overview, and in the PCTF Credentials (Relationships & Attributes) Conformance Profile.

Notes:

- Conventions may vary between PCTF components. Readers are encouraged to review the conventions for each PCTF component they are reading.
- Key terms and concepts described and defined in this section, the section on Trusted Processes, and the PCTF Glossary are capitalized throughout this document.
- Hypertext links may be embedded in electronic versions of this document. All links were accessible at time of writing.

2.1 Terms and Definitions

For purposes of this PCTF component, terms and definitions listed in the PCTF Glossary and the terms and definitions listed in this section apply.

Attestation

- A trusted verification of something as true or authentic.

Attribute

- An Attribute is information related to a characteristic or inherent part of an Entity (e.g.: a Subject's given name or residential street address). Attributes are sometimes referred to as "properties" or "claims". Attributes are stored in Credentials.

Claim

- A Claim is an assertion made about a Subject (e.g., the Subject is licensed to drive; the Subject is over 21 years of age; the Subject was incorporated in the Province of Ontario).

Credential

- A Credential is a set of one or more Claims made about a Subject by a single Entity (e.g., the Subject is licensed to drive; the Subject resides at a specified address; the Subject has a specific certification). In this document the term "Credentials" does not include Authentication Credentials unless the term "Authentication Credentials" is used explicitly (see also, Verifiable Credential).

Credential Verification

- Credential Verification is the evaluation of whether a Verifiable Credential or Verifiable Presentation authentically represents the Issuer or Subject. This includes verification that the proof is satisfied (normally via cryptographic validation), confirmation the Credential or Presentation is valid (e.g., is not suspended, revoked, or expired), and that the Credential or Presentation conforms to relevant specifications and/or standards.

Cryptographic Binding (See also: Strong Binding)

- Associating two or more related elements of information using cryptographic techniques.

Derived Predicate (See Also: Zero Knowledge Proofs)

- A Derived Predicate is a Verifiable, Boolean assertion about a Subject based upon the value of another Attribute that describes that Subject. For example, consider a Subject who wishes to prove they are eligible for services only available to people who are at least 21 years of age, and who possess a Credential which contains an Attribute that holds their date of birth. Rather than

present their birth date as proof they are eligible, the Subject could present a Derived Predicate such as "Over21" which contains a "True" or "False" value that indicates whether the Subject is greater than 21 years of age. Use of Derived Predicates better protects a Subject's privacy by not releasing detailed personally identifiable information while enabling a Verifier to validate a Subject's eligibility for a service.

Digital Wallet (Wallet, Digital Identity Wallet)

- A Digital Wallet is a software-based Credential Repository system that securely stores information for a Holder. Depending upon the nature of the Wallet, it may contain information such as Credentials, Verifiable Credentials, payment information, and/or passwords. The purpose of a Wallet is to securely store Credentials and or Identity Attributes, and to enable the Holder to assemble and prepare Verifiable Presentations. Some Wallets might have identity proofing capabilities and/or Agents to facilitate the sharing of Credentials they manage.

EULA or End User License Agreement

- A contract between a software producer and the eventual user of the product, specifying the terms and conditions of use.

Presentation

- A Presentation is data, typically representing one or more Claims about a Subject, that is derived from one or more Credentials, Verifiable Credentials, Endorsed Relationships, or Verifiable Relationships and shared with a Verifier.

Relationship

- A Relationship is a specific type of Credential that describes the way in which two or more Entities are related to each other (e.g., Fatima is a PhD student at the University of British Columbia; Eric is an employee of FictitiousCorp; Sheila is a member in good standing with the Law Society).

Render Credential

- Styling the visual presentation of various entities types and data (e.g., Credentials) is a common need that runs across many different use cases. In order to provide a predictable set of styling and data display hints to User Agents, Issuers, Verifiers, and other participants who render UI associated with entities and data, this specification endeavours to standardize a common data model to describe generic style and data display hints that can be used across any formulation of UI elements.

Repository / Credential Repository

- A Repository is a software-based system (application) such as a database, storage vault, or Verifiable Credential Wallet that stores, and controls access to, a Holder's Verifiable Credentials.

Secure Storage

- Secure storage is a facility used to ensure stored data security, privacy, and integrity. This facility may rely upon the physical protection of the hardware on which the data is stored, as well as security software. Data stored in secure storage either cannot be retrieved from storage, or can only be retrieved by authorized parties.
- *See also* https://www.techopedia.com/definition/29701/secure-data-storage .

Selective Disclosure

- A Credential may contain multiple claims as key value pairs. For example, the W3C proposed citizenship vocabulary includes given name, family name, gender, image, and birth date among other data elements in the credential schema. As a principle, data minimization should be employed whenever possible to limit the sharing of personal information. A data minimized proof of age to a Verifier, from the above example, might only include the Holder's date of birth and a possibly a photo image.
- Zero-knowledge cryptographic techniques can be employed to create a selective disclosure proof based on the original credential with blinded data elements that the Holder does not want or need to share with a Verifier and/or Relying Party. The proof is crafted in such a way that the Holder can still prove to the Verifier that Credential was signed by the Issuer and that the presented data was not tampered with. Examples of such signature schemes include CL signatures, BBS+ signatures, and SNARK based schemes.
- One powerful use of the selective disclosure is to blind the binding identifier common to a group of issued Credentials. This reduces the risk of tracking Holder activity as the binding secret is not disclosed to the Verifier.

Note: Selective disclosure can be achieved via other methods such as just in time issuance of Credentials or using a trusted broker. Such methods may allow user activity to be traced to a single source – the Issuer or the broker.

Strong Binding (See Also: Cryptographic Binding)

- Tightly associating a Holder with verified data elements stored in a Wallet using an Authenticator.

Token

- A digital representation of an attestation or container for claim(s).

Verifiable Credential

- A Verifiable Credential is a tamper-evident Credential that is encoded in a way that enables its integrity and authorship (i.e., source) to be confirmed via cryptographic Verification. Verifiable Credentials must be cryptographically secure and machine Verifiable.

Verifiable Data Registry

- A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as Verifiable Credential schemas, revocation registries, issuer public keys, and so on, which might be required to use Verifiable Credentials.
- (Reference: https://www.w3.org/TR/vc-data-model/#dfn-verifiable-data-registries)

Verifiable Presentation

- A Verifiable Presentation is a tamper-evident Presentation that is encoded in a way that enables its integrity and authorship (i.e., source) to be confirmed via cryptographic Verification.

Zero-Knowledge Proofs or ZKP

- A Zero-Knowledge Proof is a cryptographic technique that allows the Holder to prove to a Verifier that the Holder has knowledge of a value without actually sharing the value.
- A Zero-Knowledge Proof can be used within the context of digital identity to support the following key privacy preserving features:
    - Selective Disclosure – disclose a subset of Attributes from a credential to an issuer.
    - Predicates – calculations on Attributes such as equality or greater than (e.g., prove your salary is greater than X or your age is greater than Y) where actual values are not shared with Verifier.
    - Signature blinding – randomization of Issuer signature prior to sharing with the verifier to eliminate the signature as a correlating factor.
    - Private Holder blinding – the correlating identifier is not exposed to the Verifier.

2.2 Abbreviations

The following abbreviations and acronyms appear throughout this overview and the PCTF Credentials (Relationships & Attributes) Conformance Profile:

- **PCTF:** Pan-Canadian Trust Framework

- **CAL:** Credential Assurance Level
- **DID:** Decentralized Identifier
- **ZKP:** Zero-Knowledge Proofs

2.3 Roles

The following roles and role definitions are applicable in the scope and context of the PCTF Credentials (Relationships & Attributes) Component.

Notes:

- An Entity may assume one role or multiple roles, depending on the use case. For example, an Entity that is the Verifier in a transaction may also be the Verifier for that transaction.
- Role definitions do not imply or require a specific solution, architecture, implementation, or business model.

Applicant

- An Applicant is any Entity that has requested, though not yet received, a Credential (e.g., a Person who has requested, though not yet received, a drivers' license from a province or territory). This Entity may or may not be a Subject of the Credential.

Holder

- A Holder is any Entity that possesses one or more Credentials. The Holder is usually the Subject of the Credential but need not be so (e.g., a parent might possess a Credential belonging to their child; an attorney might possess a Credential belonging to their client). Holders may store Credentials they possess in a Repository.

Issuer

- An Issuer is any Entity that makes information about a Subject available by creating and issuing a Credential, Attestation Token, or Verifiable Credential (e.g., a province or territory that issues a drivers' license).

Note: This definition allows any Entity to create and issue Credentials, including the Subject.

Relying Party

- A Relying Party is any Entity which consumes digital identity information, Attributes, Relationships, or other Credentials to conduct digital transactions

(e.g., a liquor store or business owner that needs to ensure a customer is old enough to purchase alcohol). See Verifier below.

Revocation Authority

- A Revocation Authority is any Entity with exclusive or primary responsibility for revoking Credentials and maintaining information about revoked Credentials. The Revocation Authority may be the Issuer of the revoked Credential but need not be so.

Verifier

- A Verifier is any Entity that receives one or more Attestation Tokens and/or Verifiable Credentials and evaluates whether the Credential(s) authentically and accurately represent the Issuer or Subject (see Credential Verification). A Verifier is a Relying Party that consumes and verifies digital identity information in the form of Attestation Tokens or Verifiable Credentials.

3. Trust Relationships

The authenticity, validity, security, and privacy of the Entities who are involved in the creation, issuance, storage, presentation, and verification of digital Credentials are key to assessing the trustworthiness of those Credentials. This PCTF component identifies key trust relationships that are factors in assessing the trustworthiness of digital Credentials. In consideration of this, the Conformance Criteria associated with the trust relationships and processes identified in this component focus on transparency, auditability, and privacy in addition to technical methods for building trust across the parties involved. Figure 2 provides some illustrative examples of how various roles relate to one another and create the need for these trust relationships.

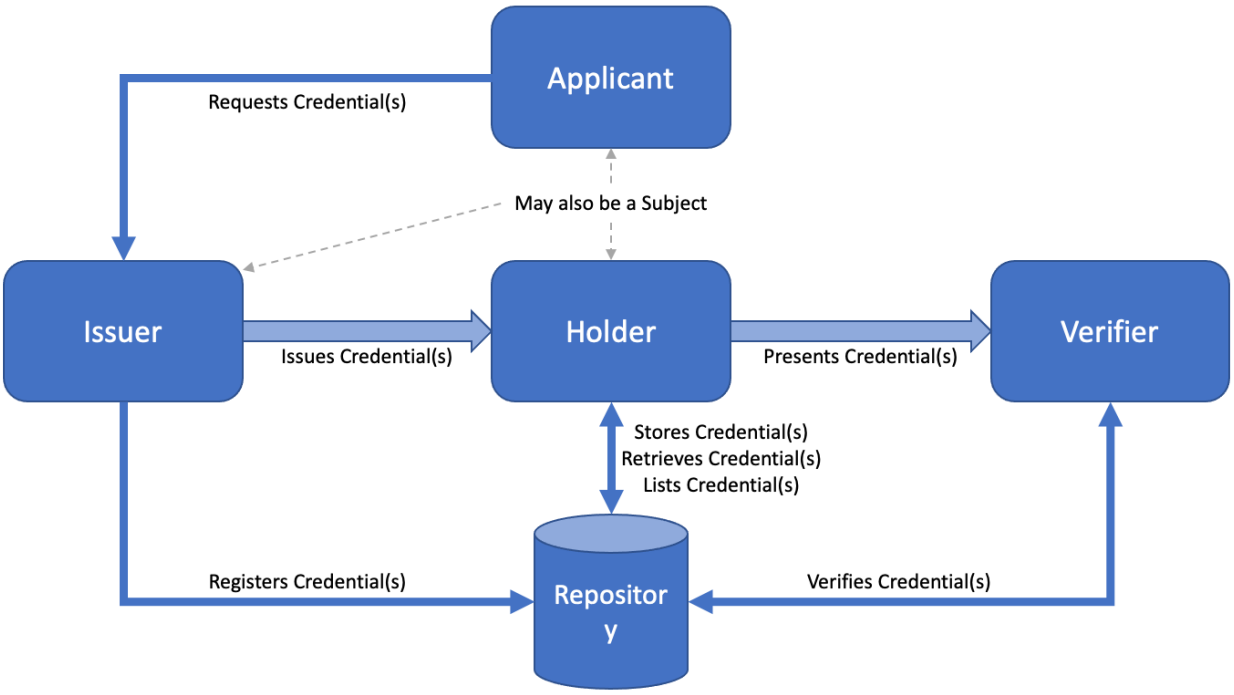

Figure 2. Digital Wallet Roles and Relationships (Illustrative)

It should be noted that this component has been developed with consideration of work that resulted in the W3C Verifiable Credentials Data Model, the Public Sector Profile of the Pan-Canadian Trust Framework, and the Hyperledger Aries project.

Trust relationships described below do not always map directly to discrete technical or business processes.

This component advises Digital Identity Ecosystem Participants to consider the following key requirements for establishing trust in these Relationships and which affect a Credential's trustworthiness:

1. Participants must be able to assess the authority and reliability of Issuers and that Issuers are thorough in establishing the accuracy of information included in a Credential.
2. Participants must be confident that Issuers issue Credentials with the consent of the Subjects, or an Entity eligible to act on behalf of the Subject, or when authorized by legislation or regulation.
3. Participants must be able to assess whether issued Credentials contain accurate, reliable, and up-to-date information.
4. Participants must be confident Issuers have adopted and implemented privacy protecting data structures within Credentials to minimize risk of correlation that could result if a Verifier requests multiple Credentials about a Subject, whether issued by one or more Credential Issuer.

5. Participants must be confident that compromised or invalid Credentials are addressed in an appropriate and timely manner, and that Credentials are only rendered unusable under legitimate circumstances.
6. Participants must be confident that information they share with other Participants, or that is stored in Repositories or Verifiable Registries, is not used by a Service Provider or Verifier except:
    1. as directed by the express consent of the Subject, or
    2. as directed by the express consent of an entity authorized to act on behalf of the Subject, or
    3. when authorized by legislation or regulation.

For example, Participants must not use Credentials with which they have been entrusted to:

- impersonate the Subjects, or
- collude with other Participants to aggregate or share information without such consent.

4. Trusted Processes

The PCTF promotes trust through a set of auditable processes.

A process is a business or technical activity, or set of activities, that transforms an input condition to an output condition upon which other processes often depend. A condition is a particular state or circumstance relevant to a Trusted Process. A condition may be an input, output, or dependency relative to a Trusted Process. Conformance Criteria specify what is required to transform an input condition into an output condition. Conformance Criteria specify, for example, what is required for the Register Digital Wallet process to transform a Verifiable Digital Wallet input condition to a Digital Wallet output condition.

A process is designated a Trusted Process when it is assessed and certified as conforming to Conformance Criteria defined in a PCTF conformance profile. The integrity of a Trusted Process is paramount because many participants may rely on the output of the process, often across jurisdictional, organizational, and sectoral boundaries, and over the short-term and long-term.

The PCTF Digital Wallet component defines the following trusted processes in 3 broad categories:

Wallet Instantiation and Security Processes

1. Create Digital Wallet
2. Register Digital Wallet
3. Authentication

Credential Management and Use Processes

1. Request Verifiable Credential
2. Store Verifiable Credential
3. Manage Verifiable Credential
4. Display Verifiable Credential
5. Render Verifiable Credential
6. Present Proof

Consent Management Processes

1. Included in the Present Proof process

4.1 Conceptual Overview

Figures 3 and 4 provide a conceptual overview, and the logical organization of, the PCTF Digital Wallet Trusted Processes.

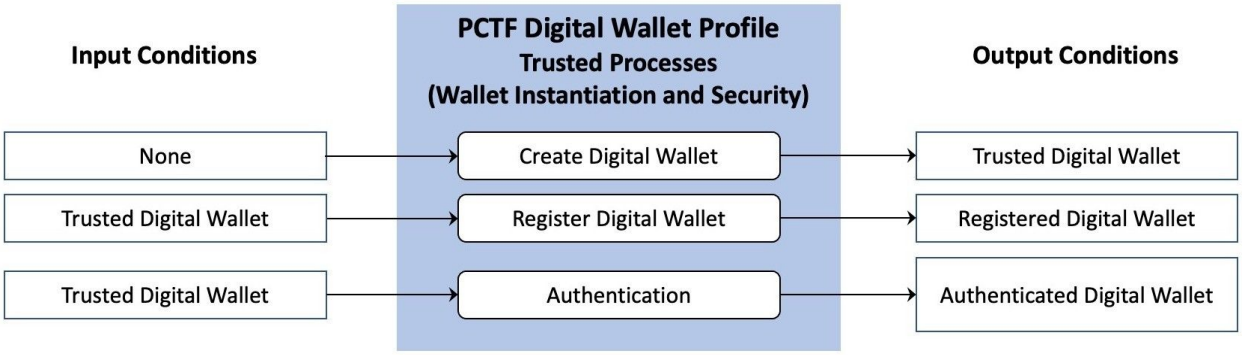

Figure 3: Digital Wallet Instantiation and Security Trusted Processes

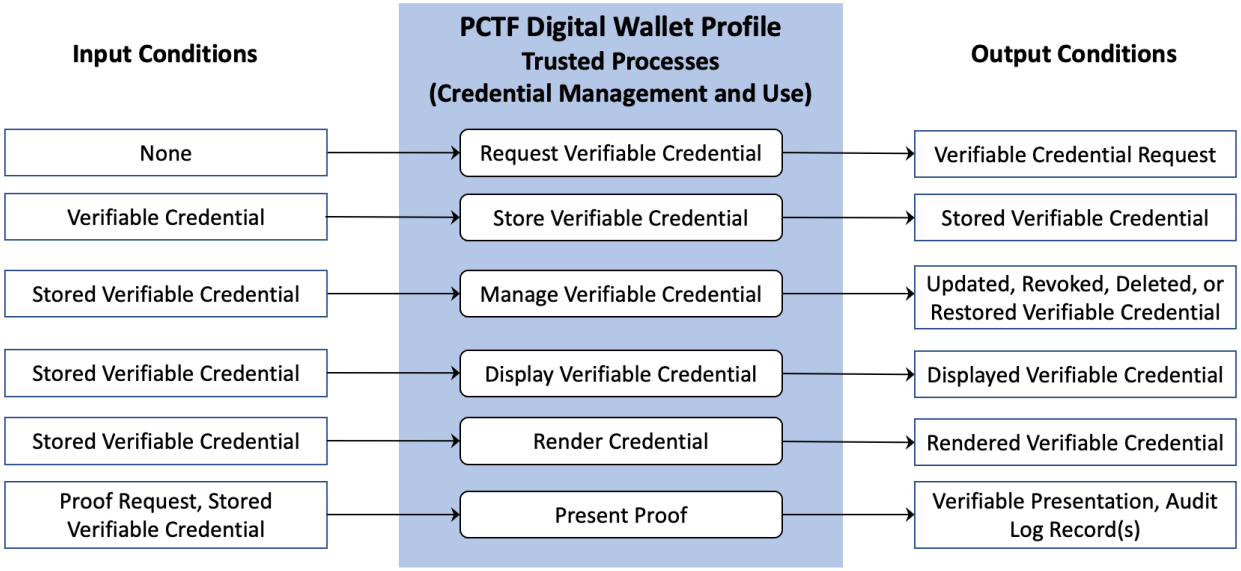

Figure 4: Digital Wallet Credential Management and Use Trusted Processes

4.2 Process Descriptions

The following sections define the PCTF Digital Identity Wallet Component's Trusted Processes. The PCTF Digital Identity Wallet Conformance Profile specifies the Conformance Criteria against which these processes can be assessed.

Trusted Processes are defined using the following structure:

1. **Description:** A descriptive overview of the process.
2. **Input Conditions:** Data that is consumed and/or acted upon on by the process.
3. **Output Conditions:** Data that is created by the process.
4. **Dependencies:** Other processes which must execute prior to the process described in the section, normally because they produce one or more required Inputs.

4.2.1 Wallet Instantiation and Security Processes

Create Digital Wallet

Digital Wallet Creation is the process of creating a Wallet that can be verified by a Verifier. Creation may involve installation of software on a mobile or non-mobile device or generating an instance of a Wallet on a server.

Input Conditions	No input
Output Conditions	Trusted Digital Wallet

Dependencies	No Dependencies

Register Digital Wallet

Digital Wallet Registration is the process of a Holder's Wallet establishing a relationship (or "connecting") a Wallet with an Issuer, Verifier, or Verifiable Data Registry. Once this process is complete, the Holder will have a Registered Digital Wallet which can be persistently managed by the Registration Service of the Issuer, Verifier, or Verifiable Data Registry.

The intent of such registration is that all participants can exercise choice in what they are willing to support and accept. Examples include:

1. A Holder may choose to register ("connect") a Wallet with an Issuer, Verifier, or Verifiable Data Registry.
2. A Verifier may choose to accept such a registration ("connection") from a Wallet.
3. An Issuer may choose to accept a registration from a Wallet that qualifies according to some pre-defined criteria.

Note: This registration may occur many times as it may take place between a Wallet and a number of other parties. This registration may be quite a light-weight process. For example, this may be something as simple as a key-exchange between two parties connecting for the first time.

Input Conditions	Trusted Digital Wallet
Output Conditions	Registered Digital Wallet
Dependencies	Create Digital Wallet

Authentication

This process establishes an authentication control that enables an Holder to bind Credentials to a Digital Wallet. This binding ensures that the Holder is in control of the Digital Wallet and is authorized to possess, control, and present the Credentials being bound to that Wallet.

The output of this process must be cryptographically verifiable.

Input Conditions	Trusted Digital Wallet
Output Conditions	Authenticated Digital Wallet
Dependencies	No Dependencies

4.2.2 Credential Management and Use Processes

Request Verifiable Credential

Through this process a Wallet Holder requests a Credential from an Issuer. The assurance of the request may be enhanced by verifying the Attributes of the Digital Wallet, a Verified Person Record, and the record of binding as a prerequisite to the Credential request.

Note: This process definition intentionally allows a Wallet to request a Verifiable Credential that is issued by the Subject, who may be the user of the Wallet. Such Credentials have been referred to as “self-issued” or “self-attested”.

Input Conditions	None
Output Conditions	Verifiable Credential Request
Dependencies	Create Digital Wallet

Store Verifiable Credential

Through this process a Verifiable Credential is secured and stored by a Digital Wallet. In cases where high levels of assurance are required processes and technologies can be a implemented as a prerequisite to securing the Credential.

Input Conditions	Verifiable Credential
Output Conditions	Stored Verifiable Credential
Dependencies	Create Digital Wallet, Request Verifiable Credential

Manage Verifiable Credential

The PCTF recognized the dynamic nature of Credentials which may be stored in a Digital Wallet. The Manage Verifiable Credential process ensures that Credentials and Attributes stored in Digital Wallets contain accurate and timely information. Through the Manage Verifiable Credential process a Verifiable Credential that is secured and accessed by a Digital Wallet may be:

1. Updated: bringing a Verifiable Credential’s Attributes to date via the Credential’s Issuer.
2. Revoked: the procedure triggered by an Issuer to revoke a Verifiable credential and notify the Verifiable Credential Holder.
3. Expired: the procedure triggered by an Issuer for Notice, and expiration of, an expired Credential.

4. Restored: the procedure used by an Issuer or Digital Wallet Holder to restore a Verifiable Credential.
5. Deleted: the procedure used by a Digital Wallet Holder for deleting a Verifiable Credential.

These functions should only be available to the legitimate Holder of the Credentials (i.e., the Holder bound to the Digital Wallet).

Input Conditions	Stored Verifiable Credential
Output Conditions	Updated, Revoked, Deleted, or Restored Verifiable Credential
Dependencies	Store Verifiable Credential

Display Verifiable Credential

This process retrieves a Credential from a Digital Wallet and displays it for the Holder.

Input Conditions	Stored Verifiable Credential
Output Conditions	Displayed Verifiable Credential
Dependencies	Store Verifiable Credential, Render Verifiable Credential

Render Verifiable Credential

This process establishes a particular state or condition for a secured Credential and displays it in a format that can be read and understood by a human.

Input Conditions	Stored Verifiable Credential
Output Conditions	Rendered Verifiable Credential
Dependencies	Store Verifiable Credential

Present Proof

A Digital Wallet must be able to present proof of Holder (i.e., the Wallet's Holder) Claims (signed credentials) to a Verifier in a compatible format to satisfy a verifier proof request. Key compatibility considerations include format of the Credentials, signature scheme, acceptable Issuer for each requested claim and if Selective Disclosure is supported or not. Ideally the Wallet (and Issuer) will support a two-way negotiation process that satisfies both the Wallet and Verifier policies as opposed to a fixed one-time exchange.

A Proof is a tamper evident presentation of the requested claims that the Verifier can validate via the appropriate cryptographic process. If selective disclosure is supported, then only the specific claims requested by the Verifier can be shared. Otherwise, the full set of credentials required to satisfy the proof request must be shared. The latter presents the risk of sharing personal information for which the verifier has no business need.

Prior to accepting a proof request the Holder must consent to sending the requested information to the Verifier. An audit log, accessible by the Holder, must record the time of the transaction, claims requested and presented, verifier details, success status, and receipt if provided. Optionally the audit log may persist and present a method to review and revoke consent.

Input Conditions	Proof Request, Stored Verifiable Credential
Output Conditions	Verifiable Presentation, Audit Log Record(s)
Dependencies	Store Verifiable Credential

4.2.3 Consent Processes

The PCTF Notice and Consent component is the authoritative source for Notice and Consent conformance criteria. Notice and Consent conformance criteria will not be provided as part of the Digital Wallet Conformance Criteria unless they are unique to interaction with Digital Wallets. Requesting consent to present a credential proof to a verifier is included in the Present Proof process.

5. References

This section lists all external standards, guidelines, and other documents referenced in this PCTF component.

Note: Where applicable, only the version or release number specified herein applies to this PCTF component.

This component of the PCTF leverages the skills, experience, and lessons learned of other organizations working to improve this domain and has taken into consideration material from the following sources:

- CIO Strategy Council: CAN/CIOSC 103-1:2020 Digital Trust And Identity – Part 1: Fundamentals
- Government of Canada, Treasury Board of Canada Secretariat: Public Sector Profile of the Pan-Canadian Trust Framework Version 1.1
- W3C: Verifiable Credentials Data Model 1.0
- W3C: Decentralized Identifiers (DIDs)

6. Revision History

Version	Date	Author(s)	Comment
0.01	2022-01-17	PCTF Digital Wallet Design Team	Initial Discussion Draft created by the PCTF Digital Wallet Design Team
0.02	2022-02-28	PCTF Digital Wallet Design Team	Updated version to incorporate TFEC feedback
0.03	2022-03-10	PCTF Digital Wallet Design Team	Removed duplication of LOA from the Overview, see the Conformance Profile
1.0	2022-03-30	PCTF Digital Wallet Design Team	TFEC approves as Draft Recommendation V1.0
1.1	2022-01-11	PCTF Digital Wallet Design Team	Initial revision edits from Disposition of Comments review.
1.0	2023-01-18	PCTF Digital Wallet Design Team	TFEC approves as Candidate for Final Recommendation V1.0
1.0	2023-4-19	PCTF Digital Wallet Design Team	Approved as Final Recommendation V1.0 through DIACC Sustaining Member Ballot