PCTF Credentials (Relationships & Attributes) Component Overview

Document Status: Final Recommendation V1.0

In accordance with the DIACC Operating Procedures, a Final Recommendation is 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. Changes to this document that may affect certification and Trustmark status will be defined in the Pan-Canadian Trust Framework Assessment component.

This document is provided "AS IS," and no DIACC Participant makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third-party intellectual property rights, and fitness for a particular purpose. Those who are seeking further information regarding DIACC governance are invited to review the DIACC Controlling Policies.

IPR: DIACC-Intellectual Property Rights V1.0 PDF | © 2020

Table of Contents

1 Introduction to the PCTF Credentials (Relationships & Attributes) Component

This document provides an overview of the PCTF Credentials (Relationships & Attributes) 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 Context

A basic task for Digital Identity Ecosystem Participants is conveying information about Subjects to other Participants. The ability to ensure that the Entity at the other end of a connection is who it purports to be is essential to interacting with trust and confidence online. The processes and Conformance Criteria necessary to build that trust are the subject of the PCTF Verified Person and Verified Organization components. Those criteria will not be repeated in this component.

Digital Identity Ecosystem Participants need to be certain not only of the Identity of other Entities with whom they are interacting, but also of additional information that further describe those Entities (e.g.: entitlements, qualifications, contact information…). This information is provided through Attributes or Claims which are stored within Credentials. It is those Credentials and Attributes which are the subject of this PCTF component.

Credentials are common in the physical world. Consider examples associated with owning and operating a vehicle. Driver's licenses tell other people their Subject is qualified and legally permitted to operate a vehicle on public highways. Car insurance slips tell other people their Subject has purchased the required coverage in the event of an accident. Power of attorney papers attest their Subject’s legal relationship with an infirm person should it become necessary to sell a vehicle that Person is no longer legally permitted to operate (a fact that may be reflected in a driver's license). College diplomas and manufacturer training certificates tell automobile owners and garage owners that the technician who services a vehicle is qualified to do so. A business permit and public garage license tell automobile owners and regulators that the garage where the car is serviced is legally entitled to operate. Memberships in local business improvement associations tell automobile owners something about the garage's legitimacy as a business in the local community.

This assortment of Credentials, issued and managed by public and private sector organizations, creates and supports confidence in a significant part of the transportation ecosystem.

1.2 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 their ecosystem protects digital Credentials and key trust relationships associated with those Credentials. This is accomplished by identifying those broad trust relationships and specifying conformance criteria that enable or increase trust in:

- The Entities that issue, Endorse, or Revoke Credentials
- The connections between the Subjects about which Credentials are issued and the Credentials themselves
- The integrity and reliability of Credentials and their contents

The purpose of this component is to establish and maintain trust beyond the integrity and provability of Credential data itself, such that acceptance of digital Credentials becomes as routine as their physical counterparts. This component accomplishes that by focussing on factors that are not wholly technical. The anticipated benefits of this focus include:

- More trust between Entities
- Reduced risk when accepting information or consuming Credentials in the absence of a direct relationship or connection between the Relying Party and the information source
- Transparency regarding key actors
- Improved insight into the validity of Credentials through evidence and Verifiability
- Methods to associate a Credential with a real, unique Person or Organization
- An understanding of the risks associated with a Credential through descriptive details
- Minimization of oversharing of Credential information to reduce the potential for aggregation of personal information or collusion

Note: PCTF 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 Scope

This component specifies Conformance Criteria that Ecosystem Participants can use to assess the degree to which the ecosystem protects the use of digital Credentials. The scope of this component includes features of the digital Credential lifecycle and focuses on ensuring transparency and auditability as the primary methods for building trust across the Entities involved. Specific items deemed in or out of scope are described in the following sections.

1.3.1 In-Scope

In scope for this PCTF component are Credentials that:

- Contain or provide information about a Subject (e.g., digital proof of educational qualifications or a license to operate a business) and an Issuer
- Contain or provide information about the Relationship between a Subject and at least one other Entity (e.g., digital proof that a person is an employee of a business)
- Contain information one Entity provides about or to another Entity
- Describes Relationships between one or more Subjects and one or more other Entities

Regardless of Credential content or the connection between an Issuer and a Subject, the scope of this component includes:

- Issuance of Credentials to Subjects
- Information that increases the trustworthiness of Credentials
- Guidance on protecting the integrity and accuracy of Credential information
- Direction on managing compromised Credentials

1.3.2 Out-of-Scope

Verification and Validation of the Identity of a Person or Organization is out-of-scope for this component. Those processes, and the creation and use of Identity Information upon which they depend, is covered in the PCTF Verified Person and Verified Organization components.

Also out-of-scope for this PCTF component are the following:

- Specific Conformance Criteria for issuance of a Credential by multiple Issuers
- Rules and policies governing who can obtain a specific Credential or specific type of Credential (e.g., requirements to obtain a license to drive in a given jurisdiction)
- Processes for assessing qualification or eligibility for a specific Credential or type of Credential (e.g., testing of new drivers), notwithstanding requirements to provide documentation of such processes
- Acceptance of a Credential for a given purpose (e.g., whether or not a driver's license is accepted as proof of address)
- Delegation of authority is out of scope for this release and will be considered for a future release

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.

Figure 1 is an illustration of the components of the draft Pan-Canadian Trust Framework.

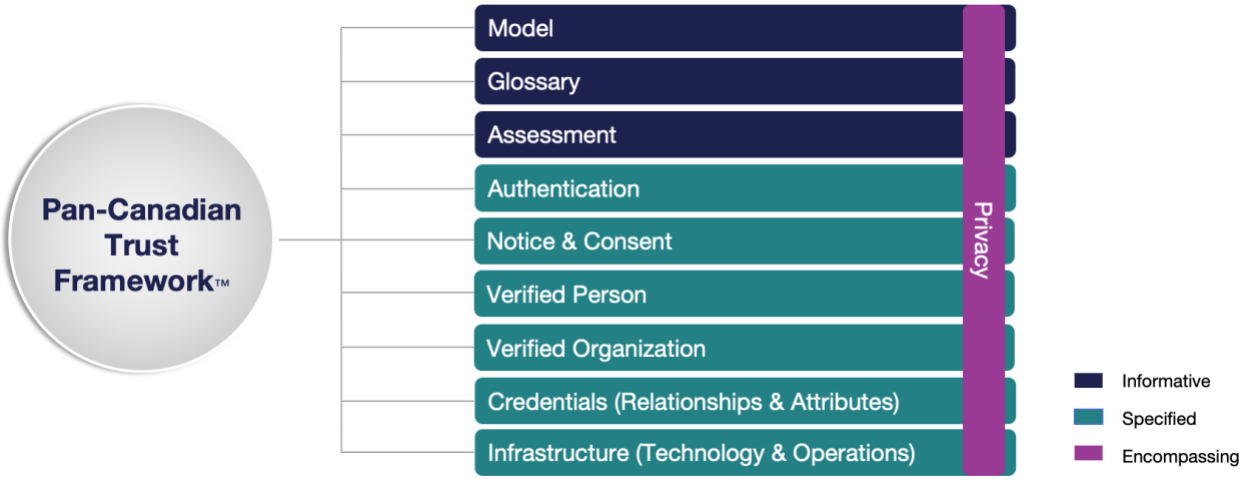


Figure 1. Components of the Pan-Canadian Trust Framework

2 Conventions

This section describes and defines key terms and concepts used in the PCTF Credentials (Relationships & Attributes) 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.

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.

Attribute Definition

An Attribute Definition is a Credential that describes a specific type, or class, of Attribute. An Attribute Definition does not describe a specific instance of an Attribute (e.g., Martina's specific date of birth; Hiren's specific degree). Rather, the Attribute Definition describes the *characteristics* of such Attributes. Attribute Definitions are created via the Define Attribute Trusted Process as described later in this document.

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).

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 and accurately represents the Issuer or Presenter. 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.

Declared Relationship

A Declared Relationship is a Credential that documents an assertion by an Entity that a Relationship exists between two or more Subjects. A Declared Relationship describes a *specific instance* of a Relationship between the Subjects (e.g., Diya and Charles are legally married in a specific jurisdiction; Fatima has earned a PhD from the University of British Columbia; Louise is a federally registered Director of FictitiousCorp). The structure of a Declared Relationship is derived from a Relationship Definition. Declared Relationships are created via the Declare Relationship process.

Derived Predicate

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 only to people who are at least twenty-one 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 twenty-one 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 / Verifiable Credential 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. A Verifiable Credential Wallet is a Digital Wallet that may store only Verifiable Credentials. (See also, Repository.)

Disclaimed Relationship

A Disclaimed Relationship is an assertion by an Issuer of an Endorsed Relationship that they believe the Endorsed Relationship is no longer valid (e.g., a membership has expired; a Relationship or one or more of its Claims has been discovered to be fraudulent). Once a Relationship has been Disclaimed, its Claims are no longer valid.

Endorsed Relationship

An Endorsed Relationship is a specific type of Credential that asserts a Subject or third party confirms their belief that a Declared Relationship is valid. An Endorsed Relationship may be endorsed by more than one Entity.

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 connected (e.g., Fatima has earned a PhD from the University of British Columbia; Eric is an employee of FictitiousCorp; Diya and Charles are legally married).

Relationship Definition

A Relationship Definition is a Credential that describes a specific *type* of Relationship that exists between two or more Subjects, or class of Relationship (e.g., a description of the structure of a marriage type of Relationship Credential or driver's license type of Relationship Credential). A Relationship Definition does not describe a specific instance of a Relationship between two Entities (e.g., Fatima has earned a PhD from the University of British Columbia; Eric is an employee of FictitiousCorp; Diya and Charles are legally married). Rather, the Relationship Definition describes the *characteristics* of such relationships. Relationship Definitions are created via the Define Relationship process.

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.

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, privacy respecting, and machine Verifiable.

Verified Credential

A Verified Credential is a Verifiable Credential which is determined to be authentic by a Verifier.

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. Verifiable Presentations must be cryptographically secure, privacy compliant, privacy respecting, and machine Verifiable.

Verifiable Relationship

A Verifiable Relationship is a tamper-evident Declared Relationship, Endorsed Relationship, or Disclaimed Relationship that is encoded in a way that enables its integrity and authorship (i.e., source) to be confirmed via cryptographic Verification. Verifiable Relationships must be cryptographically secure, privacy compliant, privacy respecting, and machine Verifiable.

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

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 Relying Party 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.

Declaring Party

A Declaring Party is any Entity that declares a relationship between two or more Subjects using the Declare Relationship process (see Trusted Processes below). The Declaring Party may, or may not, be a Subject of the Declared Relationship.

Defining Party

A Defining Party is any Entity that creates a Relationship Definition using the Define Relationship process (see Trusted Processes below).

Disclaiming Party

A Disclaiming Party is any Entity with exclusive or primary responsibility for Disclaiming Relationships (via the Disclaim Relationship Trusted Process as described below) and maintaining information about Disclaimed Relationships. The Disclaiming Party may be the Endorsing Party of a Disclaimed Relationship, or a Subject of the Disclaimed Relationship, but need not be so.

Endorsing Party

An Endorsing Party is any Entity that asserts their belief that a Declared Relationship is valid via the Endorse Relationship process (see Trusted Processes below). An Endorsed Relationship may be Endorsed by more than one Endorsing Party.

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 on 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 or Verifiable Credential (e.g., a province or territory that issues a drivers' license).

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).

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 Verifiable Credentials and evaluates whether the Credential(s) authentically and accurately represent the Issuer or Subject. (See Credential Verification.)

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.

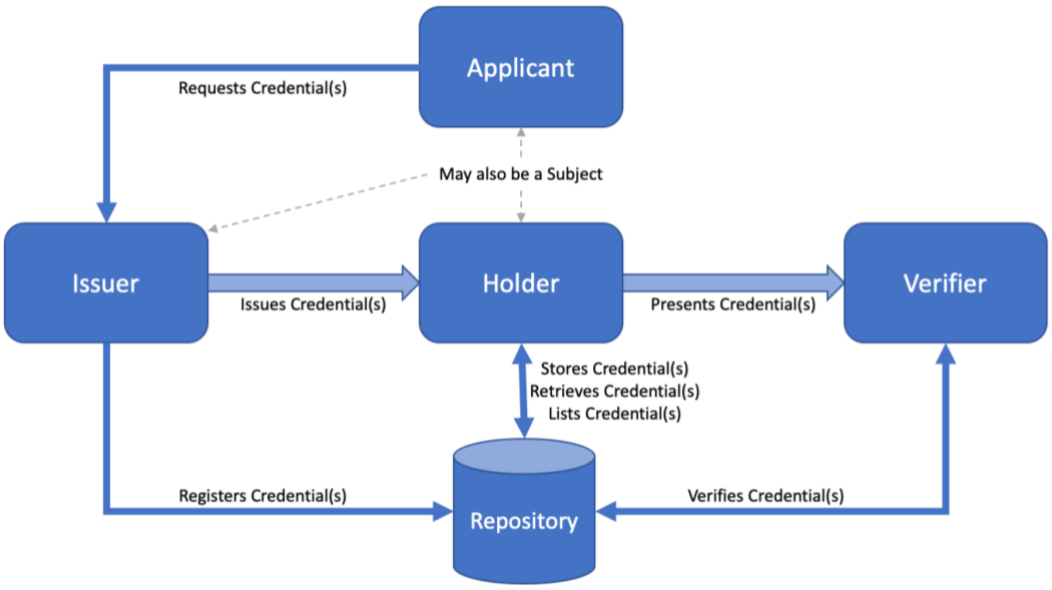


Figure 2. Credentials (Relationships & Attributes) Roles and Relationships (Illustrative)

It should be noted that both the W3C Verifiable Credentials Data Model and the Public Sector Profile of the Pan Canadian Trust Framework include great work in this area which was taken into consideration as this component was developed.

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

This component advises Digital 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 Relying Party 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 as directed by the express consent of the Subject, or an entity authorized to act on their behalf, or 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 Levels of Assurance

It is critical that Participants that create or consume Credentials understand the level of trust they can ascribe to those Credentials. The PCTF Credentials (Relationships & Attributes) component employs a Levels of Assurance approach to address this. Figure 3 provides an overview of the Credentials assurance levels (CALs). Credential assurance also involves the process of binding a Credential to one or more Subjects.

Credential Assurance Level (CAL)	Qualification Description

Level 1 (CAL1)	• Satisfies all Level 1 Conformance Criteria • Little or no confidence required • Little confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised
Level 2 (CAL2)	• Satisfies all Level 2 Conformance Criteria • Some confidence required • Some confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised
Level 3 (CAL3)	• Satisfies all Level 3 Conformance Criteria • High degree of confidence required • High confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised
Level 4 (CAL4) Optional	• Satisfies all Level 4 Conformance Criteria • Very high degree of confidence required • Very high confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised

Figure 3. Credentials Assurance Levels

These assurance levels are further described in the PCTF Credentials (Relationships & Attributes) Conformance Profile document.

In order to achieve a specific CAL a Credential must, at a minimum, satisfy that CAL for every applicable conformance criterion. For example, if a Credential met the standard for CAL4 on nine of the criteria, and met the standard for CAL1 on one criterion, the assessed CAL for the Credential can be no higher than CAL1. This is further explained in the Conformance Profile.

5 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 Endorse Relationship process to transform a Declared Relationship input condition to an Endorsed Relationship 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 Credentials (Relationships & Attributes) component defines five trusted Relationships processes:

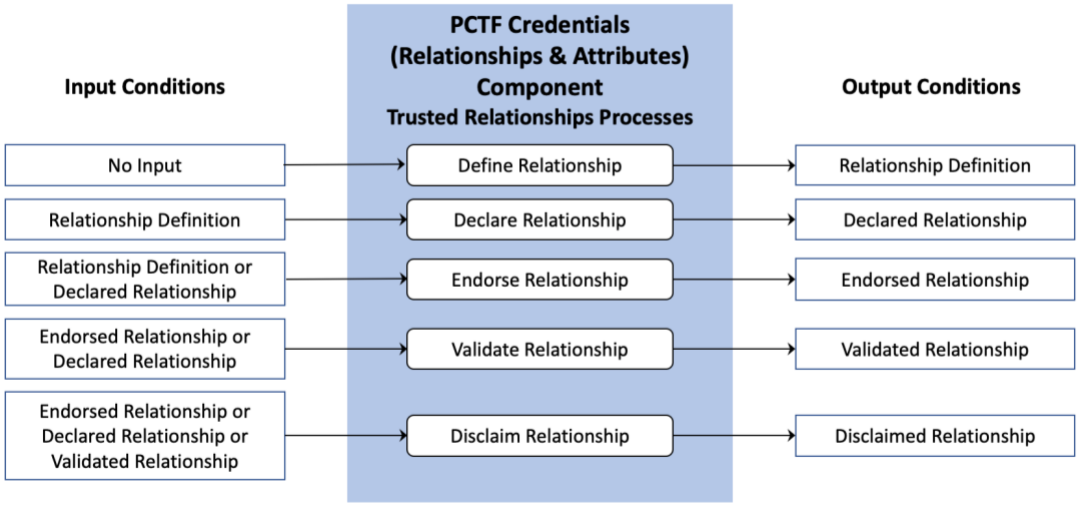
1. Define Relationship
2. Declare Relationship
3. Endorse Relationship
4. Validate Relationship
5. Disclaim Relationship

The PCTF Credentials (Relationships & Attributes) component defines four trusted Attributes processes:

1. Define Attribute
2. Bind Attribute
3. Maintain Attribute
4. Revoke Attribute

5.1 Conceptual Overview

Figure 4 provides a conceptual overview, and the logical organization of, the PCTF Credentials (Relationships & Attributes) Trusted Relationships Processes. Figure 5 provides a conceptual overview, and the logical organization of, the PCTF Credentials (Relationships & Attributes) Trusted Attributes Processes.



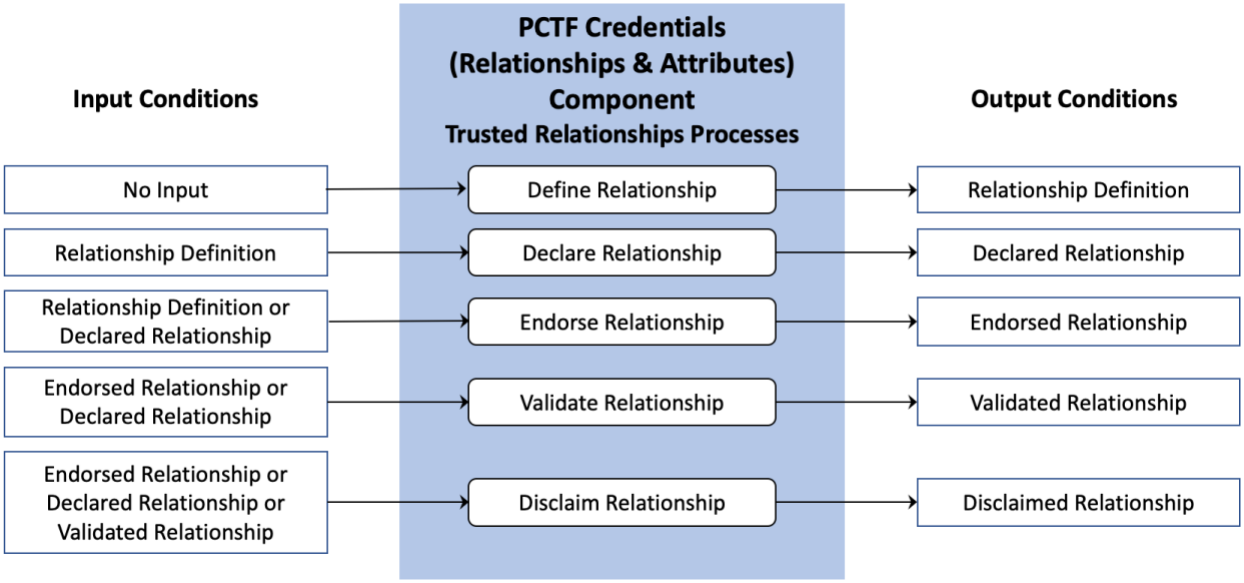


Figure 4. Relationships Conceptual Overview

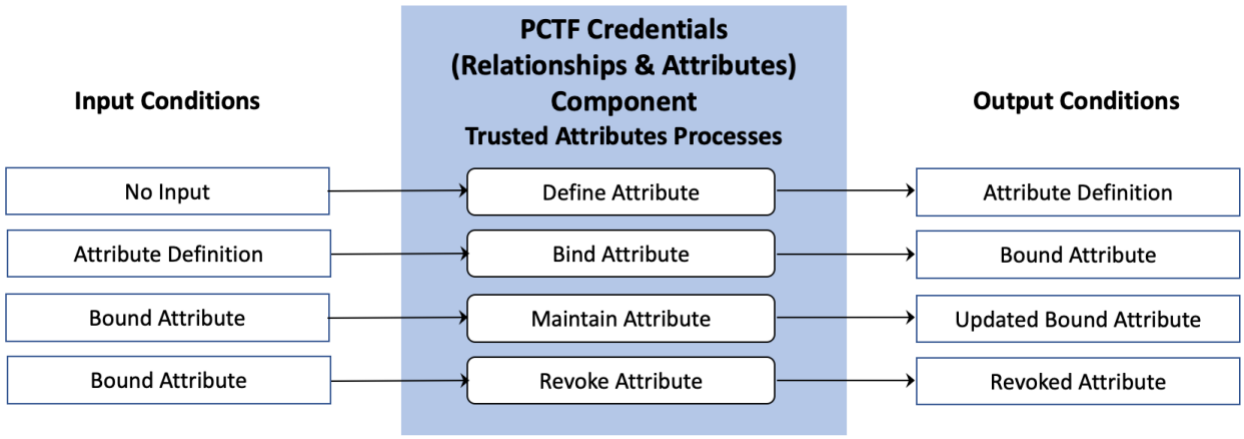


Figure 5. Attributes Conceptual Overview

5.2 Process Descriptions

The following sections define PCTF Credentials (Relationships & Attributes) Component's Trusted Processes. The PCTF Credentials (Relationships & Attributes) Conformance Profile specifies the Conformance Criteria against which these processes can be assessed.

Credentials (Relationships & Attributes) Trusted Processes are defined using the following structure:

1. Description – A descriptive overview of the process
2. Inputs – Data that is consumed and/or acted upon on by the process

3. Outputs – 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

5.2.1 Define Relationship

The Define Relationship process describes a specific *type* of Relationship that exist between two or more Subjects, or class of Relationship, in the form of a Relationship Definition. A Relationship Definition does not describe a specific instance of a Relationship between two Entities (e.g., Fatima has earned a PhD from the University of British Columbia; Eric is an employee of FictitiousCorp; Diya and Charles are legally married). Specific instances of Relationships are created by the Declare Relationship process described later in this document. Rather, the Relationship Definition describes the *characteristics* of such Relationships. The Relationship Definition:

- Defines and characterizes a type of Relationship (e.g., marriage license, driver's license, degree)
- Describes the source of the Relationship (e.g., provincial government, educational institution)
- Describes the Relationship's defining characteristics (e.g., the type of degree granted)
- Indicates whether or not a Relationship must be Endorsed before it should be trusted (see "Endorse Relationships" later in this document)
- Indicates whether the Relationship may be Disclaimed (see "Disclaim Relationships" later in this document)
- Declares known risks that should be considered for the type of Relationship that it defines (e.g., whether the Relationship is ephemeral in nature; common conditions or events that might render the Relationship invalid)
- Provides guidance to Relying Parties regarding conditions or artifacts that should be considered (in addition to the Relationship's CAL) in the evaluation of its trustworthiness (e.g., whether specific defining characteristics of the Relationship are to be considered mandatory)
- Includes relevant legal definitions, industry standard definitions of the Relationships, or references to them or to relevant schemas
- Describes any evidence of trustworthiness that exists (e.g., related Verified Credentials or Validated Relationships), or states there is none

Any Entity may define a Relationship including, though not limited to, all Entities involved in such a Relationship, an Issuer, an Authoritative Source, or a Relying Party.

Inputs	No Input
Outputs	Relationship Definition
Dependencies	No Dependencies

5.2.2 Declare Relationship

The Declare Relationship process is an assertion by any Entity that a Relationship exists between two or more Subjects. In contrast with the Define Relationship process, the Declare Relationship process describes a *specific instance* of a Relationship between the Subjects (e.g., Diya and Charles are legally married in a specific jurisdiction; Eric is a Director of FictitiousCorp; Fatima has earned a PhD from the University of British Columbia). The Declare Relationship process references a Relationship Definition to derive the structure of the Relationship it is declaring and the Relationship's mandatory Attributes.

The Entity declaring the Relationship may or may not be one of the Subjects of the Relationship (e.g., a lawyer might declare a legal relationship on behalf of two business partners; an accrediting organization might declare that Gabriel is Ali's carpentry apprentice). Each Subject of a Relationship that is a Person should be a Verified Person or Verified Organization.

In addition to its primary claim, a Declared Relationship may contain additional detailed Claims regarding its Subjects (e.g., a Subject's birth date; that a Subject resides at a specified address). Alternatively, a Claim may consist of a Derived Predicate.

When a Declared Relationship has been issued, the Holder - which is often, though not always, a Subject - may store the Declared Relationship in a Repository such as a Digital Wallet or Verifiable Credential Wallet. The Level of Assurance associated with the Repository will have a direct impact on the assurance level assigned to any Declared Relationships stored within.

Inputs	Relationship Definition
Outputs	Declared Relationship
Dependencies	Define Relationship

5.2.3 Endorse Relationship

Through the Endorse Relationship process an Entity confirms their belief that a Declared Relationship is valid. An Endorsed Relationship may be endorsed by more than one Entity. Relying Parties may take into consideration whether multiple endorsements of a Relationship is an indication of the strength of its validity. When evaluating a Relationship's trustworthiness Relying Parties must consider the source of the endorsement(s), and whether those sources are Verified Persons or Verified Organizations.

The output of the Endorse Relationship process may be an Endorsed Relationship or a Verifiable Endorsed Relationship. There are cases where an Endorsed Relationship could be created without the existence of a Declared Relationship (e.g., a province or state issuing a drivers' license could issue an Endorsed Relationship Credential). While Endorsed Relationships or Verifiable Endorsed Relationships might be issued by any Entity, they are only truly meaningful when generated by a Verified Person or Verified Organization.

When an Endorsed Relationship has been issued, the Holder may store the Relationship in a Repository such as a Verifiable Repository, Digital Wallet, or Verifiable Credential Wallet. The Level of Assurance associated with the Repository will have a direct impact on the assurance level assigned to any Relationships stored within.

Inputs	Relationship Definition or Declared Relationship
Outputs	Endorsed Relationship
Dependencies	Declare Relationship

5.2.4 Validate Relationship

When a Relationship Holder (which is normally the Subject of the Relationship, but could be a third party with the Subject's consent to share the Relationship) is requested to present one or more Claims by a Relying Party, they present a Relationship Credential containing those Claims to a Verifier in the form of a Presentation or Verifiable Presentation. Presentations and Verifiable Presentations may contain a combination of detailed Claims (e.g.:, birth date, age, address, specific qualification) and/or Derived Predicates. The Verifier confirms the Relationship(s) presented to be authentic by:

1. Confirming that the state(s) of Relationship(s) is(are) valid (e.g., not expired, suspended, or revoked)
2. Confirming that the Credential is valid, usually through cryptographic Verification
3. Confirming the Relationship(s) and/or Presentation(s) conform to any relevant standards or specifications

If the Verifier is satisfied that the Relationships are authentic, they will provide the data supplied in the Presentation or Verified Presentation to a Relying Party in the form of a Validated Relationship.

Unless required to do so by regulation, policy, or legislation, Verifiers should not retain copies of Presentations or Verified Presentations in order to limit the potential exposure of their Subject's personally identifiable information.

Verifiers must never share information presented to them as part of the Verification process with other Verifiers, other Participants, or anyone other than the Relying Party or Relying Parties without the express consent of the Subject unless permitted or required to do so by legislation or regulation. This type of collusion could enable colluders to aggregate data and derive much more information about the Subject than was in the possession of any of the colluders. This type of activity may result in significant harm to a Subject.

Relationships included in a Presentation or Verifiable Presentation that is submitted to a Verifier may be in the form of a Declared Relationship or Endorsed Relationship. Even a self-asserted Declared Relationship may become a Validated Relationship under the proper circumstances (e.g., Christine self-asserts she possesses a valid driver's license for the Province of Nova Scotia which can be validated by it's Authoritative Source, the Province; Anderson self-asserts

he is the owner of a Federally-registered Canadian business which can be validated by it's Authoritative Source, the Government of Canada).

Inputs	Declared Relationship or Endorsed Relationship
Outputs	Validated Relationship
Dependencies	Endorse Relationship or Declare Relationship

5.2.5 Disclaim Relationship

There are numerous situations where an Issuer might want to render a Relationship invalid to ensure the Subject, Holder, or anyone can not present its Claims. For example:

- A membership may expire rendering membership related Claims invalid
- The Relationship and one or more of its Claims may have been created fraudulently
- Fraud is being committed using the Relationship and a new Relationship must be created to limit harm to its Subject
- A Relationship may have been issued in error
- The Relationship and/or one or more of its Claims may have been rendered invalid via a legal judgement
- An event or change in the Subject's circumstances or qualifications may necessitate the revocation of a Validated Relationship and the issuance of a new Validated Relationship (e.g., a Subject's driver's license is upgraded from provisional to a fully qualified license; a Subject receives a promotion in rank from corporal to sergeant; a Subject's marital status changes).

In such cases Relationships must be Disclaimed. If a Subject requires the ability to present one or more of the Claims in a Disclaimed Relationship, they must request a new Relationship as described in the Declare Relationships, Endorse Relationships, and/or Validate Relationships processes in this overview.

There may be cases where Claims within a Disclaimed Relationship are accepted by a Relying Party, at the discretion of the Relying Party (e.g., a suspended driver's license *might* be acceptable proof of age to certain Relying Parties).

Inputs	Declared Relationship, Endorsed Relationship, Verifiable Endorsed Relationship, or Validated Relationship
Outputs	Disclaimed Relationship
Dependencies	Declare Relationship, Endorse Relationship, or Validate Relationship

5.2.6 Define Attribute

The Define Attribute process describes a specific *type* of Attribute that may describe a Subject, or a class of Attributes, in the form of an Attribute Definition. An Attribute Definition does not

describe a specific instance of an Attribute (e.g., Martina's specific date of birth; Hiren's specific degree). Rather, the Attribute Definition describes the *characteristics* of such Attributes. The Attribute Definition:

- Defines and characterizes a type of Attribute (e.g., year of manufacture, date, academic credential, industry certifications, qualifications)
- Provides context for the use of the Attribute (e.g., how to use it, its intended purpose, and appropriate and/or inappropriate usage)
- Describes the source of the Attribute if appropriate (e.g., provincial government, educational institution)
- Describes the Attribute's defining characteristics or format (e.g., a date in the form of DD-MMM-YYYY), and is not sufficiently qualified by its name alone (e.g., the name "Date" would not sufficiently describe whether 01-02 is January 2nd, February 1st, January 2002, February 1901…)
- Indicates whether it is an Attribute value or a Derived Predicate
- Includes a version number and/or date of origin, or other identifier that will enable Issuers and Relying Parties to distinguish different versions of the definition
- Declares known risks that should be considered for the type of Attribute that it defines (e.g., whether the Attribute is ephemeral in nature; common conditions or events that might render the Attribute invalid).
- Provides guidance to Relying Parties regarding its trustworthiness
- Creates a common vocabulary and understanding amongst issuers and consumers of the Attribute
- Includes a disclaimer of liability, or statement there is none
- Includes relevant legal definitions, industry standard definitions of the Attribute, or references to it or relevant schemas, or statements there are none
- Describes any evidence of trustworthiness that exists (e.g., related Verified Credentials or Validated Relationships), or states there is none
- Describes the authority under which the Attribute was issued, or states there was none

Though Attributes would normally be defined by an Issuer or Authoritative Party, any entity may define an attribute.

Inputs	No Input
Outputs	Attribute Definition
Dependencies	No Dependencies

5.2.7 Bind Attribute

The Bind Attribute process is an assertion by an Issuer that one or more Attributes accurately describe one or more Subjects in the form of a Bound Attribute. In contrast with the Define Attribute process, the Bind Attribute process describes a *specific instance* of an Attribute that describes one or more Subjects (e.g., Martina's date of birth is January 2, 2020; Eric is an employee of FictitiousCorp; Hiren's degree is a Master of Science). Alternatively, an Attribute may consist of a Derived Predicate.

The Bind Attribute process references an Attribute Definition to derive the required contents of the Attribute and its appropriate usage and context.

The Bind Attribute process is executed by an Issuer who is an authority in the context of the Attribute (i.e., an Authoritative Source) and that can verify the Attribute accurately describes the Subject(s) (e.g., a telecom company is an Authoritative Source for issuing a legally registered telephone number). The Subject of an Attribute may or may not be uniquely identifiable, and may or may not be a Verified Person or Verified Organization.

Bound Attributes must be cryptographically Verifiable.

When a Bound Attribute has been issued, the Holder - which is often, though not always, a Subject - may store the Bound Attribute in a Repository such as a Verifiable Repository, Digital Wallet, or Verifiable Credential Wallet. The Level of Assurance associated with the Repository will have a direct impact on the assurance level assigned to any Bound Attributes stored within.

Inputs	Attribute Definition
Outputs	Bound Attribute
Dependencies	Define Attribute

5.2.8 Maintain Attribute

Due to the nature of some of the data that may be contained in Bound Attributes it may be necessary to update them. These changes may be related to changes in the Attribute itself (e.g., a residential address change; an expiration date is extended; a membership is renewed; driver's license demerit points are earned; a license to sell alcohol is renewed) or changes in state that affect a Derived Predicate (e.g., the Subject celebrates their twenty-first birthday and is eligible to change an "Over21" Derived Predicate to "True"). In such cases an Issuer may update a Bound Attribute and provide it to the Holder.

In some cases it may be possible to update information without changing a Credential (e.g., a change in a Derived Predicate that is derived outside the Credential itself). In most other cases it will not likely be possible, desirable, or advisable to update an existing Bound Attribute. Thus, in most cases a new Bound Attribute will be issued using the Bind Attribute Processes. When a new Bound Attribute is issued, it may or may not be appropriate to revoke previously existing Bound Attributes using the Revoke Attribute process. For example, if someone was the president of a local service club for the calendar year 2019 and is not re-elected in 2020, there would be no need to revoke the Bound Attribute indicating they were president in 2019. However, if the Bound Attribute indicated they are the "current president" and they are not re-elected, it would make sense to revoke the Attribute.

Inputs	Bound Attribute
Outputs	Updated Bound Attribute
Dependencies	Define Attribute, Bind Attribute

5.2.9 Revoke Attribute

There are numerous situations where an Issuer might want to permanently render an Attribute invalid to ensure it cannot be presented by any entity as if it were a currently accurate description of the Subject(s). For example:

- A membership may expire
- The Attribute may have been bound fraudulently
- Fraud is being committed using the Attribute and a new Attribute (e.g., credit card number) must be created to limit harm to its Subject(s)
- An Attribute may have been bound to a Subject in error
- The Attribute may have been rendered invalid via a legal judgement
- An event or change in a Subject's circumstances or qualifications may necessitate the revocation of a Bound Attribute and the issuance of a new Bound Attribute (e.g., a Subject's driver's license is permanently suspended due to repeated driving while intoxicated offences)

In such cases Bound Attributes must be revoked. The intent of revocation is to permanently invalidate a Bound Attribute. If a Subject requires the ability to present a proof that depends upon a Revoked Attribute, they must request a new Bound Attribute from the Issuer as described in the Bind Attributes process in this overview.

Inputs	Bound Attribute
Outputs	Revoked Attribute
Dependencies	Define Attribute, Bind Attribute

6 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:

- W3C: Verifiable Credentials Data Model 1.0 <https://www.w3.org/TR/vc-data-model/>
- Government of Canada, Treasury Board of Canada Secretariat: Public Sector Profile of the Pan-Canadian Trust Framework Version 1.1 <https://canada-ca.github.io/PCTF-CCP/>

7 Revision History

Version Number	Date of Issue	Author(s)	Description
0.01	2020-01-20	PCTF Editing Team	Initial Discussion Draft
0.02	2020-03-18	PCTF Editing Team	Disposition of initial TFEC Comments
0.03	2020-04-08	PCTF Editing Team	Added relationship-centric processes
0.04	2020-04-22	PCTF Editing Team	Added attribute-centric processes
1.0	2020-05-13	PCTF Editing Team	Draft Recommendation V1.0
1.1	2020-07-29	PCTF Editing Team	Draft Recommendation V1.1
1.0	2020-09-16	PCTF Editing Team	Final Recommendation V1.0