PCTF Credentials (Relationships & Attributes)

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 to the PCTF Credentials (Relationships & Attributes) Component

Content herein concerns itself with the domain specific topic for this Pan-Canadian Trust Framework (PCTF) component. The overview section provides information related to and necessary for consistent interpretation of the included conformance criteria. For a general introduction to the PCTF, please see the PCTF Overview that describes the background, purpose, scope, principles, and objectives of the framework.

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.

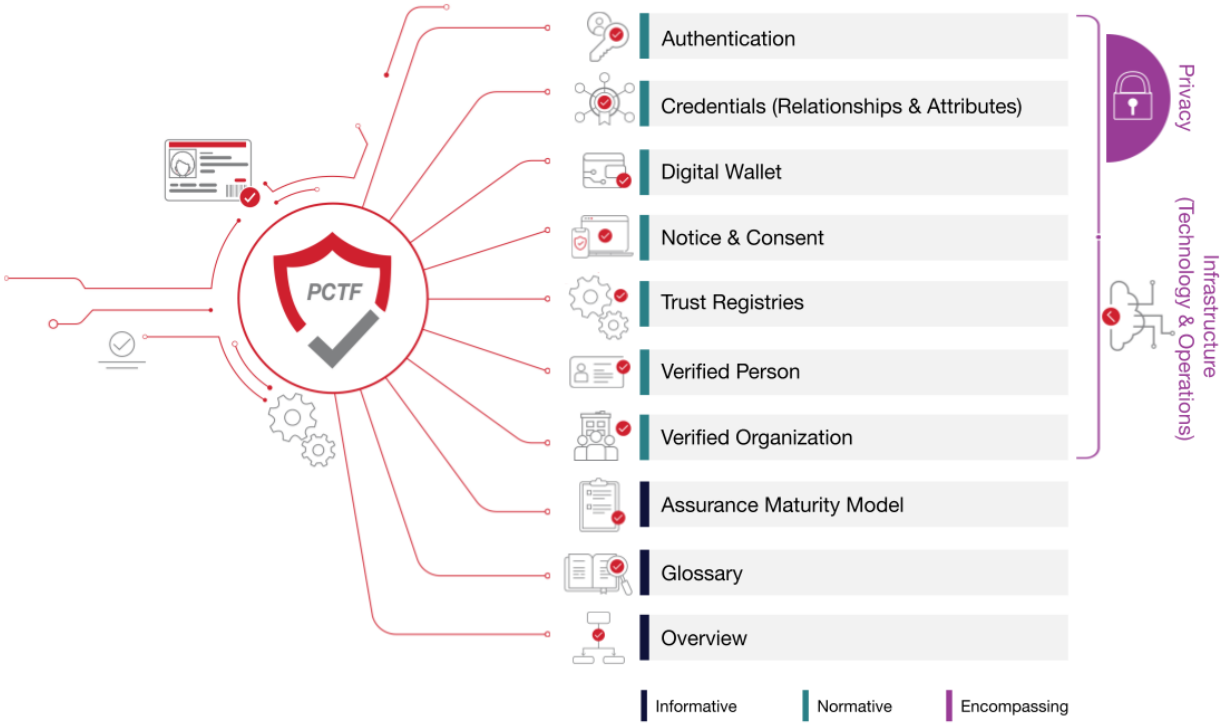

Figure 1. Components of the Pan-Canadian Trust Framework

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.

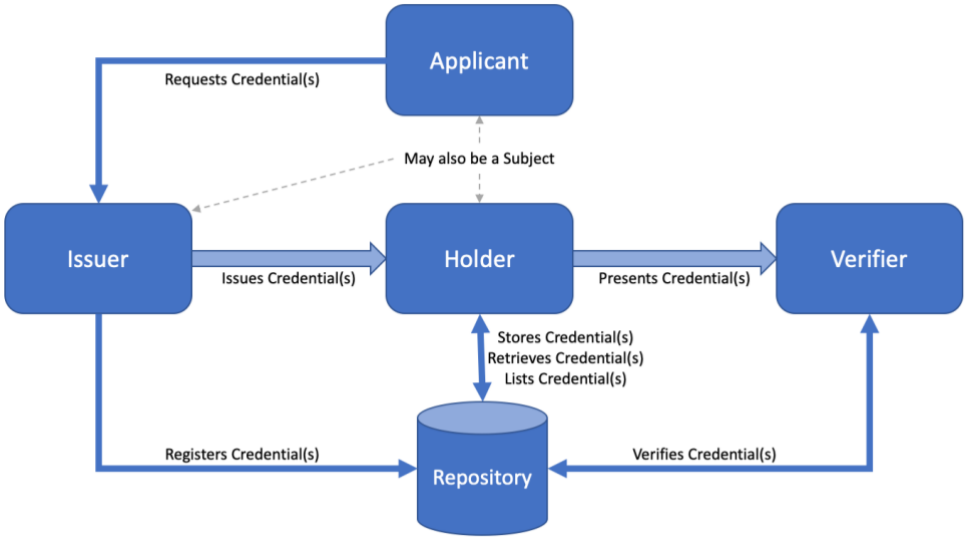

Figure 2. Credentials (Relationships & Attributes) Roles and Relationships (Illustrative)

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.

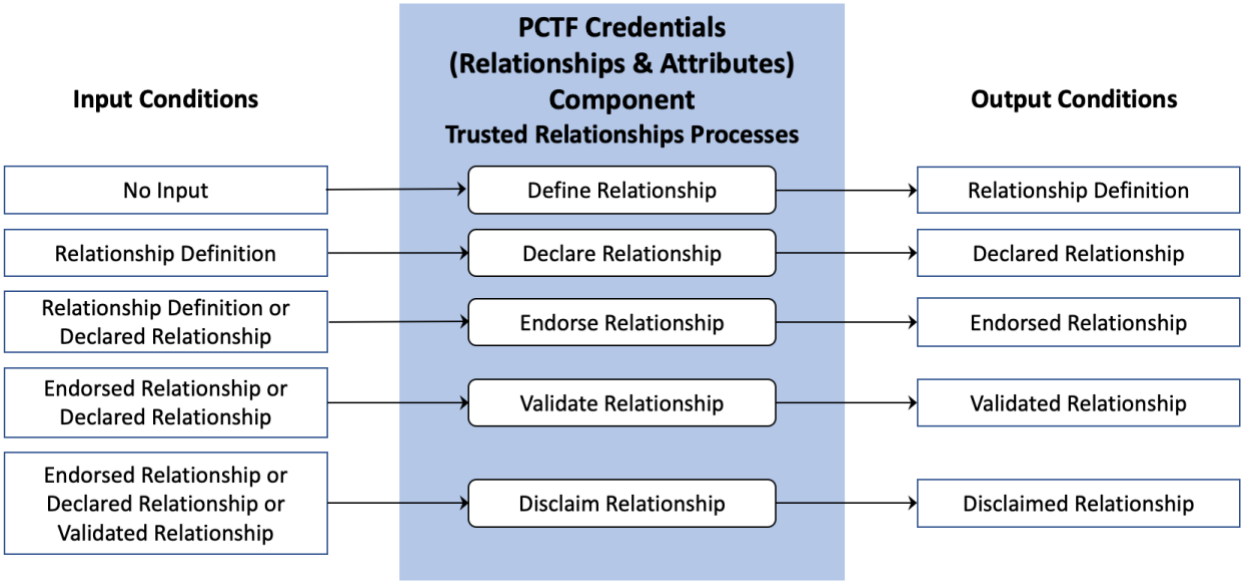

Figure 4. Relationships Conceptual Overview

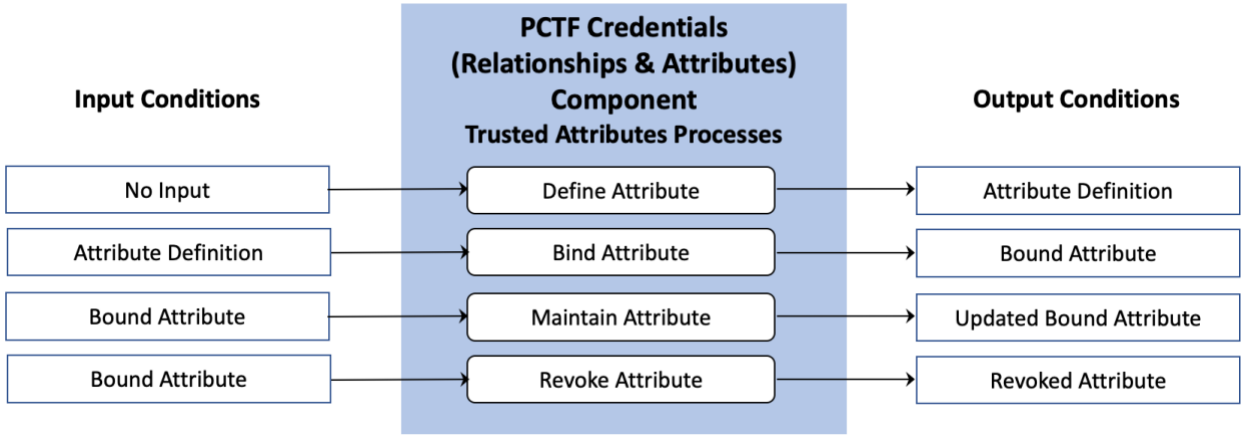

Figure 5. Attributes Conceptual Overview

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. Introduction to the PCTF Credentials (Relationships & Attributes) Conformance Profile

This section specifies the conformance criteria for the Credentials (Relationships & Attributes) component of the Pan-Canadian Trust Framework (PCTF). Conformance Criteria are central to the trust framework because they specify the essential requirements agreed to by trust framework participants to ensure the integrity of their processes. This integrity is paramount because the output or result of a trusted process may be relied upon by many participants across organizational, jurisdictional and sectoral boundaries.

The PCTF Conformance Criteria are intended to complement existing privacy legislation and regulations.

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.

6.1 Conformance Criteria Keywords

Throughout this document the following terms indicate the precedence and/or general rigidity of the conformance criteria and are to be interpreted as noted below.

- **MUST** means that the requirement is absolute as part of the Conformance Criteria.
- **MUST NOT** means that the requirement is an absolute prohibition of the Conformance Criteria.
- **SHOULD** means that while there may exist valid reasons in particular circumstances to ignore the requirement, the full implications must be understood and carefully weighed before choosing to not adhere to the Conformance Criteria or choosing a different option as specified by the Conformance Criteria. The rationale for not adhering to a criterion should be documented in cases where Conformance Criteria are not adhered to.
- **SHOULD NOT** means that a valid exception reason may exist in particular circumstances when the requirement is acceptable or even useful, however, the full implications should be understood and the case carefully weighed before choosing to not conform to the requirement as described.
- **MAY** means that the requirement is discretionary but recommended.

Note: The above listed keywords appear in **bold** typeface and ALL CAPS throughout this conformance profile.

7. 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 1 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 6. Credentials Assurance Levels

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.

8. Risk Evaluation

Figure 2 contains an enumeration of risks commonly used to assess the Level of Assurance required for a specific digital interaction. It should be noted that this table is meant to be illustrative in nature. It is not intended to be exhaustive, nor is it meant to be directive. Relying Parties must evaluate the potential risks and harms they are likely to face, and assess the levels of risk they are willing to accept for a specific transaction within their operational context. As such, some of the illustrative criteria uses terminology that is subject to interpretation (e.g., “high”, “medium”, “low”). This enables practitioners to establish a risk profile that is commensurate with their ministry, department, or type of business. For example, a large financial institution may consider the risk of losing $100,000 as “limited” or “low” whereas a risk of that size may be “severe” or “high” for a small business, startup, or individual.

Since the risk levels are a function of a Relying Party’s unique circumstances and any policy, legislation, and/or regulation they are subject to, it is incumbent upon the Relying Party to explicitly document their risk tolerance. This will ensure that risk controls are consistently implemented and that they are neither too lenient, nor too stringent regardless of the persons who implement them. It will also ensure the controls are fairly assessed when audited. These Risks should also be documented so they are evident to, and clearly understandable by, Entities with whom they interact.

The Relying Party must also consider the trustworthiness of the Entities involved in a transaction and its Verification when assessing the trustworthiness of a transaction, Relationship, or Attribute as documented in the Verified Person, Verified Organization, and Authentication components of the PCTF.

Impact Category	**Assurance Level Required**			
	CAL1	**CAL2**	**CAL3**	**CAL4**
Inconvenience, distress, damage to standing or reputation	At worst, limited, short-term inconvenience, distress, embarrassment or damage to the standing or reputation of any party	At worst, serious short-term or limited long-term inconvenience, distress or damage to the standing or reputation of any party	Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with severe effects or which affect many individuals)	A severe and permanent inconvenience, distress or damage to the standing or reputation of any party

Financial loss	At worst, an insignificant or inconsequential financial loss to any party, or at worst an inconsequential liability	At worst, a serious financial loss to any party, or a serious liability	A severe financial loss to any party, or a severe liability	A catastrophic financial loss to any party, or a catastrophic liability
Harm to a program or public interest	At worst, a limited adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness; minor damage to organizational assets or public interests)	At worst, a serious adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; significant damage to organizational assets or public interests)	A severe adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; major damage to organizational assets or public interests)	A catastrophic adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., catastrophic mission capability degradation or loss of to the extent and duration that the organization is unable to perform its primary functions; catastrophic damage to organizational assets or public interests)

Unauthorized release of sensitive personal or commercial information	At worst, a limited release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a loss of confidentiality with a low impact	At worst, a release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a moderate impact	A release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a serious impact	A release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a catastrophic impact
Unauthorized release of sensitive government information	A loss of confidentiality with a low impact	A limited adverse effect on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties	A serious adverse effect on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties	A catastrophic effect on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties

Civil or criminal violations	Private Sector: At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts Public Sector: Any compromise involving a legal violation is assessed at a minimum of Level 2	A civil or criminal violation th at may have minor consequences and that may be subject to enforcement efforts	A civil or criminal violatio n that may have serious consequences t hat are of importance to enforcement programs	A violation that may have exceptionally grave consequences that are of special importance to enforcement programs
Personal health and safety	Private Sector: At worst, minor injury not requiring medical treatment Public Sector: Any compromise health and safety is assessed at minimum of Level 2	Private Sector: At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment Public Sector: A minor personal injury not requiring medical attention	Private Sector: At worst, a low risk of serious injury or death Public Sector: A personal injury requiring medical attention	Risk of serious personal injury or death
National interest	(Any compromise involving the national interest is assessed at a minimum of Level 2)	A disadvantage to the national interest	An injury to the national interest	A serious or exceptionally grave injury to the national interest

Figure 7: Risk Evaluation Table

8.1 Evaluation of Risk Level

The risks above should be evaluated as follows:

Assurance Level Required	Criteria
Level 1 (CAL1)	One or more risks are evaluated to be at level 1 and no risk is evaluated to be greater than level 1
Level 2 (CAL2)	One or more risks are evaluated to be at level 2 and no risk is evaluated to be greater than level 2
Level 3 (CAL3)	One or more risks are evaluated to be at level 3 and no risk is evaluated to be greater than level 3
Level 4 (CAL4)	One or more risks are evaluated to be at level 4

Figure 8: Risk Level Evaluation

8.2 Credential Risks

Credentials provide the foundation for trust in a digital ecosystem. In addition to any Privacy Impact Assessments an Entity might perform, it is important that Organizations participating in a trust ecosystem understand the risks to the Credentials they create, possess, and/or consume and take appropriate action to protect their integrity. Figure 4 contains an illustrative table of risks to Credentials and examples of mitigation strategies.

Activity	Threat	Example	Example Mitigation Strategy
Credential Storage	Disclosure	Usernames and passwords, stored in a system file, are revealed.	Use access-control mechanisms that protect against unauthorized disclosure of credentials held in storage. Protect username/password databases using secure salting and hashing functions, or approved encryption techniques to make recovery of passwords from a leaked password file impractical.

	Tampering	The file that maps usernames to passwords within a CSP is hacked, the mappings are modified, and existing passwords are replaced by passwords known to a threat actor.	Use access-control mechanisms that protect against unauthorized tampering with credentials and tokens.
Credential Verification Services	Disclosure	A threat actor is able to view requests and responses between a CSP and a Verifier.	Use a communication protocol that offers confidentiality protection.
	Tampering	A threat actor is able to masquerade as a CSP and provide false responses to a Verifier's password verification requests.	Ensure that Verifiers authenticate CSPs prior to accepting a verification response from a CSP. Use a communication protocol that offers integrity protection.
	Unavailability	The password file or CSP is unavailable to provide password and username mappings.	Ensure that CSPs have a well-developed and tested contingency plan.
		Public key certificates for Claimants are unavailable to Verifiers because the directory systems are down (e.g., maintenance or as a result of a denial-of-service attempt).	

Credential issuance/renewal/re-issuance	Disclosure	Password renewed by a CSP for a Subscriber is copied by a threat actor as it is transported from the CSP to the Subscriber.	Use a communication protocol that provides confidentiality protection of session data.
	Tampering	New password created by a Subscriber is modified by a threat actor as it is being submitted to a CSP to replace an expired password.	Use a communication protocol that allows a Subscriber to authenticate the CSP prior to engaging in token re-issuance activities and protect the integrity of the data passed.
	Unauthorized Issuance	A CSP is compromised through unauthorized physical or logical access resulting in issuance of fraudulent credentials.	Implement physical and logical access controls to prevent compromise of the CSP.
	Unauthorized renewal/re-issuance	A threat actor fools a CSP into re-issuing a credential for a current Subscriber. The new credential binds the current Subscriber's identity with a token provided by the threat actor.	Establish a policy that requires a Subscriber to prove possession of the original token in order to successfully negotiate the re-issuance process. Any attempt to negotiate the re-issuance process, using an expired or revoked token, should fail.
		A threat actor is able to take advantage of a weak credential renewal protocol to extend the credential validity period for a current Subscriber.	

Token and credential revocation/destruction	Delayed revocation/ destruction of credentials	Out-of-date certificate revocation lists allow accounts, which should have been locked as a result of credential revocation, to be used by a threat actor.	Revoke/Destroy credentials as soon as notification is received that the credentials should be revoked or destroyed.
		User accounts are not deleted when employees leave a company leading to a possible use of those accounts by unauthorized persons.	
		A hardware token is used after the corresponding credential was revoked or expired.	Destroy or zeroise tokens after their corresponding credentials have been revoked.

Figure 9: Credential Risks

8.3 Credential Management

How Credentials are managed will have a direct impact on their trustworthiness. Figure 5 contains an illustrative table of requirements for the management of Credentials and how that might impact their trustworthiness. As mentioned during this document's earlier discussion of risks, Relying Parties must assess the level of risk they are willing to accept and adjust their own risk parameters accordingly. As was also stated, it is important that those levels be deliberately set and recorded to ensure consistency in their implementation and assessment. Relying Parties are also reminded that legislation and regulation should also be considered as they may impact specific aspects of Credential management such as Credential retention requirements.

Level	**Requirements**				
	Credential Storage	**Token and Credential Verification Services**	**Token and Credential Renewal / Re-issuance**	**Token and Credential Revocation and Destruction**	**Records Retention Requirements**

CAL1	Files of shared secrets used by Verifiers must be protected by access controls to limit access to administrators and authorized personnel or applications. Files of shared secrets must not be stored in plain text. One-way hashing, or a similar function, must be used before storage.	Long term token secrets should not be shared with other parties, unless absolutely necessary.	No requirements.	No requirements.	No requirements.
CAL2	Files of shared secrets used by Verifiers must be protected by access controls to limit access to administrators and authorized personnel or applications. Such shared secret files must not contain the plaintext passwords or secrets; two alternative methods may be used to protect the shared secret: 1. Passwords may be concatenated to a variable salt (i.e., variable across a group of passwords that are stored together) and then hashed	Long-term shared authentication secrets, if used, must never be revealed to any other party except Verifiers operated by CSPs. However, session (i.e., temporary) shared secrets may be provided by CSPs to independent Verifiers. Cryptographic protections are required for all messages, between a CSP and a Verifier, which contain	CSPs must establish suitable policies for renewal and re-issuance of tokens and credentials. Proof-of-possession of unexpired current tokens must be demonstrated by a Claimant prior to a CSP allowing renewal and re-issuance. Passwords must not be renewed; they should be re-issued. After expiry of current token, and any grace period, renewal and re-issuance must not be allowed. Upon re-issuance, token secrets must not be set to a	CSPs must revoke or destroy credentials and tokens within 72 hours after being notified that a credential is no longer valid, or a token is compromised, to ensure that a Claimant using the token cannot successfully be authenticated. If a CSP issues credentials that expire automatically within 72 hours, (e.g., issues fresh certificates with a 24-hour	A record of the registration, history, and status of each token and credential (including revocation) must be maintained by CSPs or a CSP's representative. The record retention period of data for Level 2 credentials is seven years and six months beyond the expiration or revocation of the credential, whichever is later.

	with an approved algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. The hashed passwords are then stored in the password file. The variable salt may be composed using a global salt (common to a group of passwords) and the username, (unique per password), or some other technique to ensure uniqueness of the salt within the group of passwords. 2. Shared secrets may be encrypted and stored using approved encryption algorithms and modes.	private credentials or assert the validity of weakly - bound or potentially revoked credentials. Private credentials should only be sent to an authenticated party to ensure confidentiality and tamper protection, through a protected session.	default or reused in any manner. All interactions should occur over a protected session such as SSL/TLS.	validity period each day), then the CSP is not required to provide an explicit mechanism to revoke the credentials. CSPs that register passwords should ensure that the revocation or de-registration of the password can be accomplished in no more than 72 hours.	

	The needed secret can be decrypted only when immediately required for authentication. In addition, any method allowed to protect shared secrets at Level 3 or 4 may be used at Level 2.				
CAL3	Files of shared secrets used by Verifiers should be protected by access controls to limit access to administrators and authorized personnel or applications. Files containing shared secrets must be encrypted. The minimum requirements for the encryption are: 1. The encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4	CSPs must provide a secure mechanism to allow Verifiers or RPs to ensure credentials are valid. Such mechanisms may include on-line validation servers or the involvement of CSP servers that have access to status records in authentication transactions. Temporary - session authentication keys may be generated from long-term shared secret keys	Renewal and re-issuance should only occur prior to expiration of the current credential. Claimants should authenticate to CSPs using the existing token and credential in order to renew or re-issue the credential. All interactions should occur over a protected session such as SSL/TLS.	CSPs should have a procedure to revoke credentials and tokens within 24 hours. Verifiers must ensure that the tokens they rely upon are either freshly issued (within 24 hours) or still valid. Shared secret based authentication systems may simply remove revoked Subscribers from the verification database.	No additional requirements over Level 2.

	cryptographic module and decrypted only as immediately required for an authentication operation. 2. Shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic modules and is not exported in plaintext from the module.	by CSPs, and distributed to third-party Verifiers, as a part of the verification services offered by CSPs. However, long-term shared secrets should not be shared with any third parties, including third party Verifiers.			
CAL4	No additional requirements over Level 3.	No additional requirements over Level 3.	Sensitive data transfers must be cryptographically authenticated using keys bound to the authentication process. All temporary or short-term keys derived during the original authentication operation must expire, and re authentication must be required after not more	CSPs must have a procedure to revoke credentials within 24 hours of authentication. Verifiers or RPs must ensure that the credentials they rely upon are either freshly issued (within 24 hours) or still valid.	All stipulations from Levels 2 and 3 apply. The minimum record retention period for Level-4 credential data is ten years and six months beyond the expiration or revocation of the credential.

			than 24 hours from the initial authentication.		

Figure 10: Credential Management

9. Conformance Criteria

Conformance Criteria are categorized by trust element. For ease of reference, a specific conformance criterion may be referred to by its category and reference number. Example: “RABS1” refers to “Baseline Conformance Criteria reference No. 1”.

Notes:

- Baseline Conformance Criteria are also included as part of this conformance profile.
- Conformance Criteria specified in other PCTF components of may also be applicable to the PCTF Credentials (Relationships & Attributes) Component under certain circumstances.

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
RABS	**These Baseline Criteria Apply to <u>All</u> Relationships and Attributes Processes**				
1	These 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.	X	X	X	X
RDEF	**Define Relationship**				
1	The Issuer **SHOULD NOT** include information about a specific instance of the type of Relationship being defined.	X	X	X	X
2	The Issuer **SHOULD** include information that clearly identifies the Defining Party.	X	X		
3	The Issuer **MUST** include information that clearly identifies the Defining Party.			X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
4	The Issuer **SHOULD** indicate the authority under which the Relationship can be Disclaimed. (e.g., a marriage certificate might only be legitimately disclaimed by an appropriate Authoritative Source such as a court or state agency; membership in a community association might be legitimately self-disclaimed or disclaimed by the association's executive)	X			
5	The Issuer **MUST** indicate authority under which the Relationship can be Disclaimed. (e.g., a marriage certificate might only be legitimately disclaimed by an appropriate Authoritative Source such as a court or state agency; membership in a community association might be legitimately self-disclaimed or disclaimed by the association's executive)		X	X	X
6	The Issuer **SHOULD** declare whether the type of Relationship being described must be Endorsed in order to be considered trustworthy (see the Endorse Relationship Trusted Process in the Overview and the criteria listed under REND for Endorsement details).	X			
7	The Issuer **MUST** declare whether the type of Relationship being described must be Endorsed in order to be considered trustworthy (see the Endorse Relationship Trusted Process in the Overview and the criteria listed under REND for Endorsement details).		X	X	X
8	Whenever possible, and as appropriate, the Issuer **MAY** use relevant legal definitions, industry standard definitions, or references to relevant schemas.	X			
9	Whenever possible, and as appropriate, the Issuer **SHOULD** use relevant legal definitions, industry standard definitions, or references to relevant schemas.		X	X	X
RDEC	**Declare Relationship**				

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
1	The Issuer **MAY** use a Relationship Definition as the basis for the Declared Relationship and reference it within the Declared Relationship.	X			
2	The Issuer **MUST** use a Relationship Definition as the basis for the Declared Relationship and reference it within the Declared Relationship.		X	X	X
3	The Issuer **MAY** provide to Participants a summary of its mandate and authority as these relate to the Relationships it declares.	X			
4	The Issuer **MUST** provide to Participants a summary of its mandate and authority as these relate to the Relationships it declares.		X	X	X
5	Where applicable, the Issuer **SHOULD** provide to Participants evidence that it meets all legal and regulatory requirements applicable to the types of Relationships it issues.	X			
6	Where applicable, the Issuer **MUST** provide to Participants evidence that it meets all legal and regulatory requirements applicable to the types of Relationships it issues.		X	X	X
7	The Issuer **MAY** provide to Participants general terms and conditions governing legitimate or prohibited use of Declared Relationships it issues. (e.g., there are cases in which a provincial health card or social insurance number should be used, and cases where is should not be used or where use is prohibited by regulation, legislation, or policy)	X			
8	The Issuer **SHOULD** provide to Participants general terms and conditions governing legitimate or prohibited use of Declared Relationships it issues. (e.g., there are cases in which a provincial health card or social insurance number should be used, and cases where is should not be used or where use is prohibited by regulation, legislation, or policy)		X	X	

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
9	The Issuer **MUST** provide specific terms and conditions governing legitimate or prohibited use of Declared Relationships it issues. (e.g., there are cases in which a provincial health card or social insurance number should be used, and cases where is should not be used or where use is prohibited by regulation, legislation, or policy)				X
10	The Issuer **MAY** provide to Participants a point of contact for information about its Relationships and associated processes.	X			
11	The Issuer **MUST** provide to Participants a point of contact for information about its Relationships and associated processes.		X	X	X
12	Where applicable, the Issuer **MUST** allow the Subject to specify the location to which the Relationship will be delivered (i.e., a local or hosted Credential Repository), unless prohibited by regulation, policy, or legislation.	X	X	X	X
13	The Issuer **MAY** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Relationship.	X			
14	The Issuer **SHOULD** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Relationship.		X		
15	The Issuer **MUST** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Relationship.			X	X
16	The Issuer **MAY** provide references to 3rd party Credentials (i.e., Credentials issued by other Entities) it used to Verify and Validate information contained in a Relationship it has issued.	X			

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
17	The Issuer **SHOULD** provide references to 3rd party Credentials (i.e., Credentials issued by other Entities) it used to Verify and Validate information contained in a Relationship it has issued.		X		
18	The Issuer **MUST** provide references to 3rd party Credentials (i.e., Credentials issued by other Entities) it used to Verify and Validate information contained in a Relationship it has issued.			X	X
19	Information contained in a Relationship **MUST** be consistent with information held in the Issuer's records.	X	X	X	X
20	The Issuer **SHOULD** provide information indicating the Issuer's confidence in the accuracy of the information contained in the Relationship when the Relationship was issued. This would normally be done by communicating the CAL associated with the Credential, though could include additional information or caveats.		X	X	X
21	The Issuer **SHOULD** provide information indicating the Issuer's confidence in the Subject's Identity or that of the Entity acting on behalf of the Subject when the Declared Relationship was issued. This would normally be done by communicating the CAL associated with the Credential, though could include additional information or caveats.	X	X		
22	The Issuer **MUST** provide information indicating the Issuer's confidence in the Subject's Identity or that of the person acting on behalf of the Subject when the Relationship was issued. This would normally be done by communicating the CAL associated with the Credential, though could include additional information or caveats.			X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
23	The Issuer or **MAY** provide the ability to demonstrate that a Declared Relationship originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Declared Relationship.	X			
24	The Issuer or **SHOULD** provide the ability to demonstrate that a Declared Relationship originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Declared Relationship.		X		
25	The Issuer or **MUST** provide the ability to demonstrate that a Declared Relationship originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Declared Relationship.			X	X
26	A Declared Relationship Credential **MUST** include information identifying its Issuer.		X	X	X
27	The Issuer **MUST** include the date the Relationship was issued, unambiguously labeled as such.		X	X	X
28	The Issuer **MAY** provide an expiry date for all Relationships it declares, or indicate the Relationship does not have an expiry date.	X			
29	The Issuer **MUST** provide an expiry date for all Relationships it declares, or indicate the Relationship does not have an expiry date.		X	X	X
30	When declaring a Relationship, the Issuer **MAY** indicate it is wholly or partly under dispute. When that is done, the Issuer **SHOULD** include a reference to other Declared Relationships that contain disputed information and/or which are under review.	X	X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
31	The Issuer **SHOULD** provide to Participants general terms and conditions under which Relationships it declares will be rendered unusable or unreliable.	X			
32	The Issuer **MUST** provide to Participants general terms and conditions under which Relationships it declares will be rendered unusable or unreliable.		X	X	X
33	The Holder **MUST** ensure that the Repository in which they store a Declared Relationship is adequately secure, legitimately sourced, and located in a jurisdiction as required by legislation, policy, and/or regulation.		X	X	X
REND	**Endorse Relationship**				
1	An Endorsing Party **MAY** be an Authoritative Source that is a Verified Person or Verified Organization.	X			
2	An Endorsing Party **MAY** be an Authoritative Source that is a Verified Person or Verified Organization.		X		
3	An Endorsing Party **MUST** be an Authoritative Source that is a Verified Person or Verified Organization.			X	X
RVAL	**Validate Relationship**				
1	Verifiers **SHOULD** provide sufficient information to the Relying Party to enable the Relying Party to properly evaluate the Level of Assurance that can be associated with each Relationship.	X	X		
2	Verifiers **MUST** provide sufficient information to the Relying Party to enable the Relying Party to properly evaluate the Level of Assurance that can be associated with each Relationship.			X	X
3	Verifiers **MAY** confirm the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.	X			

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
4	Verifiers **SHOULD** confirm the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.		X		
5	Verifiers **MUST** confirm the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.			X	X
6	Verifiers **MAY** inform the Relying Party whether the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.	X			
7	Verifiers **SHOULD** inform the Relying Party whether the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.		X		
8	Verifiers **MUST** inform the Relying Party whether the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.			X	X
9	The Endorsing Party or Declaring Party **MAY** be a Verified Person or a Verified Organization.	X			
10	The Endorsing Party or Declaring Party **SHOULD** be a Verified Person or a Verified Organization.		X		
11	The Endorsing Party or Declaring Party **MUST** be a Verified Person or a Verified Organization.			X	X
12	The Verifier **SHOULD** be a Verified Person or a Verified Organization.	X			
13	The Verifier **MUST** be a Verified Person or a Verified Organization.		X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
14	The Verifier **SHOULD NOT** retain copies of the Presentations or Verified Presentations they Verify, nor any data therein, nor data derived from the data therein unless required to do so by regulation, policy, or legislation.	X	X	X	X
15	Verifiers **MUST NOT** 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 authorized or required to do so by regulation, policy, or legislation.	X	X	X	X
16	Relationships included in a Presentation or Verifiable Presentation that is submitted to a Verifier **SHOULD** be in the form of a Declared Relationship, Endorsed Relationship, or Validated Relationship.	X	X	X	X
RDIS	**Disclaim Relationship**				
1	The Disclaiming Party **MUST** Disclaim, or otherwise render unusable or unreliable, a Relationship if it detects indications of a compromised or invalid Relationship.	X	X	X	X
2	The Disclaiming Party **MUST** make available to Participants the status of all Disclaimed, or otherwise unusable or unreliable Relationships it has issued.	X	X	X	X
3	The Disclaiming Party **MUST** capture the following details about Relationships the Issuer has rendered unusable or unreliable: Date the action was taken; reason for the action; general indication of who initiated the action (e.g., Subject or Issuer).	X	X	X	X
4	The Disclaiming Party **MUST** only disclose details captured about unusable or unreliable Relationships to known Participants with a reasonable need for the information, and within the bounds of applicable regulations, policy, or legislation.	X	X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
5	The Disclaiming Party **MUST** disclose the reason for Disclaiming the Relationship to the Subject(s).	X	X	X	X
6	The Disclaiming Party **MUST NOT** arbitrarily Disclaim Relationships. Disclaimed Relationships should be the result of relevant policies, procedures, legislation, regulation or confirmed or suspected nefarious activities, such as fraud, that would indicate undue risk should the Relationship be accepted.	X	X	X	X
7	The Endorsing Party **SHOULD** provide Subjects the ability to initiate a process to Disclaim, or otherwise render unusable or unreliable a Relationship when the Subject detects indications of a compromised or invalid Relationship.	X	X	X	X
ADEF	**Define Attribute**				
1	The Issuer **SHOULD NOT** include information about a specific instance of the type Attribute being defined.	X	X	X	X
2	The Issuer **SHOULD** include information that clearly identifies the Issuer.	X	X		
3	The Issuer **MUST** include information that clearly identifies the Issuer.			X	X
4	Whenever possible, and as appropriate, the Issuer **MAY** use relevant legal definitions, industry standard definitions, or references to relevant schemas.	X	X		
5	Whenever possible, and as appropriate, the Issuer **SHOULD** use relevant legal definitions, industry standard definitions, or references to relevant schemas.			X	X
ABND	**Bind Attribute**				
1	The Issuer **MAY** use an Attribute Definition as the basis for the Bound Attribute and reference it within the Bound Attribute.	X			

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
2	The Issuer **MUST** use an Attribute Definition as the basis for the Bound Attribute and reference it within the Bound Attribute.		X	X	X
3	The Issuer **MAY** provide to Participants a summary of its mandate and authority as these relate to the Attributes it issues.	X			
4	The Issuer **MUST** provide to Participants a summary of its mandate and authority as these relate to the Attributes it issues.		X	X	X
5	The Issuer **SHOULD** provide to Participants evidence that it meets all legal and regulatory requirements applicable to the types of Attributes it issues.	X			
6	The Issuer **MUST** provide to Participants evidence that it meets all legal and regulatory requirements applicable to the types of Attributes it issues.		X	X	X
7	The Issuer **MAY** provide to Participants general terms and conditions governing issuance and use of the Attributes it issues.	X			
8	The Issuer **SHOULD** provide to Participants general terms and conditions governing issuance and use of the Attributes it issues.		X		
9	The Issuer **MUST** provide specific terms and conditions governing issuance and use of a specific Attribute it issues.			X	X
10	The Issuer **MUST** provide Subjects requesting issuance of an Attribute with notice that providing false or misleading statements or information may result in violation of the terms or conditions governing its issuance and use.		X	X	X
11	The Issuer **MUST** confirm Subjects understand and agree with the notice that any false or misleading statements may result in violation of terms or conditions governing Credential issuance and use.		X	X	X
12	The Issuer **MAY** provide to Participants a point of contact for information about its Credentials and associated processes.	X			

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
13	The Issuer **MUST** provide to Participants a point of contact for information about its Credentials and associated processes.		X	X	X
14	Where applicable, the Issuer **MUST** allow the Subject to specify the location to which the Attribute will be delivered (i.e., a local or hosted Credential Repository), unless prohibited by regulation, policy, or legislation.	X	X	X	X
15	The Issuer **MAY** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Attribute.	X			
16	The Issuer **SHOULD** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Attribute.		X		
17	The Issuer **MUST** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Attribute.			X	X
18	The Issuer **MAY** provide references to 3rd party Credentials or Attributes (i.e., Credentials or Attributes issued by other Entities) it used to Verify and Validate information contained in an Attribute it has issued.	X			
19	The Issuer **SHOULD** provide references to 3rd party Credentials or Attributes (i.e., Credentials or Attributes issued by other Entities) it used to Verify and Validate information contained in an Attribute it has issued.		X		
20	The Issuer **MUST** provide references to 3rd party Credentials or Attributes (i.e., Credentials or Attributes issued by other Entities) it used to Verify and Validate information contained in an Attribute it has issued.			X	X
21	Information contained in a Credential **MUST** be consistent with information held in the Issuer's records.	X	X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
22	The Issuer **SHOULD** provide information indicating the Issuer's confidence in the accuracy of the information contained in the Attribute when the Attribute was issued. This would normally be done by communicating the CAL associated with the Credential, though could include additional information or caveats.		X	X	X
23	The Issuer **MUST** only issue an Attribute at the request of or with the consent of the Subject or a person eligible to act on behalf of the Subject except where permitted by policy, regulation, or legislation.	X	X	X	X
24	The Issuer **MUST** take reasonable measures to ensure Bound Attributes are issued at the request of and/or with the consent of the rightful Subject or a person authorized to act on behalf of the Subject except where permitted by policy, regulation, or legislation.	X	X	X	X
25	The Issuer **SHOULD** provide information indicating the Issuer's confidence in the Subject's Identity or that of the Entity acting on behalf of the Subject when the Bound Attribute was issued.	X	X		
26	The Issuer **MUST** provide information indicating the Issuer's confidence in the Subject's Identity or that of the Entity acting on behalf of the Subject when the Bound Attribute was issued.			X	X
27	The Issuer **MAY** provide the ability to demonstrate that an Attribute originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Bound Attribute.	X			
28	The Issuer **SHOULD** provide the ability to demonstrate that an Attribute originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Bound Attribute.		X		

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
29	The Issuer **MUST** provide the ability to demonstrate that an Attribute originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Bound Attribute.			X	X
30	A Bound Attribute **MUST** include information identifying the Issuer of that Attribute.		X	X	X
31	The Issuer **MUST** include the date the Attribute was issued, unambiguously labeled as such.		X	X	X
32	The Issuer **MAY** provide an expiry date for all Attributes it issues, or indicate the Attribute does not have an expiry date.	X			
33	The Issuer **MUST** provide an expiry date for all Attributes it issues, or indicate the Attribute does not have an expiry date.		X	X	X
34	When issuing an Attribute, the Issuer **MAY** indicate it is wholly or partly under dispute. When that is done, the Issuer **SHOULD** include a reference to other Attributes that contain disputed information and/or which are under review.	X	X	X	X
35	The Issuer **SHOULD** provide to Participants general terms and conditions under which Attributes it issues will be rendered unusable or unreliable.	X			
36	The Issuer **MUST** provide to Participants general terms and conditions under which Attributes it issues will be rendered unusable or unreliable.		X	X	X
37	The Issuer **MUST** ensure that the Repository to which they deliver an Attribute is adequately secure, legitimately sourced, and located in a jurisdiction as required by legislation, policy, and/or regulation.		X	X	X
AMNT	**Maintain Attribute**				

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
1	The Issuer **SHOULD** establish, maintain, and make known to other Participants a process for resolving disputes concerning the accuracy of information contained in Attributes it has issued.	X	X		
2	The Issuer **MUST** establish, maintain, and make known to other Participants a process for resolving disputes concerning the accuracy of information contained in Attributes it has issued.			X	X
3	The Issuer **MUST** make available to the Subject the reason for the update of any Attribute.	X	X	X	X
4	The Issuer **MUST** inform the Subject(s) of any changes it makes to an Attribute.	X	X	X	X
5	The Revocation Authority **MUST** revoke, update, or otherwise render unusable or unreliable an Attribute if it detects indications of a compromised or invalid Attribute.	X	X	X	X
6	The Issuer **MUST** capture the following details about Attributes the Issuer has updated: Date the action was taken; reason for the action; general indication of who initiated the action (e.g., Subject or Issuer).	X	X	X	X
7	Participants **MUST** only disclose details captured about unusable or unreliable Attributes to other known Participants with a reasonable need for the information.	X	X	X	X
8	The Issuer **MUST NOT** arbitrarily change Attributes. Changes should be the result of relevant policies, procedures, legislation, regulation or confirmed or suspected nefarious activities, such as fraud, that would indicate undue risk should the Attribute be accepted.	X	X	X	X
9	The Issuer **SHOULD** provide Subjects the ability to initiate a process to revoke, update, or otherwise render unusable or unreliable an Attribute they issued to that Subject when the Subject detects indications of a compromised or invalid Attribute.	X	X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
AREV	**Revoke Attribute**				
1	The Revocation Authority **MUST** initiate a process to revoke, update, or otherwise render unusable or unreliable an Attribute if it detects indications of a compromised or invalid Attribute.	X	X	X	X
2	The Revocation Authority **MUST** make the status of all revoked, or otherwise unusable or unreliable Attributes it has issued (e.g., if an Attribute is a “Revoked Attribute") available to Participants with a reasonable need for the information.	X	X	X	X
3	The Revocation Authority **MUST** capture the following details about Attributes the Issuer has rendered unusable or unreliable: Date the action was taken; reason for the action; general indication of who initiated the action (e.g., Subject or Issuer).	X	X	X	X
4	The Revocation Authority **MUST** only disclose details captured about unusable or unreliable Attributes to known Participants with a reasonable need for the information.	X	X	X	X
5	The Revocation Authority **MUST** make the reason for revocation available to the Subject.	X	X	X	X
6	The Revocation Authority **MUST NOT** arbitrarily revoke Attributes. Revocation should be the result of relevant policies, procedures, legislation, regulation or confirmed or suspected nefarious activities, such as fraud, that would indicate undue risk should the Attribute be accepted.	X	X	X	X
7	The Revocation Authority **SHOULD** provide Subjects the ability to initiate a process to revoke, update, or otherwise render unusable or unreliable an Attribute issued to that Subject by that Issuer when the Subject detects indications of a compromised or invalid Attribute.	X	X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
8	The Revoking Authority **SHOULD** establish, maintain, and make known to other Participants a process for resolving disputes concerning the accuracy of information contained in Attributes it has revoked.	X	X		
9	The Revoking Authority **MUST** establish, maintain, and make known to other Participants a process for resolving disputes concerning the accuracy of information contained in Attributes it has revoked.			X	X

10. 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/>

11. Revision History

Version	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	Approved as Final Recommendation V1.0 through DIACC Sustaining Member Ballot