PCTF Credentials (Relationships & Attributes) Component Overview Draft Recommendation V1.0

This Draft Recommendation has been developed by the Digital ID & Authentication Council of Canada (DIACC) Trust Framework Expert Committee (TFEC). The TFEC operates under the controlling policies of the DIACC. Comments submitted by the public are subject to the DIACC Contributor Agreement.

DIACC expects to modify and improve this Draft Recommendation based upon public comments. The purpose of the open commentary is to ensure transparency in development and diversity of truly Pan-Canadian input. Comments made during the review will be considered for incorporation to the next draft. DIACC will prepare a disposition of comments to provide transparency with regard to how each comment was handled.

Forthcoming PCTF releases will expand, clarify, and refine the content of this document.

While reviewing this draft, please consider the following. Responses to these questions are non-binding and serve to improve the Pan-Canadian Trust Framework.

1. The purpose of this component is to describe processes related to attributes and relationships. Is that sufficiently clear throughout the document?
2. Is the title of this component sufficiently reflective of its contents?
3. Are the attributes and relationships processes clearly explained?
4. Is the distinction between the Define Attribute process, which describes a type or class of Attribute, and the Bind Attribute process, which describes the creation of an instance of an Attribute, sufficiently clear?
5. Is the distinction between the Define Relationship process, which describes a type or class of Relationship, and the Declare Relationship process, which describes the creation of an instance of a Relationship, sufficiently clear?

Table of Contents

1 Introduction to the Credentials (Relationships & Attributes) Component

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

Each PCTF component is described in two documents:

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

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

1.1 Context

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

Digital Identity Ecosystem Participants regularly need to be certain not only of the identify other unique Entities, but also of other details that describe that unique Entity. This information about an Entity (sometimes referred to as "attributes", "properties" or "claims") and the credentials that help convey this information 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. 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 trusting information 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

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) and an Issuer
- Contain or provide information about the relationship between two Entities (e.g., digital proof that a person is an employee of a business)
- Are issued by an Issuer to a Subject that is not the Issuer
- Contain information one Entity provides about or to another Entity
- Describes relationships between one or more Subjects and their relationships to 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 unique, real, and identifiable Entities are 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 Component and the PCTF Verified Organization components.

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

- 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)

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.

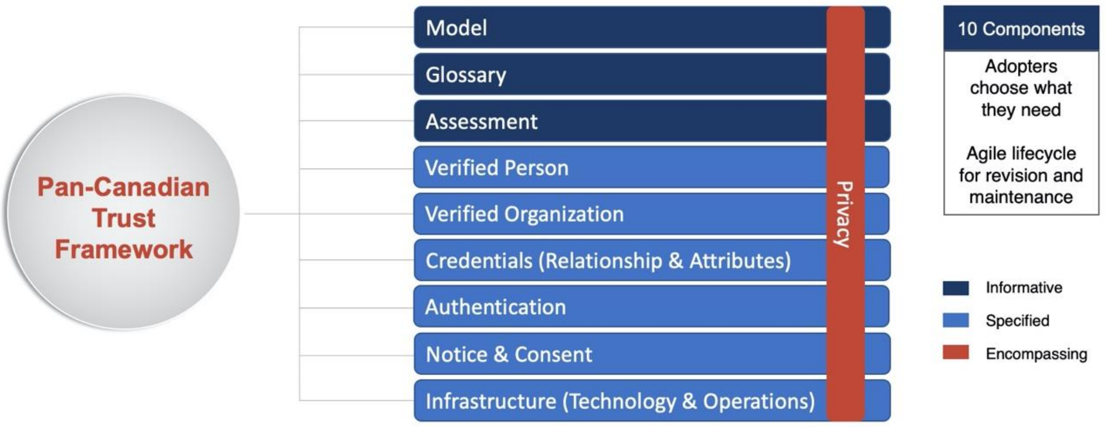
Pan-Canadian Trust Framework
Model
Glossary
Assessment
Verified Person
Verified Organization
Credentials (Relationship & Attributes)
Authentication
Notice & Consent
Infrastructure (Technology & Operations)
Privacy
10 Components
Adopters choose what they need
Agile lifecycle for revision and maintenance
Informative
Specified
Encompassing

Figure 1. Components of the draft Pan-Canadian Trust Framework

2 Credentials 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.

Claim

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 (e.g., that the Subject is licensed to drive, that the Subject resides at a specified address, or that a subject has a specific certification). A Verifiable Credential is a tamper-evident credential for whom the Issuer can be verified cryptographically. In this document the term “credentials” does not include authentication credentials unless the term “authentication credentials” is used explicitly.

Credential Verification

The evaluation of whether a Verifiable Credential or Verifiable Presentation authentically and accurately represents the Issuer or Presenter. This includes verification 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 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). 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, a Claim may consist of an attribute such as "Over21" which contains a "True" or "False" value that indicates whether the Subject is greater than twenty-one years of age, as opposed to the Subject's actual birth date or age. Use of Derived Predicates in this way better protects a Subject's privacy by not releasing detailed personally identifiable information while enabling a Verifier to validate a Subject's their eligibility for a service.

Digital Wallet / Verifiable Credential Wallet

A software-based system (application) 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.)

Presentation

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 Definition

A Relationship Definition is a Credential that describes a specific *type* of relationship that may exist between two or more Subjects, or class of relationship. 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 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 tamper-evident Credential that is encoded in a way that enables the authorship (i.e., source) to be trusted following cryptographic verification. Verifiable Credentials must be cryptographically secure, privacy respecting, and machine verifiable.

Verified Credential

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

Verifiable Presentation

A tamper-evident Presentation that is encoded in a way that enables the authorship (i.e., source) to be trusted following cryptographic verification. Verifiable Presentations must be cryptographically secure, privacy respecting, and machine verifiable.

Verifiable Relationship

A tamper-evident Endorsed Relationship that is encoded in a way that enables the authorship (i.e., source) to be trusted following cryptographic verification. Verifiable Relationships must be cryptographically secure, privacy respecting, and machine verifiable.

Zero-Knowledge Proof

A zero-knowledge proof is a method that enables an entity to prove to another entity that they know a specific value without disclosing that value. For example, an entity might prove that a Subject is over 21 years of age by using information derived from the Subject's driver's license without revealing any of the personally identifiable information contained in the driver's license Credential (e.g., birth date). Zero-knowledge proofs are normally supplied to a Relying Party in the form of a Derived Predicate. The Derived Predicate can either be created by an Issuer when a Credential or Verifiable Credential is issued, or by a Verifier.

2.2 Abbreviations

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

- PCTF – Pan-Canadian Trust Framework

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.
- Role definitions do not imply or require a specific solution, architecture, implementation, or business model.

Declaring Party

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

Any entity that creates a Relationship Definition using the Define Relationship process (see Trusted Processes below).

Disclaiming Party

An Entity with exclusive or primary responsibility for disclaiming Relationships 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

A Subject or third party that asserts their belief that a Declared Relationship is valid via the Endorse Relationship process. An Endorsed Relationship may be endorsed by more than one Endorsing Party.

Holder

An Entity that possesses one or more Credentials. The Holder is usually the Subject of the Credential but need not be so. Holders may store Credentials they possess in a Repository.

Issuer

An Entity that makes information about a Subject available by creating and issuing a Credential or Verifiable Credential.

Relying Party

An Organization or Person who consumes digital Identity Information, Attributes, Relationships, or other Credentials to conduct digital transactions.

Revocation Authority

An 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.

Service Operator

An Entity with primary responsibility for ensuring underlying services operate as expected.

Subject

A Person, Organization, or Machine that holds or is in the process of obtaining a digital representation in the Digital Identity Ecosystem system regulated by the PCTF, and that can be subject to legislation, policy and regulations within a context.

Verifier

An entity that receives one or more Verifiable Credentials and evaluates whether the credentials authentically and accurately represent the Issuer or Presenter. (See Credential Verification.)

3 Trust Relationships

The authenticity, validity, and security of the Participants 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 and auditability 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.

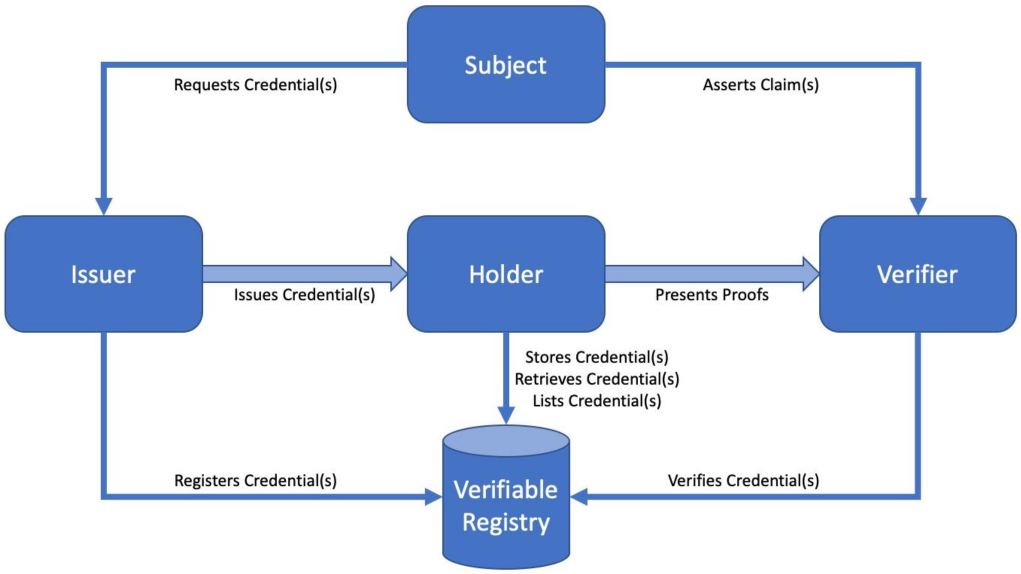

Figure 2. Credentials (Relationships & Attributes) Roles and Relationships (Illustrative)

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

The PCTF Credentials (Relationships & Attributes) Component defines 5 key areas for establishing trust in these relationships and which affect a Credential's trustworthiness:

1. Participants must trust the authority and reliability of Issuers, and that Issuers are thorough in establishing the accuracy of information included in a Credential.
2. Participants must trust that Issuers issue Credentials with the consent of the Subjects or an entity eligible to act on behalf of the subject.
3. Participants must trust that issued Credentials contain accurate reliable, and up-to-date information.
4. Participants must trust that compromised or invalid Credentials are processed in an appropriate and timely manner, and that Credentials are only rendered unusable under legitimate circumstances.
5. Participants must trust that information they share with other Participants, or that is stored in Repositories or Verifiable Registries, is not used by the Service Provider or Verifier except as directed by the express consent of the Subject or an entity authorized to act on their behalf. 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 attribute to them. 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 as used throughout the PCTF. Credential assurance involves the process of binding a credential to a unique individual. When a credential is authenticated, this process provides the party relying upon the validity of the credential the assurance that that it is the individual who is presenting the credential is same individual who originally received it.

Level of Assurance	Qualification Description
Level 1 (CAL1)	• Little confidence required that an individual has maintained control over a credential that has been entrusted to them and that the credential has not been compromised • Satisfies Level 1 Conformance Criteria
Level 2 (CAL2)	• Some confidence required that an individual has maintained control over a credential that has been entrusted to them and that the credential has not been compromised • Satisfies Level 2 Conformance Criteria
Level 3 (CAL3)	• High confidence required that an individual has maintained control over a credential that has been entrusted to them and that the credential has not been compromised • Satisfies Level 3 Conformance Criteria
Level 4 (CAL4) Optional	• Very high confidence required that an individual has maintained control over a credential that has been entrusted to them and that the credential has not been compromised • Satisfies Level 4 Conformance Criteria

Figure 3. Credentials Assurance Levels

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

It is important to note that, in order to achieve a specific credentials assurance level, a Credential must meet each applicable conformance criterion to a minimum of the standard associated with that level. That is, the maximum credentials assurance level that can be assigned to a specific Credential will the the lowest level it achieves for any of the criterion in the Conformance Profile. For example, if a Credential met the standard for CAL4 on 9 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 Verify Relationship process to transform an "Endorsed Relationship" input condition to an "Verified 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. Verify 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.

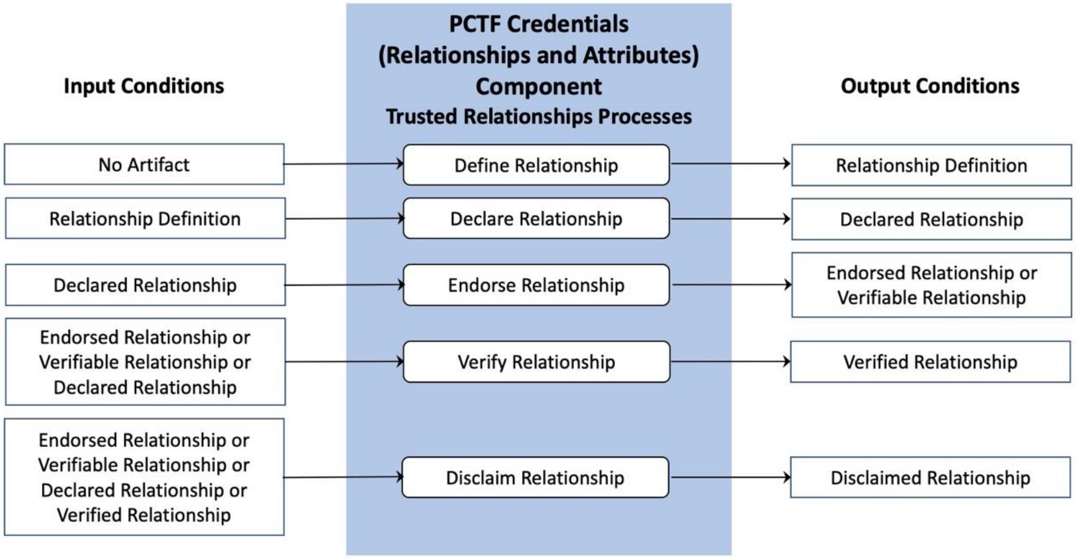

Figure 4. Relationships Conceptual Overview

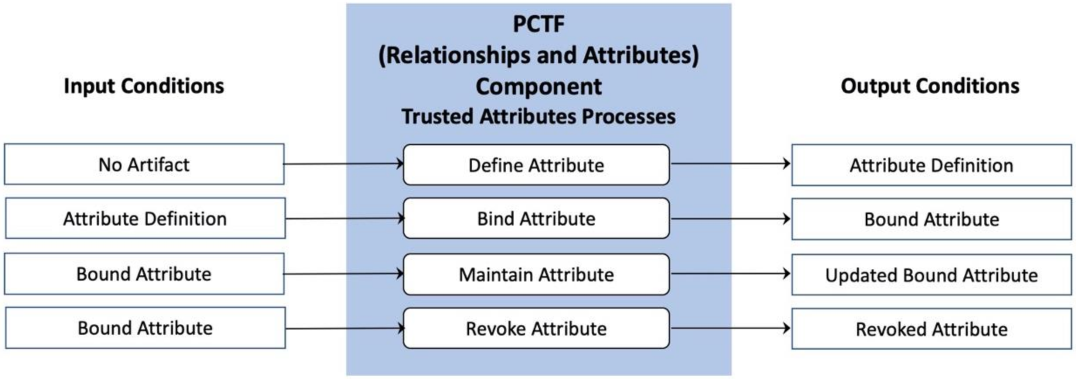

Figure 5. Attributes Conceptual Overview

5.2 Process Descriptions

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

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

1. Description – A descriptive overview of the process
2. Inputs – Data that is consumed and/or acted upon on by the trusted process
3. Outputs – Data that is created by the process
4. Dependencies – Other trusted 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 may 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). 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 its own inherent risks
- Provides guidance to Relying Parties regarding its trustworthiness
- May include relevant legal definitions, industry standard definitions of the relationships, or references to them or to relevant schemas
- May describe any evidence of trustworthiness that exists (e.g., related Verified Credentials or Verified Relationships)

Any entity may define a relationship including, though not limited to, a potential Subject of such a relationship, an Issuer, an Authoritative Party, or a Relying Party.

Inputs	
Outputs	Relationship Definition
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, 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 must be either a natural person or a juridical person, and 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. A Derived Predicate is a verifiable, Boolean assertion about a Subject based upon the value of another attribute that describes that Subject. For example, a Claim may consist of an attribute such as "Over21" which contains a "True" or "False" value that indicates whether the Subject is greater than twenty-one years of age, as opposed to the Subject's birth date or age. Use of Derived Predicates in this way 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.

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 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 Declared Relationships stored within.

Inputs	Relationship Definition
Outputs	Declared Relationship
Dependencies	Define Relationship

5.2.3 Endorse Relationship

Through the Endorse Relationship process 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. Relying Parties may take into consideration whether multiple endorsements of a relationship is an indication of its trustworthiness. Relying Parties must consider the source of the endorsement(s), and whether those sources are Verified Persons or Verified Organizations, when evaluating a relationship’s trustworthiness.

The output of the Endorse Relationship process may be an Endorsed Relationship or a Verifiable Relationship. A Verifiable Relationship is a tamper-evident Endorsed Relationship that is encoded in a way that enables the authorship (i.e.: source) to be trusted following cryptographic verification. Verifiable Relationships must be cryptographically secure, privacy respecting, and machine verifiable. While Verifiable Relationships might be generated by any entity, they are only truly meaningful when generated by a Verified Person or Verified Organization.

When an Endorsed Relationship or Verifiable Relationship has been issued, the Holder - which is often, though not always, a Subject - 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	Declared Relationship
Outputs	Endorsed Relationship or Verifiable Relationship
Dependencies	Declare Relationship

5.2.4 Verify 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) wishes to assert one or more Claims, or is requested to provide one or more Claims by a Relying Party, they present a Relationship 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 Derived Predicates. The Verifier confirms the Relationship(s) presented to be authentic by:

1. Confirming that the stats of Relationship(s) is(are) valid (e.g., not expired, suspended, or revoked)
2. Confirming that the proof of authenticity is valid, usually through cryptographic verification
3. Confirming the Relationship(s) and/or Presentation 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 Verified 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 digital ecosystem participants, or anyone other than the Relying Party or Relying Parties without the express consent of the Subject. 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, Endorsed Relationship, or Verifiable Relationship. Even a self-asserted Declared Relationship may become a Verified 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 verified by it's Authoritative Source, the Province).

Inputs	Declared Relationship, Endorsed Relationship, or Verifiable Relationship
Outputs	Verified 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 assert 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 Verifiable Relationship and the issuance of a new Verifiable 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 assert one or more of the Claims in a revoked Relationship credential, they must request a new Relationship as described in the Declare Relationships, Endorse Relationships, and/or Verify 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 *may* be acceptable proof of age to certain Relying Parties).

Inputs	Declared Relationship, Endorsed Relationship, Verifiable Relationship, or Verified Relationship
Outputs	Disclaimed Relationship
Dependencies	Declare Relationship, Endorse Relationship, or Verify 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)
- Is not sufficiently qualified by its name alone (e.g., the name “Date” would not sufficiently describe whether 01-02 is January 1st, February 2nd, January 2002, February 1901…)
- Describes the Attribute’s defining characteristics or format (e.g., a date in the form of DD-MMM-YYYY)
- 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 its own inherent risks
- Provides guidance to Relying Parties regarding its trustworthiness
- May include a disclaimer of liability
- Creates a common vocabulary and understanding amongst issuers and consumers of the attribute
- May include relevant legal definitions, industry standard definitions of the Attribute, or references to it or relevant schemas
- May describe any evidence of trustworthiness that exists (e.g., related Verified Credentials or Verified Relationships)
- May describe the authority under which the Attribute was issued

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

Inputs	
Outputs	Attribute Definition
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; Hiren’s degree is a Master of Science).

Alternatively, an Attribute may consist of a 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, rather than contain a Subject’s date of birth, an Attribute might contain the Derived Predicate "Over21", which is a "True" or "False" value that indicates whether the Subject is greater than twenty-one years of age. Use of Derived Predicates in this way 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.

The Bind Attribute process references an Attribute Definition to derive the structure 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 Party) and that can verify the Attribute accurately describes the Subject(s) (e.g., a telecom company is an Authoritative Party 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. For example, humanitarian aid organizations may want the ability to uniquely identify persons eligible for aid while respecting the individual’s right and/or desire for anonymity.

Bound Attributes should 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 an attribute itself (e.g., a residential address change, an expiration date is extended, a membership is renewed, driver's license demerit points are earned) or changes in state that affect a Derived Predicate (e.g., the Subject celebrates their twenty-first birthday and is eligible to change the "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 not be possible, desirable, or advisable to update an existing Bound Attribute. In those cases a new Bound Attribute may be issued using the Bind Attribute Processes. When a new Bound Attribute is issued, it may or may not be appropriate to revoke previously existing Bound Attributes using the Revoke Attribute process. For example, if someone was the president of a local service club for the calendar year 2019 and is not re-elected in 2020, there would be no need to revoke the Bound Attribute indicating they were president in 2019. However, if the Bound Attribute indicated they are the “current president” and they are not re-elected, it would make sense to revoke the Attribute.

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

5.2.9 Revoke Attribute

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

- A membership may expire
- The Attribute may have been bound fraudulently
- Fraud is being committed using the Attribute and a new Attribute (e.g., credit card number) must be created to limit harm to its Subject(s)
- An Attribute may have been bound to a Subject in error
- The Attribute may have been rendered invalid via a legal judgement

- An event or change in a Subject's circumstances or qualifications may necessitate the revocation of a Bound Attribute and the issuance of a new Bound Attribute (e.g., a Subject's driver's license is permanently suspended due to repeated driving while intoxicated offences)

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

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

6 References

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

Note:

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