PCTF Glossary

Document Status: Final Recommendation V1.1

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. Scope

The Pan-Canadian Trust Framework (PCTF) Glossary provides definitions and examples for terms that appear across DIACC PCTF documentation. The objective of the PCTF Glossary is to ensure all stakeholders have a shared and consistent understanding of terms used in the context of the PCTF. As terms and usage can vary across industry, the Glossary is recommended reading for anyone wanting a strong baseline understanding of the PCTF. The Glossary may also be of use in linking the various elements of PCTF documentation to each other where their use of any Terms is related.

The structure and content of the PCTF Glossary items is:

Term (Translation)

A definition statement that provides the accepted and precise meaning of the associated term in the PCTF context.

- Examples: Examples may be included to help clarify the intended meaning of a term; the examples provided are not intended to be an exhaustive list.
- Reference**:** Reference(s) may be added to indicate where the term and definition is used in other PCTF documentation.

See also: Links to similar meaning or contextually related Terms defined elsewhere in the Glossary.

Notes:

- The terms included for the current version of the Glossary are those used across the PCTF.
- Within the Glossary definitions, terms that are capitalized refer to Glossary definitions of that term, which may differ from their everyday English meaning.
- The list of Glossary terms has been kept to just the essentials.
- Terms with the same or similar meanings are collapsed to a single entry but may be expanded upon in source PCTF documentation.

- Terms used with their everyday, English dictionary meaning (e.g., stakeholders) are **not included**.

2. Conventions and Guidelines

The PCTF Glossary is a living document that will evolve as the framework is developed. The guidelines for creating definitions for the terms in the Glossary are:

1. The definition of a term should reflect the information-mapping methodology for defining concepts. The definition should clearly indicate the larger category to which the concept belongs, and the critical attributes or characteristics of that concept that distinguish it from others;
2. The meaning of the term should reflect the current usage of the term in a PCTF document; and
3. Consult existing digital identity standards or frameworks as sources for definitions, with preference being given to Canadian sources.

As a result of guidelines 1 and 2, most existing definitions could not be taken verbatim, but would need to be modified (e.g., change person to Subject) to be considered a valid definition in the context of the PCTF.

3. Terms and Definitions

Adaptive Risk (Risque adaptatif)

A dynamic measure of the risk associated with a transaction or service access based on context and behaviour.

- Example: adjust the security measures for online banking based on the user's location and recent activity, ensuring higher scrutiny for unusual access patterns
- Reference: Authentication

Adaptive Risk Authentication (Authentification du risque adaptatif)

Dynamically adjusting the specific authentication steps performed according to the Adaptive Risk.

- Example: when a banking app prompts a user for additional verification, such as a fingerprint or security question, after detecting a login attempt from a new device or unfamiliar location.
- Reference: Authentication
- See also: Adaptive Risk

Applicant (Demandeur)

An Applicant is any Entity that has requested, though not yet received, a Credential.

- Example: a Person who has requested, though not yet received, a drivers' license from a province or territory.
- Reference: Digital Wallet, Credentials, and Infrastructure
- See also: Subject

Assigned Identifier (Identifiant attribué)

Letters, numbers, symbols, or a combination thereof that a Responsible Authority allocates to an Organization and which can be used to uniquely identify the Organization within a given context, use, or system.

- Example: a unique alphanumeric code allocated by a provincial and/or federal regulatory authority to identify an organization within government digital services systems.
- Reference: Privacy and Verified Organization

Attestation (Attestation)

A trusted verification of something as true or authentic.

- Example: when an employer digitally verifies and signs a document confirming an employee's credentials, such as a professional certification, which is then used to access industry-specific systems or services.
- Reference: Digital Wallet
- See also: Claim, Attribute

Attribute (Attribut)

An Attribute is information related to a characteristic or inherent part of an Entity.

- Example: Subject's given name or residential street address.
- Reference: Digital Wallet and Credentials
- See also: Claim

Attribute Definition (Définition de l'attribut)

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.

- Example: specifying a user's residential address as a necessary attribute for verifying eligibility to access region-specific online government services, such as applying for a local driver's license.
- Reference: Credentials
- See also: Attribute

Authentication (Authentification)

The process of establishing truth or genuineness to generate an assurance that a Subject has control over an Issued Authentication Credential and that the Authentication Credential is currently valid.

- Example: when a user logs into their online banking account by entering a password and then confirming their identity through a one-time code sent to their registered mobile device.
- Reference: Authentication (Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice and Consent)

Justificatif d’authentification (obsolète) Authentication Credential (Deprecated)

A Credential used specifically for use during the Authentication process.

- Example: a security token that generates a unique, time-based code used in conjunction with a password to access a secure online account.
- Reference: Authentication, Credentials, Digital Wallet
- See Also: Authentication, Credential

Authentication Factors (Authentication Factors)

There are three Authentication Factors:

1. Something the Subject has (e.g., key card, key fob)
2. Something the Subject knows (e.g., password)
3. Something the Subject is or does (e.g., a biometric)

- Example: using a combination of something you have (a smartphone with an authentication app), something you know (a password), and something you are (a fingerprint scan) to securely access a sensitive online account.
- Reference: Authentication
- See also: Credential

Authentication Service Provider (Fournisseur de services d'authentification)

An Entity that operates a service that implements the Authentication Trusted Processes related to authentication:

1. Authentication
2. Authentication Session Initiation (optional)
3. Authentication Session Termination (optional)

- Example: Google, with their services like Google Sign-In, allowing Users to authenticate themselves across various websites and applications using their Google account credentials.
- Reference: Authentication
- See also: Identity Provider

Authenticator (Authentificateur)

Information or biometric characteristics under the control of an individual that is a specific instance of an Authenticator Type; the specific instance of the Authenticator Type that is under the control of the individual.
An Authenticator may be provided by the Subject or by a service provider. The term may also commonly refer to a physical device or application.

- Examples: private signing keys, user passwords, responses to challenge questions, or a person’s face.
- Reference: Authentication, Digital Wallet

- See also: Credential

Authenticator Binding (Liaison d’authentificateurs)

The association of one or more claims about a Subject with one or more Authenticators as part of the Credential Issuance process.

- Example: linking a user's smartphone app, which generates one-time codes, to their online banking account so that only the registered device can be used for two-factor authentication.
- Reference: Authentication
- See also: Credential Issuance

Authenticator Type (Type d’authentificateur)

A class of authenticator within a specified authentication factor.

- Example: using a biometric scanner, such as a fingerprint reader on a smartphone, as an authentication method to securely access a personal finance app.
- Reference: Authenticator
- See also: Authenticator, Authentication Factors

Authenticator Validation Data (Données de validation de l’authentificateur)

Data under the control of an Authentication Service Provider against which the Authenticator (provided by a Subject during an authentication attempt) is validated.

- Example: a server checking the time-based one-time password (TOTP) generated by a user’s authenticator app to verify that it matches the code sent to their registered email address.
- Reference: Authentication

Authoritative Party (Partie qui fait autorité)

A Role that a Participant performs to provide Identity Information or Identity Evidence at a Level of Assurance to Relying Parties.

- Examples: a bank; government department of immigration; government driver's licence program; a business registry; a telecommunications company; government-issued identity card.
- Reference: Credentials, Verified Person
- See also: Identity Provider and Disclosing Organization

Authoritative Source (Source qui fait autorité)

A collection or registry of identity records maintained by an Authoritative Party that meets the PCTF Conformance Criteria for establishing evidence of identity.

- Examples: vital statistics register; Verified Person record; business registry; bank account record.
- Reference: Credentials, Digital Wallet, Verified Organization, Verified Person

Authorized Agent (Agent autorisé)

Any Entity providing services related to Verified Organization on behalf of a Responsible Authority through a formal relationship.

- Example: a third-party service provider that handles customer verification and account management for a bank under a formal agreement with the bank’s regulatory authority.
- Reference: Verified Organization
- See also: Responsible Authority

Authorized Personnel (Personnel autorisé)

Staff of a Responsible Authority assigned to perform certain tasks. Typically, employees of or persons working under contract for the Responsible Authority.

- Example: an employee of a government agency who is specifically designated to review and process identity verification requests for access to secure government services.
- Reference: Verified Organization
- See also: Authorized Agent, Responsible Authority

Authorized Reviewer (Examinateur autorisé)

Participants impacted by a notice statement and/or consent request or approval (i.e., Disclosing Organization, Requesting Organization, and others described in this section), as well as regulatory bodies or oversight committees requiring access to a record of notice or consent for audit.

- Example: a compliance officer from a regulatory body who reviews access logs and consent records from a financial institution to ensure adherence to data protection regulations.
- Reference: Notice & Consent

Claim (Revendication)

A Claim is an assertion made about a Subject.

- Examples: the Subject is licensed to drive; the Subject is over 21 years of age; the Subject was incorporated in the Province of Ontario.
- Reference: Credentials, Digital Wallet
- See Also: Attribute

Conformance Criteria (Critères de conformité)

Requirements developed for each of the PCTF Components and used as the basis to assess compliance.

- Examples: strength of an encryption key, check expiry data on an identity document.
- Reference: Trust Registries, Infrastructure, Privacy

Consent (Consentement)

Permission, given from a User authorized to do so, to share Identity and/or Personal Information about a Subject as per the terms defined in a Notice. In the context of the PCTF, consent is equated to "Meaningful Consent" as described by the Office of the Privacy Commissioner of Canada.

Note: Some public sector organizations have the legislated authority to collect, use, disclose, update, retain, and store personal information in the execution of their functions. In these cases, public sector organizations provide notice to the person, but they do not require the person's consent. Consent requirements for each jurisdiction's legislation must be adhered to.

- Example: agreeing to share home address information to a service provider.
- Reference: Credentials, Digital Wallet, Notice & Consent, Privacy, Trust Registries
- See also: EULA

Consent Decision (Décision de consentement)

The decision by the Subject to provide consent or decline consent.

- Example: the User click's the Agree button at the end of EULA dialog or clicking 'Accept Cookies' on a website page.
- Reference: Notice & Consent, Privacy

Contextual Evidence of Identity (Preuve d’identité contextuelle)

Evidence of Identity that establishes the existence and Digital Representations of Entities within a specific context and for a specific purpose.

- Examples: bank account; health record; provincially issued driver's licence; Canadian passport; business account with a telco; better business bureau record; government-issued identity card used as evidence in the process of verifying an individual's identity.
- Reference: Verified Person
- See also: Authorized Agent, Reliable Authority

Contextual Evidence of Organizational Identity (Preuve contextuelle de l’identité organisationnelle)

Information providing evidence of Organizational Identity is usually tied to program administration or service delivery activities. Created by private sector Entities and public sector Entities. Contextual Evidence of Organizational Identity may corroborate Foundational Evidence of Organizational Identity and may include information beyond Organizational Identity Information (e.g., mailing address). This information may be used to assist in linking Organizational Identity Information across jurisdictions and services.

- Examples: CRA BN registration document, municipal business permit, a DUNS number, used as evidence in the process of verifying an Organization’s identity.
- Reference: Verified Organization

Contextual Identity Record (Dossier d’identité contextuelle)

A record that provides Contextual Evidence of Organizational Identity.

- Example: a business's tax registration document, which serves as contextual evidence of the organization's legal identity when applying for a government contract.
- Reference: Verified Organization

- See also: Contextual Evidence of Organizational Identity

Credential (Justificatif)

A data structure that uniquely binds at least one Authenticator to at least one claim about at least one Subject.

- Examples: the Subject is licensed to drive; the Subject resides at a specified address; the Subject has a specific certification.
- Reference: Authentication, Credentials, Trust Registries and Digital Wallet
- See also: Authenticator, Subject, Verifiable Credential

Credential Issuance (Délivrance des justificatifs)

A process during which a Credential is issued, describing one or more Subjects, and bound to one or more appropriate Authenticators controlled by the Holder. A Credential includes one or more identifiers which may be pseudonymous and may contain attributes verified by the Credential issuer. The Authenticators may be issued during this process, provided by the Subject or provided by a third party. The bound Authenticators will be subsequently used to prove, at a Level of Assurance, that a Credential is referring to the same Subject that was originally bound to the Authentication Credential.

- Example: when a university issues a digital diploma to a graduate, it includes the student's unique identifier and verified academic achievements, binding it to the student's authentication method for future verification.
- Reference: Authentication
- See also: Authenticator, Attributes, Credential, Subject

Credential Maintenance (Maintenance des justificatifs)

Credential Maintenance process includes life-cycle activities such as binding new Authenticators, removing Authenticators, and updating Authenticators (e.g., password change, updating security questions and answers), or updating Authentication Credential attributes.

This process is typically initiated by a User but may also be initiated by a system administrator or automatically by the system.

- Example: when a user updates their email password and security questions in an online banking account, ensuring the authentication credentials remain current and secure.
- Reference: Authentication

Credential Recovery (Récupération des justificatifs)

The Credential Recovery process provides a means to transition an Inaccessible Credential to an Issued Credential. The process may be triggered by a User, system administrator, or automatically by the system. This process is optional and may not be supported by all service providers.

- Example: when a user resets a forgotten password through an email verification process to regain access to their online government portal account.
- Reference: Authentication

Credential Revocation (Révocation des justificatifs)

The Credential Revocation process ensures that a Credential is permanently disabled or deleted. Once a Credential is revoked, it can no longer be used. The system will actively prevent further Trusted Processes from occurring in relation to this Credential. The process can be initiated by a User, system administrator, or automatically by the system.

Note that a new Credential can be issued for the same Subject. Re-issue equates to revoking a Credential and issuing a new Credential for the same Subject.

- Example: when an employee's company access card is permanently disabled by the system after their employment ends, preventing any further use of the card for building access.
- Reference: Authentication

Credential Service Provider (Fournisseur de services de justificatifs)

An Entity that operates a service that implements the Authentication Trusted Processes related to management of Credentials:

1. Credential Issuance
2. Credential Suspension (optional)
3. Credential Recovery (optional)
4. Credential Maintenance
5. Credential Revocation

- Example: an organization which manages the issuance, maintenance, and revocation of digital credentials for employees to securely access corporate systems.
- Reference: Authentication

Credential Suspension (Suspension des justificatifs)

A process that converts an Issued Credential to an Inaccessible Credential and may be initiated by User action, system administrator, or automatically by the system.

An Inaccessible Credential should not be used in the Authentication process.

- Example: when a bank temporarily disables a customer's online banking credentials after detecting suspicious activity, preventing access until the issue is resolved.
- Reference: Authentication

Credential Verification (Vérification des justificatifs)

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

- Example: when an employer verifies the authenticity of a digital diploma provided by a job applicant by checking its cryptographic signature and confirming that it hasn't been revoked or expired.
- Reference: Credentials, Digital Wallet

Cryptographic Binding (Liaison cryptographique)

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

- Example: ensuring that a user's biometric data is securely linked to their digital certificate, preventing tampering and ensuring that the biometric data matches the certified identity.
- Reference: Authentication, Digital Wallet
- See Also: Strong Binding

Declared Relationship (Relation déclarée)

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. The structure of a Declared Relationship is derived from a Relationship Definition.

Declared Relationships are created via the Declare Relationship Process

- Examples: 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.
- Reference: Credentials
- See also: Relationship Definition

Declare Relationship Process (Processus de déclaration de la relation)

An assertion by any Entity that a Relationship exists between two or more Subjects.

- Example: a university process that certifies the academic relationship between a student and their degree program.
- Reference: Credentials
- See Also: Declared Relationship

Declaring Party (Partie déclarante)

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.

- Example: a university may act as the Declaring Party by certifying the academic relationship between a student and their degree program, even though the university is not a subject of the Declared Relationship
- Reference: Credentials

Defining Party (Partie qui définit)

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

- Example: a government agency might serve as the Defining Party by creating a relationship definition that outlines the criteria for verifying an individual's eligibility for a social security benefit.
- Reference: Credentials

Derived Predicate (Prédicat dérivé)

A Derived Predicate is a Verifiable, Boolean assertion about a Subject based upon the value of another Attribute that describes that Subject. 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.

- Example: consider a Subject who wishes to prove they are eligible for services only available to people who are at least 21 years of age, and who possess a Credential which contains an Attribute that holds their date of birth. Rather than present their birth date as proof they are eligible, the Subject could present a Derived Predicate such as "Over21" which contains a "True" or "False" value that indicates whether the Subject is greater than 21 years of age.
- Reference: Credentials, Digital Wallet
- See also: Zero Knowledge Proofs

Digital Identity (Identité numérique)

A type of Digital Representation that uniquely identifies a Subject within a context, and that a User presents/uses exclusively to represent the Subject when they access online services.

Historically, has been used for the name or concept of processes involving digital credentials. Digital Trust is currently the preferred term for the overall ecosystem.

- Examples: passport chip content; BC Services Card chip; Verified Person record in a Digital Wallet.
- Reference: Authentication, Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice & Consent, Verified Organization, Verified Person.
- See also: Identity

Digital Identity Ecosystem (Écosystème de l’identité numérique)

An interconnected system for the exchange and verification of digital Identity Information, involving public and private sector Organizations that comply with a common Trust Framework for the management and use of digital identities, and the Subjects of those digital identities.

- Examples: the DIACC-endorsed Canadian Digital Identity Ecosystem; another country's Digital Identity Ecosystem; a provincial ecosystem consisting of an Identity Provider and several Relying Parties that enable a set of services for citizens, following a common provincial identity framework.
- Reference: Trust Registries, Infrastructure, Notice & Consent, Privacy (Verified Organization, Verified Person)

Digital Representation (Représentation numérique)

An electronic dataset that refers or is related to a Subject. In the context of the PCTF, there are currently three types of Digital Representations: Digital Identities, Credentials, and Authenticators.

- Examples: voice signature, QR code; a session of a logged-in user that has access to data that contains the user's name, date of birth; purchase history.
- Reference: Digital Wallet, Privacy, Verified Organization, Verified Person

Digital Wallet (Wallet, Digital Identity Wallet) (Portefeuille numérique (portefeuille, portefeuille d’identité numérique))

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.

- Example: a Digital Wallet on a smartphone may securely store a user's payment information, digital ID cards, and various credentials, allowing easy access and use for transactions and authentication.
- Reference: Credentials, Trust Registries and Digital Wallet
- See also: Repository

Digital Wallet Provider (Fournisseur de portefeuilles numériques)

An Entity that develops Digital Wallet products for use by Holders.

Digital Wallet Providers may be Issuers of Credentials to Digital Wallets to prove the authenticity of the wallet product to Issuers and Verifiers.

- Example: companies which develop Wallet apps act as Digital Wallet Providers by creating the software for securely storing and managing payment information, tickets, and other credentials.
- Reference: Trust Registries
- See also: Digital Wallet

Disclaimed Relationship (Relation démentie)

A Disclaimed Relationship is an assertion by an Issuer of an Endorsed Relationship that they believe the Endorsed Relationship is no longer valid.

Once a Relationship has been disclaimed, its Claims are no longer valid.

- Example: a membership has expired; a Relationship or one or more of its Claims has been discovered to be fraudulent.
- Reference: Credentials

Disclaiming Party (Partie qui dément)

A Disclaiming Party is any Entity with exclusive or primary responsibility for Disclaiming Relationships (via the Disclaim Relationship Trusted Process) 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.

- Example: a company that removes an employee's access credentials after discovering they were misused acts as the Disclaiming Party by officially invalidating the employee's access rights and updating the relevant records.
- Reference: Credentials

Disclosing Organization (Organisation divulgatrice)

A Role that an Organization or Person performs to hold Subject-Specific Personal Information that the User consents to disclose to a Requesting Organization, or that the Disclosing Organization can lawfully disclose under relevant legislation. In a digital identity context, this will often be an identity or attribute provider.

- Example: a health insurance company that provides a user's medical history to a bank with the user's consent, or as required by law.
- Reference: Notice & Consent, Privacy

End User License Agreement (EULA) (Contrat de licence d'utilisation (CLU))

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

- Example: when a user installs a new app and agrees to the terms outlined in the EULA, they are entering into a contract with the software producer that details how they can use the app.
- Reference: Digital Wallet

Endorsed Relationship (Relation homologuée)

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.

- Example: a university endorsement of a student's graduation status, confirming that the student's academic records are accurate and up-to-date.
- Reference: Credentials

Endorsing Party (Partie homologatrice)

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.

- Example: a university that confirms a student's enrolment status to an employer, validating the student's academic claim.
- Reference: Credentials

Entity (Entité)

Something that has a separate and distinct existence and that can be identified in a context.

- Examples: a physical person; a pet dog; a smart appliance such as a refrigerator; an automobile; a passport in paper form.
- Reference: Authentication, Credentials, Trust Registries, Verified Organization

Establish Sources (Établissement des sources)

The Establish Sources process is the preparatory activity undertaken to determine which sources of Identity Evidence can be used to validate and/or verify Identities, and the assurance of those sources. Typically, a Digital Identity system will use a range of

sources to support the requirements to validate and verify Identities in a given context, and to meet the target Levels of Assurance.

- Example: evaluating different forms of ID, like birth certificates and utility bills, to ensure they can reliably confirm a person's identity for a secure digital identity system.
- Reference: Verified Person

Event Type (Type d’événement)

A happening in the life of an Organization that may trigger one or more Verified Organization Trusted Processes. Event types include a number of happenings that are specific to Public Sector Organization Registries.

- Example: an organization's annual financial audit, which triggers the process for updating and verifying its credentials and compliance status.
- Reference: Verified Organization

Evidence of Identity (Preuve d’identité)

An information record consisting of Identity Information and Attributes maintained by an Authoritative Source that supports the integrity and accuracy of identity claims made by a Subject.

There are two categories of evidence of identity: Foundational and Contextual.

- Examples (foundational): provincial birth record; federal immigration record; certificate of incorporation.
- Examples (contextual): bank account; health record; provincially-issued driver's licence or identity card; Canadian passport; business bank account.
- Reference: Digital Wallet, Verified Person

Foundational Evidence of Identity (Preuve d’identité fondamentale)

Evidence of Identity that establishes the existence and Digital Representation of real, legally recognized Entities based on fact-based foundational events (e.g., birth, immigration, incorporation). The establishment and maintenance of foundational identity evidence is the exclusive domain of the public sector, specifically for Persons it is the Vital Statistics organizations of the provinces and territories, and Immigration, Refugees, and Citizenship Canada; for Organizations it is Provincial business registrars and Corporations Canada.

- Examples: provincial birth record; federal immigration record; certificate of incorporation; legal name change record.
- Reference: Verified Person

Foundational Evidence of Organizational Identity (Preuve fondamentale de l’identité organisationnelle)

Information providing evidence of Organizational Identity that is directly tied to a specific foundational event in the life of the Organization (e.g., registration, change of name, amalgamation). Created and issued exclusively by mandated public Organizations, specifically business registrars and Corporations Canada. Foundational Evidence of Organizational Identity establishes core Identity Information (e.g., Legal name, operating name, date of creation, and jurisdiction of creation).

- Examples: certificates of incorporation; records of business name registration.
- Reference: Verified Organization

Foundational Identity Record (Foundational Identity) (Dossier d’identité fondamentale (identité fondamentale))

A record that provides Foundational Evidence of Organizational Identity.

- Example: a business’s certificate of incorporation serves as a Foundational Identity Record by providing essential evidence of its legal status and identity.

- Reference: Verifiable Organization

Governing Body (Organe de gouvernance)

A Role that a Participant performs to make sure that the standards, processes, and the associated requirements of the Digital Identity Ecosystem are implemented, which include conformance with government legislation, regulations and policy.

They also enforce compliance by Digital Identity Ecosystem participants to agreed safeguards, guidance, best practices, rules and commercial arrangements.

- Example: payment network consortium.
- Reference: Privacy

Holder (Titulaire)

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. Holders may store Credentials they possess in a Repository.

- Example: a parent might possess a Credential belonging to their child; an attorney might possess a Credential belonging to their client.
- Reference: Authentication, Credentials, Trust Registries, Digital Wallet, Infrastructure

Identity (Identité)

Physical or digital information about a Subject that uniquely identifies a Subject within a context, and is used exclusively by that same Subject, or by a Person acting on behalf of an Organization, to access online services with trust and confidence.

- Examples: physical driver's licence; mobile drivers licence; birth certificate; immigration documents; SIN card; government-issued identity card.
- Reference: Authentication, Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice & Consent, Privacy, Verified Person, Verified Organization

Identity Establishment (Établissement de l’identité)

Identity Establishment is the process of creating Identity Evidence (i.e., a Verified Person record) within a program/service population that may be relied on by others for subsequent programs, services, and activities.

- Example: creating a verified user account in an online banking system, which a Subject can then use to access other financial services.
- Reference: Verified Person, Verified Organization

Identity Information / Attributes (Renseignements/attributs d’identité)

Properties about a Subject in any format that alone or in combination may be used to distinguish one Subject from other similar entities in a given context, and describe the Subject as required by the program or service.

- Examples: name; age; year of birth; permission to operate a vehicle; date of incorporation; business owner information; corporation status; address; generated or assigned identifier.
- Reference: Authentication, Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice & Consent, Privacy, Verified Person, Verified Organization
- See also: Attributes

Identity Maintenance (Maintenance de l’identité)

Identity Maintenance is the process of ensuring that Identity Information recorded about the Subject is as accurate, complete, and up-to-date as required. This process deals with events that may impact the validity of the previously performed Identity Information Validation and Identity Verification (e.g., Evidence used to establish the Verified Person has changed, expired or been revoked, which invalidates the Verified Person record).

- Example: regularly updating a User's expired identification documents in their digital profile to ensure they remain valid and accurate.
- Reference: Verified Person, Verified Organization

Identity Resolution (Résolution de l’identité)

Identity Resolution is the process of establishing the uniqueness of a Subject within a target population through the use of Identity Information. A Responsible Authority defines its own Identity resolution requirements in terms of identity Attributes; that is, it specifies the set of Identity Attributes that is required to uniquely identify a Subject from other Subjects within a specific population.

- Example: verifying a person’s unique identity using their passport number, biometric data, and email address to ensure they are not duplicated in a secure database.
- Reference: Verified Person, Verified Organization

Identity Evidence Validation

Identity Evidence Validation is the process of confirming that the Evidence presented (physical or electronic) can be accepted or be admissible as a proof (i.e., beyond a reasonable doubt, balance of probabilities, and substantial likelihood).

- Example: checking that a scanned driver's license matches the official database and is free from alterations.
- Reference: Verified Organization

Identity Information Validation (Validation de la preuve d’identité)

Identity Information Validation is the process of confirming the accuracy of Identity Information about a Subject when compared with Identity Information established by an Authoritative Party. Identity Information Validation relies on the Evidence obtained from the Establish Sources process to determine whether claimed Identity information exists and is valid.

Note that this process does not ensure that the User is using their own Identity Information – only that the Identity Information that the Subject is using is accurate when compared to the Identity Evidence from an Authoritative Source.

- Example: confirming that a user's provided birthdate matches the official records from a government database.
- Reference: Verified Person, Verified Organization

Identity Presentation (Présentation de l’identité)

Identity Presentation is the process of dynamically confirming that a person has a continuous existence over time (i.e., “genuine presence”).

- Example: using a live video call to verify that a person is physically present and matches their digital profile photo.
- Reference: Verified Organization

Identity Provider (Fournisseur d’identité)

A Role that a Participant performs to create, maintain and provide Digital Identities.

In federated Authentication systems, the Identity Provider is the authoritative Service that verifies a User’s login Credentials.

- Examples: provincial government; telecommunications company; business registrar, or a Participant in a single sign-on Authentication flows.
- Reference: Assurance Maturity Model
- See also: Authoritative Party, Issuer, Credential Issuer

Identity Verification (Vérification de l’identité)

Identity Verification is the process of confirming that the Identity Information being presented is under the control of the User. It should be noted that this process may use personal information that is not related to Identity. This process may use Identity Evidence obtained from the sources of Evidence confirmed in Establish Sources, as well as interactions with the User to determine that the claimed Identity belongs to the Subject it concerns.

- Example: having a User confirm their identity by answering security questions based on personal information, combined with a code sent to their registered email.
- Reference: Verified Person, Verified Organization
- See also: Verifier

Independently Audited (Audité indépendamment)

The referenced audit must be performed by an audit group that is not connected to, is discrete from, or is otherwise not part of the business unit responsible for the process or activity that is the subject of the audit.

- Example: an independent audit firm reviewing a company's data security practices, separate from the company’s internal IT department.
- Reference: Authentication

Inaccessible Credential (Justificatif inaccessible)

A Credential which is not accessible/available or exists in an incomplete state.

This can occur as a result of an incomplete process or the Credential Suspension process.

- Example: a digital certificate that cannot be used because it was not fully issued or has been temporarily revoked.
- Reference: Authentication
- See also: Credential

Issuer (Émetteur)

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).

- Example: a university that issues digital diplomas to graduates' acts as an Issuer by providing verifiable credentials of their academic achievements.
- Reference: Authentication, Credentials, Trust Registries, Digital Wallet, Infrastructure, Verified Organization
- See also: Reliable Source

IT Service Management (Gestion des services TI)

The entirety of activities – directed by policies, organized and structured in processes and supporting procedures – that are performed by an organization to design, plan, deliver, operate and control information technology services offered to customers.

- Example: a tech firm that follows a set process to maintain its software, handle user support requests, and ensure system updates demonstrates IT Service Management.
- Reference: Authentication

Legal Status (Statut juridique)

An indicator of an Organization's status as a legal Entity at a particular time.

- Example: a business registration certificate confirming a company's legal standing as an active corporation represents its Legal Status.
- Reference: Verified Person, Verified Organization
- See also: Trust Registry

Levels of Assurance (Niveaux d'assurance)

A Level of Assurance represents the level of confidence an Entity may place in the processes and other conformance criteria defined in any given component of the PCTF.

Additional details regarding Levels of Assurance can be found in the PCTF Assurance Maturity Model.

- Reference: Authentication, Assurance Maturity Model, Trust Registries, Digital Wallet, Notice & Consent, Verified Organization, Verified Person
- See also: Trust Framework

Machine (Machine)

Software and hardware that can act as intelligent agents to conduct transactions independently (i.e., requires identity verification of the machine).

Machines that can act autonomously are currently not in scope of the PCTF but may be included in future versions.

- Examples: a fridge that connects to the internet to place an order for more milk, pays for it, and specifies delivery address; automated stockbroker application.
- Reference: Credentials, Trust Registries, Digital Wallet, Infrastructure, Privacy
- See also: Service

Network Facilitator (Fournisseur de réseau)

A Role that a Participant performs to connect parties together in a multi-party identity transaction. This organization is an active participant and adds value in the delivery of the Digital Identity service.

- Examples: a blockchain provider, or Software as a Service provider (SaaS) that facilitates the network.
- Reference: Notice & Consent, Privacy

Notice (Avis)

A statement that is formulated to describe the collection, use, disclosure, and retention of Personal Information and inform a User. Notice requirements for each jurisdiction's legislation must be adhered to.

- Examples: notice to request use of identity information; notice of risks when providing consent for surgery on a child.

- Reference: Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice & Consent, Privacy, Verified Person
- See also: Consent

Notice and Consent Processor (Entité chargée du traitement des avis et consentements)

A Role that a Participant performs to provide the notice to the User of the request for Personal Information (from the Requesting Organization), to obtain and record the consent and to provide the User with the means to manage the consent going forward, including the withdrawal of consent.

- Example: an app that informs users about data collection, asks for their permission, and allows them to change or withdraw their Consent.
- Reference: Notice & Consent, Privacy
- See also: Consent

Notice Information (Renseignements servant d'avis)

Information used to formulate a statement that is presented to a Subject to formulate an appropriate Notice and, if applicable, to obtain the consent necessary to continue with the service process.

The information required is based on applicable legal, policy and contractual requirements.

- Example: a privacy policy detailing how a company collects and uses personal data is an example of Notice Information used to inform users and obtain their Consent.
- Reference: Notice & Consent
- See also: Consent

Organization (Organisation)

An Entity that consists of a person or organized body of people with a particular purpose, and whose existence is established by legal statute.

- Examples: businesses (e.g., sole proprietorships, partnerships, and corporations); associations and trade unions; government agencies; co-operatives; registered charities.
- Reference: Authentication, Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice & Consent, Verified Organization
- See also: Participant

Organization Verifier (Vérificateur d'organisations)

A Role that a Participant performs to provide one or more Organizational Identity Validation or Organizational Identity Verification Trusted Processes.

Organization Verifier is defined separately from Responsible Authority to support a wider range of potential use cases and implementation scenarios where the Responsible Authority is not directly involved in the verification process (e.g., a private business is performing verification rather than a business registry).

- Example: a compliance firm that verifies a company's Credentials and operational status for a business partner may perform this Role.
- Reference: Verified Organization, Verified Person
- See also: Verifier

Organizational Identity Establishment (Établissement de l'identité organisationnelle)

Organizational Identity Establishment is the process of creating an Organizational Identity Record (foundational or contextual).

Other parties can rely on this record for subsequent program and service delivery.

- Example: setting up a verified business profile with a government agency that other companies can use to confirm the business's legitimacy.
- Reference: Verified Organization
- See also: Identity Information

Organizational Identity Issuance (Délivrance de l'identité organisationnelle)

Organizational Identity Issuance is the process of creating and providing to the Organization evidence of its Identity. Foundational Evidence of Organizational Identity is issued by a Public Sector Organization Registry.

Contextual Evidence of Organizational Identity is issued by a public Entity (which may include a Public Sector Organization Registry when not acting in an official registrar capacity) or a private sector Entity.

- Example: providing a digital badge to a business that confirms its registration with a government agency or a private certifying body.
- Reference: Verified Organization
- See also: Issuer

Organizational Identity Linking (Liaison de l'identité organisationnelle)

Organizational Identity Linking is the process of relating two or more sets/instances of Identity Information for the same Organization.

- Example: integrating a company's legal registration data with its commercial listing on a business directory.
- Reference: Verified Organization
- See also: Identity Information

Organizational Identity Maintenance (Maintenance de l’identité organisationnelle)

Organizational Identity Maintenance is the process of ensuring that identity information recorded about the Organization is as accurate, complete, and up-to-date as required.

This process also includes Identity notification, which is the disclosure of Identity Information when triggered by a change in Organizational Identity Information. Identity notification can also be an indication that Identity Information has been exposed to a risk factor.

- Example: updating a company’s business registration details and notifying stakeholders of any changes to its contact information.
- Reference: Verified Organization

Organizational Identity Resolution (Résolution de l’identité organisationnelle)

Organizational Identity Resolution is the process of establishing an Organization as unique within a population through the use of that Organization’s Identity Information.

With this process, each program or service specifies the set of Organizational identity attributes required to achieve Organizational identity resolution within its jurisdiction.

- Example: using a company’s unique tax ID to confirm its identity as distinct from other businesses in a financial system.
- Reference: Verified Organization

Organizational Identity Validation (Validation de l’identité organisationnelle)

Organizational Identity Information Validation is the process of confirming the accuracy of identity information about an Organization against that established by a Responsible Authority.

This process involves using Contextual or Foundational Evidence of Organizational Identity to determine a claimed Identity exists and is valid.

- Example: verifying a business's registration status by comparing its details with official records from a government authority.
- Reference: Verified Organization
- See also: Authorized Agent

Organizational Identity Verification (Vérification de l'identité organisationnelle)

Organizational Identity Verification is the process of confirming that the presented Organizational Identity Information relates to the Organization making the presentation.

Verification is a separate process from Organizational Identity Validation and may employ different methods and require the collection of Organizational information that is not related to Identity.

The intent of the Organizational Identity Verification process is to ensure a service provider or other party knows the Identity of the Organization with which it is interacting while preventing duplicitous use of Identity Information.

- Example: confirming that a company's registration number matches its business records to ensure it is accurately representing itself during a contract negotiation.
- Reference: Verified Organization
- See also: Verifier, Issuer, Credential Revocation

Participant (Participant)

An Organization that performs one or more Roles in the Digital Identity Ecosystem and agrees to comply with the parameters of the PCTF.

- Examples: Identity Provider such as a provincial government or government department of immigration; telecommunications provider; network provider; technology company that operates a website and a digital service.

- Reference: Authentication, Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice & Consent, Verified Organization and Verified Person
- See also: Issuer, Verifier, Authorized Agent, Service, Relying Party

Person (Personne)

An Entity that is a biological individual, human being who is alive or deceased.

- Examples: residents of a jurisdiction (e.g., country, province); customers of a business.
- Reference: Authentication, Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice & Consent, Verified Organization and Verified Person
- See also: Verified Person

Personal Information (Renseignements personnels)

Any factual or subjective information, recorded or not, about an identifiable individual.

Note: The Privacy Component further delineates Subject-Specific and Service-Specific types of Personal Information; for details see PCTF Privacy.

- Examples: name; email address; phone number; mailing address; date of birth; account information; service-specific pseudonymous identifiers; transaction records; proofs of transactions including Consent.
- Reference: Authentication, Credentials, Digital Wallet, Infrastructure, Notice & Consent, Privacy, Verified Organization and Verified Person
- See also: Subject-Specific Personal Information

Presentation (Présentation)

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.

- Example: when a User shares their verified driver's license information with a rental service to prove their age and identity.
- Reference: Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice & Consent, Verified Organization and Verified Person

Public Sector Organization Registry (Registre d’organisations du secteur public)

A government department or registrar (regardless of formal organizational structure or status) operating under the authority of a Canadian federal, provincial, or territorial government and mandated to:

i) administer the laws and regulations that govern creation and maintenance of legal Entities, and
ii) deliver associated programs and services.

- Example: a provincial government office that registers businesses and ensures they comply with local regulations before they can legally operate.
- Reference: Verified Organization
- See also: Trust Registry

Registering Party (Partie déclarante)

An Entity (usually a real person) that is authorized to register an Entity with a Trust Registry (such as director of a company or an employee who has been delegated with this authority).

- Example: a company's director who submits the required documents to officially register the business with a government trust registry.
- Reference: Trust Registries

Registrant (Déclarant)

An Entity that is registered in a Trust Registry. Registrants are Issuers, Verifiers, Digital Wallet Providers, and other Trust Registries.

- Example: a company that provides digital wallets and is officially registered in a trust registry to issue and verify credentials.
- Reference: Trust Registries
- See also: Trust Registry

Relationship (Relation)

A Relationship is a specific type of Credential that describes the way in which two or more Entities are connected.

- Examples: Fatima has earned a PhD from the University of British Columbia; Eric is an employee of FictitiousCorp; Diya and Charles are legally married.
- Reference: Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice & Consent, Privacy, Verified Organization and Verified Person

Relationship Credential (Justificatif d’une relation)

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

- Example: when a university issues a Credential verifying a student's status, allowing them to present it as proof of enrollment to access student discounts or services.
- Reference: Credentials, Digital Wallet

Relationship Definition (Définition d’une relation)

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. Rather, the Relationship Definition describes the characteristics of such relationships. Relationship Definitions are created via the Define Relationship process.

- Example: in the context of a student-institution relationship, this describes the formal educational relationship between students and an academic institution, outlining the roles, responsibilities, and conditions under which any student engages in learning and the institution provides educational services.
- Reference: Credentials

Reliable Source (Source fiable)

A Reliable Source is an originator or issuer of information that is used to verify the identity of the client.

To be considered reliable under the FLSC Model Rule, the source should be well known and considered reputable.

- Examples: a utility bill, government issued ID, corporate or business registry
- Reference: PCTF Law Society Profile
- See also: Issuer

Relying Party (Partie dépendante)

A Role that an Organization or Person performs to consume Digital Identity Information created and managed by Participants to conduct digital transactions with Subjects.

- Examples: bank when opening a new account for a Subject; a car dealer when verifying credit of a buyer; service provider who needs some level of identity verification.
- Reference: Authentication, Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice & Consent, Privacy, Verified Organization and Verified Person
- See also: Requesting Organization, Service

Render Credential (Justificatif de rendu)

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

- Example: Display the digital Credential attribute values in a way that resembles the visual appearance of the original document or makes its interpretation more understandable.
- Reference: Digital Wallet, Infrastructure
- See also: Presentation

Repository/Credential Repository (Référentiel/Référentiel de justificatifs)

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.

- Example: an online vault where users can securely store and manage their digital IDs and certificates, ensuring only authorized access to their personal information.
- Reference: Credentials, Digital Wallet, Infrastructure

- See also: Secure Storage

Requesting Organization (Organisation requérante)

A Role that an Organization or Person performs to receive Personal Information that the User consents to disclose.

In a digital identity context, this will often be a service provider or relying party.

- Examples: a service provider in private or public sector.
- Reference: Notice & Consent, Privacy
- See also: Relying Party, Service

Responsible Authority (Autorité responsable)

A Role that a Participant performs to provide one or more of the Verified Person or Verified Organization Trusted Processes to establish that a Subject is real, unique, and identifiable, and protects related information against compromise.

- Example: a government agency that verifies an individual's identity and ensures the security of their personal data during the application for a passport.
- Reference: Verified Person, Verified Organization
- See also: Authorized Agent

Revocation Authority (Autorité qui révoque)

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.

- Example: an organization responsible for managing and updating the status of digital certificates that have been revoked due to security breaches or expiry.

- Reference: Credentials, Digital Wallet, Infrastructure
- See also: Issuer

Role (Rôle)

A set of functions that are made up of one or more Trusted Processes defined as part of the common Trust Framework of the Digital Identity Ecosystem.

Roles help to isolate the different functions and responsibilities that participants may perform within the end-to-end Authentication processes. Roles do not imply or require any particular solution, architecture, or implementation or business model.

- Examples: Identity Provider; Credential Provider; Authentication Service Provider; Relying Party; Infrastructure Provider; Assessor; Governor.
- Reference: Authentication
- See also: Participant

Secure Storage (Entrepôt sécurisé)

Secure storage is a facility used to ensure stored data’s security, privacy, and integrity.

This facility may rely upon the physical protection of the hardware on which the data is stored, as well as security software. Data stored in secure storage either cannot be retrieved from storage or can only be retrieved by authorized parties.

- Example: an encrypted database or file system, the secure element in mobile phone hardware.
- Reference: Digital Wallet, Infrastructure
- See also: Wallet

Selective Disclosure (Divulgation sélective)

A Credential may contain multiple claims as key value pairs. As a principle, data minimization should be employed whenever possible to limit the sharing of personal information.

A data minimized proof of age to a Verifier might only include the Holder's date of birth and a possibly a photo image.

One powerful use of the Selective Disclosure is to blind the binding identifier common to a group of issued Credentials. This reduces the risk of tracking Holder activity as the binding secret is not disclosed to the Verifier.

- Example: when a Credential holder shares only specific pieces of information (i.e., date of birth) while keeping other details, such as their name or image, private using cryptographic techniques.
- Reference: Digital Wallet, Infrastructure
- See also: Zero Knowledge Proofs

Service (Service)

A Service is a system, either electronic or manual, that performs a set of tasks based on User provided data to satisfy a need or to fulfil a demand.

A Service, in the context of the PCTF, requires a User to be authenticated to access the Service.

- Examples: An online portal that accepts User data to apply for employment insurance; register a business; apply for a loan; make online purchases.
- See also: Relying Party

Service-Specific Information (Renseignements spécifiques aux services)

Information collected or generated by the Participants (Disclosing Organization, Requesting Organization, Notice and Consent Processor(s), or Network Facilitator) for purposes of operating and maintaining the Service. In some cases, service-specific information may be shared, with Subject's consent.

- Examples: system or process specific pseudonymous identifiers, transaction records, proofs of transactions including consent.

- Reference: Notice & Consent, Privacy
- See also: Service

Session/Authenticated Session (Session/Session authentifiée)

A Session is a persistent interaction between a Subject's software agent (e.g., web browser, mobile app) and a software service used by service providers or Relying Parties.

An Authenticated Session is a Session (a persistent interaction between a Subject's software agent (e.g., web browser, mobile app) and a software service used by service providers or Relying Parties) that is securely linked to successful authentication of the Subject.

A Session may be required to satisfy federation and single sign-on (SSO) use cases.

- Example: a secure, ongoing interaction between a User's app and a Service that confirms the user's identity through successful authentication.
- Reference: Authentication, Credentials

Stored Consent Decision (Décision de consentement enregistrée)

The record of the notice conditions and consent decision saved to a storage medium for later reference.

- Example: a record stored confirming where the User agrees to a website's terms and conditions.
- Reference: Notice & Consent
- See also: Consent

Strong Binding (Liaison robuste)

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

- Example: when a User's digital ID and verified Credentials in their wallet are securely linked to them through biometric authentication.
- Reference: Digital Wallet, Infrastructure
- See also: Cryptographic Binding

Subject (Sujet)

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

In the context of Verified Organization, Subject always refers to an Organization.

- Examples: individual with Canadian citizenship; charitable organization; smart refrigerator that can order groceries when inventory is low; self-driving car.
- Reference: Authentication, Notice & Consent, Privacy, Verified Organization, Verified Person
- See also: Holder

Subject-Specific Personal Information (Renseignements personnels spécifiques au sujet)

Information a Subject consents to share from a Disclosing Organization to a Requesting Organization.

- Examples: name, email address, phone number, mailing address, date of birth, account information.
- Reference: Notice & Consent, Privacy

Token (Jeton)

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

- Example: an ID badge in a virtual environment, confirming a user's access rights.

- Reference: Digital Wallet, Infrastructure
- See also: Credential

Trust Framework (Cadre de confiance)

A formalized scheme of agreed-upon definitions, principles, conformance criteria, assessment approach, standards, and specifications to ensure the trustworthiness of processes that create, manage and use digital Identity Information.

- Examples: Pan-Canadian Trust Framework, Open Identity Exchange (OIX), New Zealand's Digital Trust Framework.
- Reference: Authentication, Credentials, Trust Registries, Digital Wallet, Infrastructure, Notice & Consent, Privacy, Verified Organization, Verified Person
- See also: Trust Registry

Trusted Process (Processus de confiance)

A set of business or technical activities that transform an input condition to an output condition, and that have been shown, by being assessed against conformance criteria defined in the PCTF, to be trustworthy and reliable.

- Examples: identity verification, record consent.
- Reference: Authentication

Trust Registry (Registre de confiance)

A digital service operated by a Digital Identity Ecosystem that provides information about Registrants.

The information can be human readable and/or machine readable such that people and organizations (operating technology services) can make informed decisions about the trustworthiness of a Registrant's services (e.g., assurance level, transparency, and audit status as per a Trust Framework). For example,

- Example: an online platform which Holders can check to make informed decisions prior to interacting with Issuers and Verifiers and which Verifiers can query to make informed decisions about accepting verifiable Credential presentations from Holders (and the Issuers of the Credential).
- Reference: Trust Registries
- See also: Credential Revocation, Credential Suspension

Trust Registry Operations (Opérations du registre de confiance)

The business and technology processes used to manage the infrastructure and information content of the Trust Registry as well as certify/register Entities in the Trust Registry.

The Trust Registry and its operations conform to a Trust Framework such as the PCTF.

- Reference: Trust Registries
- See also: Credential Revocation, Credential Suspension

Trust Registry Governance (Ecosystem Governance) (Gouvernance du registre de confiance (gouvernance de l'écosystème))

The management processes that define the mission, policies, procedures, and standards of an Ecosystem and its Trust Registry and or Verifiable Data Registry.

- Reference: Trust Registries

Unverified Person (Personne non vérifiée)

Any Person who is not a Verified Person. It should be noted that an Unverified Person may be a real, unique, and identifiable Person who has truthfully claimed who they are, whose identity has not been verified.

- Example: an online shopper creating a new account without verifying their identity is an Unverified Person.

- Reference: Verified Person

User (Utilisateur)

A Person who is either the Subject or authorized to represent the Subject and intentionally accessing a digital service or digital program.

- Examples: visitor to Canada accessing Government of Canada tourism site; Canadian resident registering to vote online; small business owner filing annual report online; a daughter filing a tax return on behalf her mother.
- Reference: Privacy

Validation (Validation)

A process that confirms the accuracy of Digital Identity Information about a Subject as established by an Authoritative Party.

- Examples: a driver's licence application process that confirms information as presented on physical documents or by means of electronic validation service.
- Reference: only found in the glossary

Verifiable Credential (Justificatif vérifiable)

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.

- Example: a digital diploma with a secure cryptographic signature that confirms its authenticity and prevents tampering.
- Reference: Credentials, Digital Wallet, Infrastructure

Verifiable Data Registry (Registre de données vérifiables)

A Role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on, which might be required to use Verifiable Credentials (from W3C).

- Example: Sarah applies for a job and uses a digital credential from her university to prove her degree. The employer checks a Verifiable Data Registry to confirm the university is trusted, the credential is valid, and it hasn't been revoked - all without contacting the university directly.
- Reference: Trust Registries, Infrastructure, Digital Wallet
- See also: Trust Registry

Verifiable Presentation (Présentation vérifiable)

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.

- Example: when a student submits a digital transcript to a university application system, allowing the system to securely verify that the transcript is authentic and has not been altered.
- Reference: Credentials, Trust Registries, Digital Wallet, Infrastructure

Verifiable Relationship (Relation vérifiable)

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.

- Example: when a company issues a digital verification of a business partnership to a new vendor, ensuring the partnership's authenticity and integrity through cryptographic means.
- Reference: Credentials

Verification (Vérification)

A process that confirms that the Digital Identity information being presented relates to the Subject who is making the assertion

- Examples: asking the presenting Person questions that only they would know (e.g., credit history questions, shared secrets, mailed-out access codes); a financial tracking process that confirms that the organization performs its listed services and that the owner appears in the applicable registrar.
- Reference: Credentials
- See also: Credential Verification

Verified Credential (Justificatif vérifié)

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

- Example: when a university confirms the authenticity of a digital diploma issued to a graduate, ensuring that it is genuine and accredited.
- Reference: Credentials
- See also Credential, Verifier

Verified Person (Personne vérifiée)

Knowledge, or having a degree of certainty, that an individual human being is real, unique and identifiable (i.e., a Person), and has truthfully claimed who they are.

- Example: a bank ensuring that the person is real and accurately representing themselves during the account opening process.
- Reference: Verified Person
- See also: Verifier

Verified Person record (Dossier de personne vérifiée)

A digital record that represents that a person has been verified in a specific context (e.g., decentralized identifier (DID), Identity Attributes, account number). Also referred to in the PCTF as a trusted digital representation.

- Example: a digital record or Credential, showing that a user's identity has been confirmed by an online service, including their unique identifier and verified attributes, such as their email address and phone number.
- Reference: Verified Person
- See also: Credential

Verifier (Vérificateur)

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.

- Example: a university admissions office that checks a digital transcript to confirm its authenticity and ensure it accurately reflects the student's academic record.
- Reference: Credentials, Trust Registries, Digital Wallet, Infrastructure
- See also: Credential Verification

Zero-Knowledge Proofs (ZKP) (Preuve à divulgation nulle de connaissance (PDC))

A Zero-Knowledge Proof is a cryptographic technique that allows the Holder to prove to a Verifier that the Holder has knowledge of a value without actually sharing the value

and can be used within the context of digital identity to support the following key privacy preserving features:

1. Selective Disclosure – disclose a subset of Attributes from a credential to an issuer.
2. Predicates – calculations on Attributes such as equality or greater than (e.g., prove your salary is greater than X or your age is greater than Y) where actual values are not shared with Verifier.
3. Signature blinding – randomization of Issuer signature prior to sharing with the verifier to eliminate the signature as a correlating factor.
4. Private Holder blinding – the correlating identifier is not exposed to the Verifier.

- Example: providing a cryptographic provable yes/no answer to the question “are you over 21?”
- Reference: Digital Wallet, Infrastructure
- See also: Selective Disclosure

4. References

1. Government of Canada. Treasury Board of Canada Secretariat. Directive on Identity Management - Appendix A: Standard on Identity and Credential Assurance. 2019. <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32612&section=html>
2. Government of Canada. Office of the Privacy Commissioner of Canada. PIPEDA in Brief – What is personal information? May 2019. <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ >
3. PIPEDA in Brief, Office of the Privacy Commissioner of Canada - What is personal information?)

5. Revision History

Version Number	Date of Issue	Author(s)	Description
0.01	2018-08-08	TFEC, PCTF Editors	Initial working draft
0.02	2019-05-07	PCTF Editors	Updated working draft
0.03	2019-06-12	PCTF Editors	Added Columns for Information Mapping Method based on existing Definitions
0.04	2019-07-18	PCTF Editors	Re-arranged and grouped terms to facilitate discussion at Design Group Meetings
0.05	2019-08-16	PCTF Editors	Updated first five terms based on Aug. 8 design team meeting; added definitions from PCTF Model overview for person, organization, and machines; added examples and non-examples for Entity and Subject
0.06	2019-09-20	PCTF Editors	Updated based on September 5th and 8th design team meetings, after input from team members reviewing Subject, User, and Role

0.07	2019-10-22	PCTF Editors	Re-organized terms to have a primary list of terms that are used across components to be addressed by the Glossary Design team; and a secondary list of terms that are specific to a component and addresses by the relevant Design team
0.08	2019-12-05	PCTF Editors	Integrate Glossary Design Team input into draft Glossary for TFEC review
0.09	2020-02-14	PCTF Editors	Updated Glossary based on review comments that are editorial (i.e., syntactic or modify examples), and incorporated feedback from TFEC review
1.0	2020-02-24	PCTF Editors	Approved by TFEC as Draft Recommendation V1.0
1.1	2020-05-28	PCTF Editors	Updated as per public review feedback
1.0	2020-07-02	PCTF Editors	Approved by DIACC Sustaining Member ballot as Final

			Recommendation V1.0
1.1	2025-01-15	PCTF Glossary Design Team	Approved by TFEC as Final Recommendation V1.1 Revisions included updating terms in progress, revised the Scope and Conventions & Guidelines sections, removal of Roles section, inclusion of new terms and definitions found across all PCTF documentation, organizing all terms alphabetically, replacing synonyms with “See also”, added References to note where a term and definition may appear in other PCTF documentation, and updated examples

1457

1458

1459