Pan-Canadian Trust Framework Glossary

Document Status: Final Recommendation V1.0

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

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

Table of Contents

1 Scope and Objectives

The 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 content of the PCTF Glossary is:

1. **Terms** – The words or phrases that appear frequently and that are used with a specific intent (i.e., not their everyday English meaning) in the PCTF documentation
2. **Definitions** – A statement that provides the accepted and precise meaning of the associated term in the PCTF context
3. **Examples** – Examples or non-examples may be included to help clarify the intended meaning of a term; the examples provided are not intended to be an exhaustive list.
4. **Synonyms** – Terms with same or similar meaning used in other communities of interest

Within the Glossary definitions, terms that are capitalized refer to glossary definitions of that term, which may differ from their everyday English meaning.

1.1 Scope

This list of terms in the PCTF Glossary has been assembled and defined based on their use in the Pan-Canadian Trust Framework Model and PCTF Component documents that are in Final Recommendation of Draft Recommendation" status. Earlier TFEC work to define key terms and definitions was used as a starting point for the Glossary design team discussions and worksheet. Efforts were made to keep the list of glossary terms to the essentials: terms used with their everyday, English dictionary meaning (e.g., stakeholders) were not included; terms with the same or similar meanings were collapsed to a single entry with synonyms.

The terms included for the current version of the Glossary are those used across PCTF components. Terms that are specific to a single PCTF component are defined in the Terms and Definitions section of that component, and not repeated in this Glossary. PCTF participant roles that are used in the various PCTF components are listed together in a "Roles" section of the Glossary; please refer to the specific PCTF component to fully understand a particular role and its associated functions.

1.2 Methodology

The PCTF Glossary is a living document that will evolve as the PCTF model and its components evolve. 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 recommendation or discussion draft of the PCTF Model Overview or a PCTF Component 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.

As an example of applying the methodology, consider the diagram in Figure 1 that depicts types of entities and key relationships among them.

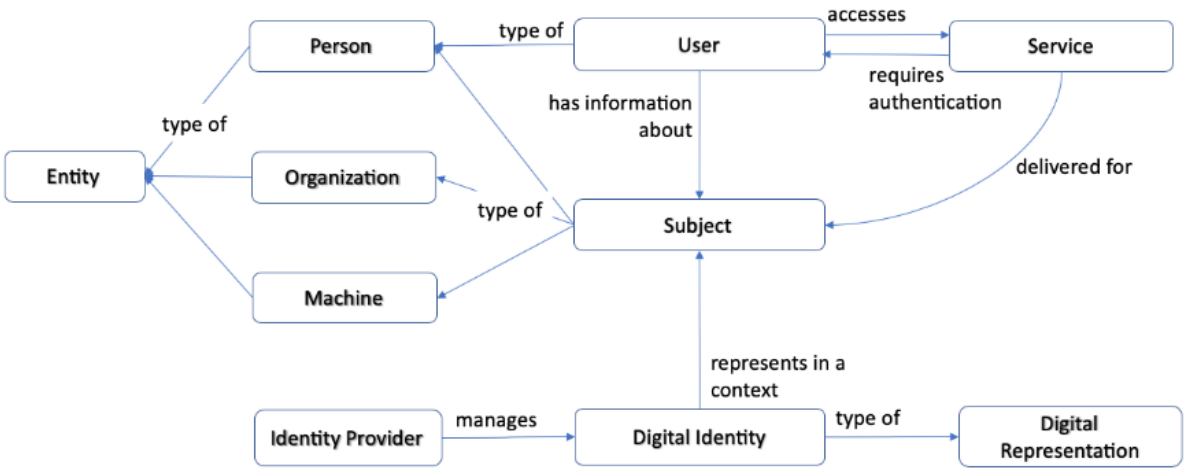

Figure 1. Terms and Relationships

2 PCTF Glossary of Terms

2.1 Agreed Upon Terms

2.1.1 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
- Non-examples: Facebook newsfeed; social media account
- Synonyms: Assurance Source

2.1.2 Conformance Criteria (Critères de conformité)

Requirements used to assess the trustworthiness of a specific process defined in the PCTF.

- Examples: strength of an encryption key, check expiry data on an identity document;
- Non-examples: requirements for website branding

2.1.3 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.

- Examples: agreeing to share home address information to a service provider
- Non-examples: not agreeing to share information
- Synonyms: consent decision; meaningful consent

2.1.4 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
- Non-examples: store loyalty card; blood donor card; fake passport; valid paper birth certificate; website of closed business
- Synonyms: supporting identity

2.1.5 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.

- Examples: passport chip content; BC Services Card chip; verified person record in a digital wallet;
- Non-examples: photocopy of a passport; driver's licence; paper certificates; paper certificate of incorporation;
- Synonyms: trusted digital identity, identity record

2.1.6 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;
- Non-examples: an Identity Provider itself; a digital service that acts as a Relying Party and Identity Provider itself, that is not part of a greater interconnected system or framework;

2.1.7 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
- Non-examples: a loyalty card without a mag-stripe or secure element

2.1.8 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
- Non-examples: wildlife (no identifier); an online service such as a search engine

2.1.9 Evidence of Identity (Preuve d'identité)

A 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
- Non-examples: fake driver's licence
- Synonyms: identity evidence

2.1.10 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
- Non-examples: driver's licence; business bank account

2.1.11 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: driver's licence; birth certificate; immigration documents; SIN card; government-issued identity card
- Non-examples: username and password shared among a group; undocumented birth(s)

2.1.12 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
- Non-examples: nickname; gender; colour of car
- Synonyms: identity credential

2.1.13 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 stock broker application;
- Non-examples: a fridge that alerts its owners that they need milk; a drill press; crane; a living organism; applications that store some credit card info and automatically renew a software licence

2.1.14 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
- Non-examples: generic statement that does not comply with applicable legislation; notification of use of cookies on website for implied consent

- Synonyms: consent form; notice statement; explicit consent capture form

2.1.15 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
- Non-examples: unregistered charity (e.g., Gofundme); community sports league (e.g., high-tech volleyball league)

2.1.16 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;
- Non-examples: a living entity that is not human; any inanimate object with the exception of a deceased human; an avatar of a human

2.1.17 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
- Non-examples: general public; Subjects in the ecosystem; lawyers for the organization; potential or past participant (i.e., not actively participating); Observer, critic or watchdog; Privacy commissioner; Software company that builds identity management products; Google as an Identity Provider that does not follow PCTF.

2.1.18 Personal Information (Renseignements personnels)

Any factual or subjective information, recorded or not, about an identifiable individual (Source: PIPEDA in Brief, Office of the Privacy Commissioner of Canada - What is personal information?). Note: The Privacy Component further delineates Subject-Specific and Service-Specific types of Personal Information; for details see the PCTF Privacy Component Overview.

- Examples: name; email address; phone number; mailing address; date of birth; account information; service-specific pseudonymous identifiers; transaction records; proofs of transactions including consent
- Non-examples: a subway token; a brand of car

2.1.19 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.

- Examples: Identity Provider; Credential Provider; Authentication Service Provider; Relying Party; Infrastructure Provider; Assessor; Governor
- Non-examples: a mother; a condo developer; a User; a Subject

2.1.20 Service (Service)

A valuable action, deed, or effort performed to satisfy a need or to fulfill a demand. A Service, in the context of the PCTF, requires a User to be authenticated to access the Service.

- Examples: applying for employment insurance; registering a business; applying for a loan; making online purchases
- Non-examples: watching news media videos

2.1.21 Subject (Sujet)

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.

- Examples: individual with Canadian citizenship; charitable organization; smart refrigerator that can order groceries when inventory is low; self-driving car
- Non-examples: individual with no identity documents; individual with only physical birth certificate (i.e. no digital id yet); pet dog; wildlife; online service; passport

2.1.22 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
- Non-examples: Any trust framework that does not include specification for creating or managing or using digital identity such as UN Collaborative Trust Frameworks

2.1.23 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 Pan-Canadian Trust Framework, to be trustworthy and reliable.

- Examples: identity verification, record consent
- Non-examples: process to make soup

2.1.24 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
- Non-examples: a senior without access to a computer; a pet dog or cat sitting on the keyboard of my computer; simply reading a public website article

2.1.25 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
- Non-examples: showing age id going into movie theatre

2.1.26 Verification (Vérification)

A process that confirms that the digital Identity Information being presented relates to the Subject who is making the assertion

- Examples: asking a 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
- Non-examples: tapping a credit card for payment

2.2 Terms In Progress

Terms in progress have not been finalized and are considered provisional. They are provided for information purposes only.

2.2.1 Authenticator (Authentificateur)

Information or biometric characteristics under the control of a Subject, and that is a specific instance of: something the Subject has, something the Subject knows, or something the Subject is or does.

- Examples: private signing keys, user passwords, responses to challenge questions, or a person’s face
- Non-examples: bank account number; serial number; username

2.2.2 Credential (Justificatif)

A type of Digital Representation that describes a set of attributes or properties of a Subject. This information may exist on its own (e.g., as a credential that contains no personal information, only a unique string identifier) or be related to Personal Information.

- Examples: a data structure that references education levels (e.g., a university degree in engineering) and/or age of a Subject
- Non-examples: anonymized purchase history
- Synonyms: identity credential; W3C credential

2.2.3 Levels of Assurance (Niveaux d'assurance)

A level of confidence that may be relied on by others. In the PCTF applied as a measure of certainty that a Subject is who or what they claim to be, or that a Subject has maintained control over an Authenticator, and that the Authenticator has not been compromised. In the context of the PCTF, Levels of Assurance are those defined by the Government of Canada Directive on Identity Management - Appendix A: Standard on Identity and Credential Assurance.

2.3 Roles

2.3.1 Authentication Service Provider (Fournisseur de services d'authentification)

A Role that a Participant performs to operate a service that implements the Authentication Trusted Processes related to authentication, authentication session Initiation, or authentication session termination. For more details, please refer to the Authentication component documents.

2.3.2 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
- Non-examples: a network provider; a mobile device manufacturer
- Synonyms: Identity Provider (role); Disclosing Organization (role in Notice and Consent); assurance party

2.3.3 Credential Service Provider (Fournisseur de services de justificatifs)

A Role that a Participant performs to operate a service that implements the Authentication Trusted Processes related to management of authentication credentials. For more details, please refer to the Authentication component documents.

2.3.4 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. For more details, please refer to the Notice and Consent, and Privacy component documents.

2.3.5 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. For more details, please refer to the Privacy component documents.

- Examples: payment network consortium

2.3.6 Identity Attribute Provider (Fournisseur d’attributs d'identité)

A Role that a Participant performs to maintain and provide Digital Identity Attributes.

- Examples: municipality that confirms home address; telco that conforms mobile phone number; employer that confirms employment status; business registry confirms address and status of organization
- Non-examples: a social media feed
- Synonyms: credential (W3C) provider; attribute provider

2.3.7 Identity Provider (Fournisseur d’identité)

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

- Examples: provincial government; telecommunications company; business registrar may perform this Role
- Non-examples: technology infrastructure provider
- Synonyms: identity service provider; authoritative party; identity issuers

2.3.8 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
- Non-examples: internet provider that passively provides internet connectivity

2.3.9 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. For more details, please refer to the Notice and Consent, and Privacy component documents.

2.3.10 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). For more details, please refer to the Verified Organization component documents.

2.3.11 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
- Non-examples: a network provider; a telecommunications company delivering mobile connectivity
- Synonyms: Requesting Organization (role in Notice and Consent); digital identity consumer

2.3.12 Responsible Authority (Autorité responsable)

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

2.3.13 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. For more details, please refer to the Notice and Consent, and Privacy component documents.

- Examples: a service provider in private or public sector

3 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/ >

4 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 comments.
1.0	2020-02-24	PCTF Editors	Approved as Draft Recommendation V1.0
1.1	2020-05-28	PCTF Editors	Updated as per public review.
1.0	2020-07-02	PCTF Editors	Final Recommendation V1.0