PCTF Verified Person

Document Status: Final Recommendation V1.2 Errata

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

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

Table of Contents

1. Introduction to the Verified Person Component

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

1.1 Overview

The ability to verify the Identity of the User and Subject participating in an online transaction is necessary to ensure accuracy, privacy, security, and trust online. Without this ability, Users remain effectively anonymous and concerns about data breaches, legal and social liabilities, and financial loss persist. The range of transactions available under such conditions is limited in terms of the sensitivity, value, and use of personal information. For this reason, DIACC invests in consistent and auditable rules that support the creation and use digital identities for Persons, which are documented here in the PCTF Verified Person Component. These rules and conventions facilitate the delivery of trusted digital services.

The PCTF Verified Person component specifies processes and Conformance Criteria used to establish that a natural person is real, unique and identifiable. This is a key ingredient in ensuring a digital representation of a Person is properly created, used exclusively to represent that same Person, and can be relied on to determine if the Person should receive valued services and to carry out transactions with trust and confidence.

1.2 Purpose and Anticipated Benefits

The purpose of the PCTF Verified Person Component is to ensure the integrity of processes used to verify a Person's Digital Identity. By applying standardized Conformance Criteria for process assessment and certification this component may be used to ensure:

- Trusted Processes result in a digital representation of a unique Subject with a Level of Assurance for their Identity commensurate to the type of service or transaction that is being conducted by the Subject.
- The reliability of Trusted Processes needed to maintain the integrity and security of that Digital Identity.
- The minimization of opportunity for Identity theft and fraud.

All participants will benefit from:

- Repeatability, consistent and continuous identification processes.

Relying Parties benefit from:

- The ability to build on the assurance of the Verified Person Trusted Processes to uniquely identify a Subject within their application or program space.

Note: PCTF Conformance Criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy and regulations in their jurisdiction.

1.3 Scope

The Verified Person component of the PCTF defines processes and specifies Conformance Criteria for:

1. **Verifying a Person**: The processes that ensure the Digital Identity of a Person is an accurate representation of that Person and can be relied on for digital service delivery and digital transactions. A Verified Person is a real, unique and identifiable human being present at the moment of Verification; and within the PCTF context such a Person can be subject to legislation, policy, or regulations within a context. These processes ensure that a Person has been properly verified, and that they are the Person who initiated, directly or through a legally authorized representative, the request for a service or a transaction.

   Notes:

   - Though a Person who is deceased can no longer be verified, they may still have a Digital Identity with an Attribute indicating a deceased status.
   - A Person who desires a service or a transaction but is unable to physically follow the Verification process themselves may have a legally authorized representative aid them in performing it.

2. **Creating a trusted Digital Identity for a Person**: The processes used to establish and maintain a digital record for a Verified Person (also referred to as a Verified Person Record) in order to uniquely distinguish them from other Persons.

There are many techniques that can be used to verify a Person is a “real, unique, and identifiable human being”. For example, a system could:

- Require the presentation of official documents (e.g., driver's license) and confirm that the user is the same Person.
- Require the provision of sufficient biometric data that allows the Person to be distinguished uniquely from the rest of the population.
- Capture a digital identity from the Person's device and use behavioural data (e.g., typing speed, touch-screen pressure, walking gait as measured by a mobile device's accelerometers) to determine that device is in that Person's possession.

The appropriateness of these methods will be determined by the requirements of the Relying Parties and will vary between sectors and use cases. Due to the potential sensitivity of biometric data, it is recommended that the relevant privacy legislation, regulations, and/or

privacy authority (e.g., Office of the Privacy Commissioner) be consulted prior to the collection of biometric data to ensure the appropriateness of its collection and use.

1.3.1 In-Scope

The scope of the PCTF Verified Person Component includes:

- Creating contextual Identity Evidence at an Authoritative Party.
- Relying on Foundational Evidence of Identity to verify a Person.
- Relying on contextual Identity Evidence to verify a Person.
- Levels of Assurance 1-3 for Identity; Level 4 use cases are currently out of scope but will be considered for future versions.
- Creating, updating, and managing a Verified Person record (i.e., a trusted Digital Representation).
- Actors include Canadian federal, provincial and territorial governments and Canadian / PCTF compliant organizations as Authoritative Parties for Identity Evidence.

1.3.2 Out-of-Scope

The scope of the PCTF Verified Person Component does not include:

- Creating Foundational Evidence of Identity. The establishment and maintenance of Foundational Evidence of Identity is the exclusive domain of mandated organizations such as the Vital Statistics organizations of the provinces and territories, and Immigration, Refugees, and Citizenship Canada.
- Using international governments or organizations as the only Authoritative Source for Identity Evidence to verify a Person. International governments may be referenced indirectly to establish foundational or contextual sources of Identity. Use cases that rely only on international Evidence of Identity may be considered in later versions of PCTF.
- Verifying non-Identity Attribute information. The Verified Person processes do not establish any particular information about the Person, only that the Person is real, unique and identifiable in a given context. Other personal information or Attributes such as address of residency may be required to deliver a service. Verification of Attributes not required for verifying a Person's Digital Identity is outside the scope of this component; please refer to the PCTF Credentials (Relationships & Attributes) component.

The scope of the Verified Person component does not currently include the following items:

- Level of Assurance 4 for Identity, as defined by Government of Canada's Directive on Identity Management - Appendix A: Standard on Identity and Credential Assurance, and associated use cases.
- Delegation of authority (i.e., acting on behalf of a Subject such as power of attorney or agency, or signing officer acting on behalf of an organization).

These items are under consideration for a future version of the PCTF.

1.4 Sources of Identity Evidence

The diagram in Figure 1 illustrates the potential sources of Identity Evidence that may be used for verifying a Person in the context of the PCTF. The number and type of sources used depends on the use case, the required Level of Assurance of the Subject's Identity, and applicable regulations, legislation, or policy. For example, the public sector may require at least two Canadian/PCTF-compliant sources of Identity Evidence, including one foundational. International sources of Identity are typically only used in conjunction with Canadian Identity Evidence. Please refer to the Conformance Profile for the specific PCTF requirements at each Level of Assurance.

Sources of Identity Evidence could include:

- The physical Person including biometric information.
- Documentary Evidence such as a birth certificate, permanent residence document, citizenship record, and other accepted documents.
- Online sources, including public and private sector databases. These could include information about the Subject established as a result of delivering a public or private sector service as well as information aggregated from such sources (notwithstanding any data protection, privacy, and legislative requirements).

Notes:

- Not all international government-issued documents are acceptable - this depends on the country and Identity Attributes in question.
- Social media sources may be acceptable to some organizations when only low levels of assurance are required. However, caution is recommended to those considering social media sources as not all such sources can guarantee the accuracy of their Information, nor that the information was gathered with informed consent when applicable.

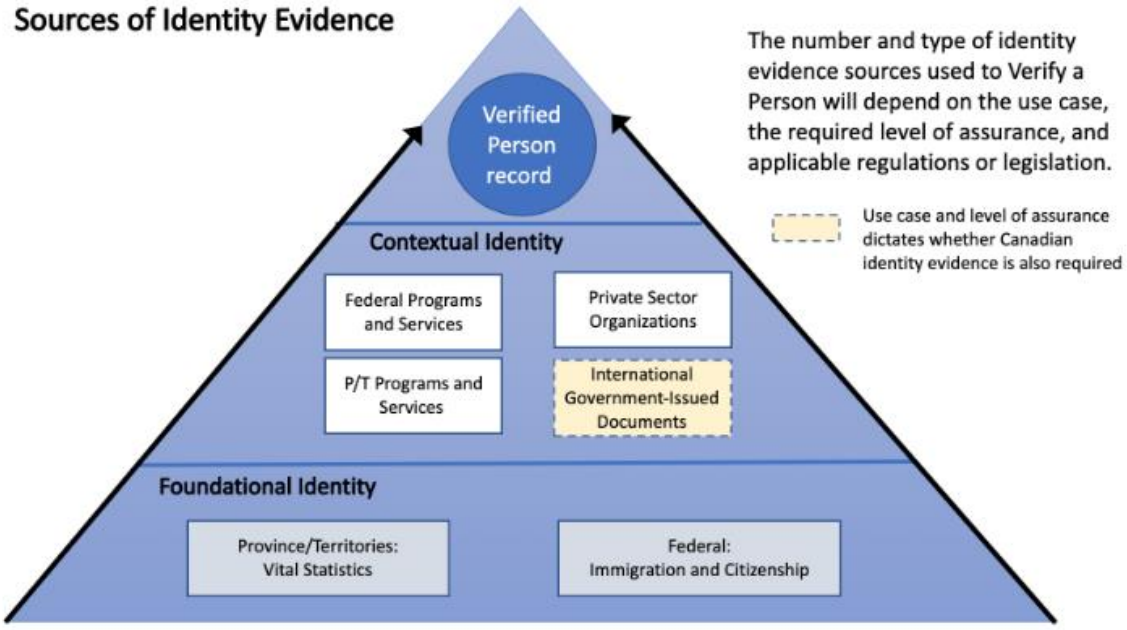

Figure 1. Source of Identity Evidence

1.5 Sufficiency of Identity Information

The following considerations apply when determining the sufficiency of Identity Information:

- Identity Information that is intended to describe a real (existing) Person or to distinguish one Person from another is subject to the accuracy of Identity Information requirements.
- For privacy and security reasons, such as protecting people's Identities, some Identity Attributes may be randomly assigned identifiers, pseudonymous identifiers, user identifiers or usernames.
  Examples of Identity Information for Persons are name, date of birth, and gender.
- An identifier may be a unique Identity Attribute assigned and managed by the program or service. Assigned identifiers may be kept internal to the program or service.
  Examples of internal identifiers are database keys and universally unique identifiers.
- Assigned identifiers may be provided to other programs; however, there may be restrictions due to privacy considerations or legislation.
- Existing or previously assigned identifiers that meet the uniqueness requirement may be used as Identity Information. Organizations need to be aware that the use of these identifiers may be subject to restrictions or have privacy implications.
- Certain identifiers may be subject to legal and policy restrictions. For example, the Directive on Social Insurance Number outlines specific restrictions on the collection, use, retention, disclosure and disposal of the Government of Canada Social Insurance Number.

1.6 Relationship to the Pan-Canadian Trust Framework

The Pan-Canadian Trust Framework consists of a set of modular or functional components that can be independently assessed and certified for consideration as trusted components. Building on a Pan-Canadian approach, the PCTF enables the public and private sector to work collaboratively to safeguard digital identities by standardizing processes and practices across the Canadian digital ecosystem.

Figure 2 is an illustration of the components of the draft Pan-Canadian Trust Framework. Note that the privacy requirements for the handling of personal information by the Verified Person processes (and all other PCTF components) within the Digital Identity Ecosystem are defined in the PCTF Privacy Component.

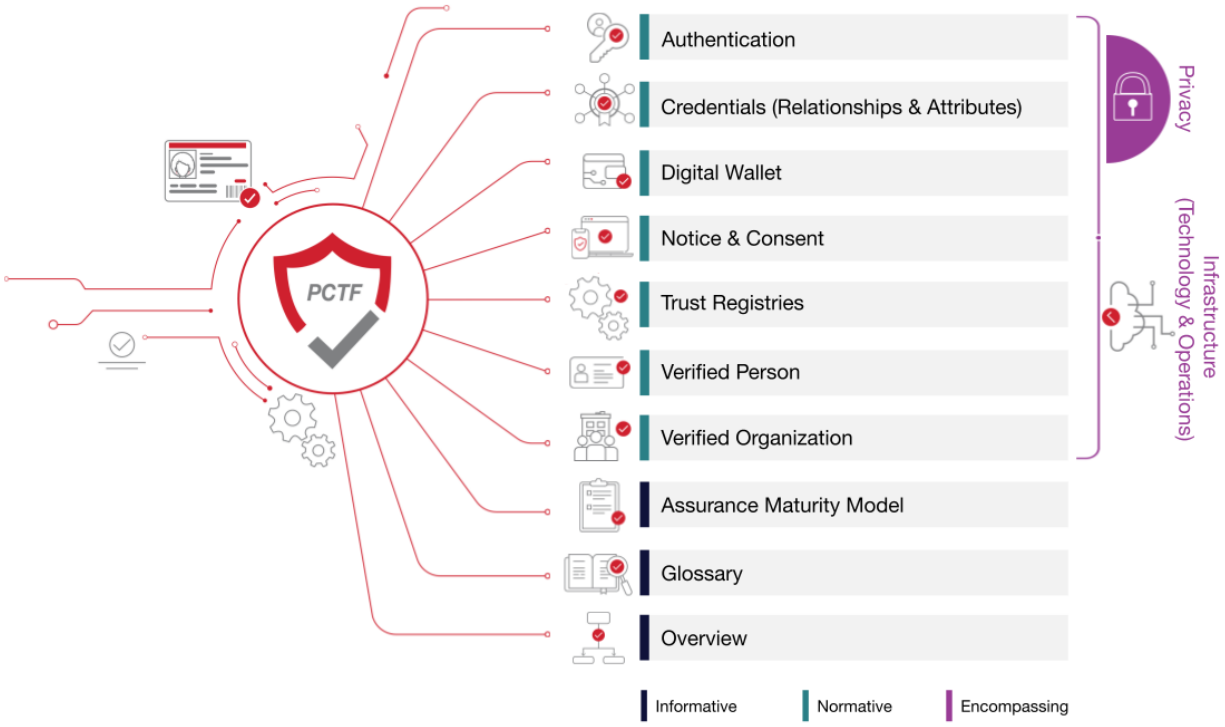

Figure 2. Components of the Pan-Canadian Trust Framework

2. Verified Person Conventions

This section describes and defines key terms and concepts used in the PCTF Verified Person Component. This information is provided to ensure consistent use and interpretation of terms appearing in this overview and the PCTF Verified Person Conformance Profile.

2.1 Terms and Definitions

The Verified Person component references the terms and definitions listed in the PCTF Glossary as well as the following terms and definitions:

Authoritative Source

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

Contextual Evidence of Identity

Evidence of Identity that establishes the existence and Digital Representations of Entities within a specific context and for a specific purpose. Also referred to as "supporting Evidence of Identity".

- 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

Foundational Evidence of Identity

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 Evidence of Identity 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

Subject

A Person 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 a physical birth certificate (i.e. no digital id yet); pet dog; wildlife; online service; passport

Unverified Person

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, who's identity has not been verified.

Verified Person

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.

Verified Person Record

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 PCTF as a trusted digital representation.

2.2 Abbreviations

The following abbreviations appear throughout this overview and the PCTF Verified Person Conformance Profile:

- PCTF – Pan-Canadian Trust Framework
- P/T – Provinces and Territories

2.3 Roles

The following roles and role definitions are applicable in the scope and context of the PCTF Verified Person component.

Authoritative Party

A role that a Participant (i.e., PCTF compliant organization) performs to provide Identity Information or Identity Evidence at a Level of Assurance to Relying Parties.

Relying Party

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

Responsible Authority

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

2.4 Levels of Assurance

Levels of Assurance are used in certain contexts, including the PCTF Verified Person Component, to indicate the robustness of the technology and processes employed to verify the Identity of a Person. The Conformance Criteria for the Verified Person component are profiled in terms of Levels of Assurance for Identity. The Level of Assurance associated with each criterion reflects the relative level of trust Relying Parties can attribute to it. The table below lists the three Levels of Assurance applied to the PCTF Verified Person Conformance Criteria.

Note: Descriptions in Table 1 align with the standards for identity assurance levels specified in A.2.2 of the "Directive on Identity Management - Appendix A: Standard on Identity and Credential Assurance" (July 2019)

Level of Identity Assurance	**Description**
Level 1	• Little confidence required that a Subject is who they claim to be. • The claimed Person is self-asserted and/or minimal checks may be done. Checks, if done, only require the use of low assurance evidence sources. • Satisfies Level 1 Conformance Criteria.
Level 2	• Some confidence required that a Subject is who they claim to be. • Validation and verification will use medium assurance evidence sources potentially supported by additional low assurance evidence sources. • Remote means can be used to verify the person. • Satisfies Level 2 Conformance Criteria.
Level 3	• High confidence required that a Subject is who they claim to be. • Validation and verification will use high assurance evidence sources potentially supported by additional medium and low assurance sources. • In-person (or equivalent) means are used to verify the person. • Satisfies Level 3 Conformance Criteria.
Level 4	• Very high confidence required that a Subject is who they claim to be • Satisfies Level 4 Conformance Criteria, when defined.

Table 1. Levels of Assurance

3. Trusted Processes

The PCTF promotes trust through a set of auditable business and technical requirements for various processes. A *process* is a business or technical activity (or set of such activities) that transforms an input condition to an output condition – an output on which others typically rely.

In the PCTF context, a process that is designated a Trusted Process is assessed according to well-defined and agreed upon Conformance Criteria. The integrity of a trusted process is paramount because many participants—across jurisdictional, organizational, and sectoral boundaries and over the short-term and long-term—rely on the output of that process.

The sequence in which the Trusted Processes are performed may vary. For example, Identity Resolution may be achieved as a result of the Identity Information Validation processes or it may be an input to the Identity Information Validation processes, depending on the Digital Identity system in question.

3.1 Conceptual Overview

The Verified Person Component defines a set of processes used to establish that a Person is real, unique and identifiable. This is a key ingredient in establishing a Trusted Digital Identity, an electronic representation of a Person, used exclusively by that same Person, to receive valued services and to carry out transactions with trust and confidence.

The objective of the Verified Person Component is to deliver a set of Conformance Criteria against which the establishment of a Person as real, unique, and identifiable can be assessed and certified. Once a process is certified it becomes a Trusted Process that can be relied on by other participants of the Pan-Canadian Trust Framework.

The Verified Person Component defines the following Trusted Processes:

1. Establish Sources
2. Identity Resolution
3. Identity Establishment
4. Identity Information Validation
5. Identity Verification
6. Evidence Validation
7. Identity Presentation
8. Identity Maintenance

Figure 3 provides a conceptual overview and logical organization of the Verified Person Component.

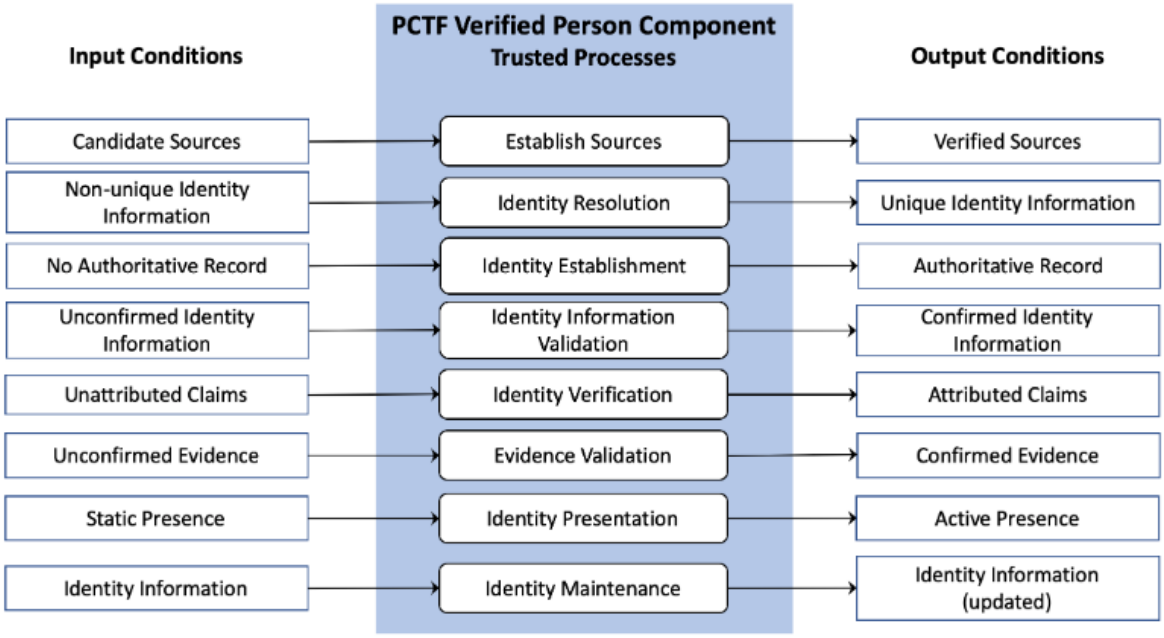

Figure 3. Verified Person Component

The following sections provide definitions of the PCTF Verified Person Trusted Processes. The PCTF Verified Person Conformance Profile defines the associated Conformance Criteria against which the trustworthiness of these processes can be assessed.

Note: It is not expected that all Trusted Processes and all associated Conformance Criteria will apply in all circumstances or use cases in the order listed above.

Verified Person Trusted Processes are defined using the following information:

- Description – A descriptive overview of the process
- Inputs – What is put in, taken in, or operated on, by the process
- Outputs – What is produced by, or results from, the process
- Dependencies – Related PCTF Trusted Processes, primarily those that produce outputs on which the process depends
- Additional information – Other relevant details

3.2 Establish 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.

Inputs	Candidate Sources	The sources proposed to be used in the Identity Information Validation and Identity Verification processes.
Outputs	Verified Sources	The vetted sources to be used in the Identity Information Validation and Identity Verification processes.
Dependencies	None	

3.3 Identity Resolution

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.

Inputs	Non-unique Identity Information, Identity Resolution Requirements	The set of Identity Attributes available to uniquely identify the Subject within the population in question.
Outputs	Unique Identity Information	The set of Identity Attributes required in order to uniquely identify a Subject from the other Subjects in the population in question has been established.
Dependencies	Establish Sources	

3.4 Identity Establishment

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.

Inputs	No Verified Person Record	No Identity Evidence for a Subject exists within a program/service population.
Outputs	Verified Person Record	Identity Evidence for a Subject (Verified Person Record) exists within a program/service population.
Dependencies	Identity Resolution	

3.5 Identity Information Validation

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.

Inputs	Unconfirmed Identity Information	Identity Information about a Subject that has not been validated against an Authoritative Source.
Outputs	Confirmed identity information	Identity Information about a Subject that has been validated against an Authoritative Source.
Dependencies	Establish Sources	

3.6 Identity Verification

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.

Inputs	Unverified Control	The Identity Information has not been verified as being under the control of the User.
Outputs	Verified Control	The Identity Information has been verified as being under the control of the User.
Dependencies	Identity Information Validation	

3.7 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).

Inputs	Unconfirmed Identity Evidence	The Evidence of Identity has not been confirmed as being an admissible proof.
Outputs	Confirmed Identity Evidence	The Evidence of Identity has been confirmed as being an admissible proof.
Dependencies	Establish Sources	

3.8 Identity Presentation

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

Inputs	Static Presence	The Identity (i.e., Verified Person record) exists sporadically and often only in association with a vital event or business event (e.g., birth, death, bankruptcy).
Outputs	Active Presence	The Identity (i.e., Verified Person record) exists continuously over time in association with many transactions.
Dependencies	Identity Information Validation, Identity Verification	

3.9 Identity Maintenance

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).

Inputs	Verified Person Record	Identity Information recorded about the Person (i.e., Verified Person Record) is no longer valid due to changes in the status of the information, or the data having become stale over time and considered expired.
Outputs	Updated Verified Person Record	The updated, re-validated and re-verified Identity Information recorded about the Person (i.e., Verified Person Record).
Dependencies	Identity Verification	

4. Introduction to the PCTF Verified Person Conformance Profile

The Verified Person Conformance Criteria specify requirements that must be met to ensure that Trusted Processes result in the representation of a real, identifiable and unique Person at the necessary Level of Assurance. This document is normative unless otherwise noted.

Note: PCTF conformance criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy and regulations in their jurisdiction.

5. Conformance Criteria Keywords

The following keywords indicate the precedence and general rigidity of a given conformance criteria, and are to be interpreted as:

- **MUST** means that the requirement is absolute as part of the Conformance Criteria.
- **MUST NOT** means that the requirement is an absolute prohibition of the Conformance criteria.
- **SHOULD** means that the requirement is expected to be met, except in limited cases where the applicant documents valid reasons or circumstances to ignore the requirement. The full implications of such an exception must be understood and carefully weighed before choosing to not adhere to the conformance criteria as described.
- **SHOULD NOT** means that a valid exception reason may exist in particular circumstances when the requirement is acceptable or even useful, however, the full implications should be understood and the case carefully weighed before choosing to not conform to the requirement as described.
- **MAY** means that the requirement is discretionary but recommended.

Keywords appear in **bold** and ALL CAPS in the Conformance Criteria.

6. Verified Person Conformance Criteria

Conformance criteria are organized by the Trusted Processes defined in the Verified Person Component Overview**,** and profiled using columns against Levels of Assurance for Identity. For ease of reference, a specific conformance criterion may be referred by its category and reference number. For example, "**SOUR-1**" refers to "Establish Sources Conformance Criteria Reference 1".

Notes:

- In the Verified Person criteria, Subject always refers to a Subject that is a Person. Criteria for Organizations and Machines that are to be verified as Subjects are dealt with in other PCTF components, such as the Verified Organization component.

- Baseline Conformance Criteria, which apply regardless of which Trusted Process a Responsible Authority is implementing, are included as part of this conformance profile.
- Level of Assurance 4 for Identity is out of scope for this version. The column is included as a placeholder for future development.

Reference	**Conformance Criteria**	**Level of Identity Assurance**				
BASE	**Baseline**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference v1.4**

1	The Responsible Authority **MUST** document a current overall description of the program or service, including:
	• Purpose statement
	  ○ The service function(s) (ie authentication, proofing, verification, etc.).
	  ○ The audience that is impacted (ie general public, subset, etc.).
	  ○ The related industries (all, healthcare, finance, etc.).
	• Services Description
	  ○ The specific location the solution is managed from.
	  ○ A general marketing overview or description of the service.
	  ○ The types of validation, authentication or technology the service includes:
	  ▪ Biometrics, mobile device integrity, ID doc validation, liveness, risk checks, OTPs, etc..
	  ▪ Service high-level design and/or architecture diagram.
	  ▪ Service user/data flow diagram.
		X	X	X		

2	The Responsible Authority **MUST** document its business role, purpose and authority as these relate to the identification of Subjects.	X	X	X		

3	The Responsible Authority **SHOULD** be a private entity registered and operating in Canada (e.g., proprietorship, corporation) or a public entity (e.g., department, agency or registrar) operating under the authority of a Canadian federal, provincial, or territorial government.	X				IDES.01
4	The Responsible Authority **MUST** be a private entity registered and operating in Canada (e.g., proprietorship, corporation) or a public entity (e.g., department, agency or registrar) operating under the authority of a Canadian federal, provincial, or territorial government.		X	X		IDES.02
5	The Responsible Authority **MUST** provide a reference to the legal authority, policy or requirement that supports the need to collect specific personal information. For example, in Ontario privacy requirements are covered under the Freedom of Information and Protection of Privacy Act (FIPPA) and the Personal Health Information Protection Act (PHIPPA).	X	X	X		
6	If the Responsible Authority relies on or supports another organization for carrying out the Identity establishment process, a written agreement, or supporting legislation or regulations **MUST** be in place.	X	X	X		
7	The Responsible Authority **SHOULD** provide Users with written notice that any false or misleading statements may result in a violation of terms or conditions.	X				
8	The Responsible Authority **MUST** provide Users with written notice that any false or misleading statements may result in violation of terms or conditions.		X	X		

9	If a Responsible Authority relies on another organization to carry out a Verified Person Trusted Process subject to the Verified Person conformance criteria, the Responsible Authority **MUST** provide: • Documentation on written agreement for the arrangement in effect; AND • Documentation on the approved Conformance Criteria assessment.	X	X	X		
10	If cases involve children, minors, and other vulnerable Subjects, the Responsible Authority **SHOULD**: • Have in place additional safeguards, compensating factors, or a documented exception process to reduce risk and to initiate interventions, as appropriate. • Confirm that the applicant (for example, a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor, or other vulnerable Subject.	X	X			IDDG.11
11	If cases involve children, minors, and other vulnerable Subjects, the Responsible Authority **MUST**: • Have in place additional safeguards, compensating factors, or a documented exception process to reduce risk and to initiate interventions, as appropriate. • Confirm that the applicant (for example, a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor, or other vulnerable Subject.			X		IDDG.11
12	Organizations and individuals **MUST** comply with applicable legislation, regulations, and policy within their jurisdiction, which are subject to change.	X	X	X		

13	The Responsible Authority **SHOULD** provide Users with a written notice requiring them to notify the Responsible Authority of changes to a Subject's information whenever it changes.	X				
14	The Responsible Authority **MUST** provide Users with a written notice requiring them to notify the Responsible Authority of changes to a Subject's information whenever it changes.		X	X		
SOUR	**Establish Sources**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference v1.4**
Establish Sources is the preparatory process undertaken to determine which sources of Identity Evidence can be used to validate and/or verify a Person (i.e., Subjects), and the assurance of those sources. Typically, a Digital Identity system will use a range of sources to support the requirements to identify Subjects in a given context, and to meet the target Levels of Assurance. Note: These criteria are not included in the Public Sector Profile (IMSC), as they are part of the policy and/or legislated requirements of the Relying Party.						
1	If appropriate, the Responsible Authority **MUST** conform to their legislated mandate for holding the information for which they are being identified as a source. The Responsible Authority **MUST** have appropriate security, accuracy, completeness and privacy of their Identity sources, and determine: • The provenance of the Evidence. • The robustness of the processes employed in collecting and storing the Evidence. • The historic performance of the source. • The ability of the source to satisfy relevant regulatory authorities. • The recognition of the source in law.	X	X	X		IDED.03

2	If the Responsible Authority uses an external source of Identity Evidence, the external source of Identity **MUST**: • Hold a recognized DIACC Verified Person Verification Trustmark, OR • Undergo an explicit assessment by the Responsible Authority.	X	X	X		IDED.04
3	A source of Identity Evidence **MUST** be assessed as Low Assurance if: • it is not possible to establish the provenance of the Evidence or the processes employed in collecting and storing the Evidence employed by the source.	X	X	X		
4	A private-sector source of Identity Information **MUST** be assessed as Medium Assurance only if: • the provenance of the data, and processes employed by the source, can be audited and deemed to be satisfactory by the appropriate governance bodies or regulators, OR • in the case of a statistical source, where the ongoing accuracy of the source can be demonstrated from historical performance data.	X	X	X		
5	A public sector source of Identity Information **MUST** be assessed as Medium Assurance only if: • the provenance of the data, and processes employed by the source, can be audited and deemed to be satisfactory by the appropriate governance bodies or regulators, OR • it is a Foundational Source of Identity (refer to definition in Overview).	X	X	X		

RESO	**Identity Resolution**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference v1.4**
Identity Resolution is the process of establishing the uniqueness of a Subject within a program/service population through the use of Identity Information. A program or service defines its Identity resolution requirements in terms of Identity Attributes; that is, the program/service specifies the set of Identity Attributes that is required to uniquely identify a Subject within its population.						
1	The Responsible Authority **MUST** document the population or clientele for which its services are currently provided.	X	X	X		
2	The Responsible Authority **MUST** ensure that the authoritative record uniquely resolves to only one Subject within their specified population of interest.		X	X		IDRE.01
3	The set of Identity Attributes **MUST** be sufficient to distinguish between different Subjects within an Identity context; and sufficient to describe the Subject as required by the service or program. (See section 4.1.4 of Government of Canada Directive on Identity Management (July 2019)).	X	X	X		
ESTAB	**Identity Establishment (Contextual)**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference v1.4**
Identity Establishment is the process of creating contextual Identity Evidence that may be relied on by others for the delivery of programs, services, and activities. Note: The establishment and maintenance of Foundational Evidence of Identity is out of scope, as it is the exclusive domain of the public sector; those criteria can be found in the Public Sector Profile of the Pan-Canadian Trust Framework.						
1	Any transaction relating to the creation of a Verified Person Record MUST be auditable and reference a relevant business event or activity.	X	X	X		IDES.05
2	The Responsible Authority **MUST** justify and document the need to collect the specific Identity Information that is required to fulfill the stated business purposes.	X	X	X		IDES.05

3	The Responsible Authority **MUST** have in place policies and procedures to safeguard the Identity Attribute(s) provided by the User.	X	X	X		IDDG.05
4	The Responsible Authority **MUST** document policies and procedures to detect and respond to the use of a User's Identity Attribute(s) without their consent.		X	X		IDDG.06
VALID	**Identity Information Validation**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference v1.4**
Identity Information Validation is the process of confirming the accuracy of Identity Information about a Subject against that established by an Authoritative Source. Identity Information Validation relies on the Evidence obtained from the Establish Sources process to determine the claimed Identity Information exists and is valid.						
1	Self-assertion of Identity Information made by a Subject **SHOULD** be accepted.	X				IDIV.01
2	Identity Information **MUST** acceptably match the assertion provided by the User and all instances of (Foundational and/or contextual) Evidence of Identity presented by the User.		X	X		IDIV.04
3	The required evidence, if any, **MAY** include low assurance sources.	X				
4	The required evidence **MUST**, at a minimum, include medium assurance sources and **MAY** be supported by low assurance sources.		X			
5	The required evidence **MUST**, at a minimum, include the use of high assurance sources and **MAY** be supported by medium and low assurance sources.			X		
6	The Responsible Authority **SHOULD** check the Evidence to confirm that it corresponds to the claimed Identity Information, and that the Evidence exists and is valid.	X				
7	The Responsible Authority **MUST c**heck the Evidence to confirm that it corresponds to the claimed Identity Information, and that the Evidence exists and is valid.		X	X		

8	The Responsible Authority **MUST** document how differences between the Evidence and the claimed Identity Information relate to their risk tolerance at each Level of Assurance. For example, a specific Responsible Authority might conclude that a difference in telephone numbers presents a low risk to them in cases where all other evidence is identical to the claimed Identity Information.	X	X	X		
9	The level of risk resulting from differences between the Evidence and the claimed Identity Information that is acceptable **MAY** be determined by the Responsible Authority.	X				
10	The level of risk resulting from differences between the Evidence and the claimed Identity Information that is acceptable **MUST** conform with the requirements of regulated industry services, if applicable.		X			
11	The level of risk resulting from differences between the Evidence and the claimed Identity Information that is acceptable **MUST** be minimal and documented.			X		
12	Contextual Evidence of identity **MUST** be confirmed as originating from the issuing authority. If confirmation from issuing authority is not feasible, then contextual Evidence of Identity **MUST** be confirmed using a trained examiner.		X	X		IDIV.05
13	Foundational Evidence of Identity **MUST** be confirmed as originating from issuing authority, who has validated the Identity Information using an authoritative record, or allows the Relying Party to validate the Identity Information at the Authoritative Source. If confirmation from originating authority or validation at source is not feasible, then Foundational Evidence of Identity **MUST** be confirmed using trained examiner.		X	X		IDIV.06
14	The Responsible Authority **MUST** ensure that the sources and technology used to perform the validation process are documented and are appropriate within the context of the validation process.	X	X	X		

15	Where Evidence is presented in the form of physical documents that are not verifiable cryptographically, then Evidence checking **SHOULD** employ best practices for fraudulent document detection.	X				
16	Where Evidence is presented in the form of physical documents that are not verifiable cryptographically, then Evidence checking **MUST** employ and document a fraud detection regimen specific to the document(s) under evaluation.		X	X		
17	Where Evidence is digital (including API-based and digital certificate-based) appropriate processes **SHOULD** be employed to ensure the integrity of the Evidence. (e.g., Tamper-evident, cryptographically signed, machine-verification of a Credential).	X				
18	Where Evidence is digital (including API-based and digital certificate-based) appropriate processes **MUST** be employed to ensure the integrity of the evidence (e.g., Tamper-evident, cryptographically signed, machine-verification of a Credential). Information provided in the Credentials and Infrastructure profiles may provide further guidance for these criteria.		X	X		
EVID	**Evidence Validation**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference v1.4**
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).						
1	There is no restriction on what kind of Evidence an Organization accepts.	X				IDEA.02
2	One instance of Evidence of Identity (contextual or foundational) **MUST** be assessed to be at least a medium level of assurance per SOUR criteria.		X			IDEA.03
3	Two instances of Evidence of Identity (at least one must be Foundational Evidence of Identity) **MUST** be assessed to be at least a medium level of assurance per SOUR criteria.			X		IDEA.04

4	Foundational Evidence **MUST** originate from an Authoritative Source that is under the control of a federal, provincial or territorial government or the local equivalent abroad; and used to maintain registration of specific vital events or to determine legal status. Acceptable Authoritative Sources, records and documents for Foundational Evidence: • Vital statistics records used in the issuance of birth certificates; • Legal status records used in the issuance of citizenship and naturalization certificates and permanent resident cards; and • Other authoritative records enabled by departmental legislation.		X	X		IDEA.05
5	Foundational Evidence of Identity Information that is incomplete or inconsistent with the information provided by the User (e.g., name, date of birth, or sex difference) **SHOULD** require additional confirmation by the Authoritative Source, or additional contextual Evidence.		X			IDEA.05
6	Foundational Evidence of Identity Information that is incomplete or inconsistent with the information provided by the User (e.g., name, date of birth, or sex difference) **MUST** require additional confirmation by the Authoritative Source.			X		IDEA.05

7	Contextual Evidence **MUST** originate from an Authoritative Source that is under the control of an Organization that is PCTF approved, or has jurisdictional or domain equivalent, or has undergone an explicit assessment by the Responsible Authority. Acceptable Authoritative Sources, records and documents for contextual Evidence may include: • Licensing and registration records or documents used in the issuance of a driver's licence; • Passport or Certificate of Indian Status; and • Accredited professional organizations used in the issuance of professional credentials.		X	X		
8	If contextual Evidence is accepted in conjunction with Foundational Evidence of Identity (Level 3): • Contextual evidence of identity is expected to be consistent with the information that is provided by the foundational evidence of identity. • Additional contextual evidence **MAY** be required in the case of incomplete or inconsistent identity information (e.g., name change). • An endorsement or certification **MAY** be required to verify that the contextual evidence is a true copy of an original.		X	X		
PRES	**Identity Presentation**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference v1.4**
Identity Presentation is the process of dynamically confirming that a Subject has a continuous existence over time (i.e., “genuine presence”). This process can be used to help detect fraudulent activity (past or present) and to address identity spoofing concerns.						
	Conformance criteria for Identity Presentation will be included in a future release of the PCTF.					

VERIF	Identity Verification	L1	L2	L3	L4	Public Sector Profile Reference v1.4
Identity Verification is the process of confirming that the Identity Information being presented relates to the Subject who is making the claim. It should be noted that this process may use personal information that is not related to identity.						
1	The Responsible Authority **MAY** undertake the verification steps it deems necessary, if any.	X				IDVE.01
2	The Responsible Authority **MUST** ensure that interactions within a given context can be linked to the Subject who is making the claim.		X	X		IDVE.02
3	The Responsible Authority **MUST**, at a minimum, verify the Subject (e.g. knowledge-based verification or contextual data). The verification **MUST** provide sufficient assurance that only the identifiable Subject in question would be able to successfully complete the verification process.		X			IDVE.03
4	The Responsible Authority **MUST** use at least one of the following methods to ensure the Identity Information relates to the User and the Subject: • Biological (e.g., photo ID), biometric (e.g.: fingerprint), or behavioural characteristic confirmation. • Face-to-face verification in person (or equivalent). • Physical possession confirmation. If the above methods are not feasible then alternative methods **MUST** be defined and documented in an exception process which **MAY** include: • Confirmation by a trusted referee (e.g., guarantor, notary, certified agent) as determined by program-specific criteria. • Additional safeguards. • Compensating factors.			X		IDVE.03

5	In addition to the conditions specified in the BASE section concerning vulnerable subjects, private and government organizations **MAY** include Evidence of Identity requirements for a parent or guardian as part of the Evidence of Identity requirements for a child, minor or other vulnerable Subject. For example, the passport of a parent could be used as contextual Evidence of Identity for the child.	X	X	X		IDEA.07
MAINT	**Identity Maintenance**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference v1.4**
Identity Maintenance is the process of ensuring that Identity Information is as accurate, complete, and up-to-date as is required. This process deals with events that may impact 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).						
1	The Responsible Authority **MAY** deem the Subject to be no longer verified if any one of the following are true: • Any contextual Evidence changes. • The status of the Foundational Evidence changes. This could include immigration, marriage, death or the status changes that impact the previous Identity Information Validation and Identity Verification processes. • The elapsed time since the Identity Information Validation or Identity Verification processes were performed exceeds a threshold specified by the Relying Party.	X				

2	The Responsible Authority **MUST** not represent a Subject as verified to an RP if the RA becomes aware of any of the following for a Subject: • Any contextual Evidence changes. • The status of the Foundational Evidence changes. This could include immigration, marriage, death or the status changes that impact the previous Identity Information Validation and Identity Verification processes. • The elapsed time since the Identity Information Validation or Identity Verification processes were performed exceeds a threshold specified by the Responsible Authority.		X	X		
3	The Responsible Authority **MAY** perform additional checks to re-validate or re-verify the Subject. In some cases, these checks may be a subset of the Identity Information Validation and Identity Verification processes. In all cases, sufficient checks **MUST** be performed to ensure that the full Identity Resolution, Identity Information Validation, and Identity Verification requirements are upheld, for the Level of Assurance in question.	X				
4	The Responsible Authority **SHOULD** perform additional checks to re-validate or re-verify the Subject. In some cases, these checks may be a subset of the Identity Information Validation and Identity Verification processes. In all cases, sufficient checks **MUST** be performed to ensure that the full Identity Resolution, Identity Information Validation, and Identity Verification requirements are upheld, for the Level of Assurance in question.		X			

5	The Responsible Authority **MUST** perform additional checks to re-validate or re-verify the Subject. In some cases, these checks may be a subset of the Identity Information Validation and Identity Verification processes. In all cases, sufficient checks **MUST** be performed to ensure that the full Identity Resolution, Identity Information Validation, and Identity Verification requirements are upheld, for the Level of Assurance in question.			X		
6	When the Responsible Authority becomes aware of any changes to Identity Information resulting from Birth or Death events it **SHOULD** correct or update the Subject's record(s) (in accordance with applicable legislation or regulations)	X				
7	When the Responsible Authority becomes aware of any changes to Identity Information resulting from Birth or Death events it **MUST** correct update the Subject's record(s) (in accordance with applicable legislation or regulations).		X	X		
8	Any changes to Foundational Identity information **MUST** be confirmed by a foundational authority for the related event for: • Name change. • Death.		X	X		IDMA.04
9	Birth and Death events **SHOULD** result in notification to Relying Parties.		X	X		
10	When the Responsible Authority becomes aware of any validated changes to Identity Information, it **SHOULD** update the Subject's record(s).	X	X			
11	When the Responsible Authority becomes aware of any validated changes to Identity Information, it **MUST** update the Subject's record(s).			X		

7. References

This section lists the external standards, guidelines, and other documents referenced in the PCTF Verified Person component.

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

The PCTF Verified Person Component has taken guidance from, and is based in part on, the following standards and guidance documents:

1. Government of Canada. Treasury Board Secretariat. *Directive on Identity Management*. 2019. < https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577>
2. Government of Canada. Treasury Board 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>
3. Joint Councils of Canada. Identity Management Sub-Committee. *Public Sector Profile of the Pan-Canadian Trust Framework Version 1.0 Recommendation) Draft).* 2019. <https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_0>

8. Revision History

Version	Date of Issue	Author(s)	Description
0.01	2018-06-08	PCTF Editing Team	First attempt of the Verified Person Component Overview Community Draft. Work in progress
0.02	2019-09-17	PCTF Editing Team	Updated draft as per Verified Person Design Team based on standardized PCTF component outline
0.03	2019-11-12	PCTF Editing Team	Consolidated latest revisions from Verified Person Design Team meetings
0.04	2019-11-21	PCTF Editing Team	Updated trusted process diagram and associated text for consistency
0.05	2019-11-26	PCTF Editing Team	Replaced supporting identity with contextual identity as per PCTF Model
0.06	2020-01-13	PCTF Editing Team	Updated to resolve outstanding wiki comments
0.07	2020-01-17	PCTF Editing Team	Updated as per January 14 Verified Person Design meeting, and final general edit before review
0.08	2020-02-14	PCTF Editing Team	Updates after February 12th Verified Person Design meeting to review TFEC comments
1.0	2020-02-24	PCTF Editing Team	Approved as Draft Recommendation V1.0
1.1	2020-05-29	PCTF Editing Team	Updated in response to public review
1.0	2020-07-02	PCTF Editing Team	Final Recommendation V1.0
1.0	2020-02-24	PCTF Editing Team	Approved as Draft Recommendation V1.0.
1.1	2021-10-29	PCTF Editor and Verified Person Design Team	Updated in response to public comments and reviewed for auditability.
1.1	2021-11-10	PCTF Editor and Verified Person Design Team	TFEC approves as a Candidate for Final Recommendation V1.1.

1.2	2022-02-11	PCTF Editor and Verified Person Design Team	Updated in response to comments from public review.
1.2	2022-03-02	PCTF Editor and Verified Person Design Team	TFEC approves as a Candidate for Final Recommendation V1.2.
1.2 Errata	2022-03-09	PCTF Editor	Updated Public Sector PCTF Profile mappings from v1.3 to v1.4: • Added: SOUR-1 mapping to IDED.03 • Added: SOUR-2 mapping to IDED.04 • Changed: EVID-6 mapping to IDEA.05 from IDEA.06 • Changed: VERIF-5 mapping to IDEA.07 from IDVE.03 Added: ESTAB-2 mapping to IDES.05
1.2 Errata	2022-03-21	PCTF Editor and Verified Person Design Team	Approved as Final Recommendation V1.2 Errata through DIACC Sustaining Member Ballot