PCTF Verified Person Component Overview

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.

This document is provided "AS IS," and no DIACC Participant makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third-party intellectual property rights, and fitness for a particular purpose. Those who are seeking further information regarding DIACC governance are invited to review the DIACC Controlling Policies.

IPR: DIACC-Intellectual Property Rights V1.0 PDF | © 2020

Table of Contents

1 Introduction to the Verified Person Component

This document provides an overview of the PCTF Verified Person Component, a component of the Pan-Canadian Trust Framework (PCTF). For a general introduction to the PCTF, including contextual information and the PCTF goals and objectives, please see the PCTF Model Overview.

Each PCTF component is made up of two documents:

1. **Overview** – Introduces the subject matter of the component. It provides information essential to understanding the Conformance Criteria of the component. This includes definitions of key terms, concepts, and the Trusted Processes that are part of the component.
2. **Conformance profile** – Specifies the Conformance Criteria used to standardize and assess the integrity of the Trusted Processes that are part of the component.

This overview provides information related to and necessary for consistent interpretation of the PCTF Verified Person Conformance Profile.

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 2 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.

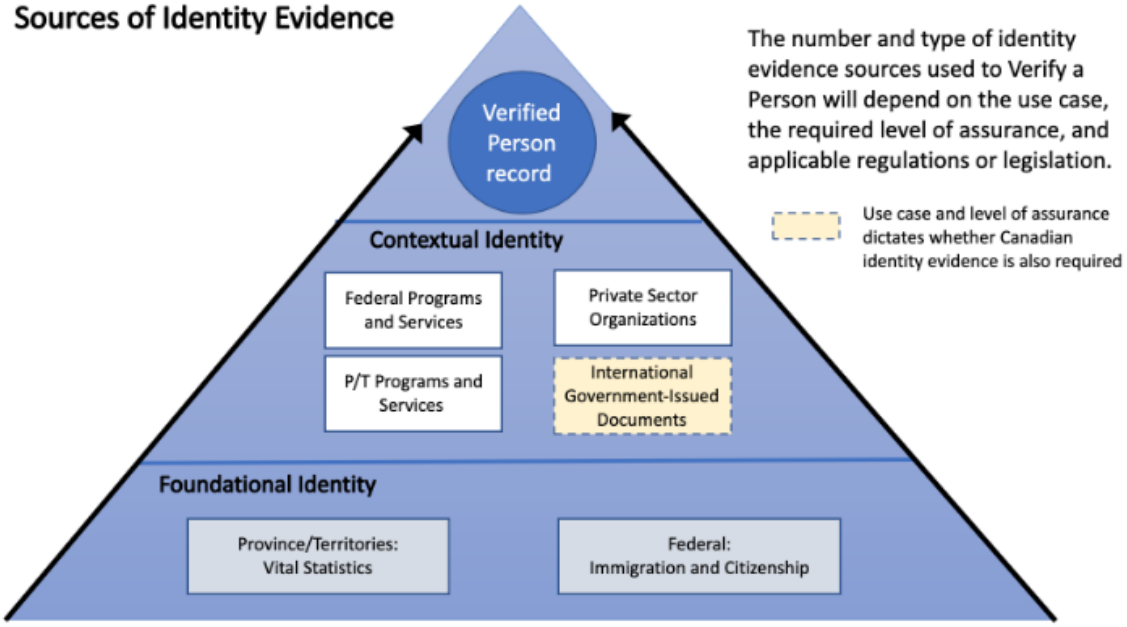

Figure 1. Source of Identity Evidence

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.

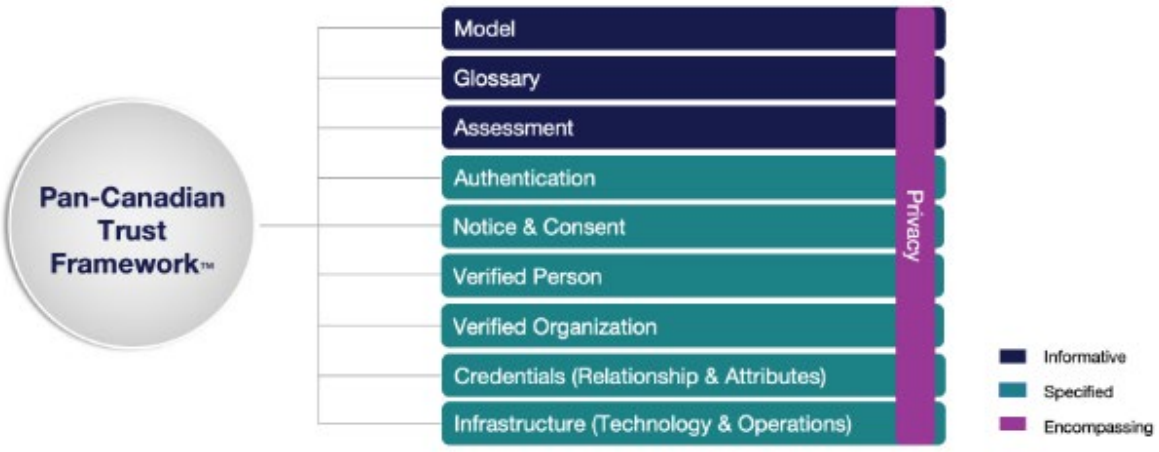

Figure 2. Components of the draft Pan-Canadian Trust Framework

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.

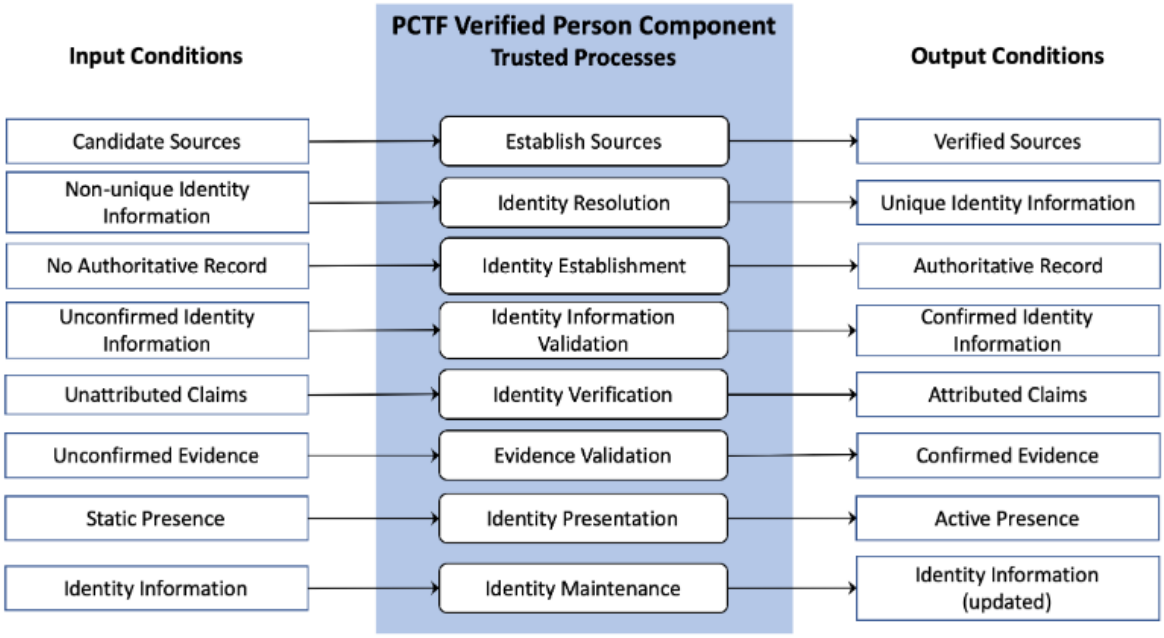

Figure 3. Verified Person Component

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 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>

5 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