PCTF Verified Person Component Overview Draft Recommendation V1.0

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

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

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

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 individuals 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 by that same person, and can be relied on to 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 on-going integrity of processes used to verify an individual's digital identity for an online service or transaction. 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.
- Minimize the opportunity for identity theft and fraud

All participants will benefit from:

- Repeatability and continuity in the identification processes that they offer or on which they depend.

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 transform an unverified person to verified person, in a manner that can be relied on or trusted. A verified person is a real, unique and identifiable human being; and within the PCTF context such a person can be subject to legislation, policy, or regulations within a context. These processes ensure that an individual has been properly verified, and that they are the person who requested to receive services or conduct transactions. Note: A person who is deceased no longer can be verified as a person, but may still have a digital identity with an attribute indicating a deceased status.

2. **Creating a trusted digital identity for a person**: The processes to establish and maintain a digital record for a verified person. This digital record is separate from the verified person. The processes ensure that a digital record of a person is properly created, used exclusively by that same person, and can be relied on for online transactions. Also referred to as a Verified Person record.

There are potentially several ways to verify a person to confirm that someone is a "real, unique and identifiable human being". Examples could include:

- Requiring the user to present official documents (e.g., passport) and confirming that the user is the same person.
- Requiring the user to provide sufficient biometric data that allows them to be distinguished uniquely from the rest of the population.
- Capturing a digital identity from the user's device and using behavioural data to determine that device is in the user's possession.

Whether any of these is appropriate will be determined by the requirements of the relying parties that wish to consume the resultant digital identities. This will vary between sectors and use cases.

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 identity evidence 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 a verified person record (i.e. a trusted digital representation)
- Updating and/or managing a verified person record (i.e. 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 identity evidence. The establishment and maintenance of foundational identity evidence is the exclusive domain of the public sector, specifically 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. They may be referenced indirectly to establish foundational or contextual sources of identity. Example use cases that may rely only on international evidence of identity to qualify for a service include loyalty reward services, or purchasing or renting property; these 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 citizenship status, 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, but will be considered for future versions:

- 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)

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 or legislation. For example, a public sector use case 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 passports 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 and privacy requirements)

Note: Not all international government-issued documents are acceptable - this depends on the country and identity attributes in question.

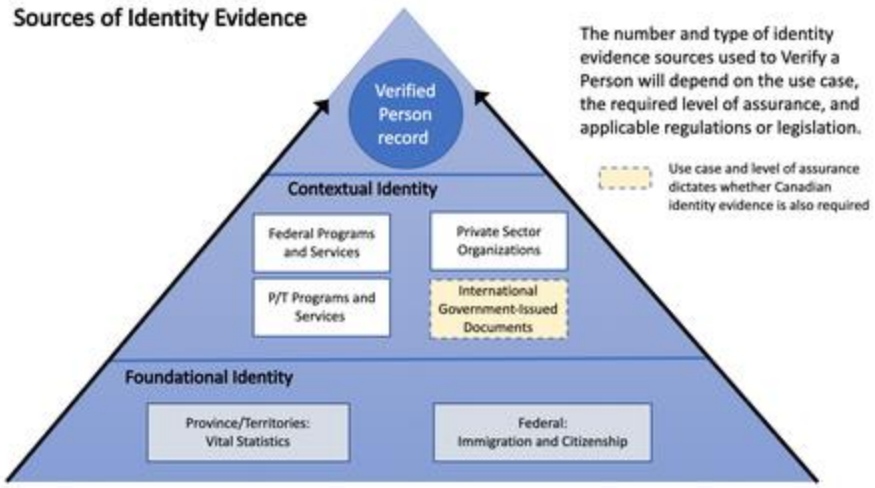

Figure 1. Source of Identity Evidence

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 accuracy of identity information requirements.
- For privacy and security reasons, such as protecting the identities of individuals, some identity attributes may be randomly assigned identifiers, pseudonymous identifiers, user identifiers or usernames.
  Examples of identity information are name, date of birth, and sex, for individuals; business registration numbers, for organizations; and serial numbers and network identifiers, for telecommunications and computing devices.
- 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 owing to privacy considerations or legislation.
- Existing or previously assigned identifiers that meet the uniqueness requirement may be used as identity information. Government 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

For purposes of the Verified Person component, terms and definitions listed in the PCTF Glossary, as well as and the following terms and definitions apply.

- **Verified person** – Knowing (or having a degree of certainty) that a human being is real, unique and identifiable, and has truthfully claimed who they are.

- **Unverified person** – Anyone who does not meet [the above] conditions.

- **Verified Person Record** – A digital record (e.g., anonymous identifier such as a DID, the set of identity attributes, account number) that represents that a person has been verified in a given context. Also referred to in PCTF as a trusted digital representation.

- **Foundational evidence of identity** – Identity evidence that is directly tied to a specific foundational Event Type, and are established exclusively by the public sector, specifically the Vital Statistics organizations of the Provinces and Territories, and Immigration, Refugees, and Citizenship Canada.
  From Government of Canada *Standard on Identity and Credential Assurance, Appendix A*: “establishes core identity information such as given name(s), surname, date of birth,

sex and place of birth. Examples are records of birth, immigration and citizenship, from a vital statistics agency or immigration authority."

- **Contextual evidence of identity –** Identity evidence that is used for a specific purpose within a specific context (e.g., first name, last name, home address, bank account). Also referred to as "supporting evidence of identity" From Government of Canada *Standard on Identity and Credential Assurance, Appendix A*": corroborates the foundational evidence of identity and assists in linking the identity information to an individual. It may also provide additional information such as a photo, signature or address. Examples are social insurance records; records of entitlement to travel, drive or obtain health insurance; and records of marriage, death or name change originating from a jurisdictional authority"

- **Event Type** – A happening in the life of a Person that may trigger one or more Verified Person Trusted Processes. Foundational event types include birth, legal name change, death, immigration, legal residency, citizenship.

- **Subject** – In the context of Verified Person, Subject always refers to a Person. Also, note that Delegated Authority, where a person is acting on behalf of a Subject is not addressed in this version.

2.2 Abbreviations

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

- LOA – Level of Assurance
- PCTF – Pan-Canadian Trust Framework
- P/T – Provinces and Territories

2.3 Roles

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

The following Roles are referenced as part of the scope and processing of the PCTF Verified Person component.

1. **Relying Party** – An organization or person who consumes digital identity information created and managed by other Participants to conduct digital transactions with Subjects.
2. **Responsible Organization** – Participant (i.e., PCTF compliant organization) that provides 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. Similar to the Responsible Authority role in the PCTF Verified Organization component.
3. **Authoritative Party** – A Participant (i.e., PCTF compliant organization) that provides an assurance of the accuracy of Identity Information or Identity Evidence to Relying Parties.

4. **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.

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 an individual. The conformance criteria for Verified Person are profiled in terms of Levels of Assurance for identity. A level of assurance reflects the relative stringency of the conformance criteria and is used to convey a relative degree of confidence which may be accepted for use by a relying party. The table below lists the three levels of assurance defined in existing trust frameworks, and are applied to the PCTF Verified Person conformance criteria. As noted in the Scope section, this version of the PCTF Verified Person Component does not define Conformance Criteria for LOA 4 for identity and its associated use cases. However, the PCTF acknowledges the existence of LOA 4 and has included it as a placeholder for future versions.

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	**Qualification 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 of Identity Assurance	Qualification Description
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 Qualification Description

Each Level of Assurance may be further refined by a qualifier. For example, a Relying Party in the health care sector may specify the requirement for an LOA3 authentication credential, with a qualifier indicating the authenticator must be issued from a health care provider.

Note

- This version of the PCTF Verified Person Component does not define Conformance Criteria for LOA 4. However, the PCTF acknowledges the existence of LOA 4 and has included it as a placeholder for future versions.

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 *conformance crit*eria. 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.

A single organization may not be responsible for carrying out all the Verified Person trusted processes. It may be the case that several organizations are involved in carrying out the trusted processes (instead of just one organization). The involvement of several organizations may introduce complexity in the assessment and certification process.

More information on trusted processes and conformance criteria is available on diacc.ca

3.1 Conceptual Overview

The Verified Person Component defines a set of processes used to establish that a natural 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 establish a set of conformance criteria against which the process of person verification 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.

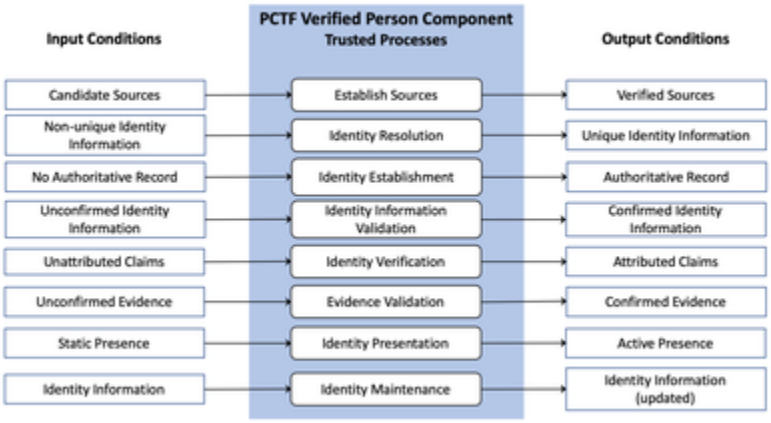

Figure 3. Verified Person Component

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 a person (i.e., a Subject), 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.

354a	Inputs	• Candidate Sources	The sources proposed to be used in the Identity Information Validation and Identity Verification processes.
354b	Outputs	• Verified Sources	The vetted sources to be used in the Identity Information Validation and Identity Verification processes.
354c	Dependencies	None	
354d	Additional Information		

3.3 Identity Resolution

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, it specifies the set of identity attributes that is required to uniquely identity a Subject within its population.

361a	Inputs	• Non-unique Identity Information	The set of identity attributes available to uniquely identify the Subject within the population in question.
361b	Outputs	• Unique Identity Information	The set of identity attributes needed to uniquely identified from the population in question has been established.
361c	Dependencies	• Establish Sources	

361d	Additional Information		

362

363 3.4 Identity Establishment

364 Identity Establishment is the process of creating identity evidence (record of identity) within a
365 program/service population that may be relied on by others for subsequent programs, services,
366 and activities.

366a	Inputs	• No Record of Identity	No identity evidence for a Subject (record of identity) exists within a program/service population.
366b	Outputs	• Record of Identity	Identity evidence for a Subject (record of identity) exists within a program/service population.
366c	Dependencies	• Identity Resolution	
366d	Additional Information		

367 3.5 Identity Information Validation

368 Identity Information Validation is the process of confirming the accuracy of identity information
369 about a Subject against that established by an authoritative party. The Identity
370 Information Validation relies on the evidence obtained from the sources confirmed in Establish
371 Sources to determine the claimed identity information exists and is valid. Note that this process
372 does not ensure that the Subject is using their own identity information – only that the identity
373 information that the Subject is using is accurate when compared to the identity evidence from an
374 authoritative source.

374a	Inputs	• Unconfirmed identity information	The identity information about the Subject prior to it being validated against an authoritative source.
374b	Outputs	• Confirmed identity information	The identity information about the Subject validated against an authoritative source.
374c	Dependencies	• Establish Sources	
374d	Additional Information		

3.6 Identity Verification

Identity Verification is the process of confirming that the identity information being presented is under the control of the Subject. 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 Subject to determine that the claimed identity belongs to the Subject making the claim.

380a	Inputs	• Unverified Control	The identity information has not been verified as being under the control of the Subject.
380b	Outputs	• Verified Control	The identity information has been verified as being under the control of the Subject.
380c	Dependencies	• Identity Information Validation	
380d	Additional Information		

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).

384a	Inputs	• Unconfirmed Identity Evidence	The evidence of identity has not been confirmed as being an admissible proof.
384b	Outputs	• Confirmed Identity Evidence	The evidence of identity has been confirmed as being an admissible proof.
384c	Dependencies	• Establish Sources	
384d	Additional Information		

Identity Presentation

Identity Presentation is the process of dynamically confirming that a person has a continuous existence over time (i.e., “genuine presence”). This process can be used to ensure that there is no malicious or fraudulent activity (past or present) and to address identity spoofing concerns.

388a	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)
388b	Outputs	• Active Presence	The identity (i.e., Verified Person record) exists continuously over time in association with many transactions
388c	Dependencies	• Identity Validation • Identity Verification	
388d	Additional Information		

389 ## Identity Maintenance

390 Identity Maintenance is the process of ensuring that identity information recorded about the
391 person is as accurate, complete, and up-to-date as is required. This process deals with events
392 that may impact the validity of the previously performed Identity Information Validation and
393 Identity Verification (e.g., evidence used to establish the Verified Person has changed, expired
394 or been revoked, which invalidates the Verified Person Record).

394a	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.
394b	Outputs	• Verified Person Record (updated)	The updated, re-validated and re-verified identity information recorded about the person (i.e., verified person record).
394c	Dependencies	• Identity Verification	
394d	Additional Information		

395

396 # 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:

- Directive on Identity Management (July 2019), Government of Canada
- Directive on Identity Management - Appendix A: Standard on Identity and Credential Assurance, Government of Canada
- Public Sector Profile of the Pan-Canadian Trust Framework Version 1.0 Recommendation Draft (July 4th, 2019), IMSC.