**IDENTITY MANAGEMENT**

**SUB-COMMITTEE**

**PAN-CANADIAN TRUST FRAMEWORK – VERIFIED PERSON COMPONENT**

|  |  |
| --- | --- |
| Version: | 0.91 |
| Status: | Revised Draft |
| Date: | 2017-04-26 |
| Security Classification: | UNCLASSIFIED |

Document Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  **Number** | **Date of Issue** | **Author(s)** | **Brief Description** |
| 0.1 | 2016-03-07 | IMSC WG | Initial draft |
| 0.2 | 2016-03-08 | IMSC WG | Revised draft |
| 0.3 | 2016-07-13 | IMSC WG | Revised draft |
| 0.4 | 2016-09-30 | IMSC WG | Revised draft |
| 0.5 | 2017-03-08 | IMSC WG | Revised draft |
| 0.6 | 2017-04-05 | IMSC WG | Revised draft |
| 0.7 | 2017-04-13 | IMSC VP sub-WG | Revised draft |
| 0.8 | 2017-04-21 | IMSC VP sub-WG | Revised draft |
| 0.9 | 2017-04-25 | IMSC VP sub-WG | Revised draft |
| 0.91 | 2017-04-26 | IMSC VP sub-WG | Revised draft |

Table of Contents

[Document Version Control ii](#_Toc480896806)

[Table of Contents iii](#_Toc480896807)

[1 Verified PErson Component Overview 1](#_Toc480896808)

[1.1 Introduction and Purpose 1](#_Toc480896809)

[1.2 Pan-Canadian Approach 1](#_Toc480896810)

[1.3 Pan-Canadian Trust Framework 1](#_Toc480896811)

[1.4 Verified Person Component 3](#_Toc480896812)

[1.5 Verified Person Shared Responsibilities 4](#_Toc480896813)

[1.5.1 Dependency Model 4](#_Toc480896814)

[2 Verified Person Trusted Processes 6](#_Toc480896815)

[2.1 Verified Person Trusted Process Overview 6](#_Toc480896816)

[2.1.1 Overview of Trusted Processes 6](#_Toc480896817)

[2.1.2 Mapping to Existing Identity-Related Processes 6](#_Toc480896818)

[2.2 Trusted Process Definitions 9](#_Toc480896819)

[2.2.1 Identity Resolution 9](#_Toc480896820)

[2.2.2 Identity Establishment (Foundational) 9](#_Toc480896821)

[2.2.3 Identity Issuance (Foundational) 10](#_Toc480896822)

[2.2.4 Identity Establishment (Supporting) 10](#_Toc480896823)

[2.2.5 Identity Issuance (Supporting) 11](#_Toc480896824)

[2.2.6 Identity Validation 11](#_Toc480896825)

[2.2.7 Identity Verification 12](#_Toc480896826)

[2.2.8 Identity Maintenance 13](#_Toc480896827)

[2.3 Trust Framework Adoption 13](#_Toc480896828)

[2.3.1 Verified Person Acceptance Policy 13](#_Toc480896829)

[2.3.2 Pan-Canadian Levels of Assurance 14](#_Toc480896830)

[2.3.3 eIDAS Levels of Assurance 14](#_Toc480896831)

[3 Notes and Assumptions 16](#_Toc480896832)

[4 Glossary 17](#_Toc480896833)

# Verified PErson Component Overview

## Introduction and Purpose

As digital service delivery models evolve, there is an increasing need for trusted digital identities that can be used by individuals across services, programs, sectors and jurisdictional boundaries. Having the right individual with a degree of certainty is especially important for high-value transactions or services such as applying for a passport, receiving social assistance, or opening a bank account.

The purpose of this document is to define and specify the **Verified Person Component** of the **Pan-Canadian Trust Framework**. The Verified Person Component ensures that an individual has been properly verified and ensures that he or she is the right recipient of program, service or transaction.

The Verified Person Component is a key ingredient to a **Trusted Digital Identity** which is 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.

## Pan-Canadian Approach

The Pan-Canadian approach for identity management is an agreement of principles and standards to develop solutions for use by all Canadians regardless where they live or work.[[1]](#footnote-2) This approach recognizes that while there are dependencies and differences between jurisdictions, a seamless and citizen-centric approach to digital service delivery can be achieved by defining agreed upon standards that are implemented and assessed in a consistent manner.

The Pan-Canadian approach allows for a multiplicity of solutions that can be relied on or ‘trusted’ across systems, organizations, and jurisdictional boundaries. Finally, for the user, the Pan-Canadian approach protects privacy, enables choice and convenience to use.

## Pan-Canadian Trust Framework

The Pan-Canadian Trust Framework (PCTF) consists of a set of modular or functional components that can be independently assessed and certified for consideration as trusted components.. Building on the 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. The Pan-Canadian Trust Framework is illustrated in Figure 1,



Figure 1: Pan-Canadian Trust Framework

The framework defines discrete components and processes that are intended to be standardized, assessed, certified to interoperate with one another in a digital identity ecosystem. The high-level components of the PCTF include: **Charter**, **Trusted Digital Identity**, **Trusted Access & Authorization**, **Trustmark Certification** and **Trusted Infrastructure**. Within each high-level component there are defined functional components (e.g., Verified Person, User Sign-In, etc.). These components have been defined in a way that they can be implemented as modular services and be independently assessed for certification as a trusted component.

Once a component is certified, it can be relied on or ‘trusted’ and integrated into a larger trusted digital ecosystem platform. This digital ecosystem is intended to interoperate seamlessly across different organizations, sectors, and jurisdictions, and be interoperable with other trust frameworks. For a detailed overview of the trust framework, please refer to Pan-Canadian Trust Framework Overview[[2]](#footnote-3) published by DIACC

## Verified Person Component

The primary purpose of the Verified Person component is to transform an **unverified person** into a **verified person**, in a manner that can be relied on or trusted. Figure 2 illustrates the Verified Person Component and elements defined within: **inputs**, **outputs**, **trusted processes** and **conformance criteria**.



Figure 2: Verified Person Component

A **verified person** is defined as knowing (or having a degree of certainty) that an individual is *real*, *identifiable*, and has *truthfully claimed* who he or she is. By contrast, an **unverified person** is anyone who does not meet these conditions.

The Verified Person Component defines eight **trusted processes.** Each trusted process has a corresponding set of **conformance criteria** profiled against **levels of assurance.** The conformance criteria are used to standardize, and assess the integrity of a trusted process in relation to specific level of assurance and in accordance with Trustmark and Certification process defined with the Pan-Canadian Trust Framework.

For each trusted process (described in detail in Section 3) there is a corresponding **input** and **output**. These correspond to an existing or desired state that are transformed or achieved by means of a trusted process. For example, having **Unique Identity Information** about an individual(such as a name, date of birth, and numeric identifier) is achieved by meeting the conformance criteria specified for the **Identity Resolution** Process. The existing or input state of **Non-Unique Identity Information** (e.g. name, date of birth only) may require the trusted process to generate and/or assign a unique identifier. Trusted processes are further described in Section 3.

## Verified Person Shared Responsibilities

### Dependency Model

A key requirement of the Verified Person Component is to ensure that an individual exists in the first place. Within the pan-Canadian context, this responsibility is shared amongst the Federal, Provincial and Territorial jurisdictions (vital statistics and immigration). These shared responsibilities is straightforward within a jurisdiction; however complications (or gaps) might arise when an individual has to prove oneself using evidence of identity originating from another jurisdiction.

These shared responsibilities are delineated using the distinction between **foundational evidence of identity** and **supporting evidence of identity** issued by public sector, private sector, and evidence whose origin is international. Figure 3 illustrates the shared responsibilities, or dependencies that existing between jurisdictions, international, and the private sector.



Figure 3: Verified Person Dependency Model

The Verified Person Component has been developed using this model. For example, a province may need to rely on a birth record or certificate issued by another province or territory. Identity-related dependencies generally relate to identity-related events, records, and documents registered, maintained and issued by jurisdictions, and which are used or relied on by many downstream services.

The Verified Person Component, based on the model, relies on *evidence of identity* issued by other jurisdictions (including international) and in certain cases, the private and non-profit sector. By definition, evidence of identity is *a record from an authoritative source (e.g., vital statistics register) that supports the integrity and accuracy of the claims made by an individual (e.g., name, date of birth)*. While today, the majority of evidence of identity is presented in documentary form (paper certificates, secure cards), digital forms of evidence of identity are emerging, such as secure mobile wallets.

Evidence of identity falls into two major categories:

* **Foundational Evidence of Identity** - issued by a government institution relating to the registration of a vital or major life event. Foundational evidence of identity is used to establish core identity information such as given name(s), surname, date of birth and place of birth. Examples of foundational evidence of identity include, but are not limited to birth certificates, permanent resident card, and certificate of citizenship.
* **Supporting Evidence of Identity** - issued by a government institution or a private sector organization. Supporting evidence of identity is used for the purposed of program administration or to facilitate service delivery. Supporting evidence of identity corroborates existing foundational evidence of identity or the corresponding authoritative record. Supporting evidence of identity also assists in linking identity information to a presenting individual. Finally, supporting evidence of identity may provide information in addition to identity information such as an address of residence.

# Verified Person Trusted Processes

## Verified Person Trusted Process Overview

### Overview of Trusted Processes

Trusted processes are crucial building blocks to ensure the integrity of digital services and the overall integrity of the digital supply chain. The integrity of a trusted process is paramount because the output or result of a trusted process is relied on many participants – across jurisdictional and sectoral boundaries, over the short term, and over the long term. The trust framework ensures integrity of a trusted process through agreed upon and well-defined conformance criteria to support an impartial, transparent and evidence-based assessment and certification process.

A trusted process can be defined as any business process or activity (or a set of business processes or activities) that results in a process output upon which others rely.

A trusted process is subjected to a range of conditions, one or several of which are utilized as *an input* to yield an *output condition*. For each trusted process, conformance criteria are defined to ensure that the process is carried out with integrity. For example, a trusted process may involve assigning an identifier to an individual. The conformance criteria may specify that that organization responsible for carrying out the trusted process must ensure that the identifier assigned to the individual is unique for a certain population (e.g. a province)

In relation to the PCTF, an existing business or technical process may be designated as a trusted process that is subject to the conformance criteria, assessment process and certification defined by the trust framework.

### Mapping to Existing Identity-Related Processes

Existing programs or services, such as birth registration or passport issuance, typically have embedded identity-related processes, usually referred to as identity-proofing or identity registration processes.

Identity-related processes that were originally developed to work within a particular context (e.g., registering a birth to create a vital statistics record) may be leveraged and relied on as trusted processes within the Pan-Canadian Trust Framework. This is done by mapping existing processes (or sub-processes) into the trusted process definitions of the Verified Person Component. Once mapped, these processes can be assessed and certified using defined conformance criteria.

Table 1 is intended to assist in mapping the Verified Person trusted process and outputs to existing identity-related processes.

| **Verified Person Component** | | **Identity-Related Processs  (e.g., Existing Identity-Proofing, Identity Registration processes, etc.)** |
| --- | --- | --- |
| **Trusted Process** | **Outputs** |
| Identity Resolution | Unique Identity Information | * There is unique identity information about the individual (e.g. name, date-of-birth, program identifier, etc.)   *Identity resolution requirements are usually met by specifying uniquely identifying biographical or ‘tombstone’ (name, dob) data associated with the individual.* |
| Identity Establishment (Foundational or Supporting) | Authoritative Record (Foundational or Supporting): | * There exists a foundational authoritative record about the individual (e.g. birth or immigration record) * There exists a supporting authoritative record about the individual (e.g. drivers’ licence record)   *Identity establishment requirements (for foundational and supporting) are usually met by creating an authoritative program record such as a birth record, or driver’s licence record.* |
| Identity Issuance  (Foundational or Supporting) | Evidence of Identity (Foundational or Supporting) | * Foundational evidence of identity (e.g., birth certificate) has been issued to, and is under control of the individual. * Supporting evidence of identity (e.g. driver’s license) has been issued to, and is under control of the individual.   *Identity issuance requirements (for foundational and supporting) are usually met by issuing an authoritative document such as a birth certificate, or driver’s licence record.* |
| Identity Validation | Confirmed Identity Information | * Identity information about the individual is confirmed against an authoritative record.   *Identity validation requirements are usually met by visually confirming information presented on physical documents or by means of an electronic identity validation service.* |
| Identity Verification | Claimed Identity Information | * Identity information relates to the individual making the claim.   *Identity verification requirements are usually met by visually comparing traits recorded on a document (e.g. facial photograph, eye colour, height, etc.) or asking the presenting individual questions that only they would know (includes shared secrets, access codes, etc.). Similar methods can be accomplished remotely through electronic means.* |
| Identity Maintenance | Current Identity Information | * Identity information about the individual is up-to-date.   *Identity maintenance requirements are usually met by means of message-based (push) notification service, dates of expiry, validity periods, or regularly-scheduled (pull) validation services.* |

Table 1: Verified Person

Once a business process is decomposed down into the various trusted processes, the requisite conformance criteria can be applied to standardize and assess as trusted processes.

Note: Mapping tools will be developed.

## Trusted Process Definitions

### Identity Resolution

**Description**

Identity resolution is the establishment of the uniqueness of a person 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 achieve identity resolution within its population.

|  |  |
| --- | --- |
| **Inputs** | * **Non-Unique Identity Information:** The identity information is not unique to a particular individual (i.e., the identity information may resolve to two or more individuals). |
| **Outputs** | * **Unique identity information**: The identity information is unique to a particular individual (i.e., the identity information resolves to one and only one individual). |
| **Dependencies** | * None specified |
| **Additional Considerations** | * None specified |

### Identity Establishment (Foundational)

**Description**

Identity establishment is the creation of an authoritative record of identity that is relied on by others for subsequent government activities, programs, and services.

|  |  |
| --- | --- |
| **Inputs** | * **No foundational authoritative record:** No foundational authoritative record of identity information. |
| **Outputs** | * **Foundational Authoritative Record:** There exists an authoritative record of identity information. |
| **Dependencies** | * **Unique Identity Information**: Output of **Identity Resolution** trusted process |
| **Additional Considerations** | * None specified |

### Identity Issuance (Foundational)

**Description**

Identity issuance is the creation of foundational evidence of identity that is relied on by others for subsequent government activities, programs, and services.

|  |  |
| --- | --- |
| **Inputs** | * **No foundational evidence of identity:** No foundational evidence of identity. |
| **Outputs** | * **Foundational evidence of identity:** There exists an authoritative record of identity information. |
| **Dependencies** | * **Foundational Authoritative Record:** Output of Identity Establishment (Foundational) trusted process |
| **Additional Considerations** | * None specified |

### Identity Establishment (Supporting)

**Description**

Identity establishment is the creation of a supporting authoritative record of identity that may be relied on by others for subsequent government activities, programs, and services.

|  |  |
| --- | --- |
| **Inputs** | * **No supporting authoritative record:** An authoritative record of supporting identity information does not exist |
| **Outputs** | * **Supporting Authoritative record:** There exists an authoritative record of supporting identity information. |
| **Dependencies** | * **Unique Identity Information**: Output of **Identity Resolution** trusted process |
| **Additional Considerations** | * None specified |

### Identity Issuance (Supporting)

**Description**

Identity issuance is the creation of supporting evidence of identity that is relied on by others for subsequent government activities, programs, and services.

|  |  |
| --- | --- |
| **Inputs** | * **No supporting evidence of identity:** Supporting evidence of identity information does not exist |
| **Outputs** | * **Supporting evidence of identity:** There exists an authoritative record of identity information. |
| **Dependencies** | * **Supporting Authoritative record:** Supporting evidence of identity has been issued. |
| **Additional Considerations** | * None specified |

### Identity Validation

**Description**

Identity validation is the confirmation of the accuracy of identity information about a person as established by an authoritative party. “Identity validation” is equivalent to the term “identity information validation.” It should be noted that identity validation does not ensure that the person is using their own identity information (this is identity verification) – only that the identity information the person is using is accurate and up to date.

|  |  |
| --- | --- |
| **Inputs** | * **Unconfirmed identity information:** The identity information has not been confirmed using an authoritative record |
| **Outputs** | * **Confirmed identity information:** The identity information has been confirmed using an authoritative record. |
| **Dependencies** | * Dependent on type of authoritative record being validated   + **Foundational Authoritative Record:** Output of Identity Establishment (Foundational) trusted process   + **Supporting Authoritative Record:** Output of Identity Establishment (Supporting) trusted process |
| **Additional Considerations** | * Must conform to:   + Pan-Canadian Identity Validation Standard   + Pan-Canadian Information Exchange Specification |

### Identity Verification

**Description**

Identity verification is the confirmation that the identity information being presented relates to the person who is making the claim. It should be noted that identity verification is a separate process from identity validation and may employ different methods and use personal information that is not related to identity.

|  |  |
| --- | --- |
| **Inputs** | * **Unclaimed identity information:** The identity information has not been verified as being claimed by the rightful owner/user of the identity information. |
| **Outputs** | * **Claimed identity information**: The identity information has been verified as being claimed by the rightful owner/user of the identity information. |
| **Dependencies** | * None specified. |
| **Additional Considerations** | * May vary on type of methods used. May be one or several of   + Knowledge-based confirmation   + Biological or behavioural confirmation   + Trusted referee confirmation   + Physical possession confirmation. |

### Identity Maintenance

**Description**

Identity maintenance is the process of ensuring that identity information is as accurate, complete, and up-to-date as is required. Identity maintenance also includes *identity notification* which is the disclosure of identity information triggered by a change in identity information, or an indication that identity information has been exposed to a risk factor. Identity notification is specified in the Pan-Canadian Identity Notification Standard.

|  |  |
| --- | --- |
| **Inputs** | * **Non-current identity information:** The identity information is not up-to-date. |
| **Outputs** | * **Current identity information:** The identity information is up-to-date. |
| **Dependencies** | * May be time-based or event-based |
| **Additional Considerations** | * + Must conform to:     - Pan-Canadian Notification Standard |

## Trust Framework Adoption

### Verified Person Acceptance Policy

Using the PCTF, a relying party, such as a government program or service provider, can develop a **Verified Person Acceptance Policy**.

A Verified Person Acceptance Policy is defined as the set of conditions (rules, conformance criteria, etc.) that determine what is acceptable for use by a relying party. The set of conditions can include, but are not limited to:

* The set of verified person trusted process outputs that together can be relied on (e.g. **Unique Identity Resolution**, **Foundational Authoritative Record**, **Identity Validation**, etc,);
* Evidence that conformance criteria for each trusted process have been met;
* Required level of assurance;
* Additional qualifiers, such as
  + Originating jurisdictions (e.g. provinces, territories, federal, international)
  + Originating sectors (e.g. financial, health, etc.)

A relying party may define its own Verified Person Acceptance Policy, or one that defined by the PCTF (definition is out of scope of this document)

Furthermore, a Verified Person Acceptance Policy may be part of a larger **Trusted Digital Identity Acceptance Policy** that may also include other components, such as:

* Verified Login
* Verified Organization
* Verified Relationship
* Consent
* Binding
* Notice.

### Pan-Canadian Levels of Assurance

The Pan-Canadian Trust Framework defines four levels of assurance specified in Table 2. The levels are used to specify the trusted process conformance criteria in the Verified Person Conformance Profile.

|  |  |
| --- | --- |
| **Level of Assurance** | **Qualification Description** |
| Level 1 | * Little or no confidence required. * Satisfies Level 1 conformance criteria. |
| Level 2 | * Some confidence required. * Satisfies Level 2 conformance criteria. |
| Level 3 | * High confidence required. * Satisfies Level 3 conformance criteria. |
| Level 4 | * Very High confidence required. * Satisfies Level 4 conformance criteria. |

Table 2: Levels of Assurance

### eIDAS Levels of Assurance

European Regulation No 910/2014 on electronic identification and trust services for electronic transactions (known as “eIDAS”) defines three levels of assurance of “low”, “substantial” and “high”.

Note: For recognition into the eIDAS scheme, the Verified Person trusted process conformance criteria may be specified for the eIDAS levels of assurance (future).

# Notes and Assumptions

1. ***A single organization may not be responsible for carrying out all he verified person trusted processes*** It may be the case that several organizations may be carrying out all trusted processes (instead on just one organization). For example, *identity validation* may be the responsibility of a vital statistics registrar, while *identity verification* may be responsibility of a credit bureau. The involvement of several organizations may introduce complexity in the assessment and certification process, but the trust framework does not constrain different implementation approaches.
2. ***A verified person may include personal information that is beyond the scope of identity information.*** There are cases when personal information, in addition to identity information, must be validated and verified. This includes personal information such as citizenship status, address of residency, etc. The focus of the Verified Person Component is identity, but may be expanded to include other personal information.

# Glossary

The definitions that follow include authoritative and working definitions used or developed for the purposes of this document. In the final version, these terms will be added to the consolidated Glossary Document.

| **Term** | **Definition** |
| --- | --- |
| 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 |
|  |  |
|  |  |

1. Available at (public sector registration required): <https://gccollab.ca/file/view/36223/imsc-paper-trusting-identities-consultation-draft-enpdf> [↑](#footnote-ref-2)
2. Available at: <https://diacc.ca/pan-canadian-trust-framework/> [↑](#footnote-ref-3)