PCTF Verified Person Conformance Profile 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.

When reviewing this draft, consider the following and note that responses to these questions are non-binding and serve to improve the Pan-Canadian Trust Framework.

1. Does the list of trusted processes for Verified Person map to processes in your organization or business?
2. Is the scope and description of the trusted processes clear and accurate?
3. Does the terminology align with your domain or sector (e.g., evidence of identity, identity information, identity claim)?
4. Do you agree with the inclusion of Establish Sources process as it is described?
5. Does the Identity Presentation process make sense in the context of Verified Person? and if so, what conformance criteria and/or requirements would make sense to include?
6. Are the conformance criteria clear and measurable?
7. If your organization were to self-assess today, would you comply? If not, what barriers (business, legal, or technical) to compliance can you identify?
8. Are there conformance criteria you would recommend adding, modifying, or removing?

Note

- This is a baseline document specifying criteria intended to apply across sectors; criteria that are specific to a particular sector or industry are included in a sector-specific profile (e.g., Public Sector Profile for PCTF)
- While in draft form, the conformance criteria table includes a cross-reference to the corresponding criteria in the Public Sector Profile of the PCTF. This will be removed in the final version.

Contents

1 Introduction to the PCTF Verified Person Conformance Profile

This document specifies the Conformance Criteria for 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.

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.

2 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 while there may exist valid reasons in particular circumstances to ignore the requirement, the full implications must be understood and carefully weighed

before choosing to not adhere to the conformance criteria or choosing a different option as specified by the conformance criteria.

- **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.

3 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 Organization is implementing, are included as part of this conformance profile.
- Level of Assurance 4 (LOA 4) for identity is out of scope for this version. 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**

102	1	The Responsible Organization **MUST** provide an overall description of the program or service, including: • Type and nature of program or service; • Intended recipients of program or service; • Approximate size, characteristics and composition of the client population.	Y	Y	Y		IDSP-1
103	2	The Responsible Organization MUST specify its business role, purpose and authority as these relate to the identification of individuals.	Y	Y	Y		IDSP-2
104	3	The Responsible Organization **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.	Y				IDSP-6
105	4	The Responsible Organization **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.		Y	Y		IDSP-7
106	5	The Responsible Organization **MUST** make sure that personal information is collected under relevant law or legal authority. If the Responsible Organization relies on or supports another organization for carrying out the identity establishment process, a written agreement **MUST** be in place.	Y	Y	Y		IDSP-4

107	6	The Responsible Organization **SHOULD** provide Subjects with written notice that any false or misleading statements may result in violation of terms or conditions.	Y				IDSP-3
108	7	The Responsible Organization **MUST** provide Subjects with written notice that any false or misleading statements may result in violation of terms or conditions.		Y	Y		IDSP-3
109	8	A Responsible Organization **MAY** rely on another organization to carry out a Verified Person trusted process subject to the Verified Person conformance criteria. If this is the case, the Responsible Organization **MUST**: • Provide documentation on written agreement for the arrangement in effect; **AND** • Provide documentation on the approved conformance criteria assessment;	Y	Y	Y		IDSP-5
110	9	If cases involve children, minors, and other vulnerable individuals, the responsible organization **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 individuals	Y	Y	Y		IDSP-9
111	**SOUR**	**Establish Sources**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference**

112	The 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.						
113	1	The Responsible Organization **MUST** conform to their legislated mandate for security, accuracy, completeness and privacy of their identity sources, and determine: • The origin 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	Y	Y	Y		
114	2	The Responsible Organization **MAY** rely on a recognized independent accreditation of the source of identity evidence instead of conducting their own explicit assessment.	Y	Y	Y		
115	3	The source of identity evidence used in the Verified Person processes **MUST** be assessed as either Low Assurance, Medium Assurance, or High Assurance.	Y	Y	Y		

116	4	A source of identity evidence **MUST** be assessed as Low Assurance if: • it is not possible to establish the provenance of the data or the processes employed in collecting and storing the evidence employed by the source.	Y	Y	Y		
117	5	A source of identity information **SHOULD** be assessed as Medium Assurance only if • the provenance of the data and processes employed by the source can be audited and shown to be satisfactory for the body responsible for regulating the consumer services, OR • in the case of a statistical source, where the ongoing accuracy of the source can be demonstrated from historical performance data.	Y	Y	Y		
118	6	A source of identity evidence **SHOULD** be assessed as High Assurance only if • the origin of the data and processes employed by the source can be audited and shown to be satisfactory for the body responsible for regulating the government services, OR • it is a Foundational Source of Identity (refer to definition in Overview)	Y	Y	Y		
119	**RESO**	**Identity Resolution**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference**

120	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 identity a Subject within its population.						
121	1	The Responsible Organization **MUST** specify the population or clientele for which its services are provided.	Y	Y	Y		IDRE-1
122	2	The Responsible Organization **MUST** ensure that the authoritative record uniquely resolves to only one Subject within their specified population of interest.		Y	Y		IDRE-2
123	3	The set of identity attributes **MUST** be sufficient to distinguish between different individuals within an identity context; and sufficient to describe the individual as required by the service or program. (See section 4.1.4 of Government of Canada Directive on Identity Management (July 2019)	Y	Y	Y		IDRE-3
124	**ESTAB**	**Identity Establishment (Contextual)**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference**
125	Identity Establishment is the process of creating contextual identity evidence that may be relied on by others for delivery of programs, services, and activities. Note: The establishment and maintenance of foundational identity evidence 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.						
126	1	Any transaction relating to the creation of an authoritative record **MUST** be confirmed and reference a relevant business event or activity.	Y	Y	Y		IDES-1
127	2	The Responsible Organization **MUST** record as part of the record of identity only the minimum identity information required for business purposes.	Y	Y	Y		IDES-2

128	3	The Responsible Organization **MUST** have in place policies and procedures to safeguard the identity attribute(s) provided by the individual.	Y	Y	Y		IDES-3
129	4	The Responsible Organization **MUST** have in place policies and procedures to detect and respond to the misuse of the identity attribute(s) provided by the individual.		Y	Y		IDES-4
130	**VALID**	**Identity Information Validation**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference**
131	Identity Information Validation is the process of confirming the accuracy of identity information about a Subject against that established by an authoritative source. The Identity Information Validation relies on the evidence obtained from the Evidence Sources to determine the claimed identity information exists and is valid.						
132	1	Identity information **MUST** acceptably match assertion provided by individual and all instances of (foundational and/or contextual) evidence of identity presented by the individual.		Y	Y		IDVA-1
133	2	The required evidence, if any, **MAY** include low assurance sources.	Y				
134	3	Self-assertion of identity information made by an individual **SHOULD** be accepted.	Y				IDVA-3
135	4	The required evidence **MUST**, at a minimum, include medium assurance sources and **MAY** be supported by low assurance sources		Y			
136	5	The required evidence **MUST**, at a minimum, include the use of high assurance sources **MAY** be supported by medium and low assurance sources.			Y		
137	6	The Responsible Organization **SHOULD c**heck the evidence to confirm that it corresponds to the claimed identity information, is genuine, and not altered.	Y	Y	Y		

138	7	The Responsible Organization **MUST** have a risk-based approach to determine the acceptable level of error, if the evidence obtained does not match the claimed identity information exactly. Level of assurance requirements should be considered when determining what is acceptable. For example, a higher LOA would tolerate minimal error.	Y	Y	Y		
139	8	The level of error that is acceptable **MAY** be determined by the responsible organization.	Y				
140	9	The level of error that is acceptable **MUST** align with the needs of regulated consumer services, if applicable.		Y			
141	10	The level of error that is acceptable **SHOULD** be minimal and limited to, for example, minor formatting and spelling differences where it is clear that the values are semantically the same.			Y		
142	11	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.		Y	Y		IDVA-2
143	12	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.		Y	Y		IDVA-10

144	13	The Responsible Organization **MUST** ensure that the sources and technology used to perform the validation process are understood, and suitable (as per SOUR1-6).	Y	Y	Y		
145	14	Where evidence is presented in the form of physical documents that are not verifiable cryptographically, then evidence checking **MAY** be sufficiently rigorous to detect fraudulent documents.	Y				
146	15	Where evidence is presented in the form of physical documents that are not verifiable cryptographically, then evidence checking **MUST** be sufficiently rigorous to detect fraudulent documents.		Y	Y		
147	16	Where evidence is digital (including API-based and digital certificate-based) appropriate processes **SHOULD** be employed to ensure the integrity of the evidence.	Y				
148	17	Where evidence is digital (including API-based and digital certificate-based) appropriate processes **MUST** be employed to ensure the integrity of the evidence.		Y	Y		
149	**EVID**	**Evidence Validation**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference**
150	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).						
151	1	No restriction on what is provided as evidence	Y				EVAL-1
152	2	One instance of evidence of identity (contextual or foundational)		Y			EVAL-2
153	3	Two instances of evidence of identity (At least one must be foundational evidence of identity)			Y		EVAL-3

154	4	Foundational Evidence **MUST** meet the following acceptability criteria: Evidence originates 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. Identity information that is incomplete or inconsistent with information provided by the individual (e.g., name change) may require additional confirmation by the authoritative source, or additional contextual evidence. Acceptable authoritative sources, records and documents: • 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.		Y	Y		EVAL-5

155	5	Contextual Evidence **MUST** meet the following acceptability criteria: Evidence originates from an authoritative source that is under the control of a PCTF approved organization. If 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. Acceptable authoritative sources, records and documents: • 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.	Y	Y	Y		EVAL-6
156	**PRES**	**Identity Presentation**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference**

157	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 ensure that there is no malicious or fraudulent activity (past or present) and to address identity spoofing concerns.						
158		Conformance criteria for Identity Presentation will be included in a future release of the PCTF.					
159	**VERIF**	**Identity Verification**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference**
160	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.						
161	1	**T**he Responsible Organization **MAY** undertake the verification steps it deems necessary, if any.	Y				IDVE-3
162	2	The Responsible Organization **SHOULD** ensure that interactions within a given context can be linked to the same Subject claiming their own identity information.		Y	Y		IDVE-2
163	3	The Responsible Organization **MUST**, at a minimum, verify the individual remotely, and **MAY** use one of the following methods: • knowledge-based verification • contextual data The verification **MUST** provide sufficient assurance that only the identifiable subject in question would be able to successfully complete the verification process.		Y			

164	4	The Responsible Organization **MUST** use at least one of the following methods to ensure the identity information relates to the presenting individual and for whom the claim applies: • Biological (e.g., photo ID), biometric (e.g.: fingerprint), or behavioural characteristic confirmation • Face-to-face verification in person (or equivalent) If the above methods are not feasible then alternative methods **MUST** be defined and documented in an exception process , which that could include: • Confirmation by a trusted referee (e.g., guarantor, notary, certified agent) as determined by program-specific criteria • Additional safeguards • Compensating factors			Y		IDVE-4
165	5	Children: Private and government organizations **SHOULD** apply the following guideline when providing services to children, minors and other vulnerable individuals: • An organization's policy or government program may decide to include evidence of identity requirements for a parent or guardian as part of the evidence of identity requirements for the child, minor or other vulnerable individual. For example, the passport of a parent could be used as contextual evidence of identity for the child.	Y	Y	Y		IDVE-1

166	**MAINT**	**Identity Maintenance**	**L1**	**L2**	**L3**	**L4**	**Public Sector Profile Reference**
167	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)						
168	1	The Responsible Organization **SHOULD** no longer deem the Subject to be verified if one of the following are true: • Any changes to contextual evidence (i.e., if the authoritative source becomes aware of the changes of identity information) that affects the level of assurance **SHOULD** be captured. • 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 period of time that has elapsed since the Identity Information Validation or Identity Verification processes were performed exceeds a threshold specified by the organization relying on the Verified Person component.	Y	Y	Y		IDMT-1

169	2	The Responsible Organization **MAY** be able to 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.	Y				
170	3	The Responsible Organization **SHOULD** be able to 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.		Y			
171	4	The Responsible Organization **MUST** be able to 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.			Y		

172	5	When the Responsible Organization becomes aware of any changes to identity information resulting from Event Types for Birth, Death and Stillbirth it **MUST** update the authoritative record of the individual (in accordance with local, provincial, or federal law)		Y	Y		IDMT-2
173	6	Any changes to foundational identity information **MUST** be confirmed by a foundational authority for the related Event Types for: • Name change • Death		Y	Y		IDMT-3
174	7	Event Types for Birth, Death and Stillbirth **SHOULD** result in notification to relying parties.		Y	Y		IDMT-4

Table 1: Verified Person Conformance Criteria