



PCTF Verified Person Conformance Profile

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 PCTF Verified Person Conformance Profile..... 3
2 Conformance Criteria Keywords..... 3
3 Verified Person Conformance Criteria..... 4
4 Revision History.....19

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 Authority is implementing, are included as part of this conformance profile.
- Level of Assurance 4 for Identity is out of scope for this version. The column is included as a placeholder for future development.

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
BASE	Baseline					
1	The Responsible Authority MUST provide an overall description of the program or service, including: <ul style="list-style-type: none"> • 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
2	The Responsible Authority MUST specify its business role, purpose and authority as these relate to the identification of Subjects.	Y	Y	Y		IDSP.2
3	The Responsible Authority SHOULD be a private entity registered and operating in Canada (e.g., proprietorship, corporation) or a public entity (e.g., department, agency or registrar) operating under the authority of a Canadian federal, provincial, or territorial government.	Y				IDSP.6

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
4	The Responsible Authority MUST be a private entity registered and operating in Canada (e.g., proprietorship, corporation) or a public entity (e.g., department, agency or registrar) operating under the authority of a Canadian federal, provincial, or territorial government.		Y	Y		IDSP.7
5	The Responsible Authority MUST make sure that personal information is collected and managed under relevant legal authorities.	Y	Y	Y		IDSP.4
6	If the Responsible Authority 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
7	The Responsible Authority SHOULD provide Users with written notice that any false or misleading statements may result in violation of terms or conditions.	Y				IDSP.3
8	The Responsible Authority MUST provide Users with written notice that any false or misleading statements may result in violation of terms or conditions.		Y	Y		IDSP.3
9	If a Responsible Authority relies on another organization to carry out a Verified Person Trusted Process subject to the Verified Person conformance criteria, the Responsible Authority MUST provide: <ul style="list-style-type: none"> • Documentation on written agreement for the arrangement in effect; AND • Documentation on the approved Conformance Criteria assessment; 	Y	Y	Y		IDSP.5

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
10	<p>If cases involve children, minors, and other vulnerable Subjects, the Responsible Authority SHOULD:</p> <ul style="list-style-type: none"> • Have in place additional safeguards, compensating factors, or a documented exception process to reduce risk and to initiate interventions, as appropriate • Confirm that the applicant (for example, a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor, or other vulnerable Subject 	Y	Y			IDSP.9
11	<p>If cases involve children, minors, and other vulnerable Subjects, the Responsible Authority MUST:</p> <ul style="list-style-type: none"> • Have in place additional safeguards, compensating factors, or a documented exception process to reduce risk and to initiate interventions, as appropriate • Confirm that the applicant (for example, a parent or guardian) has the legal authority to carry out a request or obtain a service on behalf of the child, minor, or other vulnerable Subject 			Y		IDSP.9
12	<p>These 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.</p>	Y	Y	Y		
13	<p>The Responsible Authority SHOULD provide Users with written notice requiring them to notify the Responsible Authority of changes to a Subject's information whenever it changes.</p>	Y	Y	Y		
SOUR	Establish Sources					

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
<p>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.</p> <p>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.</p>						
1	<p>If appropriate, the Responsible Authority MUST conform to their legislated mandate for holding the information for which they are being identified as a source.</p> <p>The Responsible Authority MUST have appropriate security, accuracy, completeness and privacy of their Identity sources, and determine:</p> <ul style="list-style-type: none"> • The provenance of the Evidence • The robustness of the processes employed in collecting and storing the Evidence • The historic performance of the source • The ability of the source to satisfy relevant regulatory authorities • The recognition of the source in law 	Y	Y	Y		
2	<p>If the Responsible Authority uses an external source of Identity Evidence the external source of Identity MUST either hold a recognized independent accreditation or undergo an explicit assessment by the Responsible Authority.</p>	Y	Y	Y		
3	<p>A source of Identity Evidence MUST be assessed as Low Assurance if:</p> <ul style="list-style-type: none"> • It is not possible to establish the provenance of the Evidence or the processes employed in collecting and storing the Evidence employed by the source. 	Y	Y	Y		

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
4	<p>A private sector source of Identity Information MUST be assessed as Medium Assurance only if:</p> <ul style="list-style-type: none"> the provenance of the data, and processes employed by the source, can be audited and deemed to be satisfactory by the appropriate governance bodies or regulators, OR in the case of a statistical source, where the ongoing accuracy of the source can be demonstrated from historical performance data. 	Y	Y	Y		
5	<p>A public sector source of Identity Information MUST be assessed as Medium Assurance only if:</p> <ul style="list-style-type: none"> the provenance of the data, and processes employed by the source, can be audited and deemed to be satisfactory by the appropriate governance bodies or regulators, OR it is a Foundational Source of Identity (refer to definition in Overview) 	Y	Y	Y		
RESO	Identity Resolution					
<p>Identity Resolution is the process of establishing the uniqueness of a Subject within a program/service population through the use of Identity Information. A program or service defines its Identity resolution requirements in terms of Identity Attributes; that is, the program/service specifies the set of Identity Attributes that is required to uniquely identify a Subject within its population.</p>						
1	The Responsible Authority MUST specify the population or clientele for which its services are provided.	Y	Y	Y		IDRE.1
2	The Responsible Authority MUST ensure that the authoritative record uniquely resolves to only one Subject within their specified population of interest.		Y	Y		IDRE.2

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
3	The set of Identity Attributes MUST be sufficient to distinguish between different Subjects within an Identity context; and sufficient to describe the Subject as required by the service or program. (See section 4.1.4 of Government of Canada Directive on Identity Management (July 2019))	Y	Y	Y		
ESTAB	Identity Establishment (Contextual)					
<p>Identity Establishment is the process of creating contextual Identity Evidence that may be relied on by others for delivery of programs, services, and activities.</p> <p>Note: The establishment and maintenance of Foundational Evidence of Identity is out of scope, as it is the exclusive domain of the public sector; those criteria can be found in the Public Sector Profile of the Pan-Canadian Trust Framework.</p>						
1	Any transaction relating to the creation of a Verified Person Record MUST be confirmed and reference a relevant business event or activity.	Y	Y	Y		IDES.1
2	The Responsible Authority MUST record as part of the Verified Person Record only the necessary Identity Information required for the intended business purposes. The Responsible Authority MUST NOT record information that is not required for the business purposes for which the User has engaged them.	Y	Y	Y		IDES.2
3	The Responsible Authority MUST have in place policies and procedures to safeguard the Identity Attribute(s) provided by the User.	Y	Y	Y		IDES.3
4	The Responsible Authority MUST have in place policies and procedures to detect and respond to the misuse of the Identity Attribute(s) provided by the User.		Y	Y		IDES.4
VALID	Identity Information Validation					
<p>Identity Information Validation is the process of confirming the accuracy of Identity Information about a Subject against that established by an Authoritative Source. Identity Information Validation relies on the Evidence obtained from the Establish Sources process to determine the claimed Identity Information exists and is valid.</p>						
1	Self-assertion of Identity Information made by a Subject SHOULD be accepted.	Y				IDVA.1

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
2	Identity Information MUST acceptably match (see VALID-8) the assertion provided by the User and all instances of (Foundational and/or contextual) Evidence of Identity presented by the User.		Y	Y		IDVA.6
3	The required evidence, if any, MAY include low assurance sources.	Y				
4	The required evidence MUST , at a minimum, include medium assurance sources and MAY be supported by low assurance sources		Y			
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		
6	The Responsible Authority SHOULD check the Evidence to confirm that it corresponds to the claimed Identity Information, and that the Evidence is genuine and not altered.	Y				
7	The Responsible Authority MUST check the Evidence to confirm that it corresponds to the claimed Identity Information, and that the Evidence is genuine and not altered.		Y	Y		
8	<p>The Responsible Authority MUST document how differences between the Evidence and the claimed Identity Information relate to their risk tolerance. For example, a specific Responsible Authority might conclude that a difference in telephone number presents a low risk to them in cases where all other evidence is identical to the claimed Identity Information.</p> <p>The Responsible Authority's documented risk-based approach to differences between evidence and claimed Identity Information SHOULD be taken into consideration in the context of their Level of Assurance requirements. For example, higher levels of risk are usually not acceptable for higher Levels of Assurance whereas those higher levels of risk might be acceptable in some cases where a low Level of Assurance is required.</p>	Y	Y	Y		

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
9	The level of risk resulting from differences between the Evidence and the claimed Identity Information (VALID-8) that is acceptable MAY be determined by the Responsible Authority.	Y				
10	The level of risk resulting from differences between the Evidence and the claimed Identity Information (VALID-8) that is acceptable MUST align with the needs of regulated industry services, if applicable.		Y			
11	The level of risk resulting from differences between the Evidence and the claimed Identity Information (VALID-8) that is acceptable MUST be minimal and limited to, for example, minor formatting and spelling differences where it is clear that the values are semantically the same.			Y		
12	Contextual Evidence of identity MUST be confirmed as originating from the issuing authority. If confirmation from issuing authority is not feasible, then contextual Evidence of Identity MUST be confirmed using a trained examiner.		Y	Y		IDVA.7
13	Foundational Evidence of Identity MUST be confirmed as originating from issuing authority, who has validated the Identity Information using an authoritative record, or allows the Relying Party to validate the Identity Information at the Authoritative Source. If confirmation from originating authority or validation at source is not feasible, then Foundational Evidence of Identity MUST be confirmed using trained examiner.		Y	Y		IDVA.8
14	The Responsible Authority MUST ensure that the sources and technology used to perform the validation process are understood, and suitable (SOUR-6).	Y	Y	Y		

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
15	Where Evidence is presented in the form of physical documents that are not verifiable cryptographically, then Evidence checking MAY employ best practices for fraudulent document detection.	Y				
16	Where Evidence is presented in the form of physical documents that are not verifiable cryptographically, then Evidence checking MUST employ best practices for fraudulent document detection.		Y	Y		
17	Where Evidence is digital (including API-based and digital certificate-based) appropriate processes SHOULD be employed to ensure the integrity of the Evidence. (e.g., Tamper-evident, cryptographically signed, machine-verification of a Credential.)	Y				
18	Where Evidence is digital (including API-based and digital certificate-based) appropriate processes MUST be employed to ensure the integrity of the evidence. (e.g., Tamper-evident, cryptographically signed, machine-verification of a Credential.)		Y	Y		
EVID	Evidence Validation					
Evidence Validation is the process of confirming that the Evidence presented (physical or electronic) can be accepted or be admissible as a proof (i.e., beyond a reasonable doubt, balance of probabilities, and substantial likelihood).						
1	No restriction on what kind of Evidence an organization accepts.	Y				IDVL.1
2	One instance of Evidence of Identity (contextual or foundational) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.		Y			IDVL.2
3	Two instances of Evidence of Identity (at least one must be Foundational Evidence of Identity) MUST be assessed to be at least a medium level of assurance per SOUR-5 or SOUR-6.			Y		IDVL.3

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
4	<p>Foundational Evidence MUST originate from an Authoritative Source that is under the control of a federal, provincial or territorial government, or the local equivalent abroad; and used to maintain registration of specific vital events or to determine legal status.</p> <p>Acceptable Authoritative Sources, records and documents for Foundational Evidence:</p> <ul style="list-style-type: none"> • 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		IDVL.5
5	<p>Foundational Evidence of Identity Information that is incomplete or inconsistent with information provided by the User (e.g., name change) MAY require additional confirmation by the Authoritative Source, or additional contextual Evidence.</p>		Y	Y		
6	<p>Contextual Evidence MUST originate from an Authoritative Source that is under the control of a PCTF approved organization.</p> <p>Acceptable Authoritative Sources, records and documents for contextual Evidence:</p> <ul style="list-style-type: none"> • 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		IDVL.6

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
7	<p>If contextual Evidence is accepted in conjunction with Foundational Evidence of Identity (Level 3):</p> <ul style="list-style-type: none"> 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. 		Y	Y		IDVL.6
PRES	Identity Presentation					
<p>Identity Presentation is the process of dynamically confirming that a Subject has a continuous existence over time (i.e., “genuine presence”). This process can be used to help detect fraudulent activity (past or present) and to address identity spoofing concerns.</p>						
<p>Conformance criteria for Identity Presentation will be included in a future release of the PCTF.</p>						
VERIF	Identity Verification					
<p>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.</p>						
1	The Responsible Authority MAY undertake the verification steps it deems necessary, if any.	Y				IDVE.1
2	The Responsible Authority MUST ensure that interactions within a given context can be linked to the Subject who is making the claim.		Y	Y		IDVE.2

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
3	<p>The Responsible Authority MUST, at a minimum, verify the Subject remotely, and MAY use one of the following methods:</p> <ul style="list-style-type: none"> • knowledge-based verification • contextual data <p>The verification MUST provide sufficient assurance that only the identifiable Subject in question would be able to successfully complete the verification process.</p>		Y			IDVE.3
4	<p>The Responsible Authority MUST use at least one of the following methods to ensure the Identity Information relates to the User and the Subject:</p> <ul style="list-style-type: none"> • Biological (e.g., photo ID), biometric (e.g.: fingerprint), or behavioural characteristic confirmation • Face-to-face verification in person (or equivalent) • Physical possession confirmation <p>If the above methods are not feasible then alternative methods MUST be defined and documented in an exception process which MAY include:</p> <ul style="list-style-type: none"> • Confirmation by a trusted referee (e.g., guarantor, notary, certified agent) as determined by program-specific criteria • Additional safeguards • Compensating factors 			Y		IDVE.3
5	<p>In addition to the conditions specified in BASE-10, private and government organizations MAY include Evidence of Identity requirements for a parent or guardian as part of the Evidence of Identity requirements for a child, minor or other vulnerable Subject. For example, the passport of a parent could be used as contextual Evidence of Identity for the child.</p>	Y	Y	Y		IDVE.4

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
MAINT	Identity Maintenance					
Identity Maintenance is the process of ensuring that Identity Information is as accurate, complete, and up-to-date as is required. This process deals with events that may impact the previously performed Identity Information Validation and Identity Verification (e.g., Evidence used to establish the Verified Person has changed, expired or been revoked, which invalidates the Verified Person Record)						
1	<p>The Responsible Authority MAY deem the Subject to be no longer verified if any one of the following are true:</p> <ul style="list-style-type: none"> Any contextual Evidence changes. The status of the Foundational Evidence changes. This could include immigration, marriage, death or the status changes that impact the previous Identity Information Validation and Identity Verification processes. The elapsed time since the Identity Information Validation or Identity Verification processes were performed exceeds a threshold specified by the Relying Party. 	Y				IDMT.1
2	<p>The Responsible Authority MUST deem the Subject to be no longer verified if any one of the following are true:</p> <ul style="list-style-type: none"> Any contextual Evidence changes. The status of the Foundational Evidence changes. This could include immigration, marriage, death or the status changes that impact the previous Identity Information Validation and Identity Verification processes. The elapsed time since the Identity Information Validation or Identity Verification processes were performed exceeds a threshold specified by the Relying Party. 		Y	Y		IDMT.1

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
3	<p>The Responsible Authority MAY perform additional checks to re-validate or re-verify the Subject.</p> <p>In some cases, these checks may be a subset of the Identity Information Validation and Identity Verification processes.</p> <p>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.</p>	Y				
4	<p>The Responsible Authority SHOULD perform additional checks to re-validate or re-verify the Subject.</p> <p>In some cases, these checks may be a subset of the Identity Information Validation and Identity Verification processes.</p> <p>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.</p>		Y			
5	<p>The Responsible Authority MUST perform additional checks to re-validate or re-verify the Subject.</p> <p>In some cases, these checks may be a subset of the Identity Information Validation and Identity Verification processes.</p> <p>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.</p>			Y		

Reference	Conformance Criteria	Level of Identity Assurance				Public Sector Profile Reference
		L1	L2	L3	L4	
6	When the Responsible Authority becomes aware of any changes to Identity Information resulting from Birth or Death events it SHOULD correct or update the Subject's record(s) (in accordance with applicable legislation or regulations)	Y				IDMT.2
7	When the Responsible Authority becomes aware of any changes to Identity Information resulting from Birth or Death events it MUST correct update the Subject's record(s) (in accordance with applicable legislation or regulations)		Y	Y		IDMT.2
8	Any changes to Foundational Identity information MUST be confirmed by a foundational authority for the related event for: <ul style="list-style-type: none"> • Name change • Death 		Y	Y		IDMT.3
9	Birth and Death events SHOULD result in notification to Relying Parties.		Y	Y		IDMT.4

Table 1: Verified Person Conformance Criteria

4 Revision History

Version	Date of Issue	Author(s)	Description
0.01	2018-06-08	PCTF Editing Team	First attempt of the Verified Person Component Conformance Criteria 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	2019-10-16	PCTF Editing Team	Updated conformance criteria to include Public Sector PCTF Profile for comparison review and determine applicability to baseline PCTF document
0.04	2019-10-14	PCTF Editing Team	Updated as per action items from October 23rd Design meeting
0.05	2019-11-12	PCTF Editing Team	Updates as per action items from Verified Person Design Team meetings
0.06	2019-11-26	PCTF Editing Team	Replaced supporting identity with contextual identity as per PCTF Model
0.07	2020-01-03	PCTF Editing Team	Updated to resolve outstanding wiki comments, in preparation for review period
0.08	2020-01-16	PCTF Editing Team	Updated as per January 14 Verified Person Design team meeting, and final general edit before review
0.09	2020-02-14	PCTF Editing Team	Updates after February 12th Verified Person Design team 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 comments
1.0	2020-07-02	PCTF Editing Team	Final Recommendation V1.0