PCTF Credentials (Relationships & Attributes) 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.

Table of Contents

1 Introduction to the PCTF Credentials (Relationships & Attributes) Conformance Profile 3
1.1 Conformance Criteria Keywords 3
2 Levels of Assurance 4
3 Risk Evaluation 5
3.1 Evaluation of Risk Level 9
3.2 Credential Risks 9
3.3 Credential Management 12
4 Conformance Criteria 17
5 Revision History 34

1 Introduction to the PCTF Credentials (Relationships & Attributes) Conformance Profile

This document specifies the conformance criteria for the Credentials (Relationships & Attributes) component of the Pan-Canadian Trust Framework (PCTF). Conformance Criteria are central to the trust framework because they specify the essential requirements agreed to by trust framework participants to ensure the integrity of their processes. This integrity is paramount because the output or result of a trusted process may be relied upon by many participants across organizational, jurisdictional and sectoral boundaries.

The PCTF Conformance Criteria are intended to complement existing privacy legislation and regulations.

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.

1.1 Conformance Criteria Keywords

Throughout this document the following terms indicate the precedence and/or general rigidity of the conformance criteria and are to be interpreted as noted below.

- **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. The rationale for not adhering to a criterion should be documented in cases where Conformance Criteria are not adhered to.
- **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.

Note

- The above listed keywords appear in **bold** typeface and ALL CAPS throughout this conformance profile.

2 Levels of Assurance

It is critical that Participants that create or consume Credentials understand the level of trust they can ascribe to those Credentials. The PCTF Credentials (Relationships & Attributes) component employs a levels of assurance approach to address this. Figure 1 provides an overview of the Credentials assurance levels (CALs). Credential assurance also involves the process of binding a Credential to one or more Subjects.

Credential Assurance Level (CAL)	Qualification Description
Level 1 (CAL1)	• Satisfies all Level 1 Conformance Criteria • Little or no confidence required • Little confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised
Level 2 (CAL2)	• Satisfies all Level 2 Conformance Criteria • Some confidence required • Some confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised
Level 3 (CAL3)	• Satisfies all Level 3 Conformance Criteria • High degree of confidence required • High confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised
Level 4 (CAL4) Optional	• Satisfies all Level 4 Conformance Criteria • Very high degree of confidence required • Very high confidence required that an Entity has maintained control over a Credential that has been entrusted to them and that the Credential has not been compromised

Figure 1. Credentials Assurance Levels

In order to achieve a specific CAL a Credential must, at a minimum, satisfy that CAL for every applicable conformance criterion. For example, if a Credential met the standard for CAL4 on nine of the criteria, and met the standard for CAL1 on one criterion, the assessed CAL for the Credential can be no higher than CAL1. This is further explained in the Conformance Profile.

3 Risk Evaluation

Figure 2 contains an enumeration of risks commonly used to assess the Level of Assurance required for a specific digital interaction. It should be noted that this table is meant to be illustrative in nature. It is not intended to be exhaustive, nor is it meant to be directive. Relying Parties must evaluate the potential risks and harms they are likely to face, and assess the levels of risk they are willing to accept for a specific transaction within their operational context. As such, some of the illustrative criteria uses terminology that is subject to interpretation (e.g., “high”, “medium”, “low”). This enables practitioners to establish a risk profile that is commensurate with their ministry, department, or type of business. For example, a large financial institution may consider the risk of losing $100,000 as “limited” or “low” whereas a risk of that size may be “severe” or “high” for a small business, startup, or individual.

Since the risk levels are a function of a Relying Party’s unique circumstances and any policy, legislation, and/or regulation they are subject to, it is incumbent upon the Relying Party to explicitly document their risk tolerance. This will ensure that risk controls are consistently implemented and that they are neither too lenient, nor too stringent regardless of the persons who implement them. It will also ensure the controls are fairly assessed when audited. These Risks should also be documented so they are evident to, and clearly understandable by, Entities with whom they interact.

The Relying Party must also consider the trustworthiness of the Entities involved in a transaction and its Verification when assessing the trustworthiness of a transaction, Relationship, or Attribute as documented in the Verified Person, Verified Organization, and Authentication components of the PCTF.

Impact Category	**Assurance Level Required**			
	CAL1	**CAL2**	**CAL3**	**CAL4**
Inconvenience, distress, damage to standing or reputation	At worst, limited, short-term inconvenience, distress, embarrassment or damage to the standing or reputation of any party	At worst, serious short-term or limited long-term inconvenience, distress or damage to the standing or reputation of any party	Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with severe effects or which affect many individuals)	A severe and permanent inconvenience, distress or damage to the standing or reputation of any party

Financial loss	At worst, an insignificant or inconsequential financial loss to any party, or at worst an inconsequential liability	At worst, a serious financial loss to any party, or a serious liability	A severe financial loss to any party, or a severe liability	A catastrophic financial loss to any party, or a catastrophic liability
Harm to a program or public interest	At worst, a limited adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness; minor damage to organizational assets or public interests)	At worst, a serious adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; significant damage to organizational assets or public interests)	A severe adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; major damage to organizational assets or public interests)	A catastrophic adverse effect on organizational operations or assets or government organization, program, asset or the public interest (e.g., catastrophic mission capability degradation or loss of to the extent and duration that the organization is unable to perform its primary functions; catastrophic damage to organizational assets or public interests)

Unauthorized release of sensitive personal or commercial information	At worst, a limited release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a loss of confidentiality with a low impact	At worst, a release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a moderate impact	A release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a serious impact	A release of personal information or commercially sensitive information to unauthorized parties, or breach of privacy, resulting in a catastrophic impact
Unauthorized release of sensitive government information	A loss of confidentiality with a low impact	A limited adverse effect on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties	A serious adverse effect on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties	A catastrophic effect on organizational operations and assets due to a loss of confidentiality resulting from the release of sensitive government information to unauthorized parties

Civil or criminal violations	Private Sector: At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts Public Sector: Any compromise involving a legal violation is assessed at a minimum of Level 2	A civil or criminal violation th at may have minor consequences and that may be subject to enforcement efforts	A civil or criminal violatio n that may have serious consequences t hat are of importance to enforcement programs	A violation that may have exceptionally grave consequences that are of special importance to enforcement programs
Personal health and safety	Private Sector: At worst, minor injury not requiring medical treatment Public Sector: Any compromise health and safety is assessed at minimum of Level 2	Private Sector: At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment Public Sector: A minor personal injury not requiring medical attention	Private Sector: At worst, a low risk of serious injury or death Public Sector: A personal injury requiring medical attention	Risk of serious personal injury or death
National interest	(Any compromise involving the national interest is assessed at a minimum of Level 2)	A disadvantage to the national interest	An injury to the national interest	A serious or exceptionally grave injury to the national interest

Figure 2: Risk Evaluation Table

3.1 Evaluation of Risk Level

The risks above should be evaluated as follows:

Assurance Level Required	Criteria
Level 1 (CAL1)	One or more risks are evaluated to be at level 1 and no risk is evaluated to be greater than level 1
Level 2 (CAL2)	One or more risks are evaluated to be at level 2 and no risk is evaluated to be greater than level 2
Level 3 (CAL3)	One or more risks are evaluated to be at level 3 and no risk is evaluated to be greater than level 3
Level 4 (CAL4)	One or more risks are evaluated to be at level 4

Figure 3: Risk Level Evaluation

3.2 Credential Risks

Credentials provide the foundation for trust in a digital ecosystem. In addition to any Privacy Impact Assessments an Entity might perform, it is important that Organizations participating in a trust ecosystem understand the risks to the Credentials they create, possess, and/or consume and take appropriate action to protect their integrity. Figure 4 contains an illustrative table of risks to Credentials and examples of mitigation strategies.

Activity	Threat	Example	Example Mitigation Strategy
Credential Storage	Disclosure	Usernames and passwords, stored in a system file, are revealed.	Use access-control mechanisms that protect against unauthorized disclosure of credentials held in storage. Protect username/password databases using secure salting and hashing functions, or approved encryption techniques to make recovery of passwords from a leaked password file impractical.

	Tampering	The file that maps usernames to passwords within a CSP is hacked, the mappings are modified, and existing passwords are replaced by passwords known to a threat actor.	Use access-control mechanisms that protect against unauthorized tampering with credentials and tokens.
Credential Verification Services	Disclosure	A threat actor is able to view requests and responses between a CSP and a Verifier.	Use a communication protocol that offers confidentiality protection.
	Tampering	A threat actor is able to masquerade as a CSP and provide false responses to a Verifier's password verification requests.	Ensure that Verifiers authenticate CSPs prior to accepting a verification response from a CSP. Use a communication protocol that offers integrity protection.
	Unavailability	The password file or CSP is unavailable to provide password and username mappings.	Ensure that CSPs have a well-developed and tested contingency plan.
		Public key certificates for Claimants are unavailable to Verifiers because the directory systems are down (e.g., maintenance or as a result of a denial-of-service attempt).	

Credential issuance/renewal/re-issuance	Disclosure	Password renewed by a CSP for a Subscriber is copied by a threat actor as it is transported from the CSP to the Subscriber.	Use a communication protocol that provides confidentiality protection of session data.
	Tampering	New password created by a Subscriber is modified by a threat actor as it is being submitted to a CSP to replace an expired password.	Use a communication protocol that allows a Subscriber to authenticate the CSP prior to engaging in token re-issuance activities and protect the integrity of the data passed.
	Unauthorized Issuance	A CSP is compromised through unauthorized physical or logical access resulting in issuance of fraudulent credentials.	Implement physical and logical access controls to prevent compromise of the CSP.
	Unauthorized renewal/re-issuance	A threat actor fools a CSP into re-issuing a credential for a current Subscriber. The new credential binds the current Subscriber's identity with a token provided by the threat actor.	Establish a policy that requires a Subscriber to prove possession of the original token in order to successfully negotiate the re-issuance process. Any attempt to negotiate the re-issuance process, using an expired or revoked token, should fail.
		A threat actor is able to take advantage of a weak credential renewal protocol to extend the credential validity period for a current Subscriber.	

Token and credential revocation/destruction	Delayed revocation/ destruction of credentials	Out-of-date certificate revocation lists allow accounts, which should have been locked as a result of credential revocation, to be used by a threat actor.	Revoke/Destroy credentials as soon as notification is received that the credentials should be revoked or destroyed.
		User accounts are not deleted when employees leave a company leading to a possible use of those accounts by unauthorized persons.	
		A hardware token is used after the corresponding credential was revoked or expired.	Destroy or zeroise tokens after their corresponding credentials have been revoked.

Figure 4: Credential Risks

3.3 Credential Management

How Credentials are managed will have a direct impact on their trustworthiness. Figure 5 contains an illustrative table of requirements for the management of Credentials and how that might impact their trustworthiness. As mentioned during this document's earlier discussion of risks, Relying Parties must assess the level of risk they are willing to accept and adjust their own risk parameters accordingly. As was also stated, it is important that those levels be deliberately set and recorded to ensure consistency in their implementation and assessment. Relying Parties are also reminded that legislation and regulation should also be considered as they may impact specific aspects of Credential management such as Credential retention requirements.

Level	**Requirements**				
	Credential Storage	**Token and Credential Verification Services**	**Token and Credential Renewal / Re-issuance**	**Token and Credential Revocation and Destruction**	**Records Retention Requirements**

CAL1	Files of shared secrets used by Verifiers must be protected by access controls to limit access to administrators and authorized personnel or applications. Files of shared secrets must not be stored in plain text. One-way hashing, or a similar function, must be used before storage.	Long term token secrets should not be shared with other parties, unless absolutely necessary.	No requirements.	No requirements.	No requirements.
CAL2	Files of shared secrets used by Verifiers must be protected by access controls to limit access to administrators and authorized personnel or applications. Such shared secret files must not contain the plaintext passwords or secrets; two alternative methods may be used to protect the shared secret: 1. Passwords may be concatenated to a variable salt (i.e., variable across a group of passwords that are stored together) and	Long-term shared authentication secrets, if used, must never be revealed to any other party except Verifiers operated by CSPs. However, session (i.e., temporary) shared secrets may be provided by CSPs to independent Verifiers. Cryptographic protections are required for all messages, between a CSP and a Verifier,	CSPs must establish suitable policies for renewal and re-issuance of tokens and credentials. Proof-of-possession of unexpired current tokens must be demonstrated by a Claimant prior to a CSP allowing renewal and re-issuance. Passwords must not be renewed; they should be re-issued. After expiry of current token, and any grace period, renewal and re-issuance must not be allowed. Upon re-issuance, token secrets must not	CSPs must revoke or destroy credentials and tokens within 72 hours after being notified that a credential is no longer valid, or a token is compromised, to ensure that a Claimant using the token cannot successfully be authenticated. If a CSP issues credentials that expire automatically within 72 hours, (e.g., issues fresh certificates	A record of the registration, history, and status of each token and credential (including revocation) must be maintained by CSPs or a CSP's representative. The record retention period of data for Level 2 credentials is seven years and six months beyond the expiration or revocation of the credential, whichever is later.

	then hashed with an approved algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. The hashed passwords are then stored in the password file. The variable salt may be composed using a global salt (common to a group of passwords) and the username, (unique per password), or some other technique to ensure uniqueness of the salt within the group of passwords. 2. Shared secrets may be encrypted and stored using approved encryption	which contain private credentials or assert the validity of weakly - bound or potentially revoked credentials. Private credentials should only be sent to an authenticated party to ensure confidentiality and tamper protection, through a protected session.	be set to a default or reused in any manner. All interactions should occur over a protected session such as SSL/TLS.	with a 24-hour validity period each day), then the CSP is not required to provide an explicit mechanism to revoke the credentials. CSPs that register passwords should ensure that the revocation or de-registration of the password can be accomplished in no more than 72 hours.	

	algorithms and modes. The needed secret can be decrypted only when immediately required for authentication. In addition, any method allowed to protect shared secrets at Level 3 or 4 may be used at Level 2.				
CAL3	Files of shared secrets used by Verifiers should be protected by access controls to limit access to administrators and authorized personnel or applications. Files containing shared secrets must be encrypted. The minimum requirements for the encryption are: 1. The encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic	CSPs must provide a secure mechanism to allow Verifiers or RPs to ensure credentials are valid. Such mechanisms may include on-line validation servers or the involvement of CSP servers that have access to status records in authentication transactions. Temporary - session authentication keys may be generated	Renewal and re-issuance should only occur prior to expiration of the current credential. Claimants should authenticate to CSPs using the existing token and credential in order to renew or re-issue the credential. All interactions should occur over a protected session such as SSL/TLS.	CSPs should have a procedure to revoke credentials and tokens within 24 hours. Verifiers must ensure that the tokens they rely upon are either freshly issued (within 24 hours) or still valid. Shared secret based authentication systems may simply remove revoked Subscribers from the verification database.	No additional requirements over Level 2.

	module or any FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation. 2. Shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic modules and is not exported in plaintext from the module.	from long-term shared secret keys by CSPs, and distributed to third-party Verifiers, as a part of the verification services offered by CSPs. However, long-term shared secrets should not be shared with any third parties, including third party Verifiers.			
CAL4	No additional requirements over Level 3.	No additional requirements over Level 3.	Sensitive data transfers must be cryptographically authenticated using keys bound to the authentication process. All temporary or short-term keys derived during the original authentication operation must	CSPs must have a procedure to revoke credentials within 24 hours of authentication. Verifiers or RPs must ensure that the credentials they rely upon are either freshly issued	All stipulations from Levels 2 and 3 apply. The minimum record retention period for Level-4 credential data is ten years and six months beyond the expiration or

			expire, and re authentication must be required after not more than 24 hours from the initial authentication.	(within 24 hours) or still valid.	revocation of the credential.

Figure 5: Credential Management

4 Conformance Criteria

Conformance Criteria are categorized by trust element. For ease of reference, a specific conformance criterion may be referred to by its category and reference number. Example: “RABS1” refers to “Baseline Conformance Criteria reference No. 1”.

Notes

- Baseline Conformance Criteria are also included as part of this conformance profile.
- Conformance Criteria specified in other PCTF components of may also be applicable to the PCTF Credentials (Relationships & Attributes) Component under certain circumstances.

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
RABS	**These Baseline Criteria Apply to <u>All</u> Relationships and Attributes Processes**				
1	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.	X	X	X	X
RDEF	**Define Relationship**				
1	The Issuer **SHOULD NOT** include information about a specific instance of the type of Relationship being defined.	X	X	X	X
2	The Issuer **SHOULD** include information that clearly identifies the Defining Party.	X	X		
3	The Issuer **MUST** include information that clearly identifies the Defining Party.			X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
4	The Issuer **SHOULD** indicate the authority under which the Relationship can be Disclaimed. (e.g., a marriage certificate might only be legitimately disclaimed by an appropriate Authoritative Source such as a court or state agency; membership in a community association might be legitimately self-disclaimed or disclaimed by the association's executive)	X			
5	The Issuer **MUST** indicate authority under which the Relationship can be Disclaimed. (e.g., a marriage certificate might only be legitimately disclaimed by an appropriate Authoritative Source such as a court or state agency; membership in a community association might be legitimately self-disclaimed or disclaimed by the association's executive)		X	X	X
6	The Issuer **SHOULD** declare whether the type of Relationship being described must be Endorsed in order to be considered trustworthy (see the Endorse Relationship Trusted Process in the Overview and the criteria listed under REND for Endorsement details).	X			
7	The Issuer **MUST** declare whether the type of Relationship being described must be Endorsed in order to be considered trustworthy (see the Endorse Relationship Trusted Process in the Overview and the criteria listed under REND for Endorsement details).		X	X	X
8	Whenever possible, and as appropriate, the Issuer **MAY** use relevant legal definitions, industry standard definitions, or references to relevant schemas.	X			
9	Whenever possible, and as appropriate, the Issuer **SHOULD** use relevant legal definitions, industry standard definitions, or references to relevant schemas.		X	X	X
RDEC	**Declare Relationship**				

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
1	The Issuer **MAY** use a Relationship Definition as the basis for the Declared Relationship and reference it within the Declared Relationship.	X			
2	The Issuer **MUST** use a Relationship Definition as the basis for the Declared Relationship and reference it within the Declared Relationship.		X	X	X
3	The Issuer **MAY** provide to Participants a summary of its mandate and authority as these relate to the Relationships it declares.	X			
4	The Issuer **MUST** provide to Participants a summary of its mandate and authority as these relate to the Relationships it declares.		X	X	X
5	Where applicable, the Issuer **SHOULD** provide to Participants evidence that it meets all legal and regulatory requirements applicable to the types of Relationships it issues.	X			
6	Where applicable, the Issuer **MUST** provide to Participants evidence that it meets all legal and regulatory requirements applicable to the types of Relationships it issues.		X	X	X
7	The Issuer **MAY** provide to Participants general terms and conditions governing legitimate or prohibited use of Declared Relationships it issues. (e.g., there are cases in which a provincial health card or social insurance number should be used, and cases where is should not be used or where use is prohibited by regulation, legislation, or policy)	X			
8	The Issuer **SHOULD** provide to Participants general terms and conditions governing legitimate or prohibited use of Declared Relationships it issues. (e.g., there are cases in which a provincial health card or social insurance number should be used, and cases where is should not be used or where use is prohibited by regulation, legislation, or policy)		X	X	

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
9	The Issuer **MUST** provide specific terms and conditions governing legitimate or prohibited use of Declared Relationships it issues. (e.g., there are cases in which a provincial health card or social insurance number should be used, and cases where is should not be used or where use is prohibited by regulation, legislation, or policy)				X
10	The Issuer **MAY** provide to Participants a point of contact for information about its Relationships and associated processes.	X			
11	The Issuer **MUST** provide to Participants a point of contact for information about its Relationships and associated processes.		X	X	X
12	Where applicable, the Issuer **MUST** allow the Subject to specify the location to which the Relationship will be delivered (i.e., a local or hosted Credential Repository), unless prohibited by regulation, policy, or legislation.	X	X	X	X
13	The Issuer **MAY** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Relationship.	X			
14	The Issuer **SHOULD** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Relationship.		X		
15	The Issuer **MUST** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Relationship.			X	X
16	The Issuer **MAY** provide references to 3rd party Credentials (i.e., Credentials issued by other Entities) it used to Verify and Validate information contained in a Relationship it has issued.	X			

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
17	The Issuer **SHOULD** provide references to 3rd party Credentials (i.e., Credentials issued by other Entities) it used to Verify and Validate information contained in a Relationship it has issued.		X		
18	The Issuer **MUST** provide references to 3rd party Credentials (i.e., Credentials issued by other Entities) it used to Verify and Validate information contained in a Relationship it has issued.			X	X
19	Information contained in a Relationship **MUST** be consistent with information held in the Issuer's records.	X	X	X	X
20	The Issuer **SHOULD** provide information indicating the Issuer's confidence in the accuracy of the information contained in the Relationship when the Relationship was issued. This would normally be done by communicating the CAL associated with the Credential, though could include additional information or caveats.		X	X	X
21	The Issuer **SHOULD** provide information indicating the Issuer's confidence in the Subject's Identity or that of the Entity acting on behalf of the Subject when the Declared Relationship was issued. This would normally be done by communicating the CAL associated with the Credential, though could include additional information or caveats.	X	X		
22	The Issuer **MUST** provide information indicating the Issuer's confidence in the Subject's Identity or that of the person acting on behalf of the Subject when the Relationship was issued. This would normally be done by communicating the CAL associated with the Credential, though could include additional information or caveats.			X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
23	The Issuer or **MAY** provide the ability to demonstrate that a Declared Relationship originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Declared Relationship.	X			
24	The Issuer or **SHOULD** provide the ability to demonstrate that a Declared Relationship originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Declared Relationship.		X		
25	The Issuer or **MUST** provide the ability to demonstrate that a Declared Relationship originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Declared Relationship.			X	X
26	A Declared Relationship Credential **MUST** include information identifying its Issuer.		X	X	X
27	The Issuer **MUST** include the date the Relationship was issued, unambiguously labeled as such.		X	X	X
28	The Issuer **MAY** provide an expiry date for all Relationships it declares, or indicate the Relationship does not have an expiry date.	X			
29	The Issuer **MUST** provide an expiry date for all Relationships it declares, or indicate the Relationship does not have an expiry date.		X	X	X
30	When declaring a Relationship, the Issuer **MAY** indicate it is wholly or partly under dispute. When that is done, the Issuer **SHOULD** include a reference to other Declared Relationships that contain disputed information and/or which are under review.	X	X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
31	The Issuer **SHOULD** provide to Participants general terms and conditions under which Relationships it declares will be rendered unusable or unreliable.	X			
32	The Issuer **MUST** provide to Participants general terms and conditions under which Relationships it declares will be rendered unusable or unreliable.		X	X	X
33	The Holder **MUST** ensure that the Repository in which they store a Declared Relationship is adequately secure, legitimately sourced, and located in a jurisdiction as required by legislation, policy, and/or regulation.		X	X	X
REND	**Endorse Relationship**				
1	An Endorsing Party **MAY** be an Authoritative Source that is a Verified Person or Verified Organization.	X			
2	An Endorsing Party **MAY** be an Authoritative Source that is a Verified Person or Verified Organization.		X		
3	An Endorsing Party **MUST** be an Authoritative Source that is a Verified Person or Verified Organization.			X	X
RVAL	**Validate Relationship**				
1	Verifiers **SHOULD** provide sufficient information to the Relying Party to enable the Relying Party to properly evaluate the Level of Assurance that can be associated with each Relationship.	X	X		
2	Verifiers **MUST** provide sufficient information to the Relying Party to enable the Relying Party to properly evaluate the Level of Assurance that can be associated with each Relationship.			X	X
3	Verifiers **MAY** confirm the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.	X			

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
4	Verifiers **SHOULD** confirm the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.		X		
5	Verifiers **MUST** confirm the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.			X	X
6	Verifiers **MAY** inform the Relying Party whether the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.	X			
7	Verifiers **SHOULD** inform the Relying Party whether the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.		X		
8	Verifiers **MUST** inform the Relying Party whether the Endorsing Party or Declaring Party is an Authoritative Source and the Subject(s) are either Verified Persons or Verified Organizations.			X	X
9	The Endorsing Party or Declaring Party **MAY** be a Verified Person or a Verified Organization.	X			
10	The Endorsing Party or Declaring Party **SHOULD** be a Verified Person or a Verified Organization.		X		
11	The Endorsing Party or Declaring Party **MUST** be a Verified Person or a Verified Organization.			X	X
12	The Verifier **SHOULD** be a Verified Person or a Verified Organization.	X			
13	The Verifier **MUST** be a Verified Person or a Verified Organization.		X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
14	The Verifier **SHOULD NOT** retain copies of the Presentations or Verified Presentations they Verify, nor any data therein, nor data derived from the data therein unless required to do so by regulation, policy, or legislation.	X	X	X	X
15	Verifiers **MUST NOT** share information presented to them as part of the Verification process with other Verifiers, other Participants, or anyone other than the Relying Party or Relying Parties without the express consent of the Subject unless authorized or required to do so by regulation, policy, or legislation.	X	X	X	X
16	Relationships included in a Presentation or Verifiable Presentation that is submitted to a Verifier **SHOULD** be in the form of a Declared Relationship, Endorsed Relationship, or Validated Relationship.	X	X	X	X
RDIS	**Disclaim Relationship**				
1	The Disclaiming Party **MUST** Disclaim, or otherwise render unusable or unreliable, a Relationship if it detects indications of a compromised or invalid Relationship.	X	X	X	X
2	The Disclaiming Party **MUST** make available to Participants the status of all Disclaimed, or otherwise unusable or unreliable Relationships it has issued.	X	X	X	X
3	The Disclaiming Party **MUST** capture the following details about Relationships the Issuer has rendered unusable or unreliable: Date the action was taken; reason for the action; general indication of who initiated the action (e.g., Subject or Issuer).	X	X	X	X
4	The Disclaiming Party **MUST** only disclose details captured about unusable or unreliable Relationships to known Participants with a reasonable need for the information, and within the bounds of applicable regulations, policy, or legislation.	X	X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
5	The Disclaiming Party **MUST** disclose the reason for Disclaiming the Relationship to the Subject(s).	X	X	X	X
6	The Disclaiming Party **MUST NOT** arbitrarily Disclaim Relationships. Disclaimed Relationships should be the result of relevant policies, procedures, legislation, regulation or confirmed or suspected nefarious activities, such as fraud, that would indicate undue risk should the Relationship be accepted.	X	X	X	X
7	The Endorsing Party **SHOULD** provide Subjects the ability to initiate a process to Disclaim, or otherwise render unusable or unreliable a Relationship when the Subject detects indications of a compromised or invalid Relationship.	X	X	X	X
ADEF	**Define Attribute**				
1	The Issuer **SHOULD NOT** include information about a specific instance of the type Attribute being defined.	X	X	X	X
2	The Issuer **SHOULD** include information that clearly identifies the Issuer.	X	X		
3	The Issuer **MUST** include information that clearly identifies the Issuer.			X	X
4	Whenever possible, and as appropriate, the Issuer **MAY** use relevant legal definitions, industry standard definitions, or references to relevant schemas.	X	X		
5	Whenever possible, and as appropriate, the Issuer **SHOULD** use relevant legal definitions, industry standard definitions, or references to relevant schemas.			X	X
ABND	**Bind Attribute**				
1	The Issuer **MAY** use an Attribute Definition as the basis for the Bound Attribute and reference it within the Bound Attribute.	X			

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
2	The Issuer **MUST** use an Attribute Definition as the basis for the Bound Attribute and reference it within the Bound Attribute.		X	X	X
3	The Issuer **MAY** provide to Participants a summary of its mandate and authority as these relate to the Attributes it issues.	X			
4	The Issuer **MUST** provide to Participants a summary of its mandate and authority as these relate to the Attributes it issues.		X	X	X
5	The Issuer **SHOULD** provide to Participants evidence that it meets all legal and regulatory requirements applicable to the types of Attributes it issues.	X			
6	The Issuer **MUST** provide to Participants evidence that it meets all legal and regulatory requirements applicable to the types of Attributes it issues.		X	X	X
7	The Issuer **MAY** provide to Participants general terms and conditions governing issuance and use of the Attributes it issues.	X			
8	The Issuer **SHOULD** provide to Participants general terms and conditions governing issuance and use of the Attributes it issues.		X		
9	The Issuer **MUST** provide specific terms and conditions governing issuance and use of a specific Attribute it issues.			X	X
10	The Issuer **MUST** provide Subjects requesting issuance of an Attribute with notice that providing false or misleading statements or information may result in violation of the terms or conditions governing its issuance and use.		X	X	X
11	The Issuer **MUST** confirm Subjects understand and agree with the notice that any false or misleading statements may result in violation of terms or conditions governing Credential issuance and use.		X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
12	The Issuer **MAY** provide to Participants a point of contact for information about its Credentials and associated processes.	X			
13	The Issuer **MUST** provide to Participants a point of contact for information about its Credentials and associated processes.		X	X	X
14	Where applicable, the Issuer **MUST** allow the Subject to specify the location to which the Attribute will be delivered (i.e., a local or hosted Credential Repository), unless prohibited by regulation, policy, or legislation.	X	X	X	X
15	The Issuer **MAY** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Attribute.	X			
16	The Issuer **SHOULD** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Attribute.		X		
17	The Issuer **MUST** provide to Participants details about the evidence and processes on which it relied to Verify and Validate Subject information contained in a Attribute.			X	X
18	The Issuer **MAY** provide references to 3rd party Credentials or Attributes (i.e., Credentials or Attributes issued by other Entities) it used to Verify and Validate information contained in an Attribute it has issued.	X			
19	The Issuer **SHOULD** provide references to 3rd party Credentials or Attributes (i.e., Credentials or Attributes issued by other Entities) it used to Verify and Validate information contained in an Attribute it has issued.		X		
20	The Issuer **MUST** provide references to 3rd party Credentials or Attributes (i.e., Credentials or Attributes issued by other Entities) it used to Verify and Validate information contained in an Attribute it has issued.			X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
21	Information contained in a Credential **MUST** be consistent with information held in the Issuer's records.	X	X	X	X
22	The Issuer **SHOULD** provide information indicating the Issuer's confidence in the accuracy of the information contained in the Attribute when the Attribute was issued. This would normally be done by communicating the CAL associated with the Credential, though could include additional information or caveats.		X	X	X
23	The Issuer **MUST** only issue an Attribute at the request of or with the consent of the Subject or a person eligible to act on behalf of the Subject except where permitted by policy, regulation, or legislation.	X	X	X	X
24	The Issuer **MUST** take reasonable measures to ensure Bound Attributes are issued at the request of and/or with the consent of the rightful Subject or a person authorized to act on behalf of the Subject except where permitted by policy, regulation, or legislation.	X	X	X	X
25	The Issuer **SHOULD** provide information indicating the Issuer's confidence in the Subject's Identity or that of the Entity acting on behalf of the Subject when the Bound Attribute was issued.	X	X		
26	The Issuer **MUST** provide information indicating the Issuer's confidence in the Subject's Identity or that of the Entity acting on behalf of the Subject when the Bound Attribute was issued.			X	X
27	The Issuer **MAY** provide the ability to demonstrate that an Attribute originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Bound Attribute.	X			

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
28	The Issuer **SHOULD** provide the ability to demonstrate that an Attribute originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Bound Attribute.		X		
29	The Issuer **MUST** provide the ability to demonstrate that an Attribute originated with the Issuer and was not altered in transit to another Participant (Subject, Holder, Relying Party, etc.). This would usually be done in the form of a Verifiable Bound Attribute.			X	X
30	A Bound Attribute **MUST** include information identifying the Issuer of that Attribute.		X	X	X
31	The Issuer **MUST** include the date the Attribute was issued, unambiguously labeled as such.		X	X	X
32	The Issuer **MAY** provide an expiry date for all Attributes it issues, or indicate the Attribute does not have an expiry date.	X			
33	The Issuer **MUST** provide an expiry date for all Attributes it issues, or indicate the Attribute does not have an expiry date.		X	X	X
34	When issuing an Attribute, the Issuer **MAY** indicate it is wholly or partly under dispute. When that is done, the Issuer **SHOULD** include a reference to other Attributes that contain disputed information and/or which are under review.	X	X	X	X
35	The Issuer **SHOULD** provide to Participants general terms and conditions under which Attributes it issues will be rendered unusable or unreliable.	X			
36	The Issuer **MUST** provide to Participants general terms and conditions under which Attributes it issues will be rendered unusable or unreliable.		X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
37	The Issuer **MUST** ensure that the Repository to which they deliver an Attribute is adequately secure, legitimately sourced, and located in a jurisdiction as required by legislation, policy, and/or regulation.		X	X	X
AMNT	**Maintain Attribute**				
1	The Issuer **SHOULD** establish, maintain, and make known to other Participants a process for resolving disputes concerning the accuracy of information contained in Attributes it has issued.	X	X		
2	The Issuer **MUST** establish, maintain, and make known to other Participants a process for resolving disputes concerning the accuracy of information contained in Attributes it has issued.			X	X
3	The Issuer **MUST** make available to the Subject the reason for the update of any Attribute.	X	X	X	X
4	The Issuer **MUST** inform the Subject(s) of any changes it makes to an Attribute.	X	X	X	X
5	The Revocation Authority **MUST** revoke, update, or otherwise render unusable or unreliable an Attribute if it detects indications of a compromised or invalid Attribute.	X	X	X	X
6	The Issuer **MUST** capture the following details about Attributes the Issuer has updated: Date the action was taken; reason for the action; general indication of who initiated the action (e.g., Subject or Issuer).	X	X	X	X
7	Participants **MUST** only disclose details captured about unusable or unreliable Attributes to other known Participants with a reasonable need for the information.	X	X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
8	The Issuer **MUST NOT** arbitrarily change Attributes. Changes should be the result of relevant policies, procedures, legislation, regulation or confirmed or suspected nefarious activities, such as fraud, that would indicate undue risk should the Attribute be accepted.	X	X	X	X
9	The Issuer **SHOULD** provide Subjects the ability to initiate a process to revoke, update, or otherwise render unusable or unreliable an Attribute they issued to that Subject when the Subject detects indications of a compromised or invalid Attribute.	X	X	X	X
AREV	**Revoke Attribute**				
1	The Revocation Authority **MUST** initiate a process to revoke, update, or otherwise render unusable or unreliable an Attribute if it detects indications of a compromised or invalid Attribute.	X	X	X	X
2	The Revocation Authority **MUST** make the status of all revoked, or otherwise unusable or unreliable Attributes it has issued (e.g., if an Attribute is a “Revoked Attribute") available to Participants with a reasonable need for the information.	X	X	X	X
3	The Revocation Authority **MUST** capture the following details about Attributes the Issuer has rendered unusable or unreliable: Date the action was taken; reason for the action; general indication of who initiated the action (e.g., Subject or Issuer).	X	X	X	X
4	The Revocation Authority **MUST** only disclose details captured about unusable or unreliable Attributes to known Participants with a reasonable need for the information.	X	X	X	X
5	The Revocation Authority **MUST** make the reason for revocation available to the Subject.	X	X	X	X

Reference	Conformance Criteria	Assurance Level			
		CAL1	CAL2	CAL3	CAL4
6	The Revocation Authority **MUST NOT** arbitrarily revoke Attributes. Revocation should be the result of relevant policies, procedures, legislation, regulation or confirmed or suspected nefarious activities, such as fraud, that would indicate undue risk should the Attribute be accepted.	X	X	X	X
7	The Revocation Authority **SHOULD** provide Subjects the ability to initiate a process to revoke, update, or otherwise render unusable or unreliable an Attribute issued to that Subject by that Issuer when the Subject detects indications of a compromised or invalid Attribute.	X	X	X	X
8	The Revoking Authority **SHOULD** establish, maintain, and make known to other Participants a process for resolving disputes concerning the accuracy of information contained in Attributes it has revoked.	X	X		
9	The Revoking Authority **MUST** establish, maintain, and make known to other Participants a process for resolving disputes concerning the accuracy of information contained in Attributes it has revoked.			X	X

Figure 8: Credentials (Relationships and Attributes) Conformance Criteria

5 Revision History

Version Number	Date of Issue	Author(s)	Description
0.01	2020-01-20	PCTF Editing Team	Initial Discussion Draft
0.02	2020-03-24	PCTF Editing Team	Incorporate TFEC comments
0.03	2020-04-23	PCTF Editing Team	Restructure for new Relationships and Attributes Processes
0.04	2020-04-29	PCTF Editing Team	Updated conformance criteria
1.0	2020-05-13	PCTF Editing Team	Draft Recommendation V1.0
1.1	2020-07-29	PCTF Editing Team	Draft Recommendation V1.1
1.0	2020-09-16	PCTF Editing Team	Final Recommendation V1.0