PCTF Assessment Component Overview Draft Recommendation V1.0

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

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

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

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. As always, comments are welcome on any aspect of the draft document. The items below are meant simply to highlight some areas that may be of more concern.

1. Is the description of roles and responsibilities clear at this level?
2. This draft describes a tiered assessment process with varying levels of evidence examination applied depending on risk and usage profile of the service being examined for certification
    1. Are the two processes defined enough? If not, what would be the nature of any additional discrete process? What would it apply to? Would its addition change the nature of either of the two processes defined?
    2. If the two process versions defined are sufficient, do the differences between them meet the goals of application of a less onerous certification process to some applications for certification? If not, then what would you suggest as an alternative?
    3. Keeping in mind the noting of potential adjustment based on the output of the TFEC Working group on LoA, are the criteria for determining which certification process applies acceptable in principle?
    4. A draft definition of classification based on service usage is included. Does this meet the needs of this Profile at this level? If not, what alternative would you suggest?
3. Are there concepts or terminology that remain unclear or inconsistently applied?
4. This Overview is meant to define the high level model and process for certification. Development of the significant Programme execution supporting information has been deferred until the model at this level is ratified. Are there any significant omissions from this high level Overview that would preclude you from understanding the model at this level?

5. Do you agree with the process for certification of Services as described? If not, what specific modifications would you suggest?
6. Do you agree with the process for certification of Accredited Assessors as described? If not, what specific modifications would you suggest?
7. The last section of the document identifies a number of required documents to support this certification process. The intent is to capture detailed process-oriented content in these documents after the Certification Assessment Program has been approved in principle. With this in mind, and considering the level of detail appropriate for this document, are there any major elements of the certification program not yet addressed in this draft?
8. Note that elements of examination for certification may be adjusted based on the finalization of the Working group on LoA, please keep this in mind when commenting on this document.

Table of Contents

1. Introduction to the PCTF Assessment Component

This document provides an overview of the **PCTF Assessment Component**, a component of the Pan-Canadian Trust Framework (PCTF). For an introduction to the PCTF, please see the

PCTF Model. The PCTF Model Overview provides the PCTF's goals and objectives, a high-level model outline of the PCTF, and contextual information.

PCTF components are normally made up of two documents:

1. **Component Overview –** Introduces the subject matter of the component. It provides essential information to help understand the Conformance Criteria of the component. This includes definitions of key terms, concepts, and the trusted processes that are part of the component.
2. **Component Conformance Profile –** Specifies the Conformance Criteria used to standardize and assess the integrity of the trusted processes that are part of the component.

Note: All PCTF components include a Component Conformance Profile document with the exception of the Assessment Component. The Assessment Component primarily elaborates the process by which compliance certification with PCTF profiles is achieved. As such, the criteria from all other profiles are the criteria against which compliance is assessed.

This overview provides information related to and necessary for consistent interpretation of the PCTF Assessment Component.

1.1. Purpose and Anticipated Benefits

The objective of the PCTF Assessment Component is to establish the procedures to examine the process, service, service network, or product of a Digital Identity Ecosystem participant and certify that it is compliant with Conformance Criteria defined in relevant PCTF components. Assessment and compliance certification with PCTF Conformance Profiles demonstrates proven implementation of PCTF principles and processes. This assures compliant implementation of digital identities, their underlying authorities, and their secure management. For the purposes of this document "service" will be used to refer to the product, service, service network, or process being examined for the purposes of Certification Assessment.

A service that has been certified is a Trusted Process that can be relied on by other participants of the Pan-Canadian Trust Framework (PCTF). The PCTF Conformance Criteria are intended to complement existing legislation and regulations; Participants in a DIACC-certified Digital Identity Ecosystem are required to meet the applicable legislated requirements and regulations in their jurisdictions.

The PCTF Assessment Component defines:

- The Assessment Program governance model, overseen by DIACC, to assess compliance with the Conformance Profiles of other PCTF components.
- The scope and processes to audit and certify compliance with implementation of the Conformance Profiles of other PCTF components.

1.2. Scope

This section defines the scope of the PCTF Assessment Component. In-scope activities are described at a high level such that primary roles, responsibilities, and activities can be understood. In-depth process detail for such things as certification process(es) will be addressed elsewhere.

1.2.1. In-Scope

This PCTF component describes the operation of the DIACC Certification Assessment Program (CAP) and the roles and responsibilities of stakeholder actors during the assessment and certification process. Specifically, this includes:

1. The roles and primary responsibilities of the organizations responsible for assessment and compliance:
    1. Certifying Authority
    2. Trustmark Issuer
    3. Accredited Assessor
    4. Certification Candidate
2. Within the identified organizations, a breakdown of pro forma roles and responsibilities within each of those organizations
3. High level descriptions of assessment methods and procedures, and their application
4. Certification program procedures and norms such as:
    1. Certificate issuance, publication, and maintenance
    2. Certification renewal procedures
    3. Assessment appeals procedures

This component addresses the compliance examination and certification of services against PCTF Profile(s). A service may be under the direction of a single organization or be a service network with component services provided by multiple organizations. In the case of a service network, the application for PCTF Profile compliance certification must be sponsored by a single representative of the service providers that comprise the service network.

1.2.2. Out-of-Scope

This scope of this PCTF component does not include:

1. The internal processes of the Certification Candidate related to certification processes. Internal preparation for, and response to, Conformance Profile assessment procedures will vary based on the Certification Candidate's established internal governance and management processes. However, the core touchpoints and requirements are governed by the PCTF Assessment Component.
2. Assessment and Conformance Criteria for individual DIACC PCTF Profiles. Each PCTF Conformance Profile provides specific criteria against which compliance is evaluated, when and where necessary.

3. Supplemental detailed assessment process, business model, submission and certification guidance, forms, and instructions will be developed after ratification of the high level model overview addressed in this document.

1.3. Relationship to the PCTF

The PCTF consists of a set of modular or functional components that can be independently assessed and certified for consideration as trusted components. Building on a Pan-Canadian approach, the PCTF enables the public and private sector to work collaboratively to safeguard digital identities by standardizing processes and practices across the Canadian digital ecosystem.

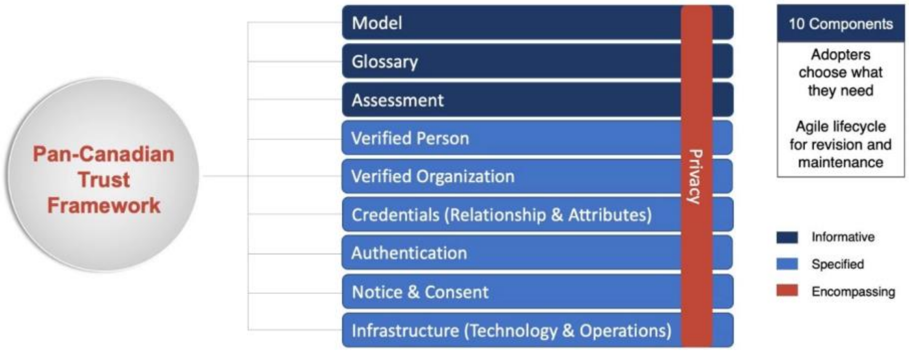

Pan-Canadian Trust Framework
Model
Glossary
Assessment
Verified Person
Verified Organization
Credentials (Relationship & Attributes)
Authentication
Notice & Consent
Infrastructure (Technology & Operations)
Privacy
10 Components
Adopters choose what they need
Agile lifecycle for revision and maintenance
Informative
Specified
Encompassing

Figure 1 - Components of the draft Pan-Canadian Trust Framework

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. Assessment and Compliance Conventions

This section describes and defines key terms and concepts used in the PCTF Assessment Component. This information is provided to ensure consistent use and interpretation of terms throughout this component.

Notes:

- Conventions may vary between PCTF components. Readers are encouraged to review the conventions for each PCTF component they are reading.
- Defined Terms – Key terms and concepts described and defined in this section and the PCTF Glossary are capitalized throughout this document.

- Hypertext Links – Hypertext links may be embedded in electronic versions of this document for reader reference. All links were accessible at time of writing.

2.1. Terms and Definitions

For purposes of this PCTF component, terms and definitions listed in the PCTF Glossary and the following terms and definitions apply.

- Certification Assessment - The performance of a assessing a Certification Candidate in accordance with the DIACC Certification Assessment Program.
- Certification Assessment Recommendation - A recommendation regarding a Certification Assessment.
- Certified Service - A process, service, service network, or product, submitted by a Certification Candidate, and successfully certified under CAP.
- Conformance Criteria – Requirements used to assess the trustworthiness of a specific process defined in the PCTF. These are used as the basis to assess compliance.
- Conformance Profile - Documentation, typically consisting of an Overview and more detailed Conformance profile document, identifying Conformance Criteria for each of the PCTF components.
- DIACC Certification Assessment Program - The DIACC Certification Assessment Program (CAP) is developed and operated by DIACC to assess compliance to standards and practices included in the PCTF.

Where the terms "compliance" and "conformance", or their variants, are used in lower case, they are meant to imply their traditional meanings. Conformance, usually self asserted, means a claim of alignment with or implementation of a requirement as elaborated in a standard, law, or regulation. In this case usually a set of PCTF Profile Conformance Criteria. Compliance refers to an enforced or verified conformance, in this case usually by virtue of the conduct of a Certification Assessment.

2.2. Abbreviations

The following abbreviations appear throughout this PCTF component.

- PCTF – Pan-Canadian Trust Framework
- DIACC – Digital ID and Authentication Council of Canada
- CAP – Certification Assessment Program
- CRB - Certification Review Board
- CISSP - Certified Information Systems Security Professional
- ISACA - Information Systems Audit and Control Association
- CISA - Certified Information Systems Auditor
- CDPSE - Certified Data Privacy Solutions Engineer
- eiDAS - Electronic Identification, Authentication and Trust Services
- NIST - National Institute of Standards and Technology

2.3. Roles

The following roles and role definitions are applicable in the scope and context of the PCTF Assessment Component, as they apply to the primary purpose of examining submitted services considered for certification. These roles help to isolate the different functions and responsibilities within the end-to-end Assessment & Compliance Trusted Processes. These processes exist within the CAP.

Note: Role definitions do not imply or require any particular solution, architecture, or implementation or business model.

- **Accredited Assessor -** An individual accredited by the Certifying Authority to conduct CAP assessments of compliance to standards and practices, including PCTF Conformance Profiles.
- **Certification Candidate -** An organization, or service network, submitting a candidate Certified Service seeking certification of compliance with one or more PCTF Conformance Profiles.
- **Certifying Authority -** The certifying authority responsible for overseeing the CAP. This includes compliance assessment and certification governance and policy. DIACC is the Certifying Authority for the CAP that verifies compliance with the PCTF.
- **Trustmark Issuer -** The entity authorized by the Certifying Authority to issue Trustmarks and maintain their currency and validity under the direction of the Certifying Authority. Each of the above listed roles encompass specific responsibilities as defined in the PCTF Assessment Conformance Profile. The figure below illustrates these enterprise roles and the primary responsibilities for each of these roles.

Note: An Organization may perform multiple roles. As an example, the Certifying Authority may also act as Trustmark Issuer. Some roles cannot be played by the same organization – specifically, An Accredited Assessor cannot also be the Certifying Authority.

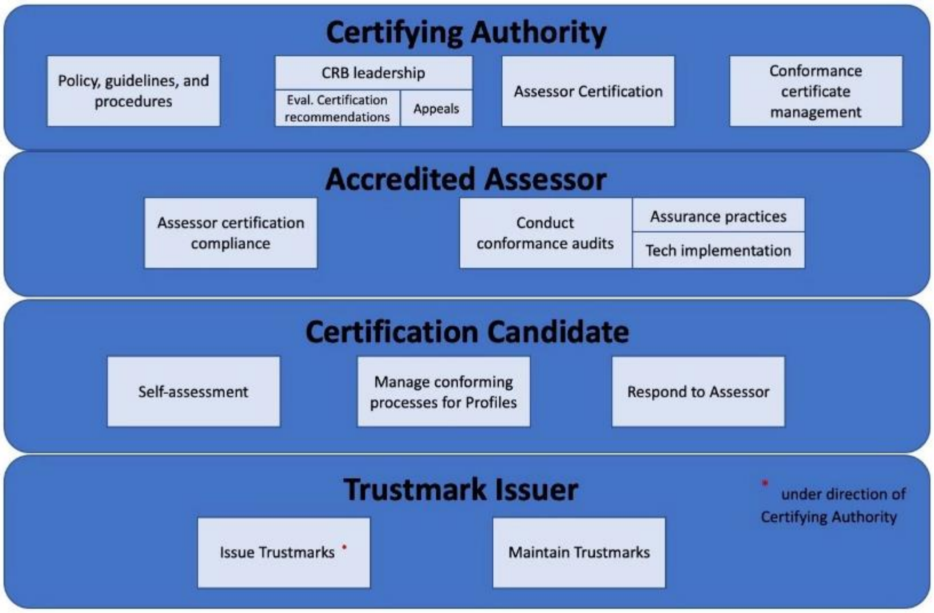

Certifying Authority
Policy, guidelines, and procedures
CRB leadership
Eval. Certification recommendations
Appeals
Assessor Certification
Conformance certificate management
Accredited Assessor
Assessor certification compliance
Conduct conformance audits
Assurance practices
Tech implementation
Certification Candidate
Self-assessment
Manage conforming processes for Profiles
Respond to Assessor
Trustmark Issuer
* under direction of Certifying Authority
Issue Trustmarks *
Maintain Trustmarks

Figure 2 - CAP roles and primary responsibilities

2.4. Responsibilities for the roles under the Certification Assessment Program (CAP)

Responsibilities at a more granular level for each role are as follows:

1. Certifying Authority
    1. Policy, guidelines and procedures
        1. Develop, publish, and maintain PCTF Conformance Criteria
        2. Develop, publish, and maintain CAP policy and procedures
        3. Responsible for Trustmark Definition
        4. Govern CAP operations and procedures
    2. Appeals
        1. Develop and maintain appeals guidelines
        2. Lead the conduct of submitted appeal review
        3. Adjudicate submitted appeals
    3. Accredited Assessor certification
        1. Develop and publish Accredited Assessor certification policy, requirements, and procedures
        2. Conduct Accredited Assessor evaluation and authorization to conduct certification audits
    4. Compliance certificate management
        1. Receive, review, and finalize results of Certification Candidate audits
        2. Develop, maintain, and publish directory of successful Certification Candidates and Certified Services
            1. The directory of Certified Services will contain essential metadata such as certification dates, service and PCTF version used in the assessment, which Profiles were assessed, and certification history
        3. Initiate Certification Candidate re-certification or de-certification processes as applicable
        4. Certification Review Board (CRB) leadership
2. Accredited Assessor
    1. Authorization compliance
        1. Maintain Accredited Assessor good standing as per Certifying Authority policy and procedures
        2. Initiate Accredited Assessor authorization or re-authorization processes as applicable
    2. Compliance audits
        1. Receive and evaluate Certification Candidate self and third-party assessment data as required
        2. Execute certification assessments per Certifying Authority policy and procedures
        3. Develop and submit to the Certifying Authority certification assessment or self-assessment review findings and a Certification Assessment Recommendation
3. Certification Candidate
    1. Self-assessment

        1. Develop and submit annual responses to PCTF Conformance Criteria based on templates developed by the Certifying Authority
    2. Manage compliance processes for PCTF Conformance Profiles
        1. Operate governance and on-going operations in alignment with information submitted during the certification process
        2. Maintain evidentiary audit data applicable to PCTF Conformance Criteria
    3. Respond to Assessor
        1. Respond to Accredited Assessor requests within the certification guidelines developed and published by the Certifying Authority
4. Trustmark issuer
    1. Validate Trustmark definition
    2. Issue Trustmarks based on Trustmark definition and Trustmark issuance procedures as defined with Certifying Authority
        1. Issued Trustmarks will be annotated in some form and have associated metadata that will indicate the PCTF Profile(s) certified against.
    3. Maintain integrity of Trustmark issuance and assurance systems/processes

2.4.1. Certification Review Board

The Certification Review Board (CRB) is an operational and authoritative body of the DIACC Certification Assessment Program. The CRB is seated through a nomination process overseen by the DIACC Board of Directors.

The CRB reviews applications, evidence, and Certification Assessment Recommendations provided by DIACC Accredited Assessors. The CRB recommends grant of the DIACC PCTF Trustmark to the DIACC Board of Directors. Multiple instances of the CRB may be created based on the specific needs of a community of interest seeking assessment for the purposes of certification. When processing matters related to the CAP the DIACC Board of Directors conducts a conflict review and call for recusals where CRB members may self-recuse or may be asked to recuse by another party to mitigate real or perceived conflicts.

PCTF certification assessment applies to:

- Services seeking to validate conformance to PCTF components
- Integrations of components between services operated by different entities
- Specific networks or communities of interest.

3. Compliance and Assessment

The PCTF promotes trust through a set of auditable business and technical requirements for various processes performed in the digital identity ecosystem. DIACC has created a number of Conformance Profiles that define the criteria for compliance with the PCTF.

This PCTF component defines the processes and procedures for assessing and certifying a participant's compliance with the relevant/applicable PCTF Conformance Profile. It is possible for a Certification Candidate to certify compliance with one or more components of the PCTF. This PCTF component also defines primary participant roles and responsibilities. Conformance Criteria for each PCTF component are not defined herein. Conformance Criteria for each of the PCTF components may be found in the DIACC Conformance Profile documentation for each of the Conformance Profiles.

There are processes and requirements for two certification processes.

1. The primary certification process applies to Certification Candidates applying to the Certifying Authority for assessment of a proposed Certified Service.
2. The Certifying Authority will also operate a formal process for the certification of Accredited Assessors.

3.1. Certification Candidate Assessment

Assessment is achieved using a combination of self-assessment and third-party audits, conducted by and Accredited Assessor, of compliance with Conformance Criteria. Assessment procedures and the scope of Accredited Assessor queries and data examination will be governed by the detailed audit procedures, developed and maintained by the certifying Authority, for each PCTF Profile.

Self-assessment addresses each of the Conformance Criteria as defined in the relevant DIACC PCTF components. The information gathered during self-assessment will answer the following key questions:

- How are specific Conformance Criteria addressed during day-to-day operations?
- What audit and reporting tools, processes, and procedures are in place to measure conformance?
- What verification tools, processes, and procedures are in place to ensure consistent criteria conformance?
- What governance and operational control processes are in place to address issues and deficiencies? These should address continuous quality management.

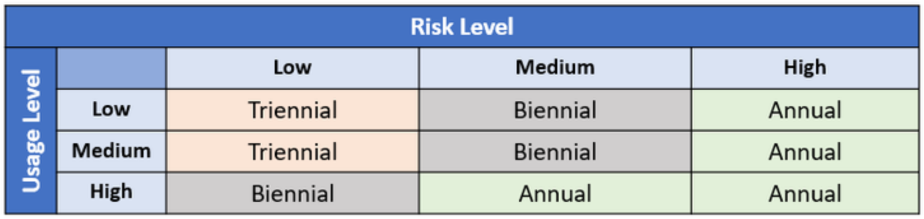
Accredited Assessor audit processes, building upon the data collected during self-assessment and consist of evidentiary examination of:

- Key standard processes, tools, and their usage as they apply to Conformance Criteria
- Examination of recent historical audit, reporting, verification, and governance artefacts
- Specific queries based on questions raised during evaluation of the self-assessment data

3.2. Certification, Certified Services

Certification of PCTF Profile compliance entitles the Certification Candidate to display the DIACC Trustmark (sometimes referred to as a Certification Seal) on written and electronic communication material during the Trustmark grant validity. The Certifying Authority will maintain a public status list of Certified Services&Solutions and Accredited Assessors available at http://diacc.ca/. Certified Services may opt-out of public listing on a case-by-case basis and with explicit notification to the Certifying Authority.

A DIACC Certification Trustmark is valid for a limited period of time and based on a DIACC Accredited Assessor's examination of PCTF Conformance Criteria. The period of validity will vary from one to three years depending on the risk and usage volume classification of the service. The highest frequency of assessment will apply to High Risk/High Volume services, The figure below identifies the frequency of assessment.



		Risk Level		
		Low	Medium	High
Usage Level	Low	Triennial	Biennial	Annual
	Medium	Triennial	Biennial	Annual
	High	Biennial	Annual	Annual

Figure 3 - Assessment frequency decision matrix

Note:

1. The frequency matrix may be adjusted to reflect the output of a DIACC Working group examining Levels of Assurance (LoA) for services and how they will affect the PCTF Profiles. The working group is currently working to define the number of levels and their classification criteria. This section will be modified, if required, when the DIACC Working Group on LoA has completed its work.
2. Certification may be extended for an additional 6 months after expiry when the re-certification process has been initiated prior to expiry of the current certification.
3. Certification applies to the service version examined and the PCTF Profile version under which it was examined. Service upgrades (i.e. functional changes, not usually regular maintenance releases) are subject to re-certification in order to apply the Trustmark.

3.2.1. Certification Assessment Process

DIACC governs the certification process as the Certifying Authority. DIACC authorizes and governs the activities of third-party Accredited Assessors. These Accredited Assessors are responsible for conducting PCTF compliance audits with Certification Candidates.

The assessment process is variable depending on two significant factors:

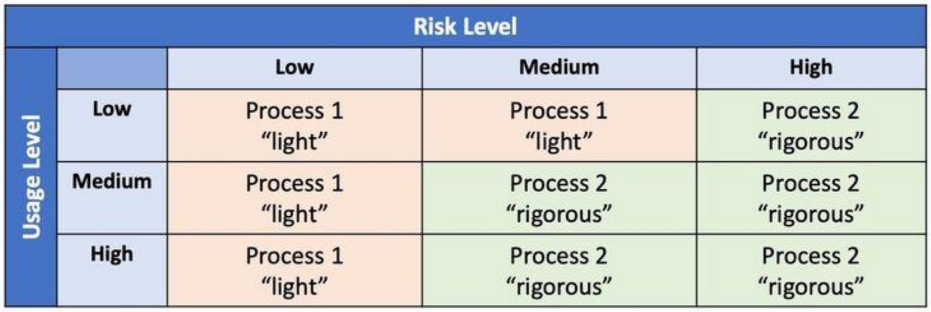
1. The level of risk associated with the process, service, or product submitted for examination. **NOTE:** *Risk levels are likely to be mapped to LoA, however, this is dependent on the results of the DIACC Working Group currently examining the treatment of LoA across all DIACC profiles. For the purposes of this draft document, risk level will be equated with LoA level. This will be re-examined upon the completion of the Working Group efforts. The intent of the model outlined is not expected to change.*
2. The level of service usage by individual clients in its targeted end user community. The guidelines for classification are as follows:
    1. High indicates usage one or more times weekly, on average, by typical service clients
    2. Medium indicates monthly usage that cannot be classified as High, on average, by typical service clients
    3. Low indicates usage frequency lower than Medium

There are two assessment process variants defined. These are:

1. Process 1, a "light" process, relies more on self attestation and little or no interactive examination of Candidate claims by the Accredited Assessor. This process would apply to lower risk/lower usage services submitted
2. Process 2, a more "rigorous" examination that relies more on closer (interactive) examination of Candidate claims by the Accredited Assessor.

The two processes are identical in terms of process steps required. the difference is the level of engagement and burden of proof required by the more rigorous process. The more rigorous process will require more interactive examination of conformance claims.

The assessment process to be applied is determined as shown in the figure below.



		Risk Level		
Usage Level		Low	Medium	High
	Low	Process 1 “light”	Process 1 “light”	Process 2 “rigorous”
	Medium	Process 1 “light”	Process 2 “rigorous”	Process 2 “rigorous”
	High	Process 1 “light”	Process 2 “rigorous”	Process 2 “rigorous”

Figure 4 - Assessment process decision matrix

3.2.1.1. Certification Process 1

The figure below illustrates the certification cycle and the primary responsibilities of the primary participants in the certification process (Process 1 - "light").

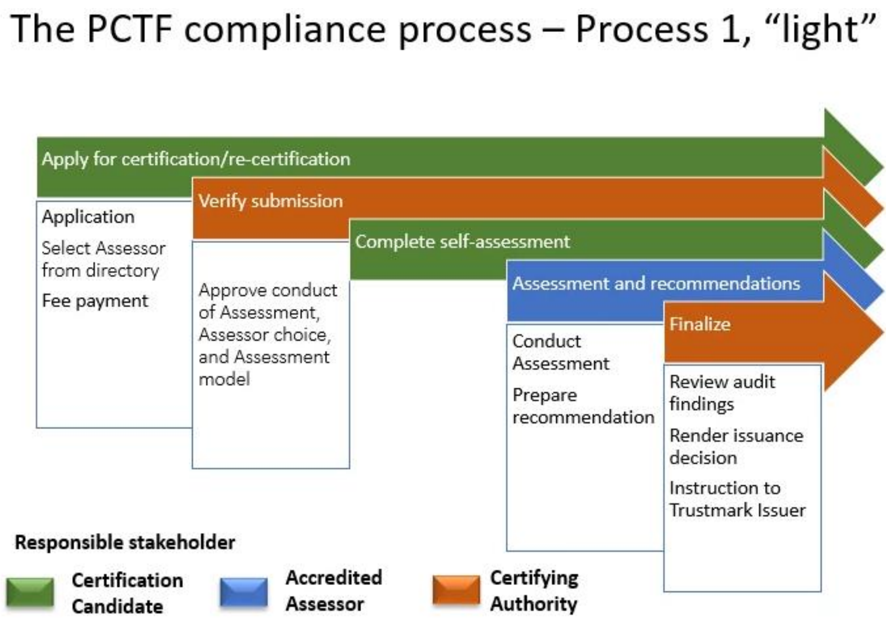

The PCTF compliance process – Process 1, “light”
Apply for certification/re-certification
Application
Select Assessor from directory
Fee payment
Verify submission
Approve conduct of Assessment, Assessor choice, and Assessment model
Complete self-assessment
Assessment and recommendations
Conduct Assessment
Prepare recommendation
Finalize
Review audit findings
Render issuance decision
Instruction to Trustmark Issuer
Responsible stakeholder
Certification Candidate
Accredited Assessor
Certifying Authority

Figure 5 - The certification process, primary roles of each participant (Process 1)

The less onerous certification process consists of the following steps, the **bolded** participant role indicates the party primarily responsible for each task:

- Application for certification (**Certification Candidate**)
    - Completion of initial application for certification based on materials available from DIACC
        - Certification Candidates will identify the PCTF Profiles that apply in their context and identify the process they believe applies based on the determining factors identified above.
    - Selection of Accredited Assessor(s) from directory
        - Chosen Accredited Assessor(s) are subject to approval from the Certifying Authority to prevent conflict of interest
            - Should the examination involve audit if both assurance practices and technology implementation, two separate qualified individuals may be identified
    - Identification of applicable model and its components
        - Does the assessment require only examination of assurance practices, or does an examination of technology implementation practice apply as well?
    - Submission of application and initial fees
        - Submission of fees covering the examination process up to, and including, CRB review. Ancillary fees covering Trustmark issuance will be applicable upon successful CRB review
- Initial review and permission to proceed (**Certifying Authority**)
    - Review ensures completeness of initial application information and eligibility of the applicant for certification
    - Approval of Accredited Assessor(s)
    - Acceptance of fees

- Completion of self-assessment (**Certification Candidate**)
    - Complete business agreement with Accredited Assessor(s)
    - Complete self-assessment/self-attestation
        - Certifying Authority support in the form of online self-assessment guidance and detailed form or template help material
- Audit completed self-assessment material (**Accredited Assessor**)
    - Review of submitted self-assessment data in detail to ensure complete coverage and completeness of responses to Conformance Criteria
        - Examination of assurance practices
        - Examination of technology implementation (if required - based on whether there is a technology product to evaluate and the nature of the Conformance Criteria against which the proposed Certified Service wishes to be evaluated)
    - Limited interaction with Certification Candidate on points of clarification or coverage
    - Assessment findings review, and potential adjustment, with Certification Candidate
    - Submission of findings and a Certification Assessment Recommendation
- Review findings and Certification Assessment Recommendation (**Certifying Authority - CRB**)
    - Potential for requests for additional clarification
    - Render Trustmark issuance decision
- Appeal findings (optional)
    - Submit appeal and appeal rationale (**Certification Candidate**)
    - Review appeal submission and rationale (**Certifying Authority**)
    - Upon acceptance of appeal, conduct Appeals process (**Certifying Authority**)
- Trustmark issuance, in the case of a successful application and audit (**Certifying Authority oversight**)
    - Issue notification of success to Certification Candidate (**Certifying Authority**)
    - Submission of ancillary Trustmark issuance fees (**Certification Candidate**)
    - Issue program templates and supporting materials, as applicable (e.g. program seal templates, rights documentation, etc.) (**Trustmark Issuer**)
    - Update directory of Certified Services (**Trustmark Issuer**)

3.2.1.2. Certification Process 2

The figure below illustrates the certification cycle and the primary responsibilities of the primary participants in the certification process (Process 2 - "rigorous").

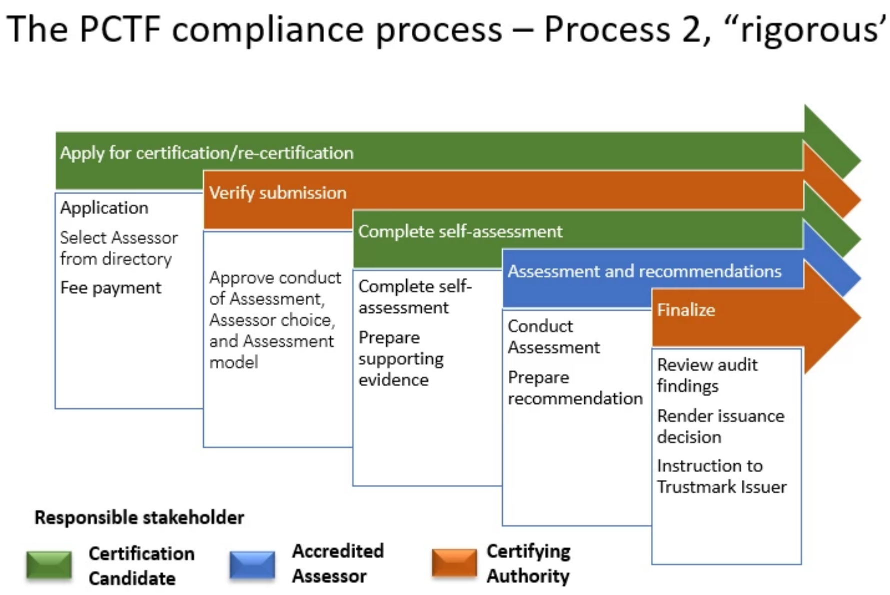

The PCTF compliance process – Process 2, "rigorous'
Apply for certification/re-certification
Application
Select Assessor from directory
Fee payment
Verify submission
Approve conduct of Assessment, Assessor choice, and Assessment model
Complete self-assessment
Complete self-assessment
Prepare supporting evidence
Assessment and recommendations
Conduct Assessment
Prepare recommendation
Finalize
Review audit findings
Render issuance decision
Instruction to Trustmark Issuer
Responsible stakeholder
🟩 Certification Candidate
🟦 Accredited Assessor
🟧 Certifying Authority

Figure 6 - The certification process, primary roles of each participant (Process 2)

The more rigorous certification process consists of the following steps, the **bolded** participant role indicates the party primarily responsible for each task. The process is essentially the same, the primary difference is the level of examination by the Accredited Assessor:

- Application for certification (**Certification Candidate**)
  - Completion of initial application for certification based on materials available from DIACC
    - Certification Candidates will identify the PCTF Profiles that apply in their context and identify the process they believe applies based on the determining factors identified above.
  - Selection of Accredited Assessor(s) from directory
    - Chosen Accredited Assessor(s) is subject to approval from the Certifying Authority to prevent conflict of interest
      - Should the examination involve audit if both assurance practices and technology implementation, two separate qualified individuals may be identified
  - Identification of applicable model and its components
    - Does the assessment require only examination of assurance practices, or does an examination of technology implementation practice apply as well?
  - Submission of application and initial fees
    - Submission of fees covering the examination process up to, and including, CRB review. Ancillary fees covering Trustmark issuance will be applicable upon successful CRB review
- Initial review and permission to proceed (**Certifying Authority**)
  - Review ensures completeness of initial application information and eligibility of the applicant for certification
  - Approval of Accredited Assessor(s)
  - Acceptance of fees

- Completion of self-assessment (**Certification Candidate**)
    - Complete business agreement with Accredited Assessor(s)
    - Complete self-assessment
        - Certifying Authority support in the form of online self-assessment guidance and detailed form or template help material
    - Gather evidence to the extent possible to prepare for Accredited Assessor examination
- Audit completed self-assessment material (**Accredited Assessor**)
    - Review of submitted self-assessment data in detail to ensure complete coverage and completeness of responses to Conformance Criteria
        - Examination of assurance practices
        - Examination of technology implementation (if required - based on whether there is a technology product to evaluate and the nature of the Conformance Criteria against which the proposed Certified Service wishes to be evaluated)
    - Examine evidence of Certification Candidate claims
        - This will be more interactive than Process 1, likely including secondary questions for additional materials or demonstration of claims
        - Specific requirements for examination will be identified in detailed process documentation that will vary somewhat depending on the Profile(s) and associated Conformance Criteria being examined
    - Assessment findings review, and potential adjustment, with Certification Candidate
    - Submission of findings and a Certification Assessment Recommendation
- Review findings and Certification Assessment Recommendation (**Certifying Authority - CRB**)
    - Potential for requests for additional clarification
    - Render Trustmark issuance decision
- Appeal findings (optional)
    - Submit appeal and appeal rationale (**Certification Candidate**)
    - Review appeal submission and rationale (**Certifying Authority**)
    - Upon acceptance of appeal, conduct Appeals process (**Certifying Authority**)
- Trustmark issuance, in the case of a successful application and audit (**Certifying Authority oversight**)
    - Issue notification of success to Certification Candidate (**Certifying Authority**)
    - Submission of ancillary Trustmark issuance fees (**Certification Candidate**)
    - Issue program templates and supporting materials, as applicable (e.g. program seal templates, rights documentation, etc.) (**Trustmark Issuer**)
    - Update directory of Certified Services (**Trustmark Issuer**)

3.2.1.3. Accredited Assessors

Accredited Assessors are third parties, independent from the Certifying Authority (DIACC) and the Certification Candidate, certified by the Certifying Authority to conduct compliance audits for the purpose of informing the granting of certification. These third-party auditors will be experts in the fields of privacy, digital identity, and other fields related to the establishment and maintenance of online trust. Independence from the Certifying Authority applies to management and staff of the Certifying Authority. Employees or other individuals associated with DIACC members may become Accredited Assessors, subject to the accreditation requirements identified in this document.

Similar to PCTF Profile compliance certification itself, these Accredited Assessors are subject to periodic review and re-certification. The Certifying Authority will conduct annual reviews of authorized third-party assessors to ensure they continue to retain and enhance the core knowledge and experience required of its Accredited Assessors. Certification of Accredited Assessors will focus on authorized individuals within the organization and not the organizations themselves.

A directory of Accredited Assessors will be maintained and published by the Certifying Authority.

3.2.1.4. Certification Assessment Appeals

Should the Certification Candidate wish to appeal a negative certification decision from the CRB or a submitted negative Certification Assessment Recommendation from an Accredited Assessor, there is an appeals process that can be invoked if all informal avenues of resolution are exhausted. The appeal process begins with an appeal notification and rationale, developed by the Certification Candidate, submitted to the Accredited Assessor and DIACC (CRB).

The Certifying Authority will conduct a preliminary examination of the submitted appeal and associated rationale with the Certification Candidate and the Accredited Assessor, to ensure that there are no information gaps that may preclude evaluating the appeal. In this phase DIACC may attempt to mediate, and perhaps adjust the assessment, if the resolution looks straightforward.

If the appeal remains unresolved, then an appointee authorized to perform this role oversees a formal review of the assessment detail that may result in any one of:

- Re-assessment with another Accredited Assessor due to Accredited Assessor shortcomings
- Identification of PCTF Profile shortcomings that may have contributed to an incorrect result
- Upholding of the original assessment
- Review findings with a period of time to supply additional evidence to DIACC reviewer
- Overturning of original assessment and granting of certification

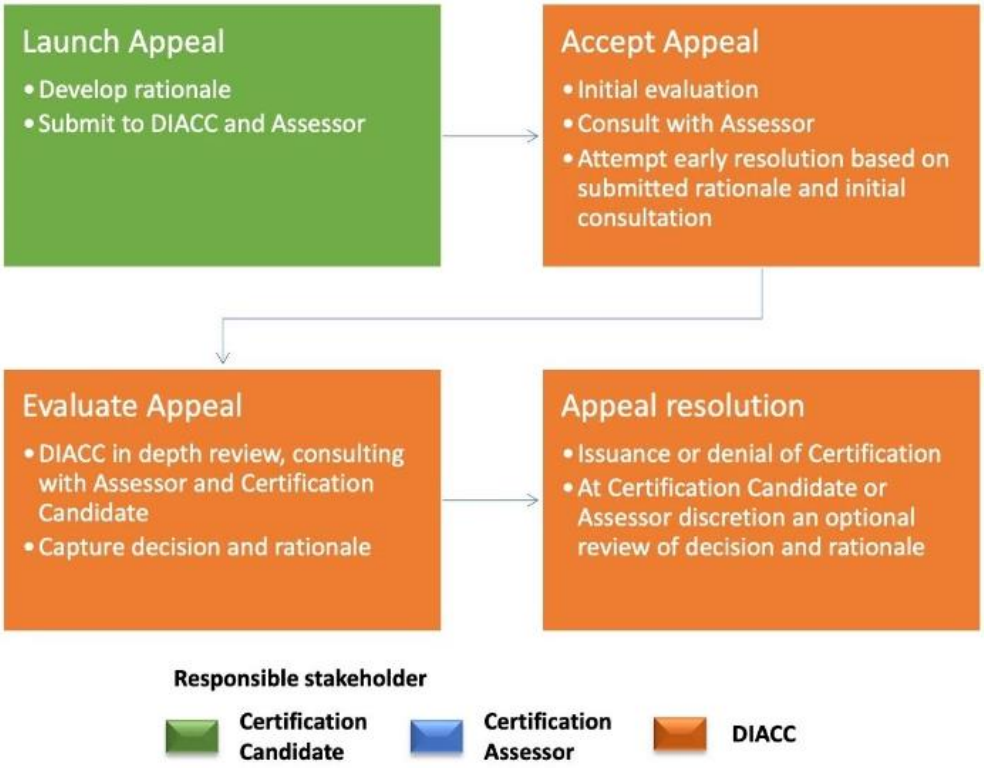

Launch Appeal
• Develop rationale
• Submit to DIACC and Assessor
Accept Appeal
• Initial evaluation
• Consult with Assessor
• Attempt early resolution based on submitted rationale and initial consultation
Evaluate Appeal
• DIACC in depth review, consulting with Assessor and Certification Candidate
• Capture decision and rationale
Appeal resolution
• Issuance or denial of Certification
• At Certification Candidate or Assessor discretion an optional review of decision and rationale
Responsible stakeholder
Certification Candidate
Certification Assessor
DIACC

Figure 7 - Certification Assessment appeal process

Note: The appeal will be presided over by an arms-length appointee of DIACC to help mitigate issues that might arise due to the appeals body and original CRB participants being the same individual(s).

3.2.1.5. Continuous monitoring

In addition to the appeals process for the findings and recommendations emanating from Assessments examinations, there should be a real-time process operated by the Certifying Authority to accept complaints or questioning that current validity of issued certification of a Certified Service. Under this continuous monitoring program:

- Existence of a complaint and the status of its examination will be noted in a directory of Certified Services.
- An accepted complaint will trigger initial investigation by the Certifying Authority.
- At the discretion of the Certifying Authority a formal ad hoc Assessment may be required to retain certified status. The process required would be the same as the original examination process, based upon the risk and usage profiles of the service to be examined.

3.3. Certification, Accredited Assessors

Accredited Assessors will also be subject to a certification process. This will be conducted by the Certifying Authority upon application, and submission of fees, by the applicant wishing to become an Accredited Assessor. Accredited Assessors will be subject to annual re-certification.

Accredited Assessors may apply to be accredited for either, or both, components that may be required for an assessment. These are:

- Assurance practices - required for every assessment. These will examine elements such as standards, delivery processes, audit and control processes, and governance practices.
- Technology implementation - may be required for an assessment. This will be determined during the initial application process. In this component the technology standards and their implementation in the components delivering the service(s) will be examined.

The figure below illustrates the certification cycle and the primary responsibilities of the primary participants in the certification process.

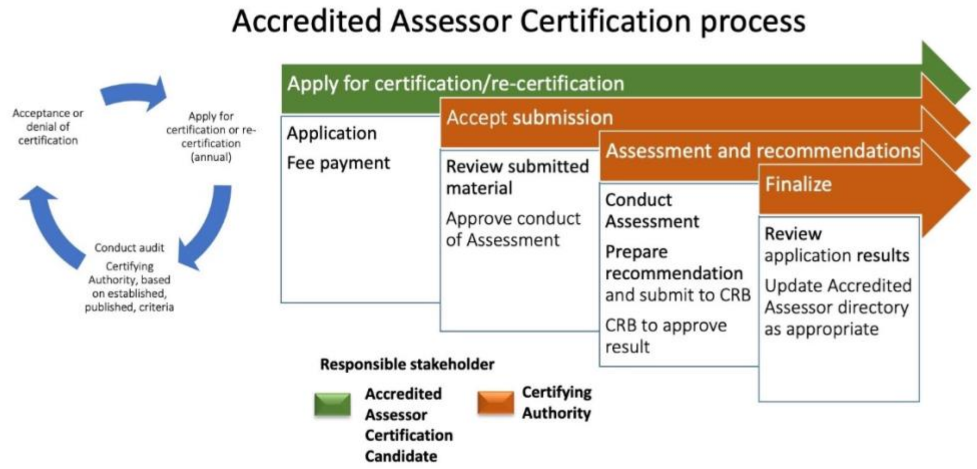

Accredited Assessor Certification process
Acceptance or denial of certification
Apply for certification or re-certification (annual)
Conduct audit
Certifying Authority, based on established, published, criteria
Apply for certification/re-certification
Application
Fee payment
Accept submission
Review submitted material
Approve conduct of Assessment
Assessment and recommendations
Conduct Assessment
Prepare recommendation and submit to CRB
CRB to approve result
Finalize
Review application results
Update Accredited Assessor directory as appropriate
Responsible stakeholder
Accredited Assessor Certification Candidate
Certifying Authority

Figure 8 - Accredited Assessor certification process

The Accredited Assessor certification process consists of the following steps, the **bolded** participant role indicates the party primarily responsible for each task:

- Preparation and submission of application materials as specified (**Accredited Assessor applicant**)
- Submission of application fees (**Accredited Assessor applicant**)
- Examination of application and approval to proceed with examination process (**Certifying Authority or designate**)
- Conduct of examination and follow-up to ensure qualifications (**Certifying Authority or designate**)
- Development of findings and recommendations (**Certifying Authority or designate**)
- Submission to CRB (**Certifying Authority**)

- Final approval or rejection of application (**CRB**)
- Update of Accredited Assessor directory as appropriate (**Certifying Authority**)
- Development of service delivery framework and processes, in alignment with Certifying Authority policy and related requirements (**Accredited Assessor**)

3.4. Equivalence of other certifications

At this time, there are no direct correlation to existing certifications that can be drawn to establish a cross certification relationship where one certification can serve as a proxy for another. That said there are certifications that exist in areas that will serve to reduce the examination required for certification.
Specifically:

- For certification of Accredited Assessors, security certifications such as CISSP or certifications from ISACA (e.g. CISA, CDPSE), may serve to provide credit towards the examination of requirements to become an Accredited Assessor
- For certification against one or more PCTF profiles, formal audit results evaluating compliance with eiDAS (EU) or NIST 800-3 (USA) may serve as a proxy for compliance with specific requirements for examination of PCTF Profile conformance. However, audit results for evaluation of compliance against these standards cannot form the entire basis for evaluation of PCTF Profile compliance.

4. References

This section lists all other documents referenced in this PCTF component.

Note: Where applicable, only the version or release number specified herein applies to this PCTF component.

Component Conformance Profiles containing the specific criteria against which Certification Candidates will be assessed:

- Verified Person Conformance Profile
- Verified Organization Conformance Profile
- Credentials: Relationships & Attributes Conformance Profile
- Authentication Conformance Profile
- Notice & Consent Conformance Profile
- Infrastructure: Technology and Operations Conformance Profile
- Privacy Conformance Profile
- PCTF Profiles Glossary

Detailed procedural and template documents supporting the assessment process (*to be developed after initial ratification of this Overview document*):

- Certification Assessment Program process detail
- Accredited Assessor application template
- Certification Application
- Self-assessment template
- Certification audit findings template
- Certification Audit detailed procedures
- Appeal submission template
- Appeals process detailed procedures
- Various guides and other help resources
- Trustmark license agreement
- Certification review Board non-disclosure agreement
- Additional legal agreements (TBD)