PCTF Assessment Component Overview

Document Status: Final Recommendation V1.0

In accordance with the DIACC Operating Procedures, a Final Recommendation is a deliverable that represents the findings of a DIACC Expert Committee that have been approved by an Expert Committee and have been ratified by a DIACC Sustaining Member Ballot.

This document was developed by DIACC's Trust Framework Expert Committee with input from the public gathered and processed through an open peer review process. It is anticipated that the contents of this document will be reviewed and updated on a regular basis to address feedback related to operational implementation, advancements in technology, and changing legislation, regulations, and policy. Notification regarding changes to this document will be shared through electronic communications including email and social media. Notification will also be recorded on the Pan-Canadian Trust Framework Work Programme. Changes to this document that may affect certification and Trustmark status will be defined in the Pan-Canadian Trust Framework Assessment component.

This document is provided "AS IS," and no DIACC Participant makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third-party intellectual property rights, and fitness for a particular purpose. Those who are seeking further information regarding DIACC governance are invited to review the DIACC Controlling Policies.

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 Overview. The Model Overview identifies the PCTF's goals and objectives, a high-level model outline of the framework, 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 verification with PCTF Conformance Profiles, and trustmark issuance, is achieved. As such, the Conformance 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 verify that it is compliant with Conformance Criteria defined in relevant PCTF Conformance Profiles. Assessment and compliance verification with PCTF Conformance Profiles demonstrates proven implementation of PCTF principles and processes. This assures conforming 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 Verification Assessment.

A service, that has been verified, is a Trusted Process that can be relied on by other participants of the PCTF. The PCTF Conformance Criteria are intended to complement existing legislation and regulations. Participants in a verified Digital Identity Ecosystem are required to meet the applicable legislated requirements and regulations in their jurisdictions.

The PCTF Assessment Component defines:

- the Trustmark Assessment Program governance model, overseen by DIACC, to assess compliance with PCTF Conformance Profiles.
- the scope and processes applicable to a Verification Assessment conducted under the Trustmark Assessment Program.

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 detail pertaining to verification process(es), templates, and other guidance will be addressed elsewhere.

1.2.1 In-Scope

This PCTF component describes the operation of the DIACC Trustmark Verification Program (TVP) and the roles and responsibilities of stakeholder actors during the verification process. Please see the Assessment and Compliance section of this document for a definition of roles and terminology used throughout. Specifically, this includes:

1. The roles and primary responsibilities of the organizations responsible for assessment and compliance verification:
    - Trustmark Authority;
    - Trustmark Assessor; and
    - Trustmark Applicant.
2. Within the identified organizations, additional elaboration of roles and responsibilities for each of those organizations.
3. High level descriptions of assessment methods and procedures, and their application.
4. Trustmark Verification Program procedures and norms such as:
    - trustmark issuance, publication, and maintenance;
    - trustmark application and renewal procedures, and
    - assessment appeals procedures.

This component addresses the compliance verification of services within the context of the PCTF Conformance 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 verification 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:

- The internal processes of the Trustmark Applicant related to verification processes.
    - Internal preparation for, and response to, Conformance Profile assessment procedures will vary based on the Trustmark Applicant's established internal governance and management processes. However, the core touchpoints and requirements are governed by the PCTF Assessment Component.

- Assessment and Conformance Criteria for individual DIACC PCTF Profiles.
  - Each PCTF Conformance Profile provides specific criteria against which conformity is evaluated, when and where necessary.
- Supplemental detailed assessment process, business model, submission and certification guidance, forms, and instructions are identified but not elaborated upon.
  - These will be developed after ratification of the high-level model described 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 verified 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 Identity Ecosystem.

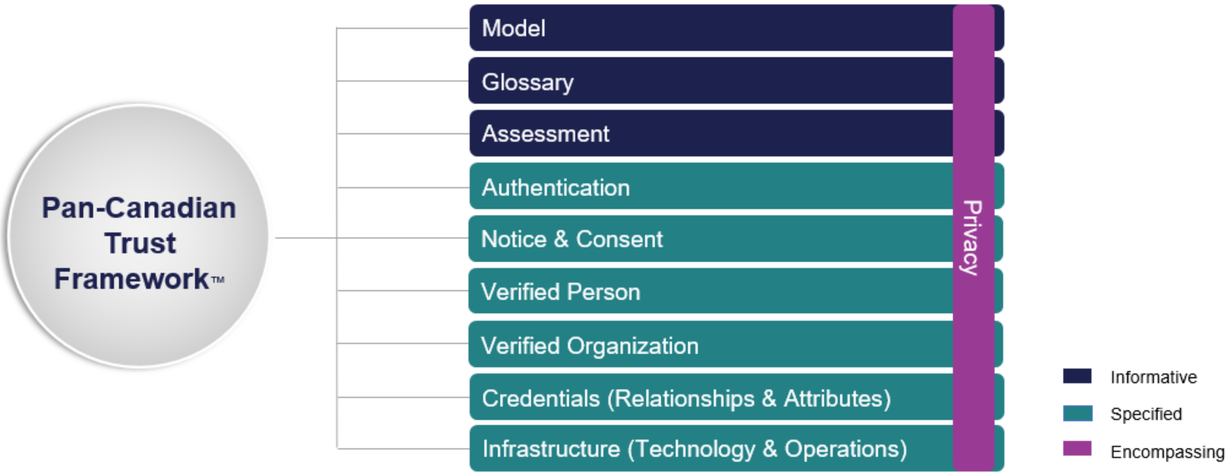


Figure 1 - Components of the Pan-Canadian Trust Framework

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.

Conformance Criteria

Requirements used to assess the trustworthiness of a specific process defined in the PCTF, and captured in PCTF Conformance Profiles. These are used as the basis of a Verification Assessment.

Conformance Profile

Documentation, typically consisting of an Overview and more detailed Conformance Profile document, identifying Conformance Criteria for each of the PCTF components.

DIACC Trustmark Verification Program

The DIACC Trustmark Verification Program (TVP) is developed and operated by DIACC to assess compliance with Conformance Criteria included in the PCTF Conformance Profiles.

Digital Identity Ecosystem

An interconnected system for the exchange and verification of digital Identity Information, involving public and private sector Organizations that comply with a common Trust Framework for the management and use of digital identities, and the Subjects of those digital identities.

Technology Evaluation

Refers to the hands-on verification of the Trustmark Applicant claims related to the technology components of a submitted service being examined during a Verification Assessment.

Trustmark

Refers to a trustmark issued as a result of a successful Verification Assessment under the TVP.

Verification Assessment

The action of assessing a Trustmark Applicant service in accordance with the DIACC Trustmark Verification Program.

Verification Assessment Recommendation

A recommendation developed by the Trustmark Assessor during a Verification Assessment.

Verified Service

A process, service, service network, or product, submitted by a Trustmark Applicant, and successfully verified under TVP.

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 Verification Assessment. Similarly, "trustmark" is meant to refer to a generic indicator of compliance with a formal set of standards against which the trustmark recipient has been assessed by the trustmark issuer or its designate, typically under a formal assessment programme.

2.2 Abbreviations

The following abbreviations appear throughout this PCTF component.

- PCTF – Pan-Canadian Trust Framework
- DIACC – Digital ID and Authentication Council of Canada
- TVP – Trustmark Verification Program
- TRB - Trustmark 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 verifying submitted services considered for Trustmark issuance. These roles help to isolate the different functions and responsibilities within the end-to-end Verification Assessment process.

- **Trustmark Assessor -** An individual or organization accredited by the Trustmark Authority to conduct TVP Verification Assessments of compliance to requirements contained in PCTF Conformance Profiles.
- **Trustmark Applicant -** An organization, or service network, submitting a candidate Verified Service and seeking verification of compliance with one or more PCTF Conformance Profiles for the purposes of Trustmark issuance.

- **Trustmark Authority -** The body responsible for overseeing the TVP. This includes compliance assessment and verification governance and policy. DIACC is the Trustmark Authority for the TVP.

Note

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

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.

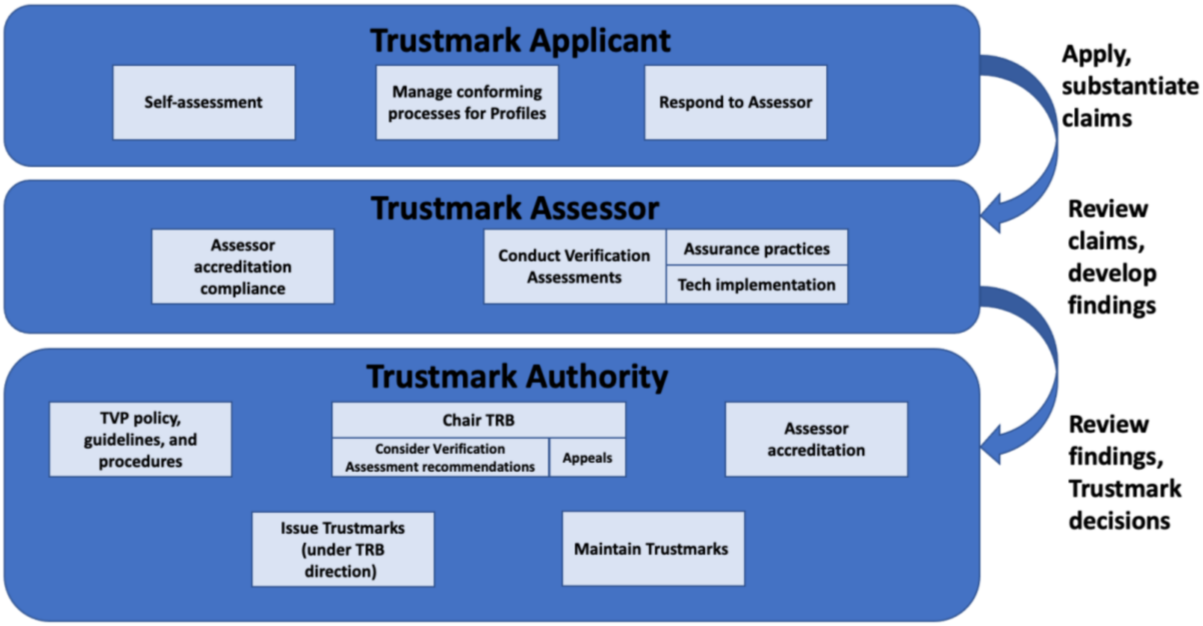

Trustmark Applicant
Self-assessment
Manage conforming processes for Profiles
Respond to Assessor
Apply, substantiate claims
Trustmark Assessor
Assessor accreditation compliance
Conduct Verification Assessments
Assurance practices
Tech implementation
Review claims, develop findings
Trustmark Authority
TVP policy, guidelines, and procedures
Chair TRB
Consider Verification Assessment recommendations
Appeals
Assessor accreditation
Issue Trustmarks (under TRB direction)
Maintain Trustmarks
Review findings, Trustmark decisions

Figure 2 - TVP roles and primary responsibilities

Note

- An Organization may perform multiple roles, but not in the same instance of a Verification Assessment (e.g. cannot be both Trustmark Applicant and Assessor, however, an organization may be a Trustmark Applicant or Assessor at different times). Some roles cannot be played by the same organization during a specific instance of a Verification Assessment. For instance, a Trustmark Assessor or Trustmark Applicant cannot act in any other role; the Trustmark Authority may not act in either Trustmark Assessor or Trustmark Applicant roles.

2.4 Responsibilities for the Roles under the Trustmark Verification Program (TVP)

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

1. **Trustmark Authority**
    1. Policy, guidelines and procedures
        1. Develop, publish, and maintain PCTF Conformance Criteria
        2. Develop, publish, and maintain TVP policy and procedures (please see References section for a list of supporting documentation to be developed)
        3. Govern TVP operations and procedures
    2. Appeals
        1. Develop and maintain appeals guidelines
        2. Lead the conduct of submitted appeal review
        3. Adjudicate submitted appeals (with TRB)
    3. Trustmark Assessor accreditation
        1. Develop and publish Trustmark Assessor accreditation policy, requirements, and procedures
        2. Conduct Trustmark Assessor evaluation and authorization to conduct Verification Assessments
    4. Trustmark management
        1. Validate initial Trustmark Applicant application, approve Verification Assessment model and Trustmark Assessor choice
        2. Receive, review, and finalize results of Trustmark Applicant audits under the auspices of the TRB
        3. Develop, maintain, and publish directory of successful Trustmark Applicants and Verified Services
            1. The directory of Verified Services will contain essential metadata such as certification dates, service and PCTF version used in the Verification Assessment, which PCTF Profiles were assessed, and verification history
        4. Initiate Trustmark Applicant de-certification processes if applicable
        5. Chair of the Trustmark Review Board (TRB)
        6. Issue Trustmarks based on Trustmark definition and Trustmark issuance procedures as defined with Trustmark Authority
            1. Issued Trustmarks will be annotated in some form to reflect the metadata identified above.
        7. Maintain integrity of Trustmark issuance and assurance systems/processes
2. **Trustmark Assessor**
    1. Accreditation compliance
        1. Maintain Trustmark Assessor good standing as per Trustmark Authority policy and procedures
        2. Initiate Trustmark Assessor accreditation or accreditation renewal processes as applicable
    2. Verification Assessments
        1. Receive and evaluate Trustmark Applicant self and third-party assessment data as required
        2. Execute Verification Assessments per Trustmark Authority policy and procedures

        3. Develop and submit, to the Trustmark Authority, Verification Assessment review findings and a Verification Assessment Recommendation

3. **Trustmark Applicant**
    1. Self-assessment
        1. Develop and submit responses, as required, to PCTF Conformance Criteria based on templates developed by the Trustmark Authority
    2. Manage conforming processes for PCTF Conformance Profiles
        1. Operate governance and on-going operations in alignment with information submitted during the verification process
        2. Maintain evidentiary audit data applicable to PCTF Conformance Criteria
    3. Respond to Assessor
        1. Respond to Trustmark Assessor requests within the Verification Assessment guidelines developed and published by the Trustmark Authority
    4. Initiate Trustmark renewal processes when required

2.4.1 Trustmark Review Board

The Trustmark Review Board (TRB) is an operational and authoritative body of the DIACC Trustmark Verification Program. The TRB is seated through a nomination process overseen by the DIACC Board of Directors and is chaired by the Trustmark Authority.

The TRB reviews Verification Assessment Recommendations and supporting information provided by TVP Trustmark Assessors. The TRB renders Trustmark issuance decisions and recommends grant of the DIACC PCTF Trustmark to the DIACC Board of Directors. Multiple instances of the TRB may be created based on the specific needs of a community of interest seeking Verification Assessment. When processing matters related to the TVP, the TRB conducts a conflict review and call for recusals where TRB members may self-recuse or may be asked to recuse by another party to mitigate real or perceived conflict of interest.

TVP Verification Assessment applies to:

- Services seeking to validate conformance to PCTF components
- Specific service networks or communities of interest offering a defined service.

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 conformity with the PCTF.

This PCTF component defines the processes and procedures for verifying a Trustmark Applicant's compliance with the relevant/applicable PCTF Conformance Profile(s). Trustmark Applicants can choose to have their Verification Assessment apply to any 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 PCTF Conformance Profiles.

There are processes and requirements for two verification processes.

1. The primary verification process (Verification Assessment) applies to Trustmark Applicants applying to the Trustmark Authority for examination of a proposed Verified Service.
2. The Trustmark Authority will also operate a process for the accreditation of Trustmark Assessors.

3.1 Verification Assessment, Proposed Verified Services

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

Self-assessment addresses each of the Conformance Criteria as defined in the relevant 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 conformance?
- What governance and operational control processes are in place to address issues and deficiencies? These should address continuous quality management.

Trustmark Assessor verification processes, are built 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;
- recent historical audit, reporting, verification, and governance artefacts; and
- specific queries based on questions raised during evaluation of the self-assessment data.

A Verification Assessment will focus on two high level components of the service being examined. The first is an examination of the policies, processes, standards, and other supporting materials governing service operation and delivery. Hereafter this is referred to as "*assurance practices*", for the sake of brevity. The second is an examination of the key technology components required to deliver the service(s). Technology assessments seek to verify if the technology is performing as per Conformance Criteria specifications.

It is important to note that a Verification Assessment may;

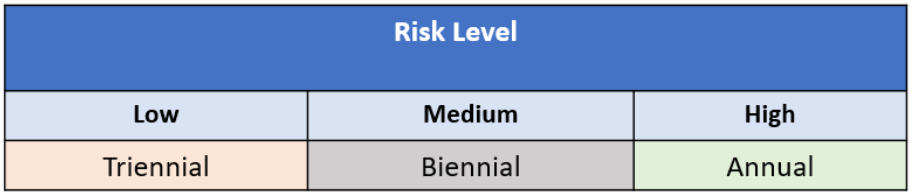
- consist of one or both types of examination, depending on whether there is a technology component to be examined. While most submitted services are expected to include a technology component, it is possible that a submitted service may be entirely policy, process, or standards based - relying upon others for implementation. In this case, the policies/processes/standards would be verified but individual downstream implementations would be subject their own examination and Trustmark issuance processes based on individual implementer's preference.
- involve more than one Trustmark Assessor depending on the qualifications of the Trustmark Assessor(s) retained (please see the *Certification, Trustmark Assessors* section of this document).

Successful verification of PCTF Conformance Profile compliance entitles the Trustmark Applicant to display the DIACC Trustmark (sometimes referred to as a Verification Seal) on written and electronic communication material during the Trustmark grant validity period. The Trustmark Authority will be responsible for a public status list of Verified Services available at http://diacc.ca/. Verified Services may opt-out of public listing on a case-by-case basis and with explicit notification to the Trustmark Authority.

The Trustmark indicates arms-length verification of compliance with PCTF Conformance Profiles, demonstrating proven implementation of PCTF Conformance Profile principles, processes, and standards. This assures conforming implementation of digital identities, their underlying authorities, and their secure management as defined in the PCTF Conformance Profiles.

3.1.1 Trustmark Validity Period

A Trustmark is valid for a limited period of time and based on a TVP Trustmark Assessor's verification of conformity with PCTF Conformance Criteria. The period of validity will vary from one to three years depending on the risk classification of the service. The highest frequency of assessment will apply to highest risk services. The figure below identifies the frequency of assessment.



Risk Level		
Low	Medium	High
Triennial	Biennial	Annual

Figure 3 - Assessment frequency decision matrix

Note

- The frequency matrix and type of audit (i.e. assurance practices, technology, both) required 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.

- The Trustmark validity period may be extended for an additional 6 months after expiry when the renewal process has been initiated prior to expiry of the current Trustmark.
- The issued Trustmark applies to the service version examined and the PCTF Conformance Profile version under which it was examined. Service upgrades affecting conformity with PCTF Conformance Criteria (i.e. significant functional changes, not usually regular maintenance releases) are subject to a Verification Assessment in order to apply the Trustmark.

3.1.2 Verification Assessment Process(es)

DIACC governs the TVP as the Trustmark Authority. The Trustmark Authority specifies the manner in which Trustmark Assessors shall perform Verification Assessments. Trustmark Assessors are responsible for conducting Verification Assessments with Trustmark Applicants.

The verification process is variable depending on the level of risk associated with any compromise to service delivery or service information.

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 PCTF 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.*

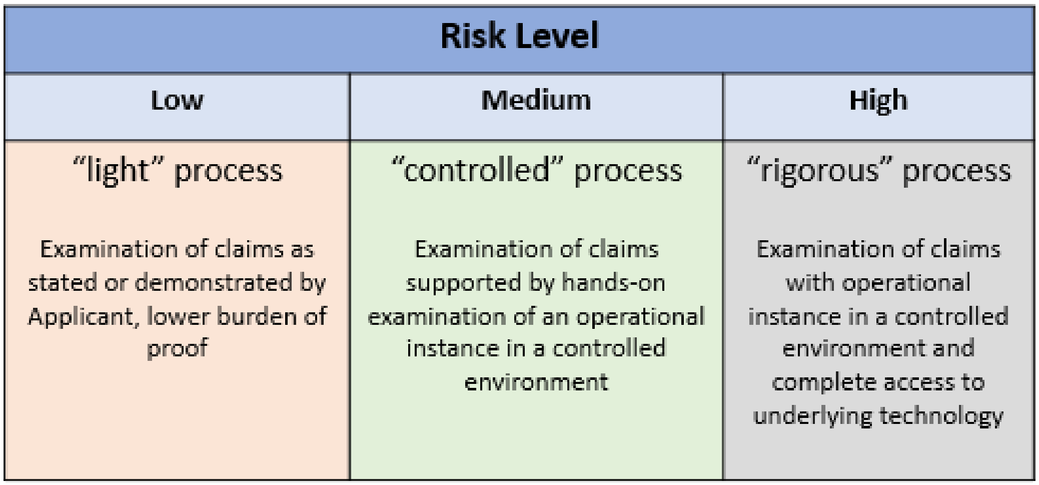
There are three assessment process variants defined, the definitions below assume a Verification Assessment that includes assessment of both assurance practices and technology. These are:

1. A "light" assessment which relies more on the examination by the Trustmark Assessor of claims made by the Trustmark Applicant and provides for little interactive verification of those claims. This process would apply to lower risk services submitted. Trustmark Applicant/Trustmark Assessor interaction during examination of claims will generally feature information requests to improve clarity and Trustmark Applicant operational demonstration(s) to support claims.
2. A "controlled" assessment that relies on interactive examination of Trustmark Applicant claims by the Trustmark Assessor. This process would apply to medium risk services submitted. This process will include a high level Technology Evaluation to confirm data going in and out of the assessed solution or network and will be supported by an operational service instance in a controlled environment. Assurance practice and technology component assessment will be subject examination of the operational service instance, in operation, to observe compliance with PCTF Conformance Criteria.
3. A "rigorous" assessment that relies on (**A**) interactive examination of Trustmark Applicant claims by the Trustmark Assessor; (**B**) includes activities identified in the "*controlled"* assessment process; and (**C**) a low level Technology Evaluation to confirm

software and/or hardware conformance claims made by the Trustmark Applicant, to ensure compliance with PCTF Conformance Criteria.

The difference between processes is the level of engagement and burden of proof required as risk level increases. Candidate Verified Services classified as Medium or High risk will require more interactive examination of conformance claims and supporting evidence. Additional process detail will be available in the supplemental programme documentation identified in the References section of this document.

The figure below illustrates the application of these process variants.

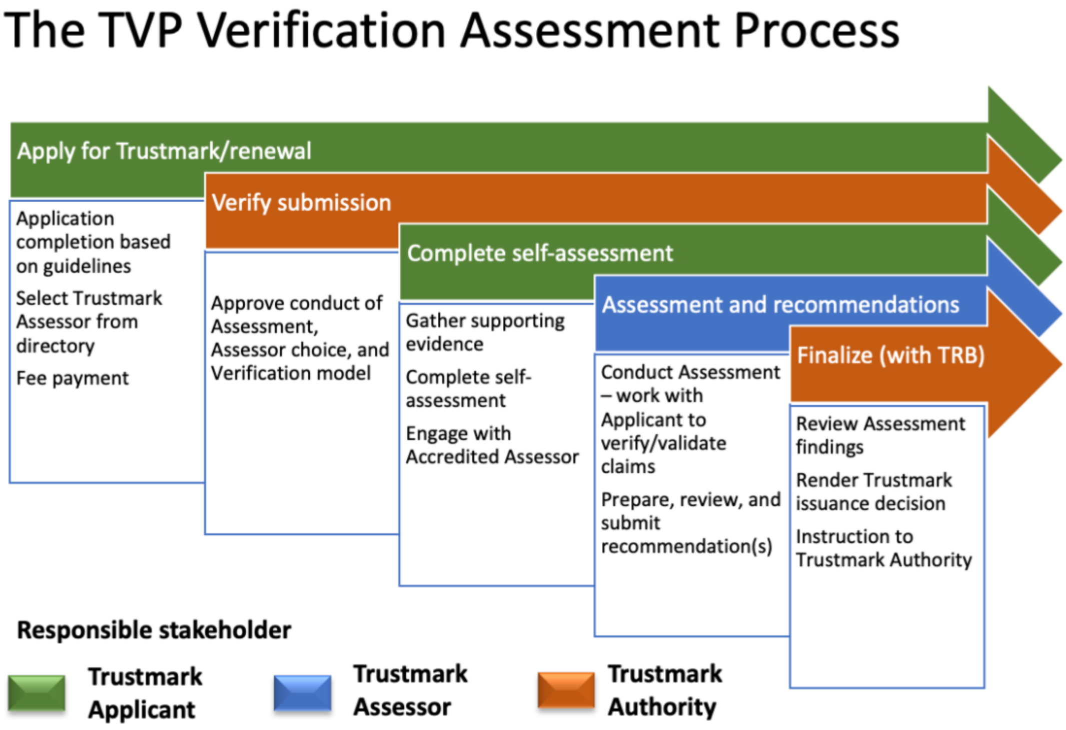


Risk Level		
Low	Medium	High
“light” process Examination of claims as stated or demonstrated by Applicant, lower burden of proof	“controlled” process Examination of claims supported by hands-on examination of an operational instance in a controlled environment	“rigorous” process Examination of claims with operational instance in a controlled environment and complete access to underlying technology

Figure 4 - Assessment process variants

3.1.3 Verification Assessment Process, High-level Tasks, Workflow, and Participants

The figure below illustrates the Verification Assessment cycle and the primary responsibilities of the primary participants in the process. This diagram identifies the process on a successful path. Detailed process documentation, identified in the References section of this document, will provide additional information on the variations for this process and provisions for mitigating the failure of any one step in the process. As well, the Appeals section of this document identifies the optional process to be followed in the case of a negative Trustmark issuance decision.


The TVP Verification Assessment Process
Apply for Trustmark/renewal
Application completion based on guidelines
Select Trustmark Assessor from directory
Fee payment
Verify submission
Approve conduct of Assessment, Assessor choice, and Verification model
Complete self-assessment
Gather supporting evidence
Complete self-assessment
Engage with Accredited Assessor
Assessment and recommendations
Conduct Assessment – work with Applicant to verify/validate claims
Prepare, review, and submit recommendation(s)
Finalize (with TRB)
Review Assessment findings
Render Trustmark issuance decision
Instruction to Trustmark Authority
Responsible stakeholder
🟩 Trustmark Applicant
🟦 Trustmark Assessor
🟧 Trustmark Authority

The sections below identify the primary activities for each of the high-level process steps defined in the Figure above.

3.1.3.1 Apply for Trustmark issuance/renewal

The Trustmark Applicant is the primary actor in this phase, responsible for initiating an application for a Verification Assessment or Trustmark renewal. Other actors may be called upon to participate at the discretion of the Trustmark Applicant. Specifically, the expertise of the proposed Trustmark Assessor may be drawn upon to assist in the completion of application templates and other requirements. The Trustmark Authority will provide static reference material such as templates and process guidance, but may also be called upon in an ad hoc manner for points of clarification.

With this in mind, the primary activities at this stage include:

- Application for Trustmark issuance/renewal (**Trustmark Applicant**):
    - Completion of initial application based on materials available from the Trustmark Authority;
        - Trustmark Applicants will identify the PCTF Conformance Profiles that apply in their context and identify the process they believe applies based on the determining factors identified above. This may be done in consultation with their preferred Trustmark Assessor.
    - Selection of Trustmark Assessor(s) from directory;
        - Chosen Trustmark Assessor(s) are subject to approval from the Trustmark Authority to prevent conflict of interest.

        - Should the examination involve audit of both assurance practices and technology implementation, two separate qualified individuals or organizations may be identified.
    - In consultation with chosen Trustmark Assessor, identification of the applicable Verification Assessment model, defined earlier as the "light", "controlled", or "rigorous" processes; and
        - Does the assessment require only examination of assurance practices, or does an examination of technology implementation(s) apply as well?
    - Submission of application and initial fees.
        - Submission of fees to the Trustmark Authority covering the verification process up to, and including, TRB review. Ancillary fees covering Trustmark issuance will be applicable upon successful TRB review. These fees do not cover the business agreement between Trustmark Applicant and Trustmark Assessor.

3.1.3.2 Verify Submission

The Trustmark Authority will receive the initial application and validate the following:

- Ensure the completeness of initial application information and eligibility of the proposed Verified Service for a Verification Assessment;
- The proposed applicable model ("light", "controlled", or "rigorous") and the PCTF Profile(s) that apply as identified by the Trustmark Applicant, adjusting if required;
- Approval of Trustmark Assessor(s); and
- Acceptance of fees.

The goals of this stage in the process are:

- to ensure eligibility of the Verified Service candidate prior to significant time and effort being expended by the Trustmark Applicant and the Trustmark Assessor.
- to ensure the proposed assessment model and its components are aligned with the intent of the TVP.
- to validate there is no real or perceived conflict of interest with the chosen Trustmark Assessor.

This review and validation process will be relatively high level and is not intended to be onerous for any party. The result may include some adjustment to the application, and permission to proceed with a Verification Assessment.

3.1.3.3 Complete Self-assessment

The first stage of an approved Assessment puts the onus on the Trustmark Applicant to gather, the the extent possible, the supporting evidence to support their application. This includes completion of various templates that elaborate their conformance claims against the Conformance Criteria in the PCTF Conformance Profiles against which they have chosen to be evaluated. This will position both the Trustmark Applicant and the Trustmark Assessor for a more efficient verification of claims in the next phase. The primary activities at this stage include:

- Complete business agreement with Trustmark Assessor(s).
- Completion of self-assessment (**Trustmark Applicant**):
    - Complete self-assessment; and
        - Trustmark Authority support in the form of online self-assessment guidance and detailed form or template help material is available for reference.
    - Gather evidence to the extent possible to prepare for Trustmark Assessor examination.

3.1.3.4 Assessment and Recommendations

This stage is driven primarily by the Trustmark Assessor examination, validation, elaboration of of the Trustmark Applicant conformance claims and supporting evidence. This stage will feature significant interaction between Trustmark Applicant and Trustmark Assessor to validate claims. The nature of this interaction varies depending on the process being followed, i.e. "light", "controlled", or "rigorous" process. The high level activities at this stage include:

- Verify completed self-assessment material (**Trustmark Assessor**):
    - Review of submitted self-assessment data in detail to ensure complete coverage and completeness of responses to Conformance Criteria including;
        - Examination of assurance practices; and
        - Examination of technology implementation (if required - based on whether there is a technology product to examine).
    - Examine evidence of Trustmark Applicant claims;
        - Specific requirements for examination will be identified in detailed process documentation that will vary somewhat depending on the PCTF Conformance Profile(s) and associated Conformance Criteria being examined.
    - Develop Verification Assessment findings, review and perhaps adjust, with the Trustmark Applicant; and
    - Submission of findings and a Verification Assessment Recommendation.

It is this phase in which the primary differences between the "light", "controlled", and "rigorous" verification processes may be found. Please refer to the process variant definitions earlier in this document.

All processes will include an examination of claims associated with assurance practices, and potentially, technology components. For all claims, the Trustmark Applicant will have provided responses to Conformance Criteria, along with evidence of conformity to the extent possible. This evidence may consist of service documentation or other associated material, specialized descriptive material created solely for the purposes of demonstrating conformance claims, or operational data (e.g. audit trails or other measurement data) that support the claims. The differences will exist in the level of engagement, examination techniques, and burden of proof required as the Trustmark Assessor evaluates the Trustmark Applicant claims. Briefly, the process differences can be characterized as follows:

- The "light" process relies primarily on arms-length examination of claims and proof of claims as developed by the Trustmark Applicant. The interaction between Trustmark Assessor and Trustmark Applicant will be more limited, primarily on points of clarification or coverage. Verification will rely upon supplied enterprise documentation and prepared responses addressing the Conformance Criteria, perhaps supplemented by Trustmark Applicant demonstration of the operating proposed Verified Service.

- The "controlled" process will feature closer interaction between Trustmark Assessor and Trustmark Applicant with a more onerous burden of proof and hands-on examination of Trustmark Applicant claims and supporting evidence. Technology component verification will be subject to a hands-on Technology Evaluation in a controlled environment. Technology Evaluation will be high level, focused on observation of operational results of the proposed Verified Service.
- The "rigorous" process includes all elements of the "controlled" process. The primary differentiation is that Technology Evaluation will feature low-level examination of the underlying technology and its implementation to confirm compliance with PCTF Conformance Criteria.

3.1.3.4.1 Protection of Confidential Data

By necessity, during a Verification Assessment the Trustmark Assessor will be exposed to Trustmark Applicant confidential information. There are two requirements to be considered with regards to this information.

First and foremost, is the protection of Trustmark Applicant confidential information. Only the Trustmark Assessor is to be exposed to this information and that exposure should be governed by confidentiality clauses in the business arrangement between Trustmark Assessor and Trustmark Applicant. The Trustmark Authority and the TRB should only see appropriate summary information supporting the submitted findings and recommendations for a Verification Assessment.

The second concern is an audit requirement from the Trustmark Authority. Should a Verification Assessment be questioned, it may be necessary to re-examine the evidence supporting the findings and recommendations. There is a requirement that supporting evidence used in a Verification Assessment be retained in a tamper-proof manner (e.g. encrypted and signed) for the lifetime of the currently issued Trustmark. This evidence package should be retained by the Trustmark Applicant, and its tamper-proof nature attested to by the Trustmark Assessor. Detailed requirements will be elaborated in the supplemental documentation identified in the References section of this document.

3.1.3.5 Finalize Verification Assessment Process

With Assessment findings and recommendations submitted, the TRB with the Trustmark Authority as chair, will consider the submitted material for the purposes of rendering a Trustmark issuance decision. The TRB will examine the findings and supporting rationale only, they should not be exposed to the detailed supporting evidence for privacy and Trustmark Applicant IP protection reasons. The trust granted the Trustmark Assessor by virtue of their accreditation as Trustmark Assessors will be relied upon to ensure the appropriate level of due diligence and expertise has been applied to the examination of evidence.

A negative Trustmark issuance decision can be appealed (see Certification Appeal section of this document). With a positive decision, the Trustmark Authority will be instructed to complete the operational elements of the process, including Trustmark issuance and the update of the Verified Services directory.

The primary tasks during this stage include:

- Review findings and Verification Assessment Recommendation (**TRB, chaired by Trustmark Authority**):
  - Potential for requests for additional clarification; and
  - Render Trustmark issuance decision.
- Appeal findings (optional):
  - Submit appeal and appeal rationale (**Trustmark Applicant**);
  - Review appeal submission and rationale (**Trustmark Authority**); and
  - Upon acceptance of appeal, conduct Appeals process (**Trustmark Authority**).
- Trustmark issuance, in the case of a successful application and verification:
  - Issue notification of success to the Trustmark Applicant (**Trustmark Authority**);
  - Submission of ancillary Trustmark issuance fees to the Trustmark Authority (**Trustmark Applicant**);
  - Issue program templates and supporting materials, as applicable (e.g. program seal templates, rights documentation, etc.) (**Trustmark Authority**); and
  - Update directory of Verified Services (**Trustmark Authority**).

3.1.4 Assessing a Service Network

In the introduction, we identified the purpose of this document as being 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". It is worth noting that examination of a service network will differ significantly from examination of a service put forward from a single enterprise. A service network in the context intended herein can be defined as a structure existing to deliver a service objective by multiple interconnected and independent entities, working in a unified manner, governed by a common set of norms and standards.

There are a number of key elements of this type of assessment that should be noted:

- Evaluation of a service network will examine the formal standards, mandated protocols, mandated processes, and policies that a participant in the network would need to adhere to in order to participate in the network.
- Most typically, the service network would rely upon participants to develop and deliver their own implementations of the service.
- Examination of technology implementations would extend only to technology components required, by the service network, as part of any participant's implementation.
- Full examination of any individual participant's implementation would typically not be in scope. Should an individual participant wish to additionally certify their complete implementation that would be subject to a separate Verification Assessment.
- The issued Trustmark from a Verification Assessment would apply to the higher level network. Service network participants could claim to be operating within a PCTF verified network, but **COULD NOT** claim that their product had received a Trustmark.

To help further set context, consider the example of a financial settlement service network. A central authority sets the standards or requirements for participation. Individual institutions then implement their own instantiation of a compliant service offering within the network. A Verification Assessment of the network service would examine the policies, standards, and any mandated common technology implementation that all participants must adhere to. Full service implementations by individual participants would not be examined. The former would be eligible to receive a Trustmark, the latter would not unless they undergo a separate Verification Assessment for their product or service. The Trustmark Applicant in this example would be the governing body for the service network.

3.1.5 Verification Assessment Appeals

Should the Trustmark Applicant wish to appeal a negative certification decision from the TRB or a submitted negative Verification Assessment Recommendation from an Trustmark 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 Trustmark Applicant, submitted to the TRB with prior notification to the Trustmark Assessor. At the Trustmark Applicant's discretion, they may also have consulted with the Trustmark Assessor to develop the submitted appeal and its rationale.

The Trustmark Authority will conduct a preliminary examination of the submitted appeal and associated rationale with the Trustmark Applicant and the Trustmark Assessor to ensure that there are no information gaps that may preclude evaluating the appeal. In this phase, the Trustmark Authority may attempt to mediate, and perhaps adjust the findings and recommendations, 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. This TRB appointee, meant to be an independent party similar to an ombudsman function found in some organizations, will review the Verification Assessment and its result. Recommendations from this review may result in any one of the following:

- Re-assessment with another Trustmark Assessor due to Trustmark Assessor shortcomings;
- Identification of PCTF Conformance Profile shortcomings that may have contributed to an incorrect result;
- Upholding of the original Trustmark issuance decision;
- Review findings with a period of time to supply additional evidence to the TRB; or
- Overturn of the original Trustmark issuance decision.

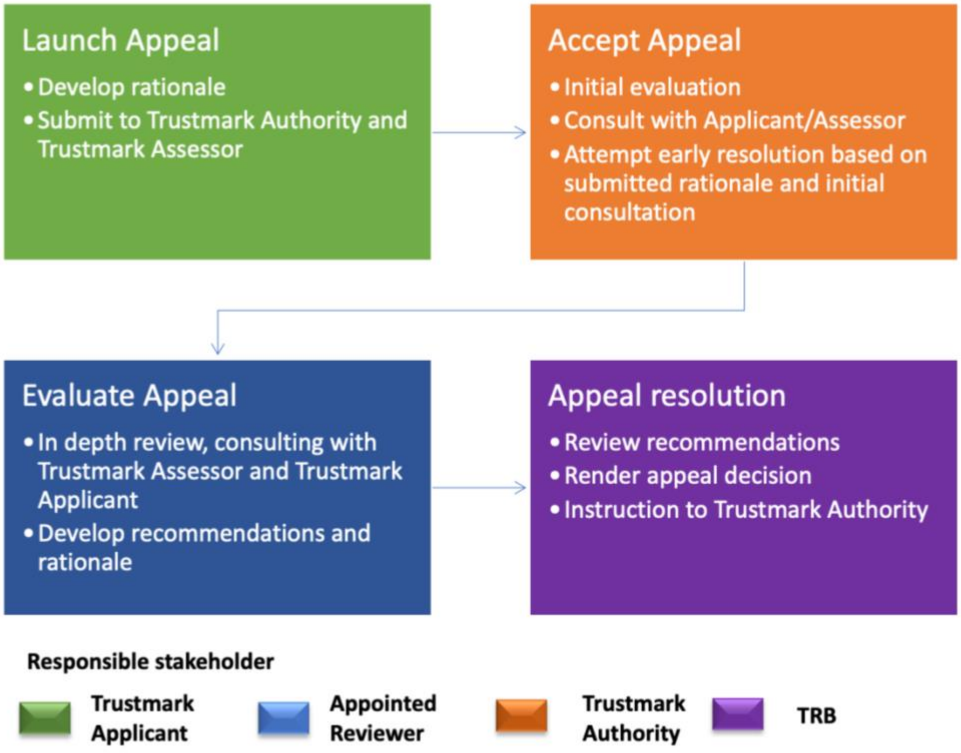

Launch Appeal
• Develop rationale
• Submit to Trustmark Authority and Trustmark Assessor
Accept Appeal
• Initial evaluation
• Consult with Applicant/Assessor
• Attempt early resolution based on submitted rationale and initial consultation
Evaluate Appeal
• In depth review, consulting with Trustmark Assessor and Trustmark Applicant
• Develop recommendations and rationale
Appeal resolution
• Review recommendations
• Render appeal decision
• Instruction to Trustmark Authority
Responsible stakeholder
Trustmark Applicant
Appointed Reviewer
Trustmark Authority
TRB

Figure 7 - Verification Assessment appeal process

3.1.6 Continuous Monitoring

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

- Existence of a complaint and the status of its examination will be noted in a directory of Verified Services.
- An accepted complaint will trigger initial investigation by the Trustmark Authority.
- At the discretion of the Trustmark Authority, additional Assessment may be required to retain verified status. The process required would be the same as the original examination process, based upon the risk profile of the service to be examined.

3.2 Trustmark Assessors

Trustmark Assessors are individuals and organizations, independent from the Trustmark Authority and the Trustmark Applicant, accredited by the Trustmark Authority to conduct Verification Assessments. These assessors 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 Trustmark Authority applies to management and staff of the Trustmark

Authority. Employees or other individuals associated with DIACC members may become Trustmark Assessors, subject to the accreditation requirements.

Trustmark Assessors are subject to periodic review and accreditation renewal. The Trustmark Authority will ensure they continue to retain and enhance the core knowledge and experience required of its Trustmark Assessors. Accreditation of Trustmark Assessors will focus on authorized individuals within the organization and the organizations themselves.

A directory of accredited Trustmark Assessors will be published and maintained by the Trustmark Authority. The directory will identify individuals accredited to conduct assessments of assurance practices for one or more of the PCTF Conformance Profiles, and organizations accredited to conduct Technology Evaluations.

3.2.1 Accreditation, Trustmark Assessors

Trustmark Assessors are subject to periodic accreditation by the Trustmark Authority. This will be conducted by the Trustmark Authority upon application, and submission of fees, by the applicant wishing to become a Trustmark Assessor. Trustmark Assessors will be subject to annual accreditation renewal.

Organizations and individuals can be accredited to perform Verification Assessments. Further, for organizations, they will be asked to qualify one or more individuals within their organization to be authorized to conduct Verification Assessments. The accreditation process to perform Verification Assessments will examine the qualifications of the organization and/or the proposed individuals. Accreditation requirements and associated detail will be developed in the TVP supplemental documentation identified in the References section of this document.

Trustmark Assessors may apply to be accredited for either, or both, components that may be required for a Verification 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. An accredited named individual will be required to conduct this portion of a Verification Assessment. These individuals will be authorized to conduct assessments of assurance practices applicable to individual PCTF Conformance Profiles (i.e. some individuals may not have the qualifications to examine all of the PCTF Conformance Profiles).
- 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. An accredited organization with the proven skills, experience, and tooling required for a Technology Evaluation will be required for this portion of a Verification Assessment.

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

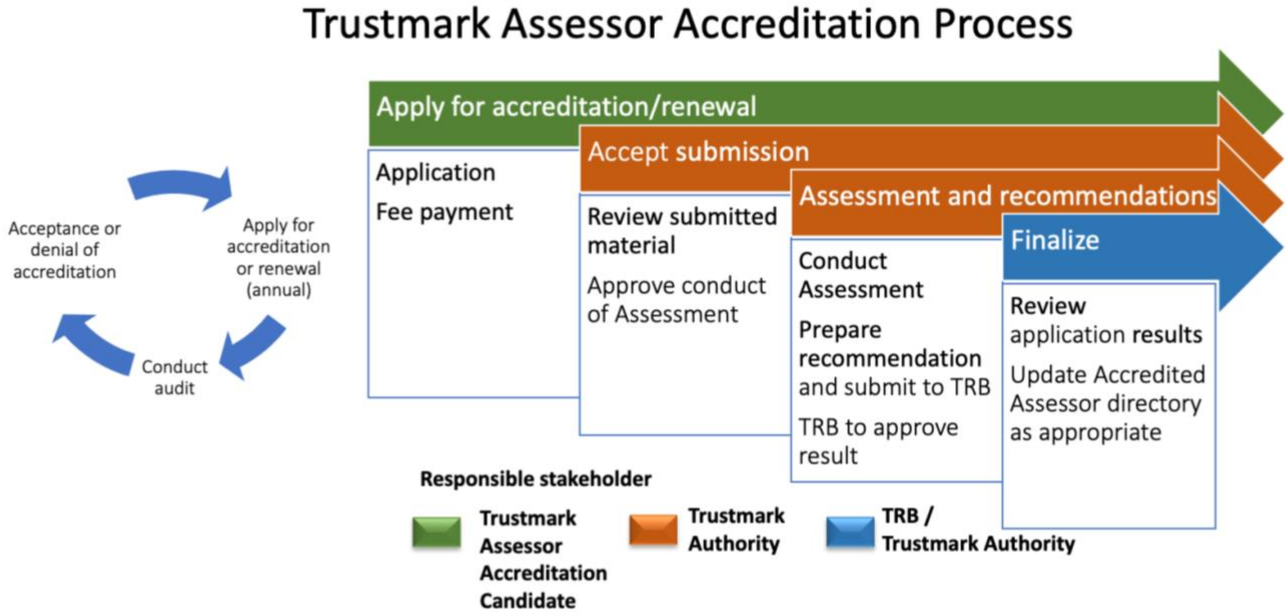

Trustmark Assessor Accreditation Process
Acceptance or denial of accreditation
Apply for accreditation or renewal (annual)
Conduct audit
Apply for accreditation/renewal
Application
Fee payment
Accept submission
Review submitted material
Approve conduct of Assessment
Assessment and recommendations
Conduct Assessment
Prepare recommendation and submit to TRB
TRB to approve result
Finalize
Review application results
Update Accredited Assessor directory as appropriate
Responsible stakeholder
🟩 Trustmark Assessor Accreditation Candidate
🟧 Trustmark Authority
🟦 TRB / Trustmark Authority

Figure 8 - Trustmark Assessor certification process

The Trustmark 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 (**Trustmark Assessor applicant**)
- Submission of application fees (**Trustmark Assessor applicant**)
- Examination of application and approval to proceed with examination process (**Trustmark Authority or designate**)
  - Examine organization qualifications
  - Examine qualifications of proposed individuals
- Development of findings and recommendations (**Trustmark Authority or designate**)
- In the case of a negative recommendation, an opportunity to provide additional information, context, or evidence of remedial action to address real or perceived shortcomings (**Trustmark Assessor applicant**)
  - Adjustment of findings and recommendations as required (**Trustmark Authority or designate**)
- Submission to TRB (**Trustmark Authority**)
- Final approval or rejection of application (**TRB**)
- Update of Trustmark Assessor directory as appropriate (**Trustmark Authority**)
- Development of service delivery capability and processes, in alignment with Trustmark Authority policy, requirements, guidance, and other relevant direction. (**Trustmark Assessor**)

Notes

- Organizations may choose to add or subtract qualified individuals outside the annual accreditation renewal process, subject to appropriate examination of qualifications.

- Should a certified individual leave the certified organization, they would be subject to certification with another organization before being authorized to conduct a Verification Assessment.
- Trustmark Assessors will be accredited to conduct Assessments for the PCTF Conformance Profile(s) in effect at the time. Should newer Profile versions be ratified, The Trustmark Authority may require, at their discretion, accreditation for the new Profile versions or simply extend existing accreditation to encompass the newer version. Should additional accreditation be required, the Trustmark Assessor, at their discretion, may trigger accreditation renewal earlier than their annual schedule dictates.

3.3 Equivalence of Other Certifications

At this time, there are no direct correlation to existing certifications or trustmarks 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 both Verification Assessments and the Trustmark Assessor accreditation processes.

Specifically:

- For accreditation of individuals as Trustmark 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 Trustmark Assessor
- For verification against one or more PCTF Conformance Profiles, formal audit results evaluating compliance with eIDAS (EU) or NIST 800-3 (USA) may serve as a proxy for demonstrated conformity with specific requirements of a PCTF Conformance Profile. However, audit results for evaluation of compliance with these standards cannot form the entire basis for evaluation of PCTF Conformance 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.

PCTF Conformance Profiles containing the specific criteria against which Trustmark Applicants 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*). Listed below are the envisioned artefacts and their initial envisioned scope. Please note that the final implementation of this supplemental information and guidance may combine some of these artefacts.

- Verification Assessment Program process detail - detailed process descriptions and self-help material
- Trustmark Assessor application template - templates, forms, and guidance for initiating the process to be certified as a Trustmark Assessor
- Certification Application - templates, forms, and guidance for initiating the process to examine a service submitted by a Trustmark Applicant
- Self-assessment template - templates, forms, and guidance for completion of a self-assessment of a service being submitted for examination
- Verification Assessment findings template - templates, samples and guidance for completion of audit findings by a Trustmark Assessor
- Verification Assessment detailed procedures - templates and guidance for Trustmark Applicants and Trustmark Assessors to help govern the conduct of an examination of a submitted service
- Appeal submission template - templates and guidance for the preparation and submission of an appeal of a Certification decision
- Appeals process detailed procedures - supplemental process information pertaining to the appeals process
- Various guides and other help resources (TBD)
- Trustmark license agreement - Trustmark Authority license agreement governing the use of an issued Trustmark
- Verification Assessment non-disclosure agreement - governs confidentiality requirements for all involved in the creation and review of a Verification Assessment
- Additional legal agreements (TBD)

5 Revision History

Version	Date	Author	Description
0.01	2019-12-02	PCTF Editing Team	Initial framework draft
0.02	2020-01-12	PCTF Editing Team	Initial content-complete draft
0.03	2020-02-14	PCTF Editing Team	Adjustments based on DIACC feedback
0.04	2020-03-30	PCTF Editing Team	Adjustments based on initial Design team interviews
0.05	2020-05-01	PCTF Editing Team	Final adjustments for publication of Draft
0.06	2020-06-05	PCTF Editing Team	Updates based on TFEC input to V0.04 and V0.05
0.07	2020-06-29	PCTF Editing Team	Updates based on a short supplemental TFEC review period
1.0	2020-07-8	PCTF Editing Team	TFEC approved as Draft Recommendation V1.0
1.1	2020-09-18	PCTF Editing Team	Updates per comments received during Draft Recommendation public review period.
1.1	2020-09-30	PCTF Editing Team	TFEC approved as Candidate for Final Recommendation V1.0
1.0	2020-10-20	PCTF Editing Team	Final Recommendation V1.0